Maschinensicherheit durch zuverlässige Echtzeitsysteme

Max Walter, Jan. 2025

SIEMENS

Digital transformation has the potential to drive progress and growth and reduce resource consumption in all countries

Industry

Up to **50% material savings** can be realized using digital twins and innovative production technologies such as additive manufacturing.

Infrastructure

Buildings are currently responsible for **39% of global energy related carbon emissions**. Data analytics and automated building management can unlock large saving potentials.

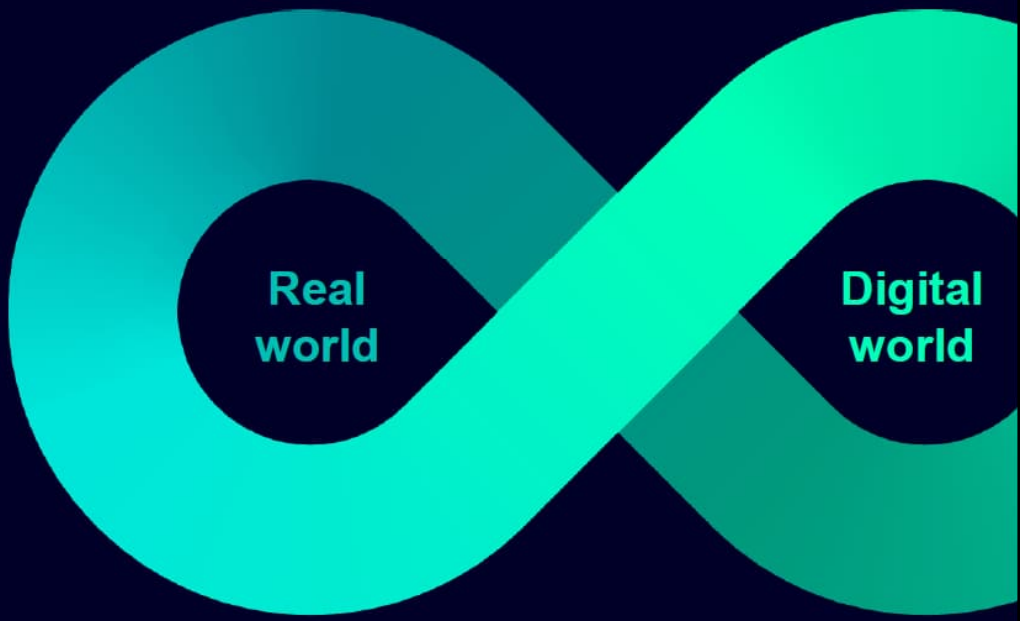
Mobility

Up to **30% higher network capacity** can be achieved through automatic train operation and by optimizing train flows and rail operations.

SIEMENS

By combining the real and the digital worlds, Siemens empowers customers to accelerate their digital and sustainability transformation

- Glass Production
- Pharma-ceutical Industry
- Campus
- Tire Industry
- Mining Industry
- Cement
- Transpor-tation and Logistics
- Panel Building
- Wind Energy
- Pulp and Paper
- Life Science
- Healthcare
- Oil and Gas Industry
- Automotive Manu-facturing
- Airports
- Electronics Industry
- Semi-conductors
- Data Centers
- Machinery and Plant Production
- Food and Beverage
- Water and Wastewater Industry
- Chemical Industry
- Municipalities and DSOs
- Cranes
- Intralogistics
- Aerospace
- Battery Manu-facturing



SIEMENS

Our digital portfolio

Top 10

Siemens is one of the top 10 software companies[1]

€6.5 bn

digital revenue[1] with 10% CAGR until FY 2025

>1,000

digital offerings on Siemens Xcelerator Marketplace[2]

€14 bn

invested in digital companies since 2007[1]

Data analytics

AI and IoT

Simulation tools

New business models

Secure connectivity

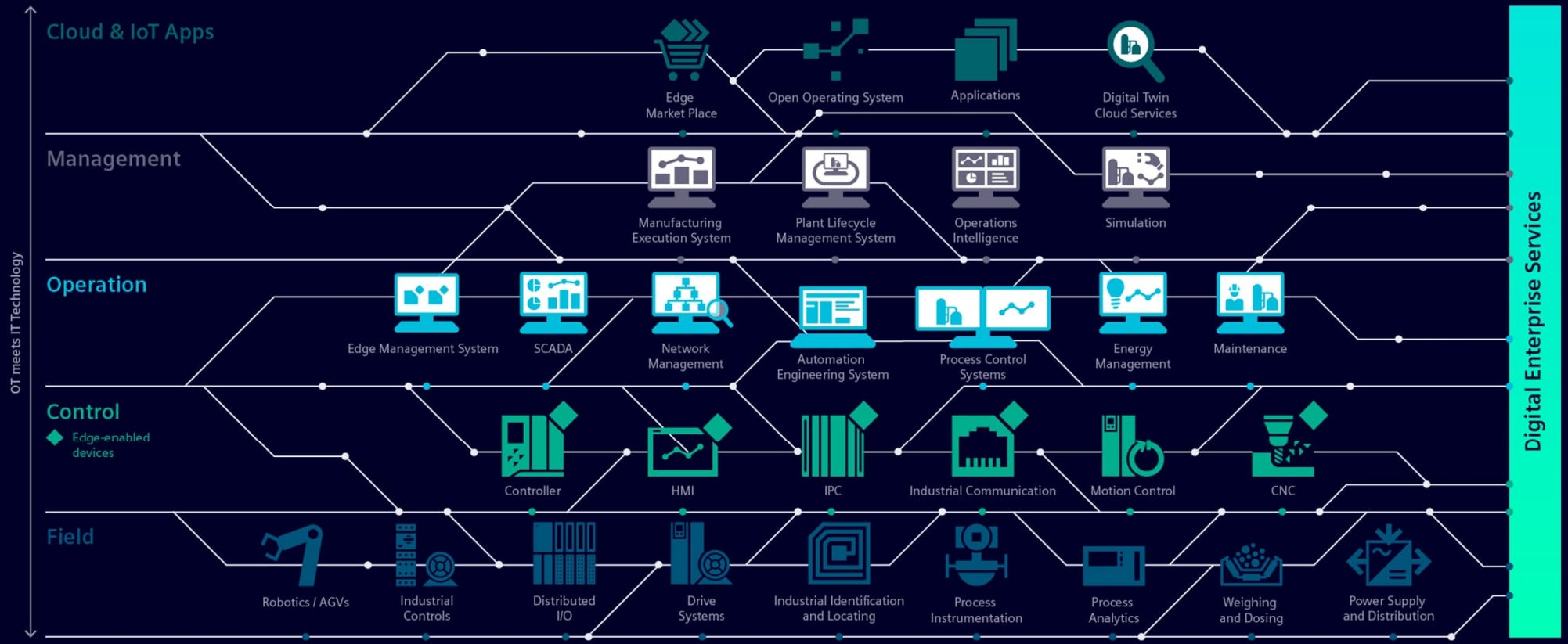
Cyber-security

1 As of September 30, 2022

2 Includes offerings by Siemens Xcelerator Marketplace sellers as well as Siemens offerings, as of October 31, 2024

SIEMENS

Automatisierung - Produktportfolio



SIEMENS

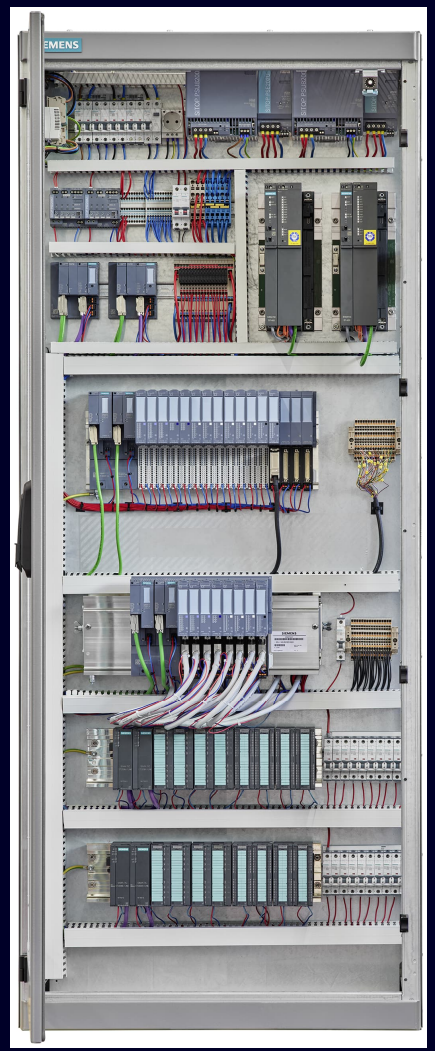
Industriesteuerungen

S7-1200 G2

S7-…

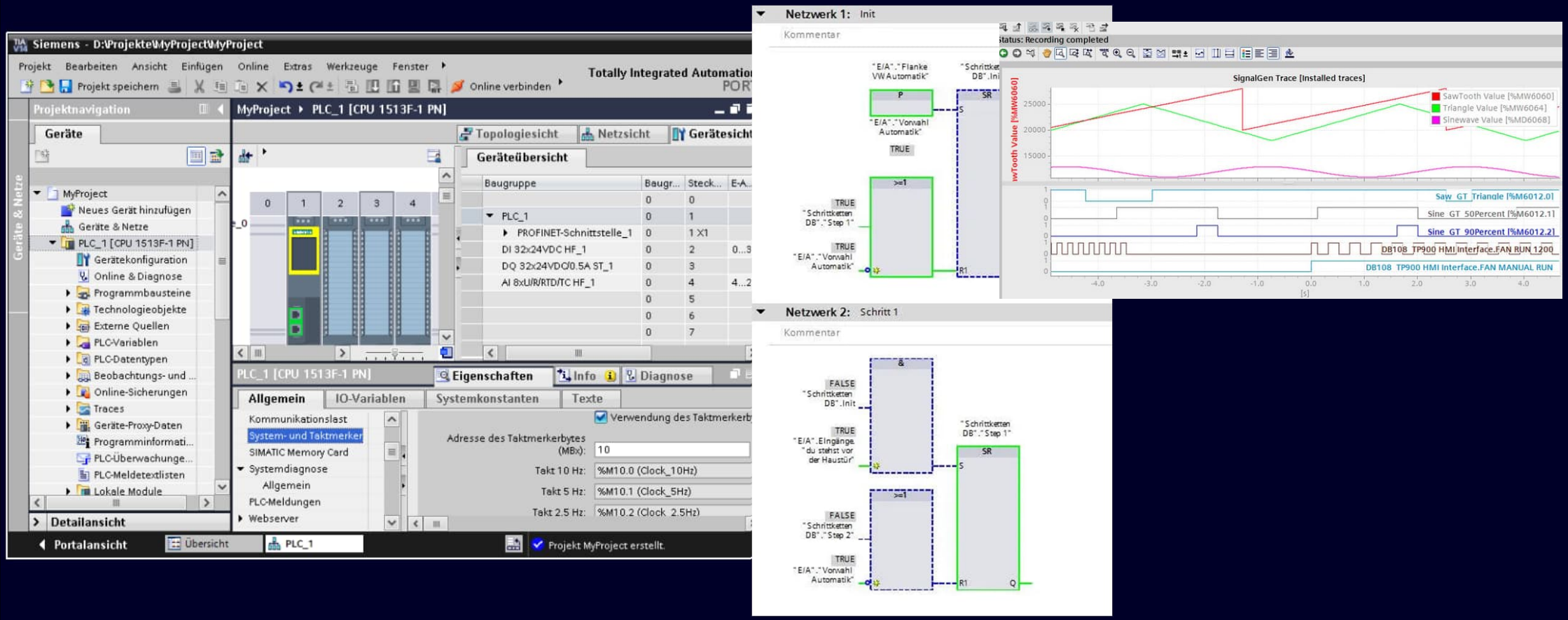
S7-1518 HF

ET200-SP



SIEMENS

Engineering: TIA-Portal
Konfigurieren, Programmieren, Testen, Fehlersuche …



SIEMENS

Rahmenbedingungen, funktionale und nicht-funktionale Anforderungen an „industrietaugliche“ Steuerungen

Rahmenbedingungen:
- Bauform (Hutschiene)
- lüfterlos
- lange Lieferbarkeit (10, 20, 30 Jahre)
- Software - Kompatibilität mit existierenden Projekten
- …

Funktionale Anforderungen:
- Echtzeit
  - garantierte maximale Reaktionszeit
  - garantierte Gleichzeitigkeit (Isochronität)
- programmierbar
  - leicht erlernbar
  - einfache Aufgaben können schnell gelöst werden
  - Funktionsumfang an Automatisierung angepasst
  - schnelle Fehlersuche, beobachtbar

Nicht-funktionale Anforderungen
- Performance
  - Mengengerüst
  - Reaktionszeit im ungünstigsten Fall
- Verlässlichkeit
  - Zuverlässigkeit (auch in widriger Umwelt)
  - Schnelle Fehlersuche (Diagnose)
  - Schnelle Reparatur
  - Security (Schutz vor Sabotage und Ausspähen)
- Funktionale Sicherheit
- Hochverfügbarkeit

Unerwünschte Ereignisse

SIEMENS

Fehlende Sicherheit als KO-Kriterium

Fehlende Sicherheit kann ein Projekt auf einen Schlag beenden.

Sicherheit muss daher von Anfang an mitbetrachtet werden.

Gegenbeispiel:

- Verlust der LZ139 “Hindenburg” 1937 in Lakehurst, NY.
- Das war der letzte kommerzielle Antlantikflug eines Luftschiffes!
- Problem: kein Lösungsansatz für Sicherheitsbedenken

Hinweis: die Briten hatten Luftschiffe bereits am Anfang der 1930 Jahre aufgegeben – aus Sicherheitsgründen.

Murphy's Law

Anything that can go wrong …
… *will* go wrong.

Edward A. Murphy (1918-1990)

- Ingenieur an der Edwards Air Force Base
- Tests für Schleudersitze von Überschallflugzeugen
- 1949 gabe es noch keine Crash-Test-Dummies
- Tests mussten mit echten Personen gemacht werden
- Auf dem Photo: Arzt des Projekts, Paul Stapp

Stapp: „Due to Murphy‘s Law … nobody had been severely injured.“

Merke: Um Unfälle zu vermeiden, denke immer an Murphy‘s Law!

SIEMENS

Funktionale Sicherheit (Functional Safety)

Sicherheit: Freiheit von unvertretbarem Risiko (IEC 61508-4)

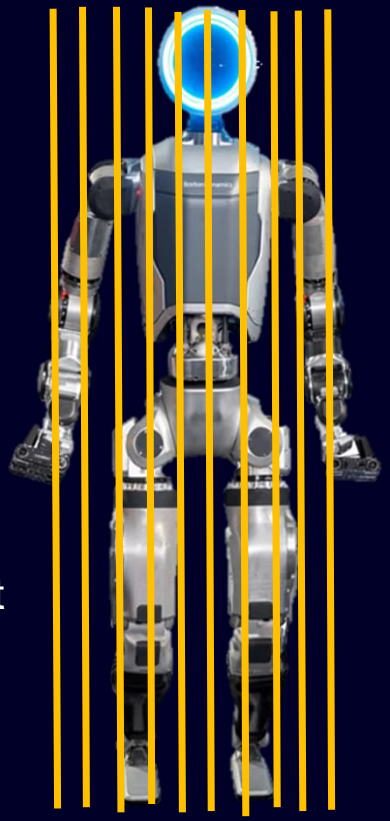
Funktionale Sicherheit:

Teil der Gesamtsicherheit, bezogen auf das „equipment under control EUC“ und das EUC-Leit- oder Steuerungssystem, der von der korrekten Funktion des sicherheitsbezogenen elektrischen / elektronischen oder programmierbaren elektronischen (E/E/PE)-Systems und anderer risikomindernder Maßnahmen abhängt.

Beispiel

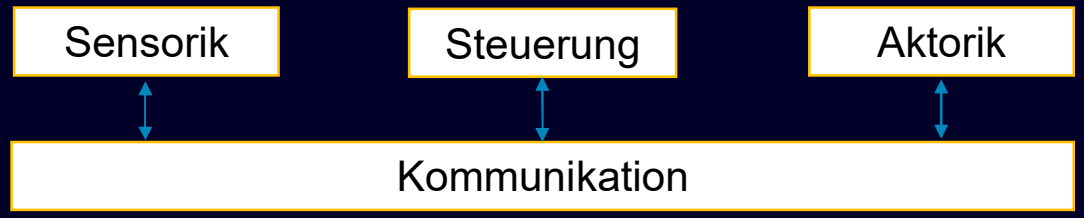
„EUC control system“

Standardkomponenten:



„equipment under control“

Überwachung („E/E/EP-System“):



„geeignet, das Risiko akzeptabel abzusenken“

SIEMENS

Weitere Beispiele für Sicherheitsfunktionen

Bereich	Nutzfunktion	Sicherheitsfunktion(en)
Robotik	Schweißen, Bohren, … Bahnplanung	Sicher begrenzte Geschwindigkeit Sicher begrenzte Position Sicher begrenzte Kraft Zustimmtaster bei Tipp-Betrieb …
Pressen	Metallumformung	Zweihandschaltung Sicherer Stopp bei Eingriff …
Autonome Flurförderfahr-zeuge	Transport von Material Bahnplanung	Sicher begrenzte Geschwindigkeit Sicher begrenzter Abstand …
Verpackungs-maschinen	Verpackung, Palettierung, …	Sicherer Stopp bei Zutritt
Hochregallager	Lagerung	Sicherer Stopp bei Zutritt Vermeidung von Überlastung von Regalböden

+ Nothalt

“Unvertretbares Risiko”

Sicher ist, dass nichts sicher ist.
(Joachim Ringelnatz)

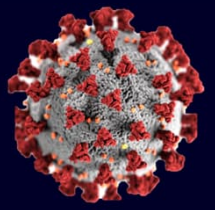
100% Sicherheit gibt es nicht.

Aber das Risiko kann verringert werden …

Ab wann ist ein Risiko vertretbar?
Welche Maßnahmen sind zumutbar?

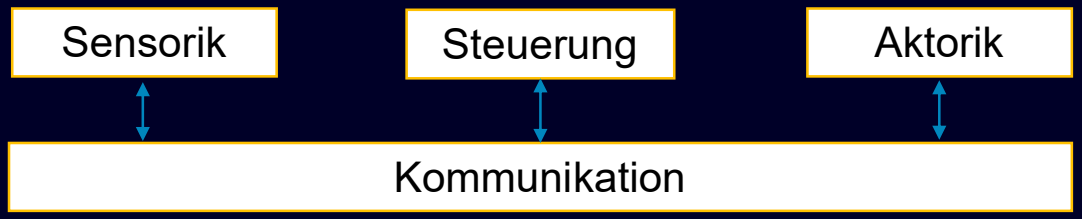
Politische Diskussion, oft abhängig vom Thema.

Industrie: häufig internationale Standards, z.B. IEC 61508 oder ISO 13849



SIEMENS

Aufgabe des E/E/PE-Systems



Erkennen von

- **sicherheitsrelevanten Fehlern im „equipment under control“**
- **Fehlern im E/E/PE-System selbst**

→Sicherer Zustand (z.B. Stillstand der Anlage)

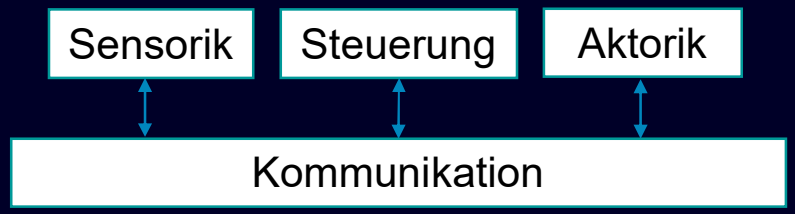
Mit nachweisbarer Ausfallwahrscheinlichkeit
Z.B. SIL-3 nach IEC 61508: PFH < 10^{-7} / h

„höchstens ein gefährlicher Fehler im E/E/PE System alle 1000 Jahre“

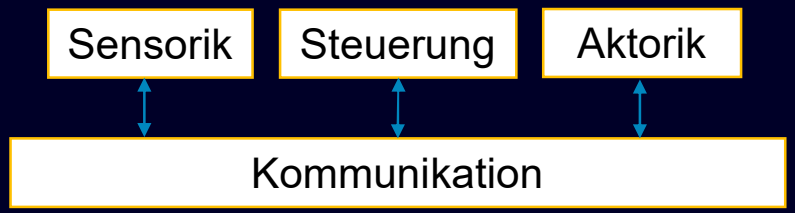
Safety Integrated

Früher:

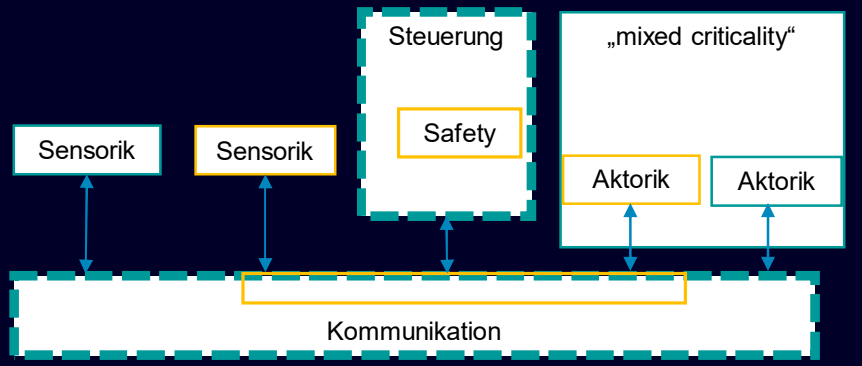
Standardkomponenten (EUC):



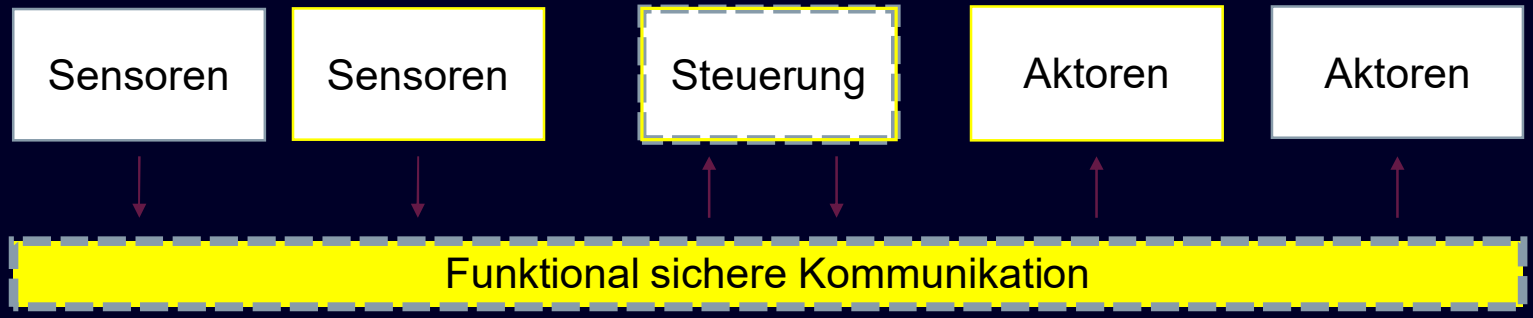
Überwachung („E/E/EP-System“):

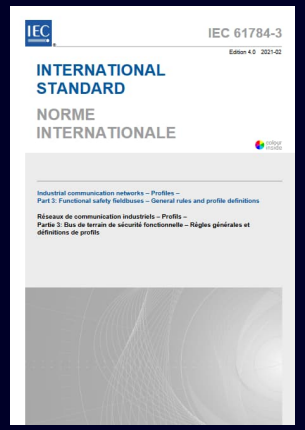


Heute („Safety Integrated“):



Funktional sichere Kommunikation



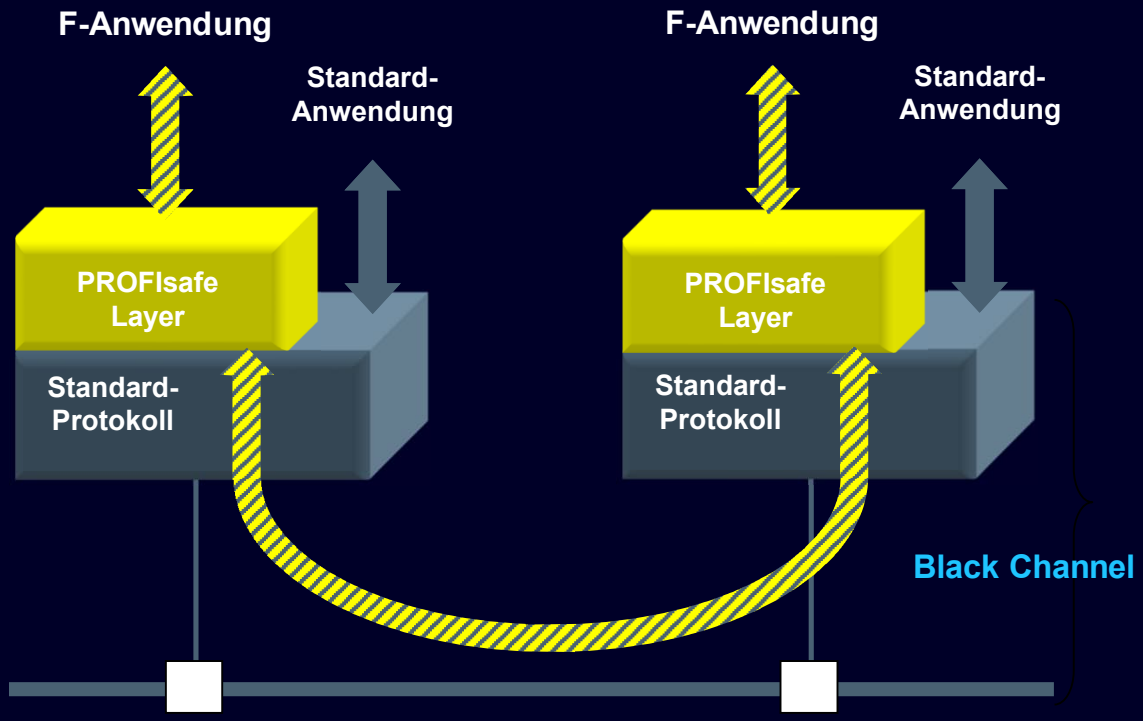


Funktional sichere Kommunikation

- Grundbaustein zum Aufbau von Sicherheitsfunktionen
- Übertragungsfehler müssen erkannt werden (SIL 3: $PFH_{Comm} < 10^{-9}/h$)
- Über Standard-Feldbus, gemeinsam genutzt mit Standard-Kommunikation
- Sicherheit durch Software-Protokoll gewährleistet (PROFIsafe)

„PROFIsafe“

Black-Channel-Prinzip



Black Channel = Feldbus (PROFINET), Rückwand-Bus, W-LAN etc.

Anforderung:

Sämtliche Übertragungsfehler müssen im Empfänger durch die PROFIsafe-Layer erkannt werden.

Fehler erkannt
-> Meldung an F-Anwendung

Klassifizierung von Fehlern nach IEC 61784-3 (Anything that can go wrong …)

Klassifizierung von Fehlern nach IEC 61784-3 (Anything that can go wrong …)

Zeitüberwachung

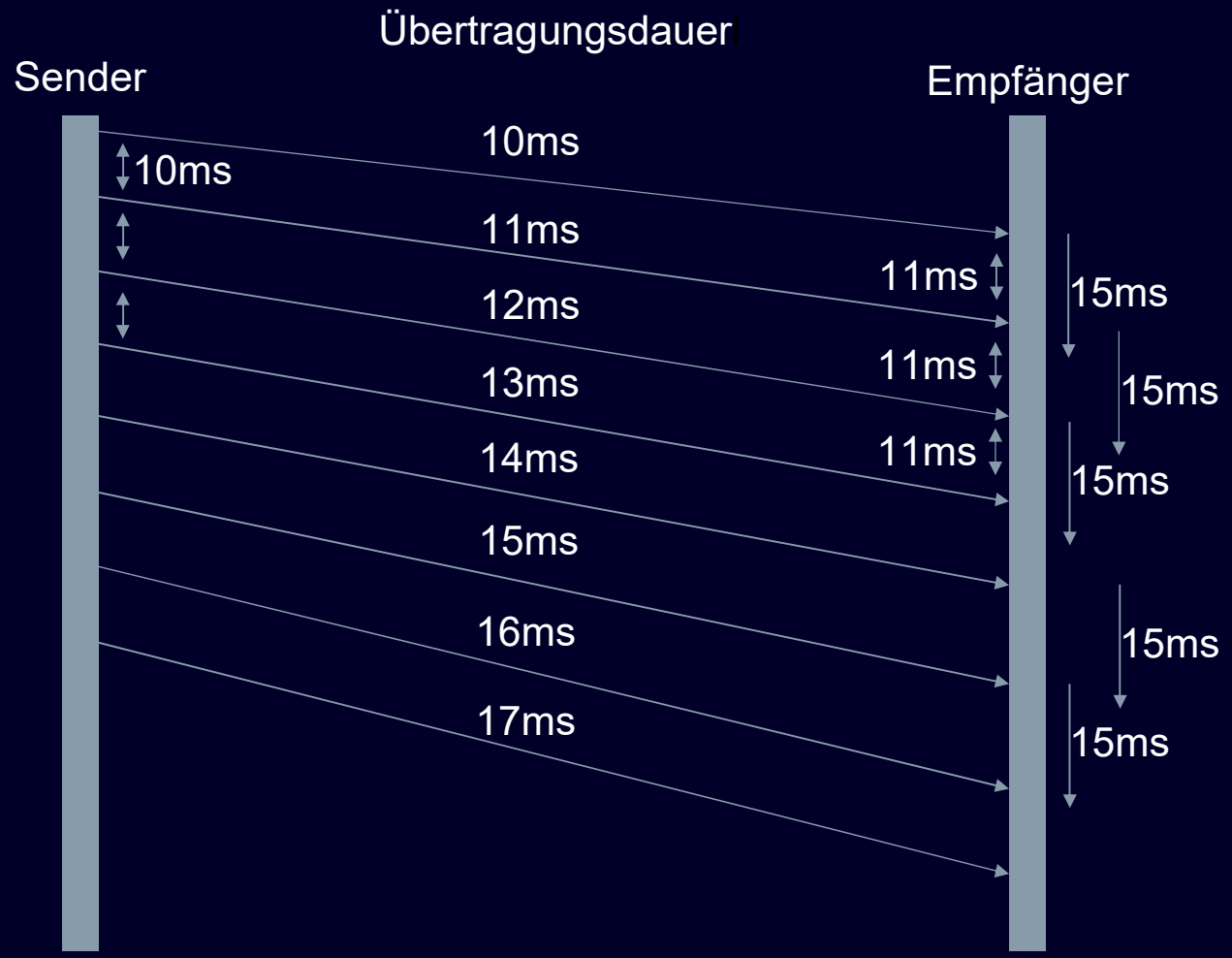
Sichere Kommunikation ist immer zyklische Kommunikation.

Empfänger hat eine Erwartung, die erfüllt werden muss. Andernfalls -> sicherer Zustand

Gesendete Telegramme müssen auf Rechtzeitigkeit geprüft werden.

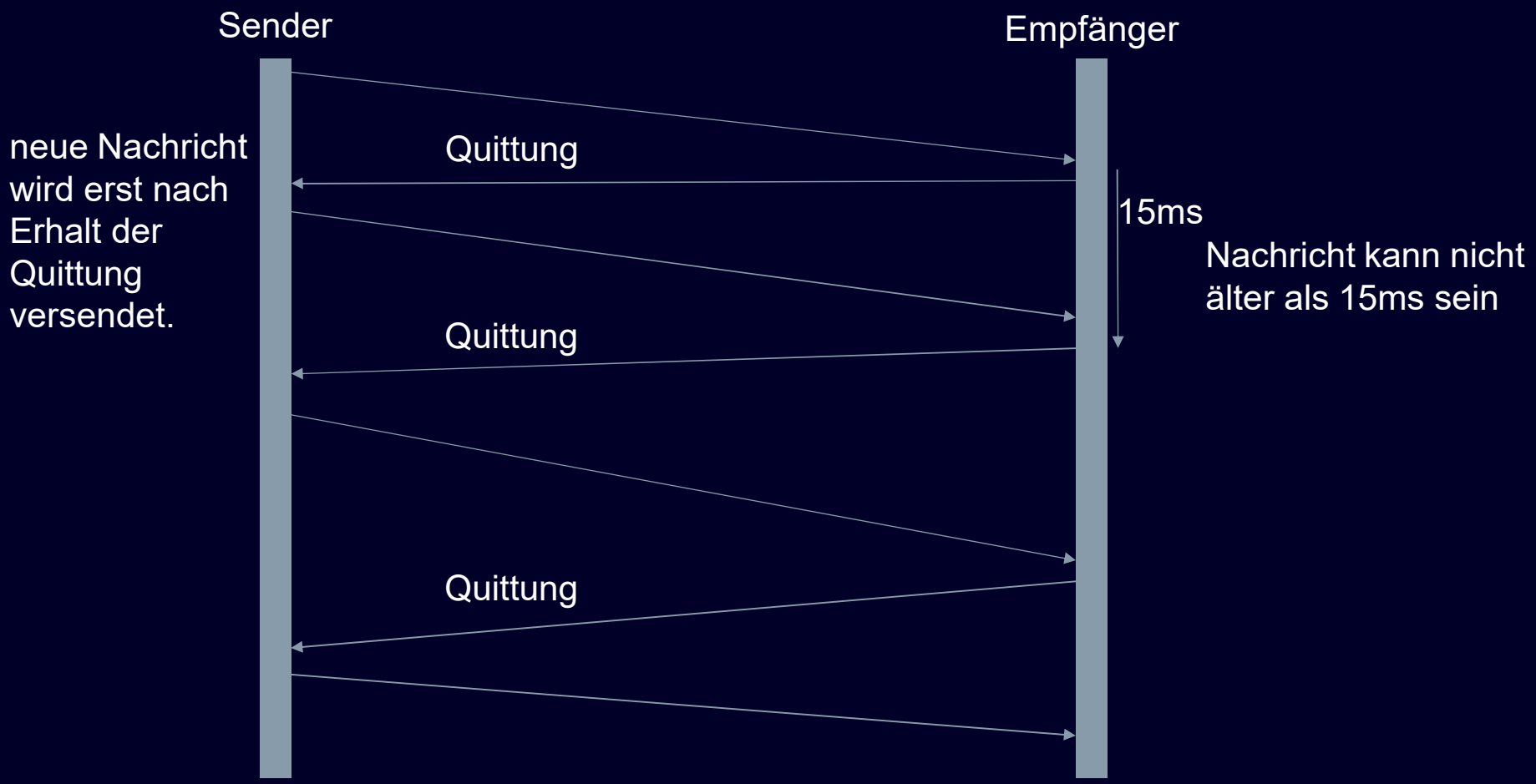
1. Möglichkeit: Zeitstempel
   Problem: Uhren im Empfänger und Sender müssen sicher synchronisiert sein.
2. Möglichkeit: Zeitüberwachung allein im Empfänger
   Wichtig: bidirektionale Verbindung nötig!
   Vgl. IEC 61784-3 „slowly increasing message delays“

Problem: „Slowly increasing message delays“



Obwohl die Übertragung länger braucht, läuft der 15ms-Timer nicht ab.

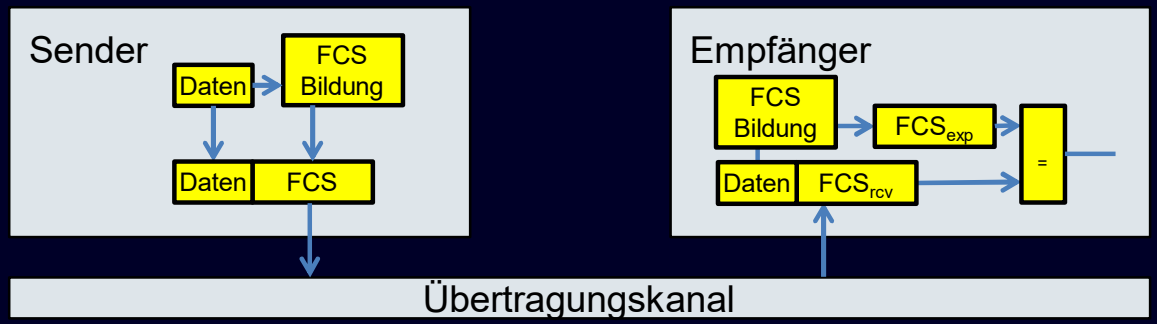
Zeitüberwachung mit Quittung



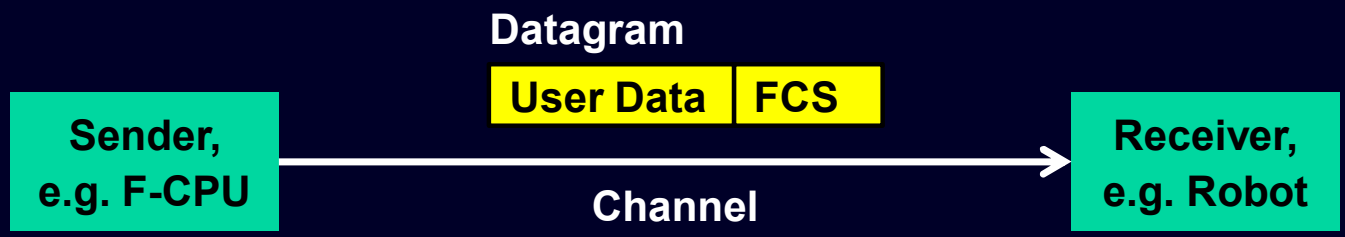
Fehlererkennende Codes, Prinzip

Prinzip:

- An die Nachricht wird eine r-Bit breite Frame-Check-Sequence (FCS) angehängt
- Der Empfänger berechnet FCS_{exp} aus den empfangenen Daten
- Stimmen FCS_{rcv} und FCS_{exp} nicht überein, wird das Paket nicht akzeptiert.



Fehlererkennende Codes

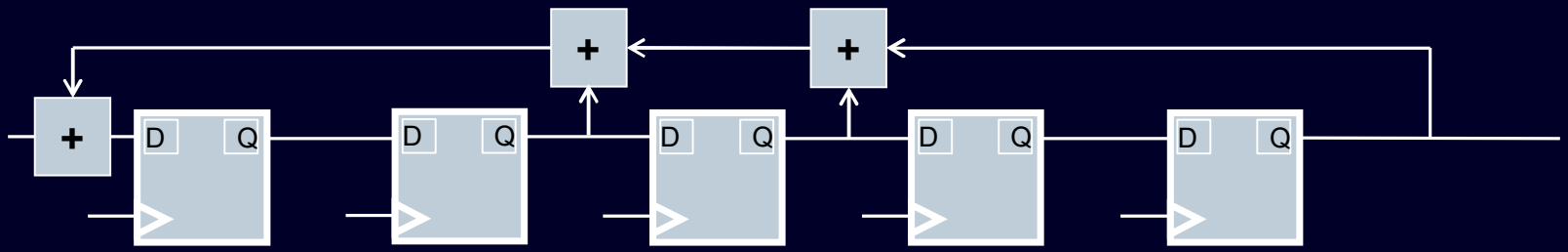


Wie soll die FCS gebildet werden?

• bitwise xor (=„parity bit“)	ungenügend: Zweitbit-Fehler werden nicht erkannt
• word-wise (16- or 32-bit) xor	ungenügend: auch hier Zweibit-Fehler, die nicht erkannt werden
• 16- or 32-bit addition (=„checksum“)	ungenügend, ähnlich xor
• and, or, multiplication	noch schlechter als xor
• Rest einer Integer Division?	gut, aber langsam: $O(n^2)$
• Cyclic redundancy codes: Polynomdivision im $\mathbb{Z}_2$	gut und schnell: O(n)

SIEMENS

Hardware-Implementation der FCS-Erzeugung: linear feedback shift register (LFSR)



Benutzung:

- Bit-string der Länge n in das LFSR schieben.
- Danach befindet sich die FCS im LFSR

Das ist äquivalent zu:

- Polynomial-division des Bi-Strings durch sogenanntes Generatorpolynom g (hier: $x^5+x^3+x^2+1$)
- Rest der Division entspricht bits der FCS
- „Einer“ in Polynom entsprechen „xor“ im LFSR

SIEMENS

Qualität von CRC-Verfahren

Sehr gut erforscht (seit 1960, W. W. Peterson).

Einige Ergebnisse aus der Theorie:

- Alle Einzelfehler werden erkannt (wenn r≥1)
- Fehlerbündel mit Länge ≤ r werden erkannt (x^0-term muss 1 sein)
- Hammingabstand hängt von g und n ab (Tabellen in der Literatur)
- Alle Fehler mit ungerader Anzahl von Bits werden erkannt, wenn g durch (x+1) teilbar ist
- …

n: Nachrichtenlänge

r: Länge der FCS / Grad des Generatiorpolynoms g

Aber: was heißt das denn nun in der Praxis?

- Wie hoch ist letztendlich die Wk., dass ein Fehler nicht erkannt wird?

PFH < 10^{-9} h^{-1} ?

SIEMENS

Annahmen über Fehler im Kanal : Binary Symmetric Channel (BSC)

BSC ist das grundlegendste Kanalmodell

Annahmen:

- konstante Bitfehlerwahrscheinlichkeit p
- Symmetrie: Bitkipper von 1→0 sind genauso wahrscheinlich wie Bitkipper von 0→1
  Dadurch sind Fehlerwahrscheinlichkeiten unabhängig von den gesendeten Daten
- Bitfehler sind unabhängig voneinander

Restfehlerwahrscheinlichkeit P_{re}

Definition: Paket wird akzeptiert, obwohl es fehlerhaft ist.

Worst case: p = 0.5

- FCS_{rcv} ist gleichverteilte Zufallszahl
- die Wahrscheinlichkeit, dass FCS_{rcv} und FCS_{exp} sie übereinstimmen, ist 2^{-r}

Folgerung: P_{re} ist durch 2^{-r} beschränkt.

Oder etwa nicht?

[J.K. Wolf and R.D. Blakeney, 1988]:

“p = 0.5” ist nicht immer der Worst-Case!

„Intuition ist eine schlechte Ratgeberin beim Rechnen mit Wahrscheinlichkeiten“

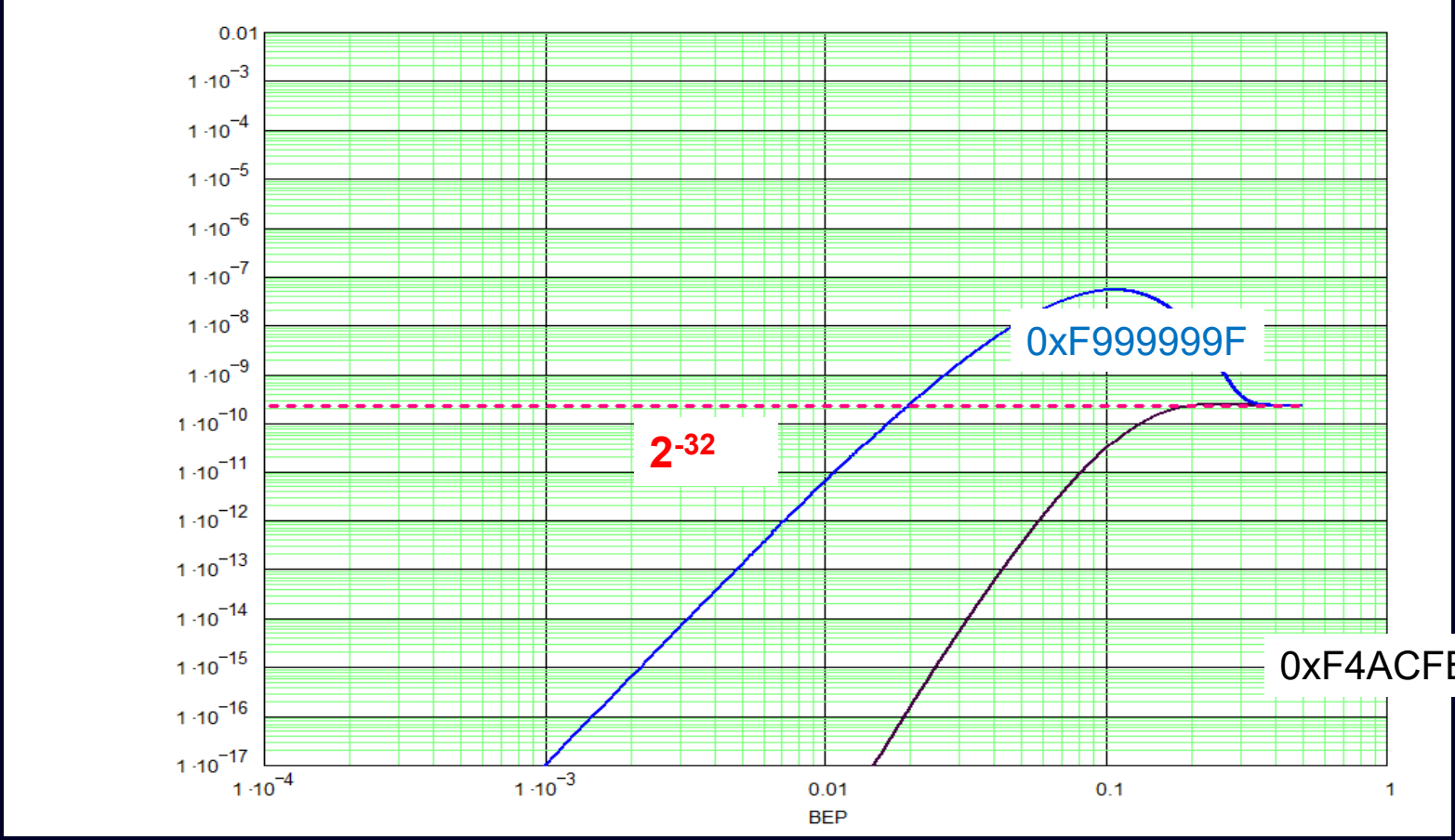
Gero von Randow

Folge:

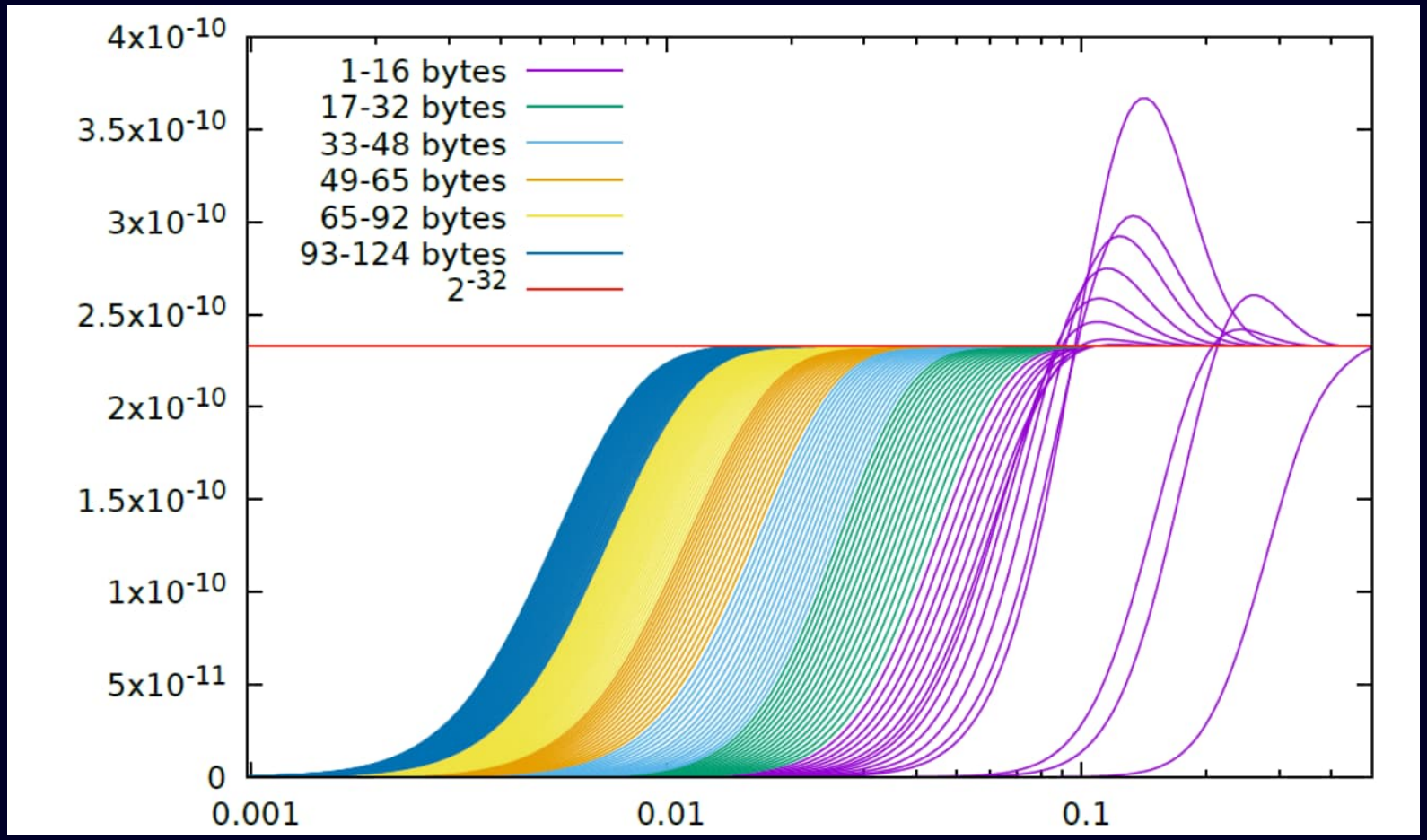
- Man muss ein CRC-Verfahren (inkl. Polynom) für alle $p \in]0; 0.5]$ bewerten!

Übrigens: Man muss ein CRC-Verfahren (inkl. Polynom) für alle verwendeten Nachrichtenlängen bewerten!

„Properness“


0.01
1 ·10−3
1 ·10−4
1 ·10−5
1 ·10−6
1 ·10−7
1 ·10−8
1 ·10−9
1 ·10−10
1 ·10−11
1 ·10−12
1 ·10−13
1 ·10−14
1 ·10−15
1 ·10−16
1 ·10−17
1 ·10−4
1 ·10−3
0.01
0.1
1
BEP
0xF999999F
2-32
0xF4ACFB13

Ergebnisse – Evaluation PROFIsafe, Polynom 0xF4ACFB13



SIEMENS

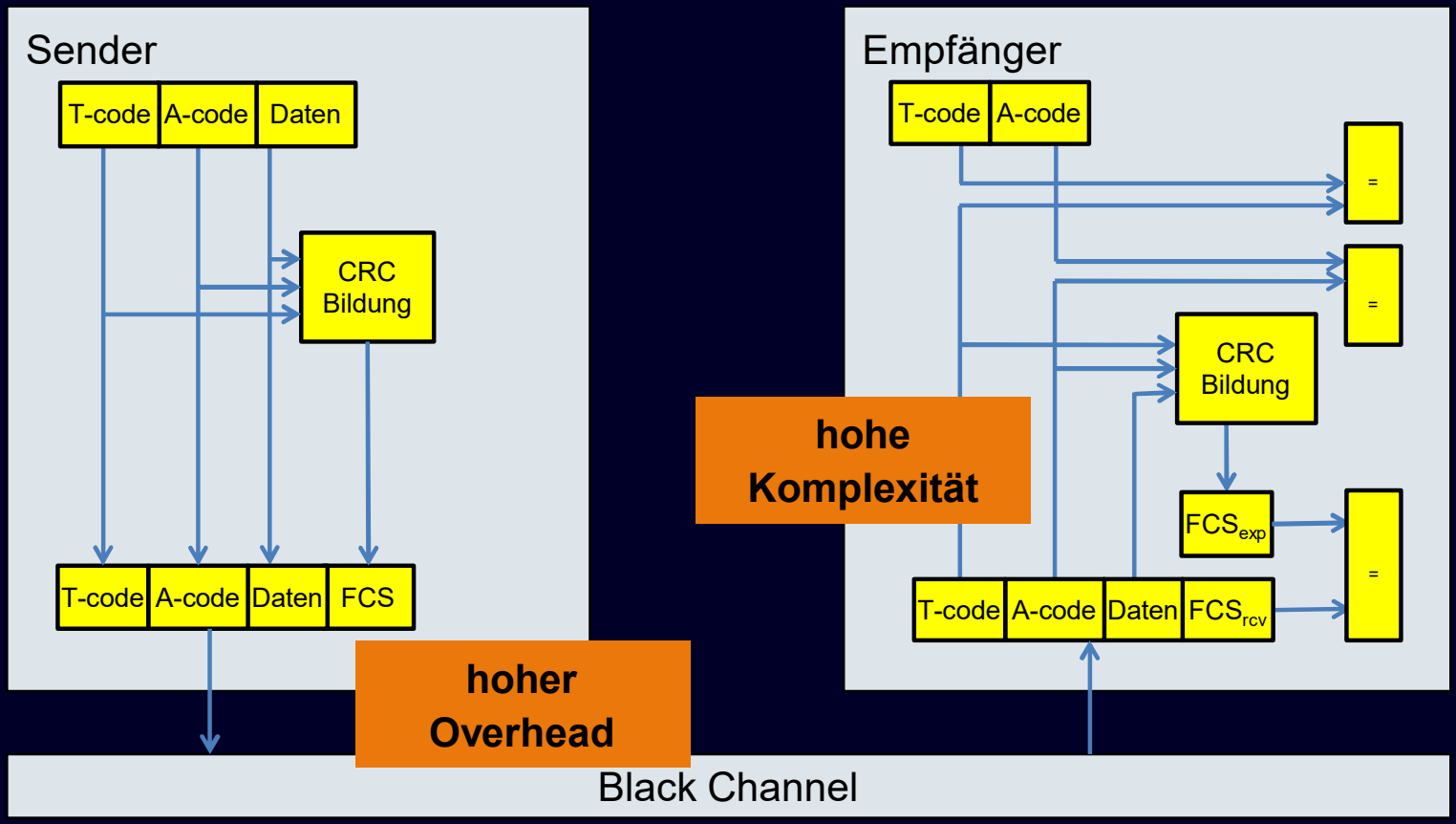
TADI-Fehlermodell

CRC-Verfahren schützen gegen „Data Integrity“-Fehler.

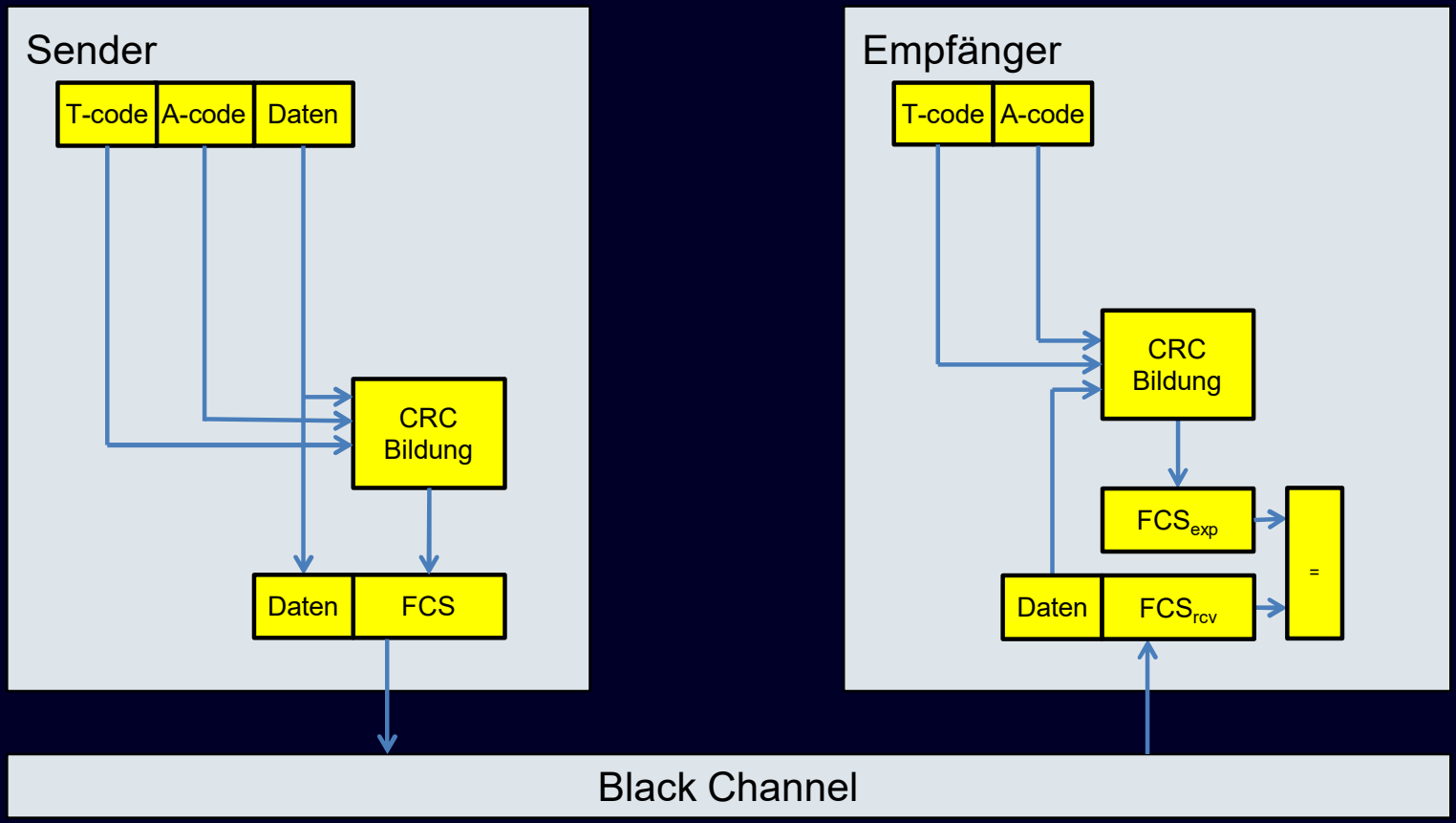
Es gibt keinen Schutz gegen

- Timeliness Fehler (z.B. Empfang veralteter Nachrichten)
- Authenticity Fehler (z.B. Fehleradressierung)

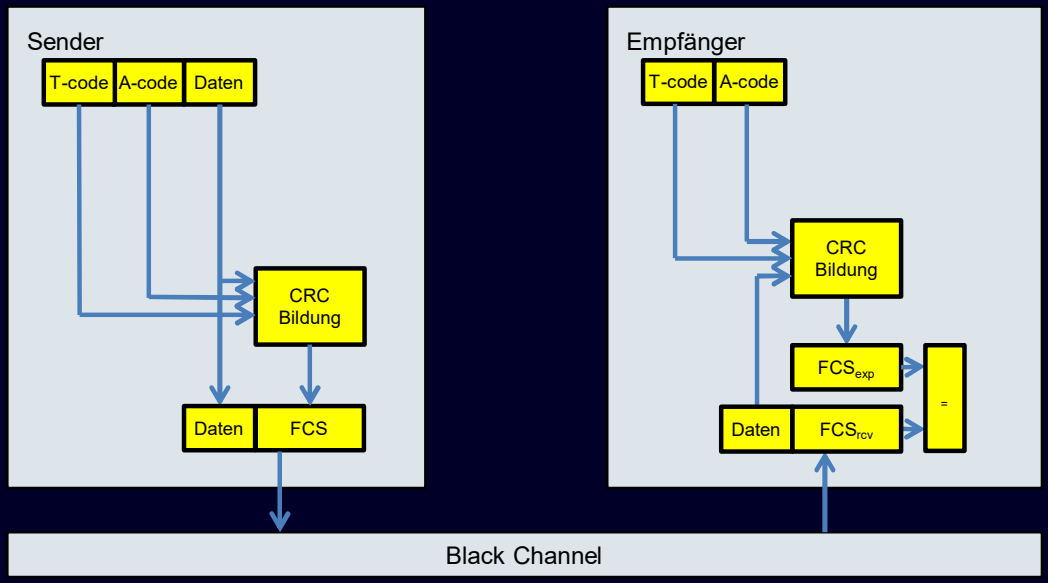
Explizite Übertragung des T- und A-Codes



Implizite Übertragung des T- und A-Codes



Implizite Übertragung des T- und A-Codes



Annahme:

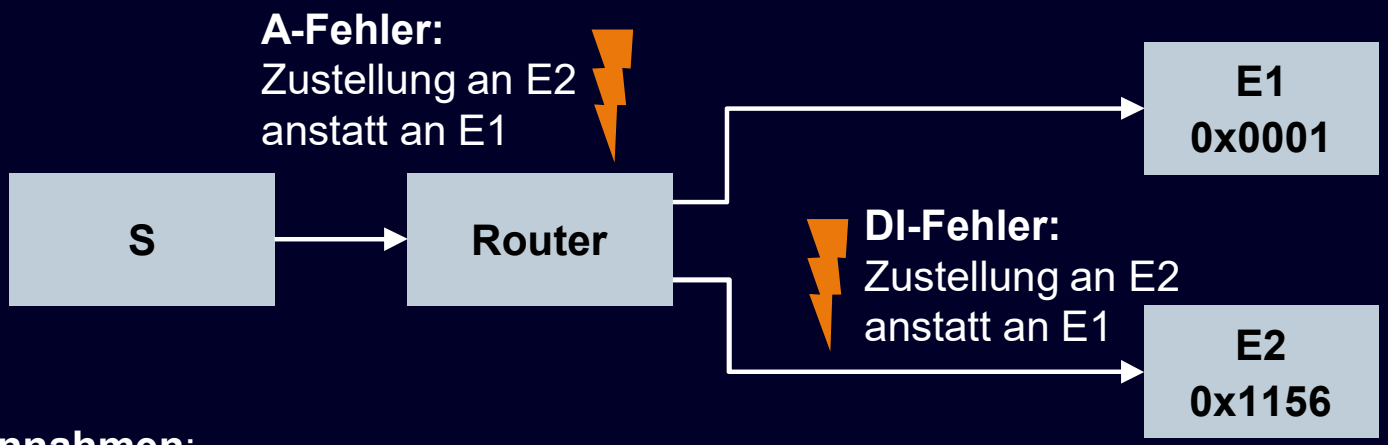
A- und T - Code eindeutig.

Authenticity-Fehler:	A-code im Sender und Empfänger stimmen nicht überein Länge des Fehlermusters ist kleiner gleich Länge des A-Codes Da Länge des A-Code kleiner gleich r, wird Fehler zu 100% erkannt
Timeliness-Fehler:	analog dazu 100% Fehlererkennung
kombinierte Fehler (z.B. DI & A):	CRC-Verfahren wirkt wie bisher mit $P_{re} < 2^{-r}$

Oder etwa nicht?

„Intuition ist eine schlechte Ratgeberin beim Rechnen mit Wahrscheinlichkeiten“

Beispiel: Mehrfachfehler

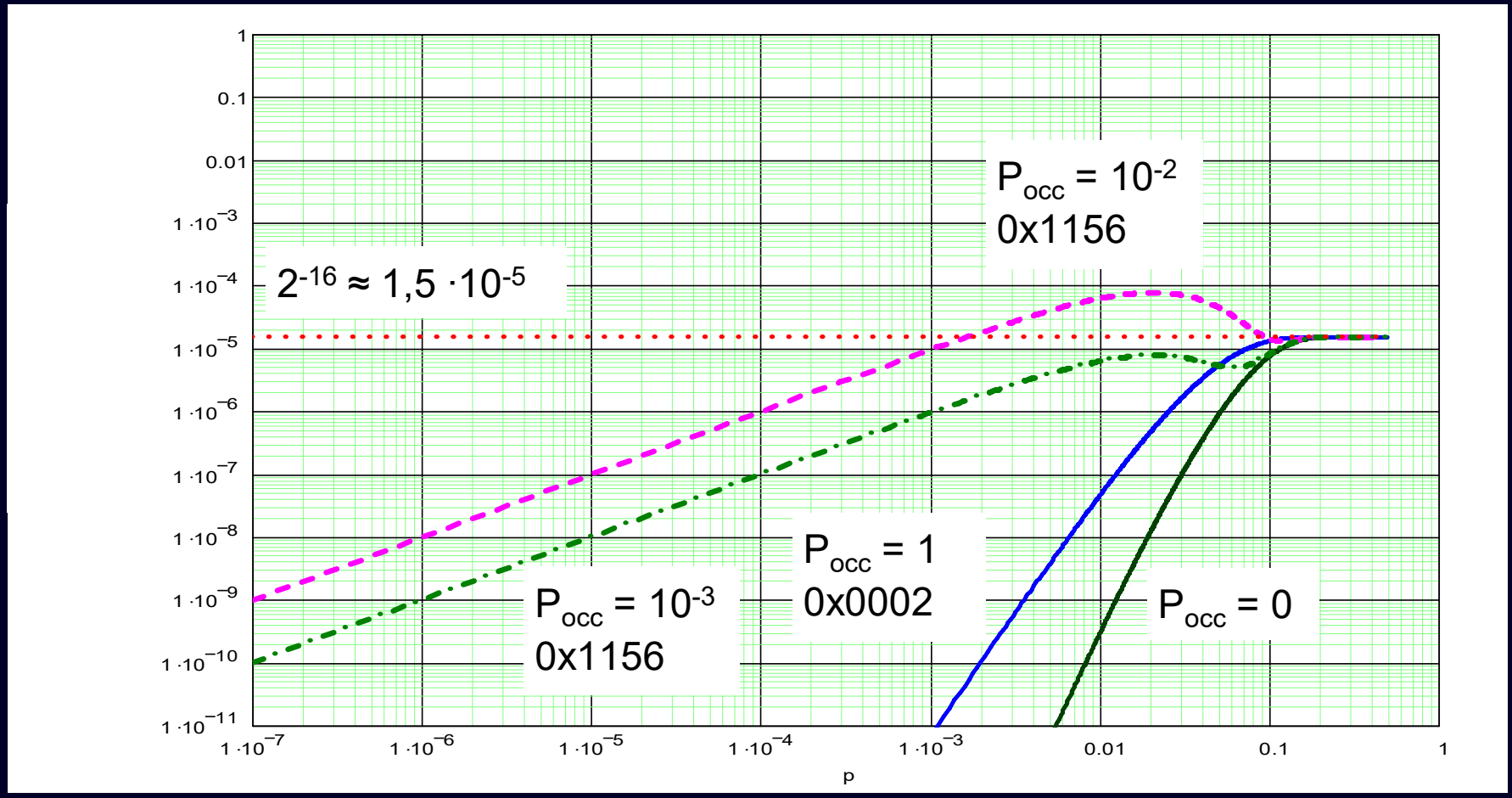


Annahmen:

- genau zwei Empfänger, mit Adressen 0x0001 und 0x1156
- kombinierter Fehler: A und DI
- Fehlermuster durch A-Fehler mit Wahrscheinlichkeit P_{occ}:
  0x0001 XOR 0x1156 = 0x1157 = const.
- DI-Fehler: BSC-Fehlermodell mit Bitfehler-Wahrscheinlichkeit p

Fragestellung: Wie hoch ist die Restfehler-Wahrscheinlichkeit RP?

RP, ermittelt durch vollständige Simulation aller Fehlerkombinationen



Problem & Lösungsansatz

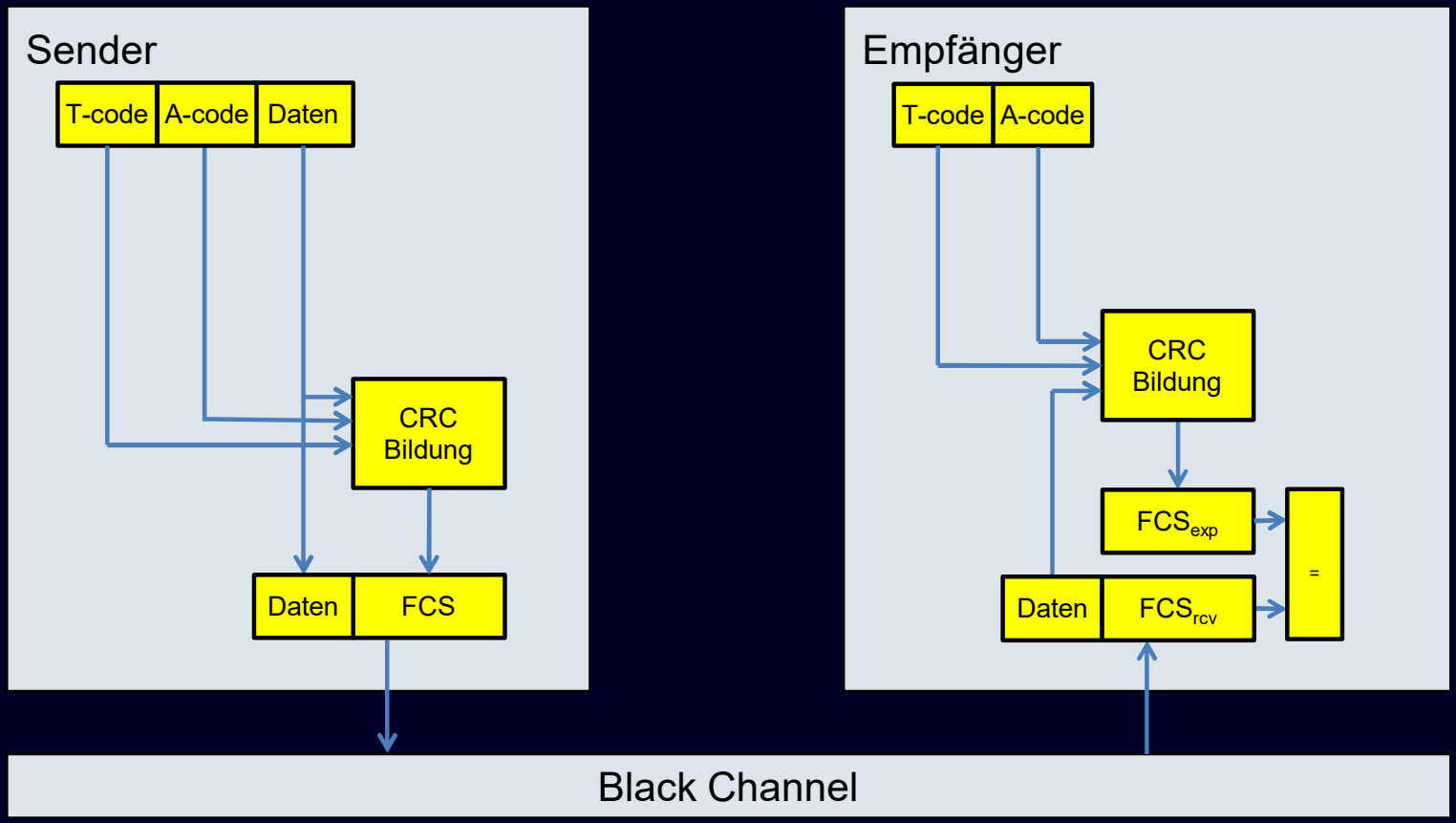
Problem bei der Verwendung impliziter Daten:

- bei Mehrfachfehlern gilt Schranke 2^{-r} nur unter bestimmten Annahmen
- im Beispiel: Schranke verletzt, z. B. bei Adressen 0x0001 und 0x1156
- widerspricht dem Black-Channel-Prinzip

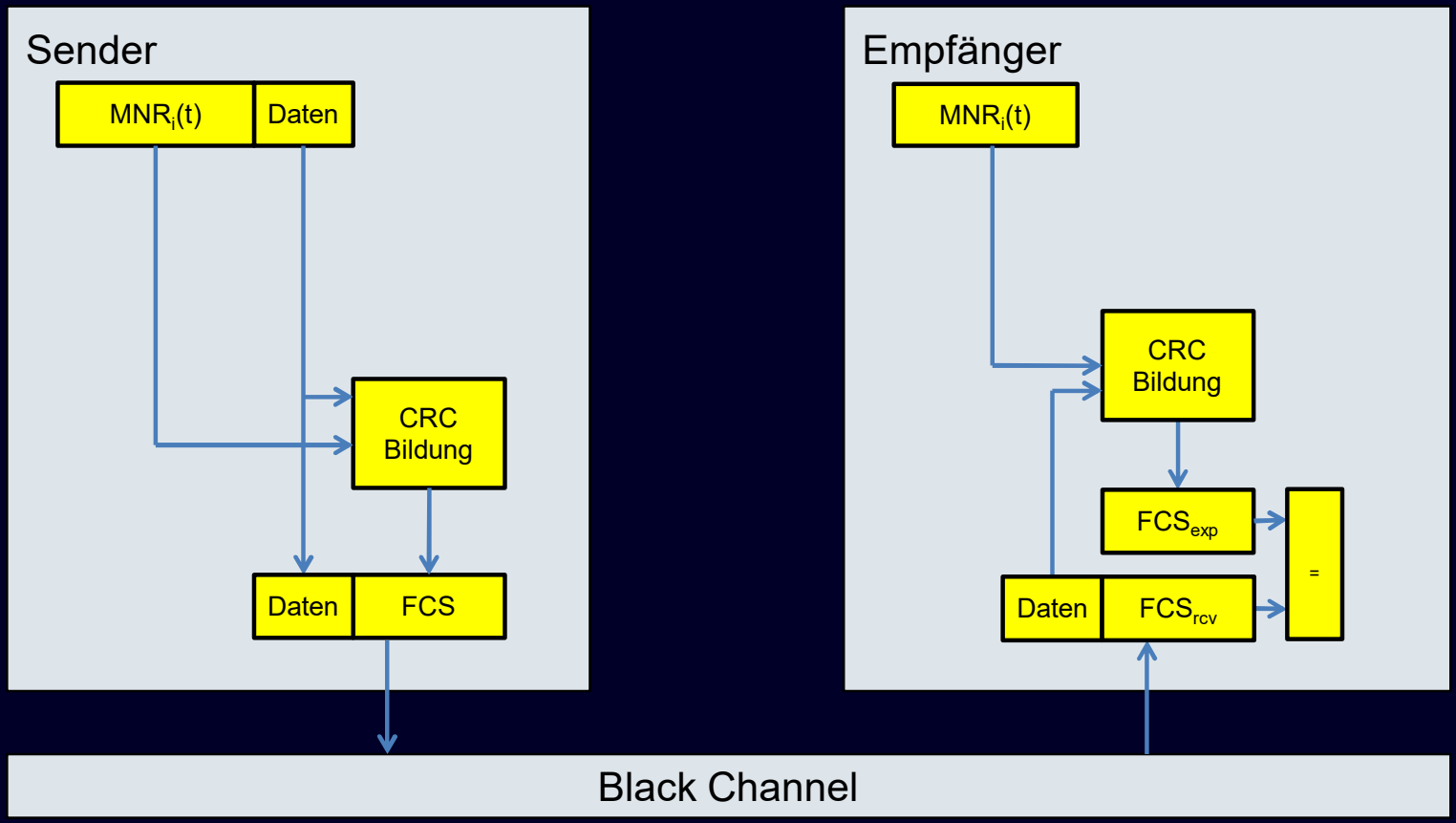
Lösungsprinzip bei PROFIsafe:

- Fehlermuster von Adress- oder Sequenzfehlern muss zufällig sein
- ist der Fall, wenn implizite Daten „zufällig“ sind
- statt A- und T-Code: pseudozufällige „Monitoring Number (MNR)“

Implizite Übertragung des T- und A-Codes



Implizite Übertragung der Monitoring Number



Zusammenfassung

- Industriesteuerungen sind ein interessantes Betätigungsfeld für Informatiker
- „Reale Welt“: Zuverlässigkeit ist entscheidend!
- Nicht vergessen: “Anything that can go wrong … will go wrong.”
- Vorgehen:
  - Liste der unerwünschten Ereignisse / Risikobewertung
  - Fehlermodell -> Liste mit Ursachen, abstrahiert
  - Gegenmaßnahmen
  - Safety: formale Bewertung (ggf. probabilistisch) nötig
- Keep things simple!
- „Intuition ist eine schlechte Ratgeberin beim Rechnen mit Wahrscheinlichkeiten“

Danke!

Kontakt:

Max Walter
max.walter@siemens.com

SIEMENS