BEB SOLUTIONS

Sichere Ethernetkommunikation zwischen ecomatControllern

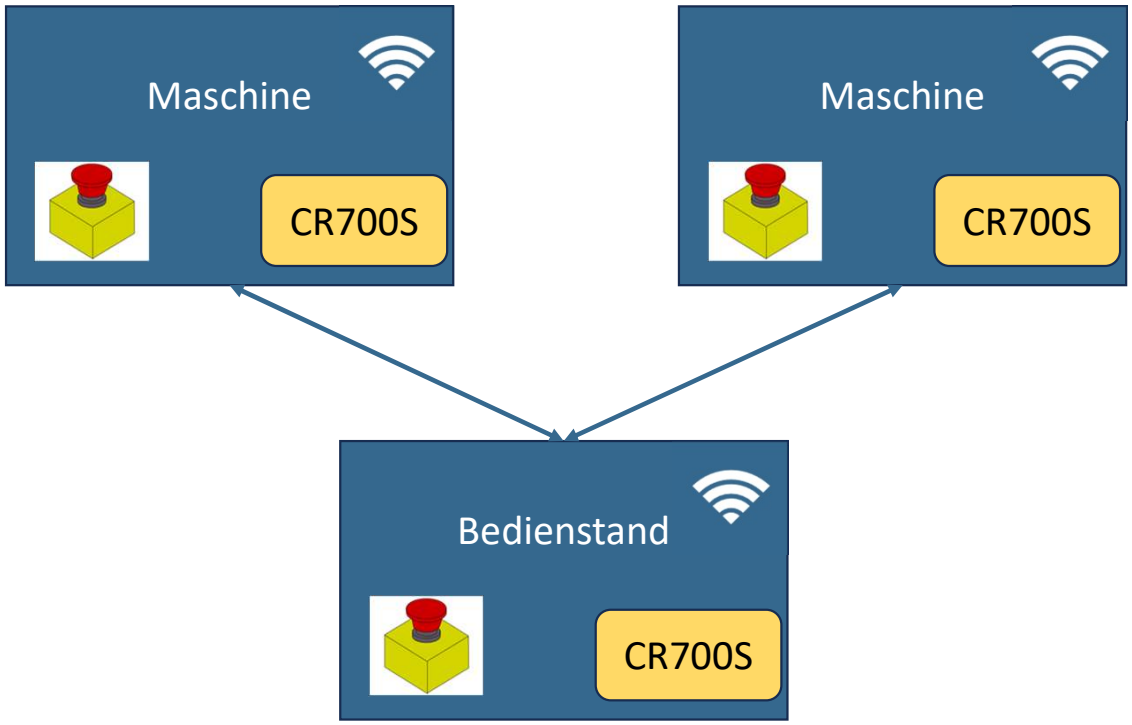
Abgrenzung des Begriffs „Sicherheit“

Bereich	Fokus	Zielsetzung
Cyber-Sicherheit	Schutz vor **absichtlichen Angriffen**	Verhindern von Datenverlust, Systemmanipulation oder unbefugtem Zugriff
Funktionale Sicherheit	Schutz vor **zufälligen Fehlern** im System	Sicherstellen, dass das System bei Fehlern **kontrolliert** reagiert und keine Gefahr entsteht

In diesem Vortrag geht es rein um die funktionale Sicherheit.



Szenario



Jede Maschine hat mindestens eine Sicherheitsfunktion

Bedienstand hat auch eine Sicherheitsfunktion

Wie kann man hier die sicherheitsgerichteten Signale zwischen den Maschinen und dem Bedienstand **sicher** über WLAN übertragen?

Grundlagennorm

Grundlagennorm: IEC 61508 – Allgemeine Basis für die Funktionale Sicherheit sicherheitsbezogener elektrischer / elektronischer / programmierbarer elektronischer Systeme

Was steht hier zum Thema Kommunikation?



Fehlerarten

Die Grundlagennorm IEC 61508 beschreibt allgemeine Kategorien von Übertragungsfehlern

- Verlust von Nachrichten: z.B. Nachricht wird unterwegs verworfen
- Einfügen zusätzlicher Nachrichten: z.B. defekter Bus-Controller
- Falsche Reihenfolge: z.B. durch Pufferung und Vertauschung
- Nachrichtenwiederholung: z.B. durch Doppelversand des Puffers
- Verspätete Nachrichten: z.B. hohe Latenzen, Pufferungen
- Veränderung des Inhalts: z.B. durch EMV
- Adressierungsfehler: z.B. Hardwaredefekt, das Adressbits verfälscht



Sicherheitsmechanismen

IEC 61508 beschreibt allgemeine Kategorien von Übertragungsfehlern	**IEC 61784-3** definiert Sicherheitsmechanismen (Auszug)
Verlust von Nachrichten	Timeout-Überwachung
Einfügen zusätzlicher Nachrichten	Sequenznummern, CRC-Prüfsummen
Falsche Reihenfolge	Sequenznummern
Nachrichtenwiederholung	Sequenznummern, Zeitstempel
Verspätete Nachrichten	Timeout-Überwachung, Zeitstempel
Veränderung des Inhalts	CRC-Prüfsummen
Adressierungsfehler	Adressvalidierung

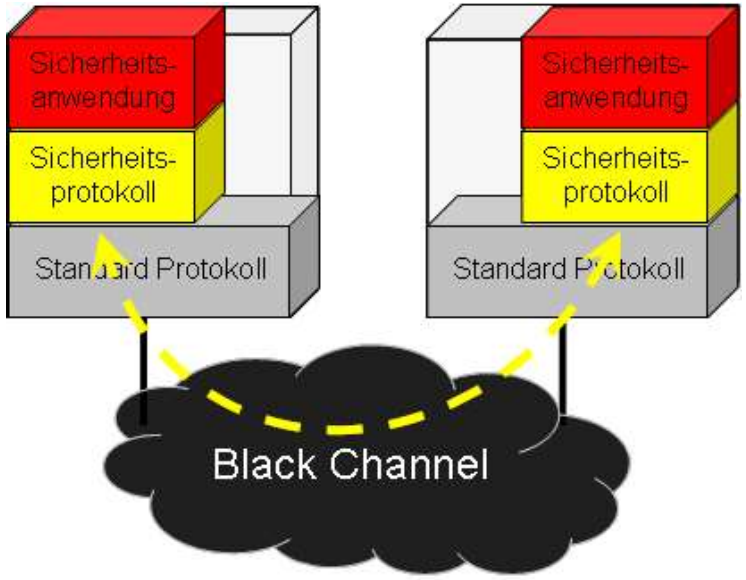


Black-Channel-Prinzip

Das Übertragungsmedium wird als „unsicher“ betrachtet.

Sicherheit wird allein durch das Protokoll hergestellt.

→ Nur das Protokoll erfüllt die 61508



Bildquelle: Wikipedia

Hingegen White-Channel:
Gesamter Kommunikationskanal erfüllt die 61508

↓

Großer Implementierungsaufwand. Technisch und wirtschaftlich schwer erreichbar und wenn dann nur durch den Hersteller der Steuerung.

Zusammenfassung Sicherheitsmechanismen

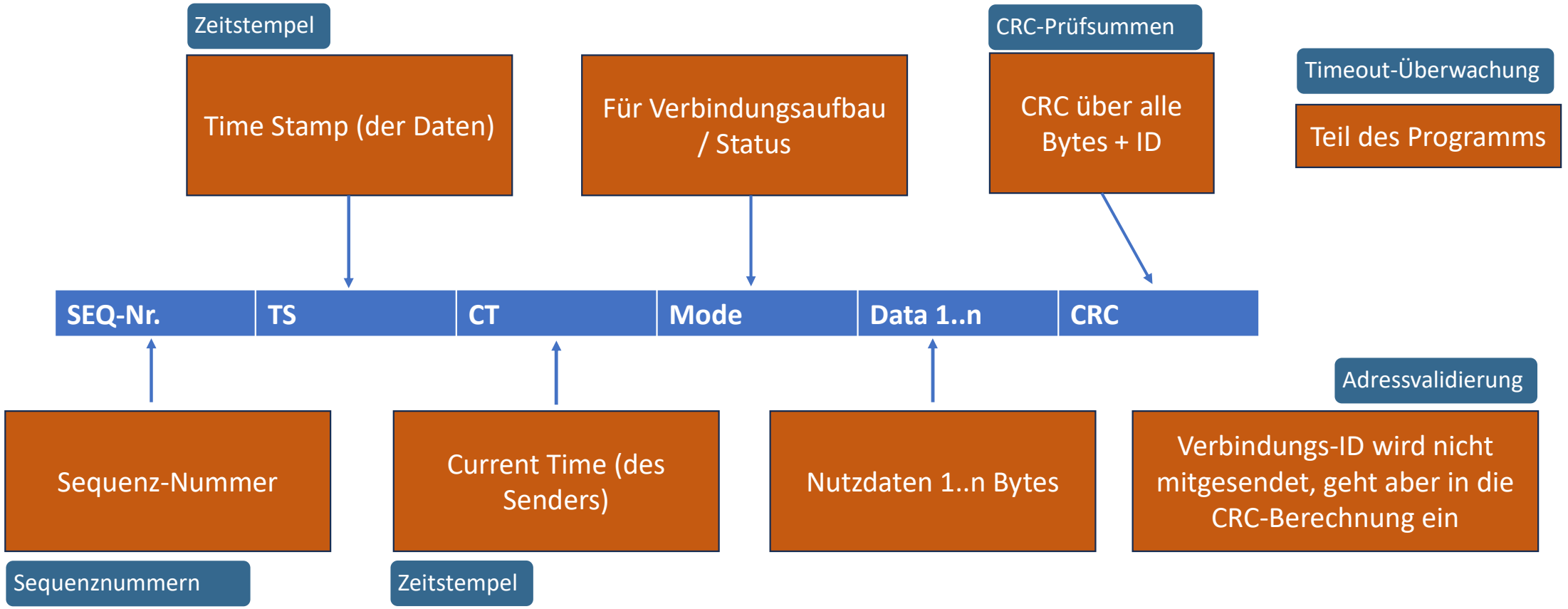
- Timeout-Überwachung
- Sequenznummern, CRC-Prüfsummen
- Sequenznummern
- Sequenznummern, Zeitstempel
- Timeout-Überwachung, Zeitstempel
- CRC-Prüfsummen, redundante Codierungen
- Adressvalidierung

→

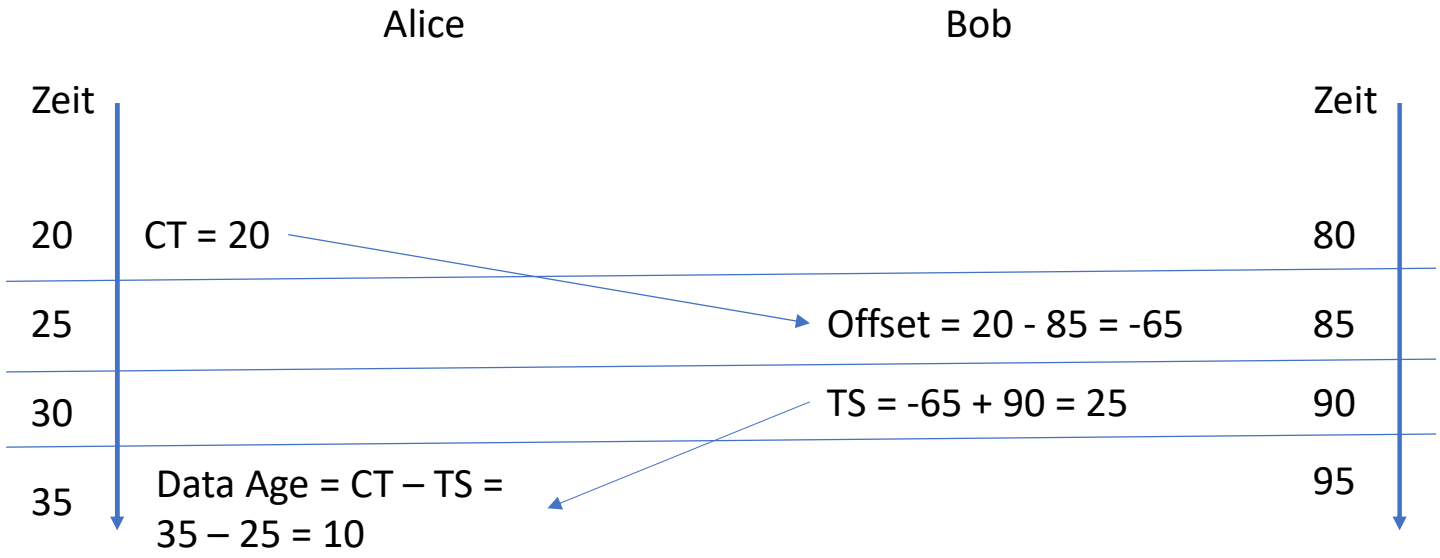
- Timeout-Überwachung
- Sequenznummern
- CRC-Prüfsummen
- Zeitstempel
- Adressvalidierung



Möglicher Telegrammaufbau



Zeitstempel



CRC-Polynome

Mit einem Cyclic Redundancy Check (CRC) kann ein Prüfwert errechnet werden, mit dessen Hilfe Fehler bei der Datenübertragung erkannt werden können.

Es beruht auf **Polynomdivision**.

Es gibt verschieden gute CRC-Polynome. Man kann grundsätzlich beliebige Polynome wählen. Die IEC 61784 schreibt aber vor, dass die Wahl in einer Sicherheitsanalyse begründet und dokumentiert wird. hierbei sind folgende Punkte Relevant:

- das Polynom muss zur **Fehlermustererkennung** geeignet sein (Bitfehler, Burstfehler)
- es muss eine ausreichende **Hamming-Distanz** bieten
- die Anforderungen an die **Restfehlerwahrscheinlichkeit** müssen erfüllt sein (SIL 2 < 10^-8)



Hamming-Distanz

Je **größer** die minimale Hamming-Distanz eines CRC-Polynoms, desto **besser** ist seine Fähigkeit, **mehrere Bitfehler** zu erkennen.

Die Hamming-Distanz hängt ab von:

- dem verwendeten **Polynom**
- der **Länge der Nachricht**

Laut IEC 61784-3 muss die Hamming-Distanz für SIL 2 mindestens 4 betragen. Für SIL 3 bereits 6.

Bei einer Hamming-Distanz von 4 erkennt das CRC-System **alle 1-, 2- und 3-Bitfehler** zuverlässig.

Hinweis: Das bei Ethernet verwendete Polynom hat eine Hamming-Distanz von 3.



Restfehlerrate

In der IEC 61508 sind die Restfehlerraten je nach SIL festgelegt. PFH = Anzahl gefährlicher Ausfälle pro Stunde.

SIL	PFH
2	< 10^-6
3	< 10^-7

In der IEC 61784 wird darüber hinaus das Restrisiko auf 1 % der jeweiligen SIL-Grenze festgelegt.

SIL	PFH for safety communication system
2	< 10^-8
3	< 10^-9

$$R_{CRC}(p, N, k) \approx \frac{1}{2^k} \cdot \sum_{n=d}^{N+k} \binom{N+k}{n} \cdot p^n \cdot (1-p)^{(N+k-n)}$$

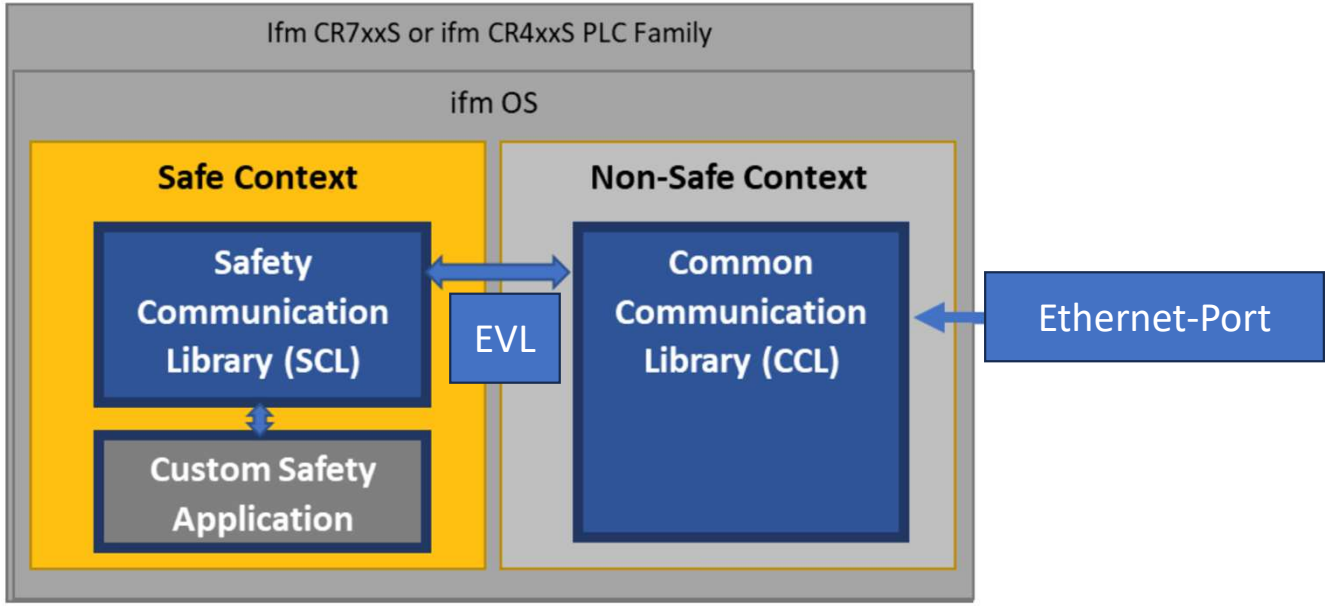
$$\Lambda = R(p) \cdot 3600 \cdot \nu$$

Implementierung in IEC-Code

Kann man ein sicheres Ethernet-Protokoll in einer IEC-Sprache (ST) auf dem ecomatController implementieren?

=> Ja, es wurde bereits gemacht. Siehe CP9060 (Safety Laser-Scanner Anbindung).

Wie sieht die Architektur hier aus?



Zusammenfassung

Es ist möglich sicherheitsgerichtete Signale sicher über „unsichere“ Wege zu übertragen.

Die IEC 61784-3 definiert hierzu Sicherheitsmechanismen.

Es ist möglich, ein eigenes (einfaches) Protokoll zu entwerfen und in einer IEC-Sprache für den ecomatController zu implementieren.

Wichtig: **Die Entwicklung und Verifikation von sicherheitsgerichteten Protokollen ist im Allgemeinen im Rahmen einer IEC 61508 konformen Produktentwicklung vorzunehmen.**