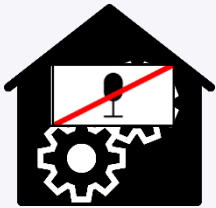
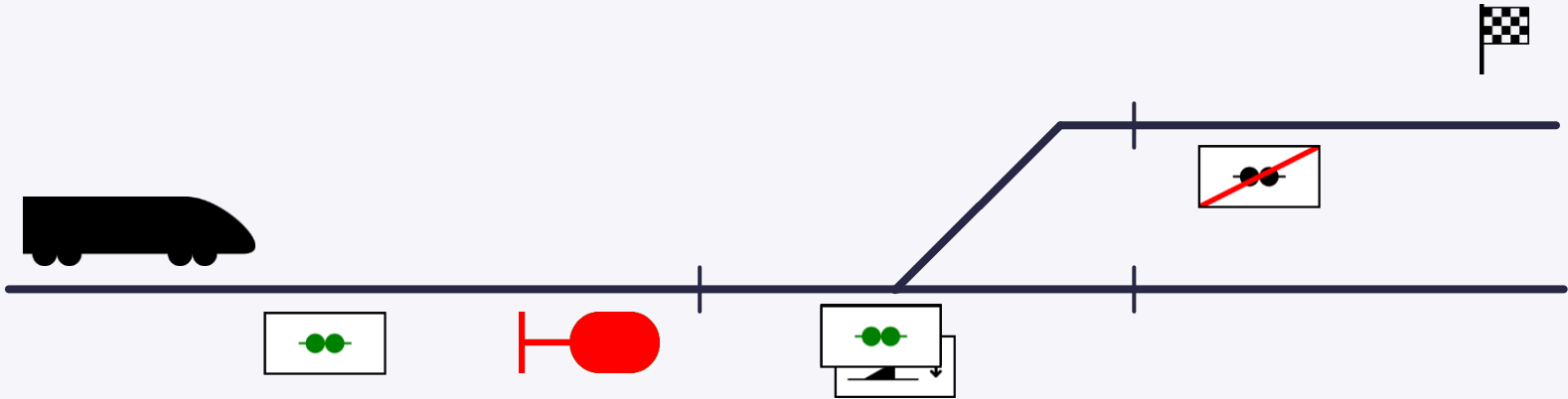


RaSTA im Safety und Security Kontext

Digital Rail Summer School 2021

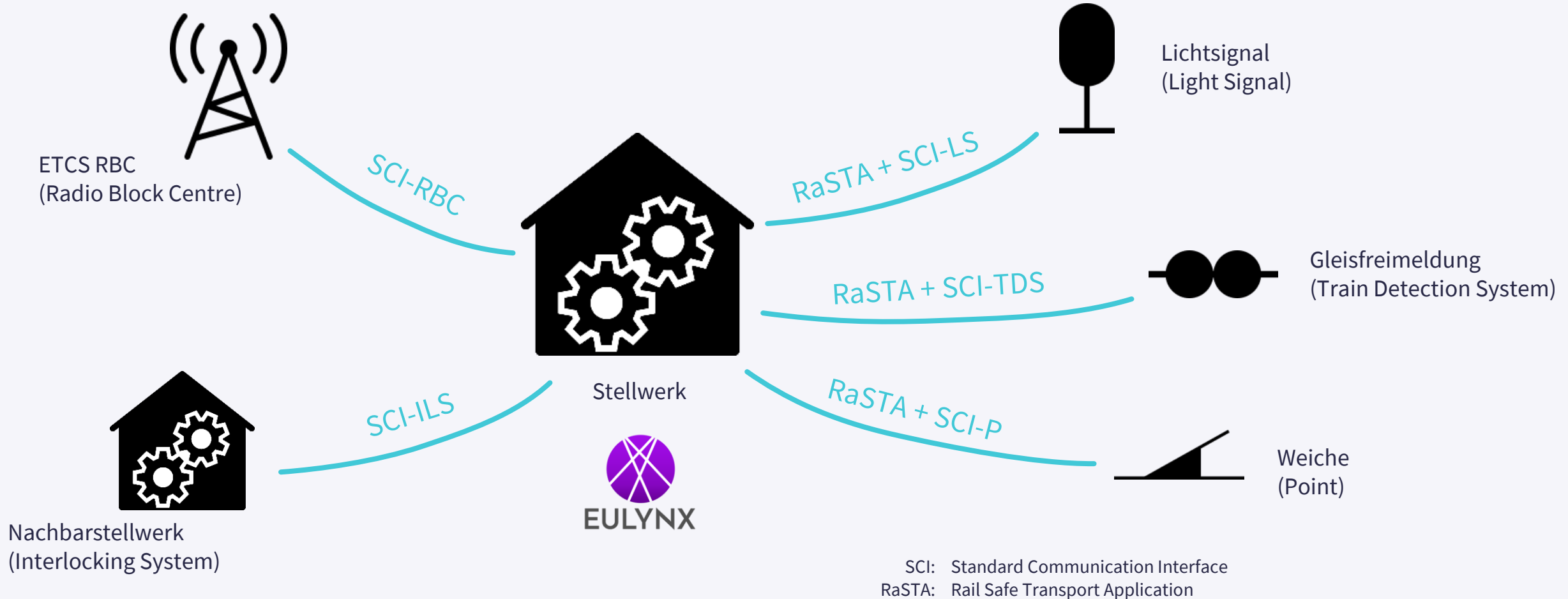
Stellwerke sind für die Safety verantwortlich



Datagrams

Signal		
	clear	stop
Point		
	left	right
TDS		
	clear	occupied

Signaltechnik verwendet standardisierte Protokolle

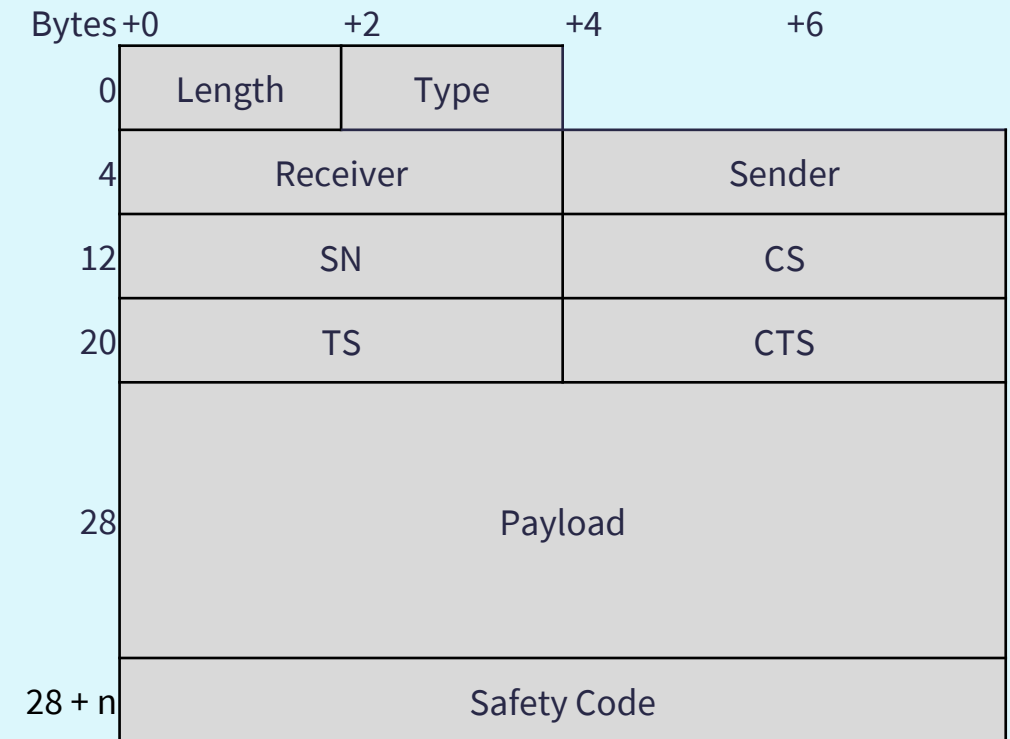
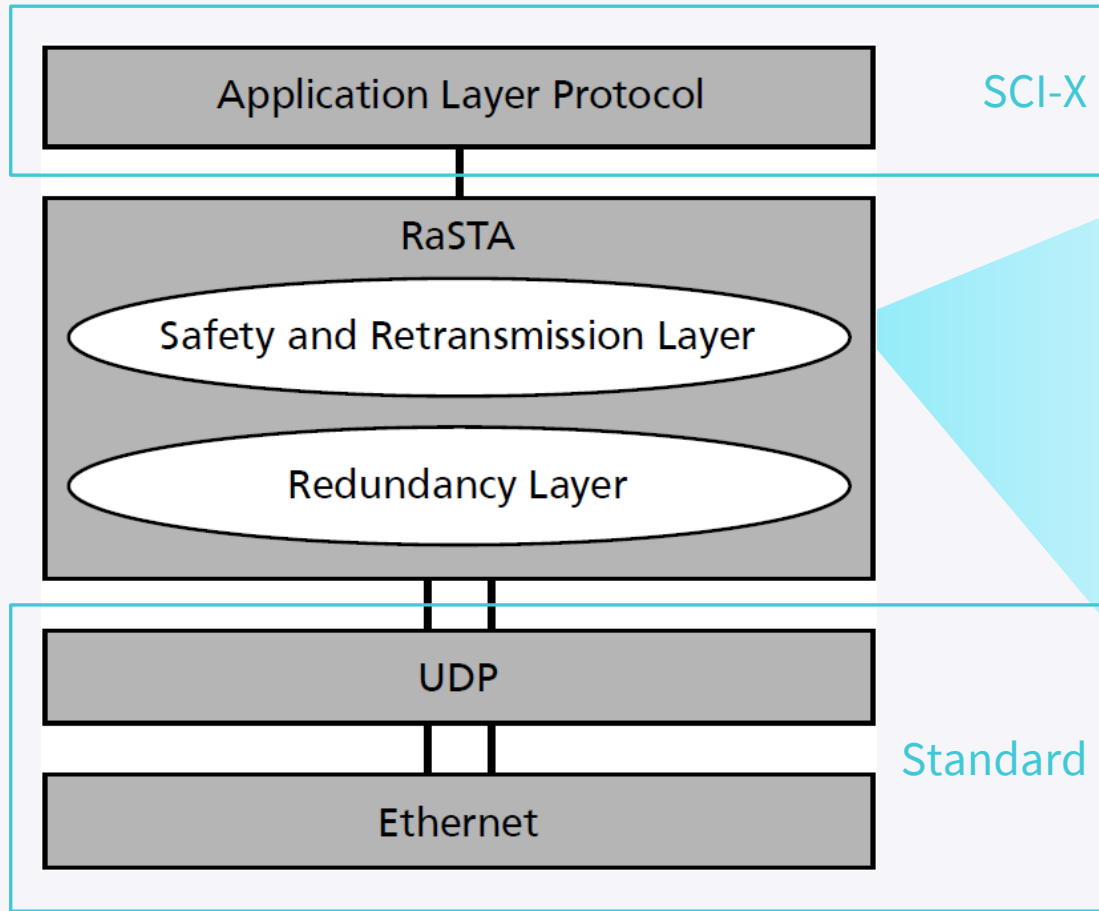


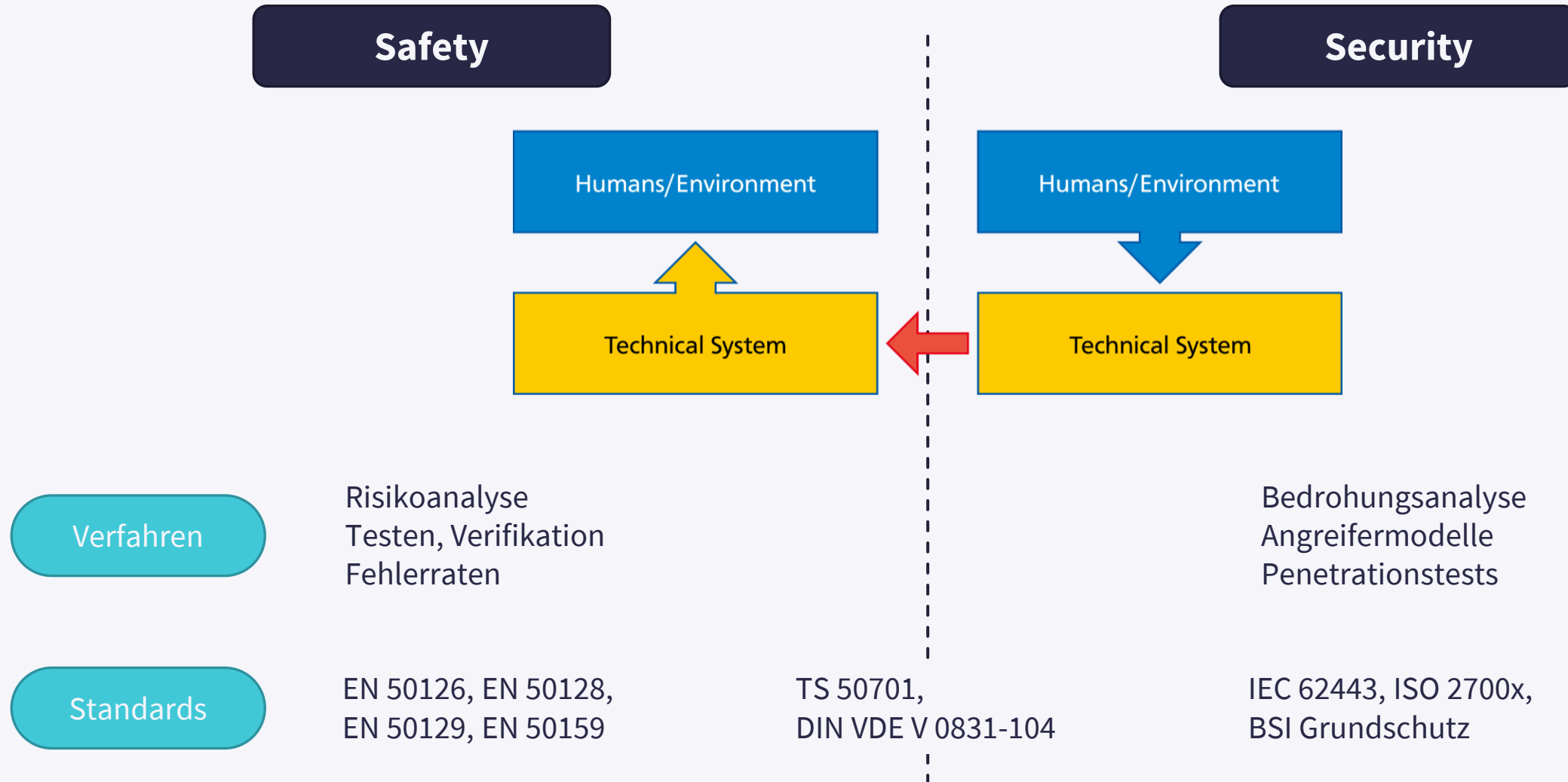
Ziele der Safety in der Datenübertragung



Ziel	Bedeutung	Einfluss Safety	RaSTA
Integrität 	• Steuerbefehle für Feldelemente müssen unverändert übertragen werden • Zustand der Feldelemente muss im Stellwerk korrekt abgebildet werden	• Hardwarefehler • Kosmische Strahlung • Bitflips	• Safety Code (MD4) • Sequenznummern • Sendewiederholung
Verfügbarkeit 	• Ausfallsicherheit • Fehleroffenbarung	• Materialversagen • Naturgefahren • Unbeabsichtigte Beschädigung	• Multipath (Redundanz) • Sendewiederholung • Lebenszeichen

RaSTA ist in einen Protokollstack eingebettet





Ziele der Security in der Datenübertragung



Ziel	Bedeutung	Einfluss Safety	Einfluss Security
Integrität Authentizität 	• Steuerbefehle für Feldelemente müssen unverändert übertragen werden • Zustand der Feldelemente muss im Stellwerk korrekt abgebildet werden	• Hardwarefehler • Bitflips • Kosmische Strahlung	• Fälschung • Nachrichten löschen • Nachrichten einschleusen • Man-in-the-Middle
Verfügbarkeit 	• Ausfallsicherheit • Fehleroffenbarung	• Materialversagen • Naturgefahren • Unbeabsichtigte Beschädigung	• Gezielte Manipulation • DoS-Angriffe
Vertraulichkeit 	• Für Nutzdaten sekundär	• Keiner	• Datagramme mitlesen

Kann RaSTA auch Security bieten?



Out of the box

Security Erweiterung

Im Protokoll-Stack



Der Dolev-Yao-Angreifer ...

- ... kann alle Nachrichten **lesen**. → Kein Problem
- ... kann alle Nachrichten **abfangen**. → Auch Safety kennt Nachrichtenverlust
- ... kann alle Nachrichten **manipulieren**. → Fahrt statt Halt, Weiche rechts statt links, Gleis frei statt besetzt
- ... kann neue Nachrichten **einschleusen**. → Manipulation zu jedem Zeitpunkt möglich
- ... kann kryptographische Primitive **nicht brechen**.



Hashfunktionen erstellen einen Fingerabdruck eines Datagramms



$$MD4_{IV}(\text{message}) \rightarrow \text{digest}$$

1. Einwegfunktion
(preimage resistance)
 2. Schwache Kollisionsresistenz
(2nd-preimage resistance)
 3. Starke Kollisionsresistenz
(collision resistance)
- Stand der Technik (Security):
SHA-2, SHA-3 (BSI-Empfehlung)

No.	Time	Source	RaSTA Src	SCI Src	Destination	RaSTA Dst	SCI Dst	Protocol	Info
1	0.000000000	192.168.10.50	102		192.168.10.1	100		RaSTA	9998 → 8888 Len=58 ConnReq
2	0.000096751	192.168.10.50	102		192.168.10.1	100		RaSTA	9999 → 8889 Len=58 ConnReq
3	0.078755401	192.168.10.1	100		192.168.10.50	102		RaSTA	8888 → 9998 Len=58 ConnResp
4	0.078796951	192.168.10.1	100		192.168.10.50	102		RaSTA	8889 → 9999 Len=58 ConnResp
5	0.079872115	192.168.10.50	102		192.168.10.1	100		RaSTA	9998 → 8888 Len=44 HB
6	0.079931463	192.168.10.50	102		192.168.10.1	100		RaSTA	9999 → 8889 Len=44 HB
7	0.569978025	192.168.10.1	100		192.168.10.50	102		RaSTA	8888 → 9998 Len=44 HB
8	0.570004265	192.168.10.1	100		192.168.10.50	102		RaSTA	8889 → 9999 Len=44 HB
9	0.657695759	192.168.10.50	102	G22_HV_ANALOG ...	192.168.10.1	100	ESTW ...	SCI	9998 → 8888 Len=96 Data (Indi...
10	0.657960669	192.168.10.50	102	G22_HV_ANALOG ...	192.168.10.1	100	ESTW ...	SCI	9999 → 8889 Len=96 Data (Indi...
11	1.071282924	192.168.10.1	100		192.168.10.50	102		RaSTA	8888 → 9998 Len=44 HB
12	1.071308826	192.168.10.1	100		192.168.10.50	102		RaSTA	8889 → 9999 Len=44 HB
13	1.112845995	192.168.10.50	102	G22_HV_ANALOG ...	192.168.10.1	100	ESTW ...	SCI	9998 → 8888 Len=96 Data (Indi...
14	1.112898211	192.168.10.50	102	G22_HV_ANALOG ...	192.168.10.1	100	ESTW ...	SCI	9999 → 8889 Len=96 Data (Indi...
15	1.572666411	192.168.10.1	100		192.168.10.50	102		RaSTA	8888 → 9998 Len=44 HB
16	1.572696636	192.168.10.1	100		192.168.10.50	102		RaSTA	8889 → 9999 Len=44 HB

Frame 5: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: 0a:70:34:c2:3b:4d (0a:70:34:c2:3b:4d), Dst: Wistr
Internet Protocol Version 4, Src: 192.168.10.50, Dst: 192.168.10.1
User Datagram Protocol, Src Port: 9998, Dst Port: 8888
RaSTA Protocol
Redundancy Layer
Length: 44
Reserve: 0
Sequence number: 1
Check code: <MISSING>
Safety and Retransmission Layer
Message length: 36
Message type: Heartbeat (6220)
Receiver identification: 100
Sender identification: 102
Sequence number: 38173125
Confirmed Sequence Number: 3408235966
Time stamp: 80558
Confirmed time stamp: 6519787
Safety code: c5a86de6bc7ce71e
[Safety code valid: True]

Kann RaSTA auch Security bieten?



Out of the box

Replay-Angriffe → Sequenznummer
Modifikation/Fälschung → MD4?

Security Erweiterung



Nachrichten können mit MACs authentifiziert werden



- Ersetze MD4 durch eine Keyed-Hashfunktion: BLAKE2B, SipHash-2-4
- Vertraulichkeit des Schlüssels beachten
 - Sicherer Speicher
 - Sicherer Schlüsseltausch
- Erfordert Erweiterung der RaSTA-Spezifikation

$$H(\underbrace{\{0,1\}^*}_{\text{message}}, \underbrace{\{0,1\}^n}_{\text{key}}) \rightarrow \underbrace{\{0,1\}^n}_{\text{digest}}$$

Kann RaSTA auch Security bieten?



Out of the box

Replay-Angriffe → Sequenznummer
Modifikation/Fälschung → MD4?

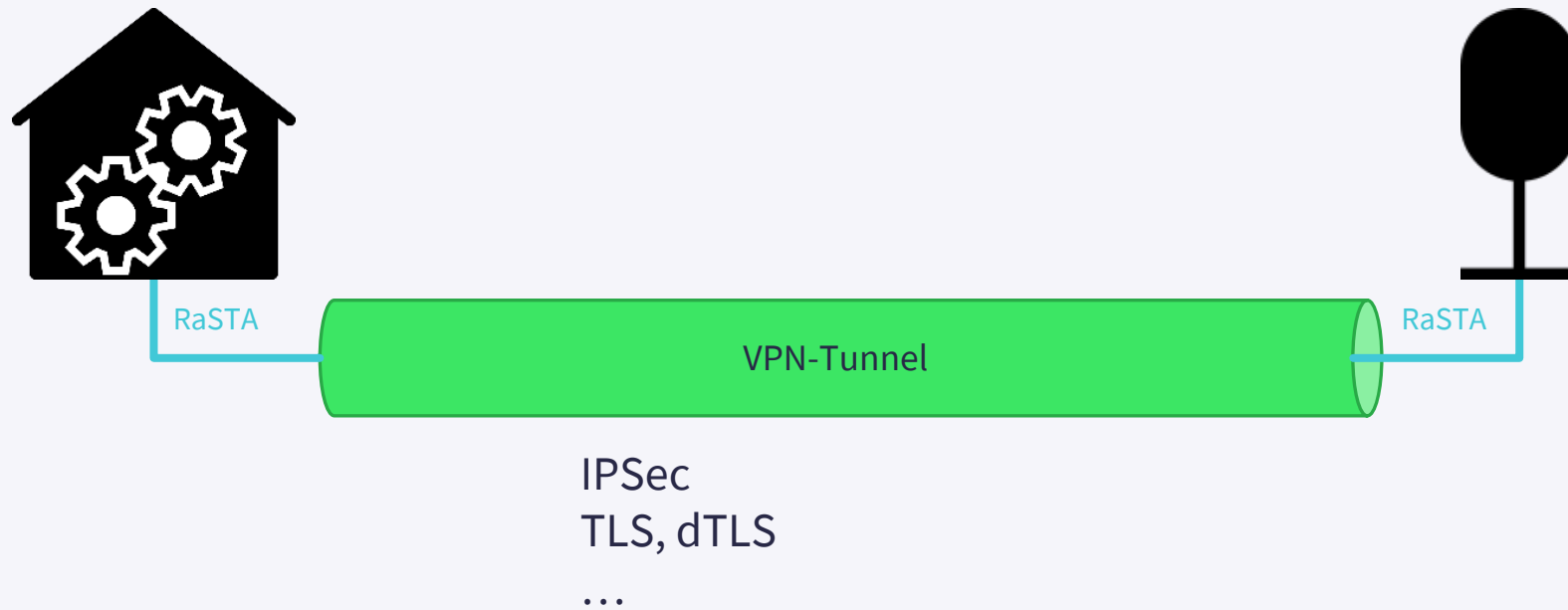
Security Erweiterung

Keyed-Hashfunktion
Sicherer Schlüsselspeicher

Im Protokoll-Stack



VPN-Tunnel sichern die Kommunikation im Protokoll-Stack



Kann RaSTA auch Security bieten?



Out of the box

Replay-Angriffe → Sequenznummer
Modifikation/Fälschung → MD4?

Security Erweiterung

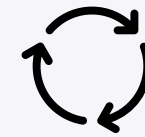
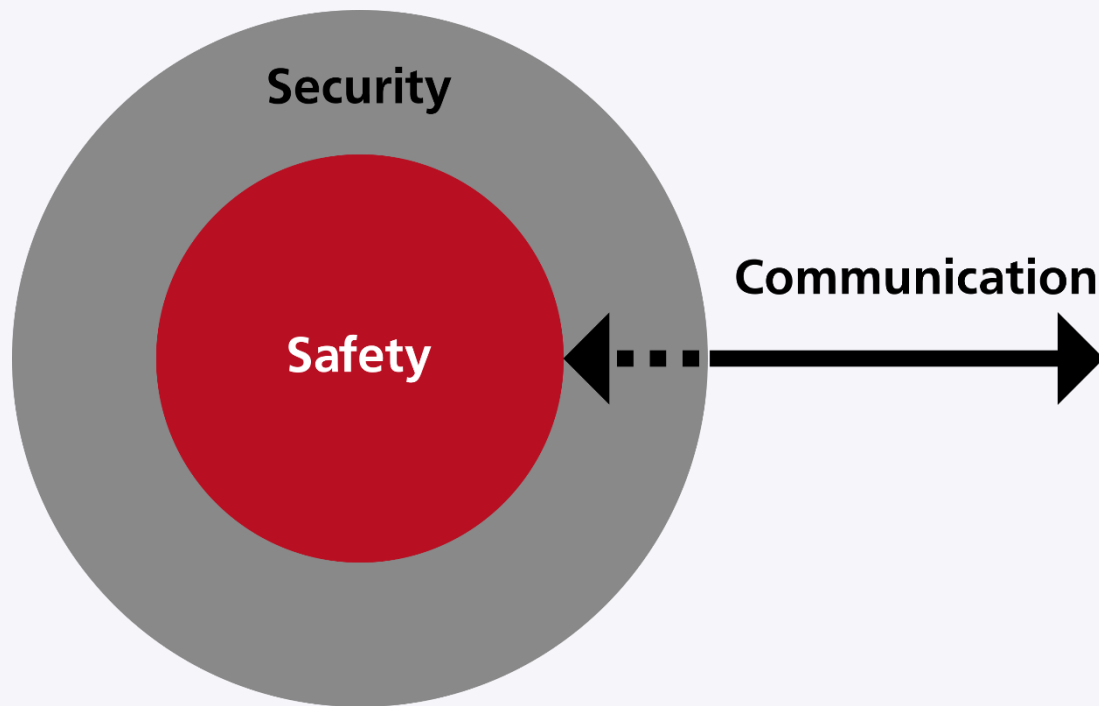
Keyed-Hashfunktion
Sicherer Schlüsselspeicher

Im Protokoll-Stack

IPSec
TLS, dTLS
SSH
...



Soll RaSTA auch Security bieten?



Update-Zyklen



Safety-Zulassung



Rückwirkungsfreiheit

Stellwerk und Feldelement haben unterschiedliche Security-Anforderungen

Stellwerk



- Starker physischer Schutz
- Zugangsbeschränkt
- Überwachung möglich
- Steuert zahlreiche Feldelemente

Feldelemente



- Schwacher physischer Schutz
- Leicht zugänglich
- Überwachung unpraktikabel
- Steuert ein Feldelement

End-to-End Security

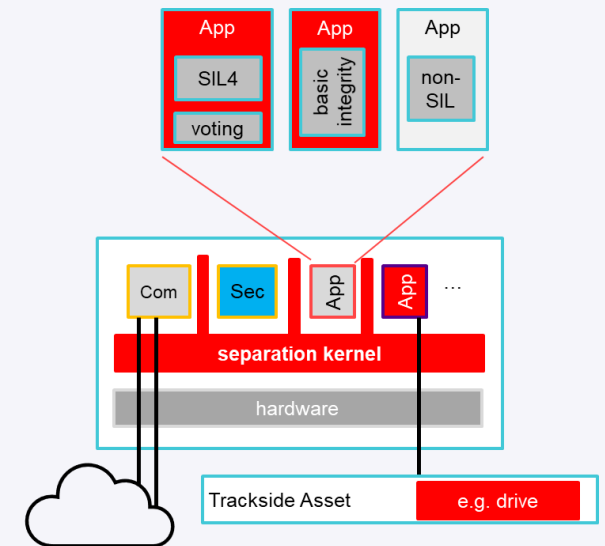
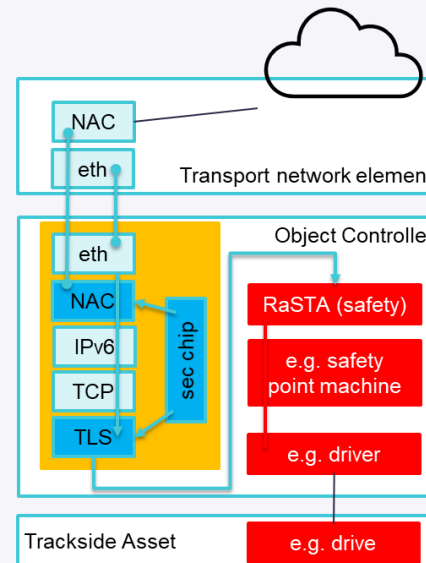
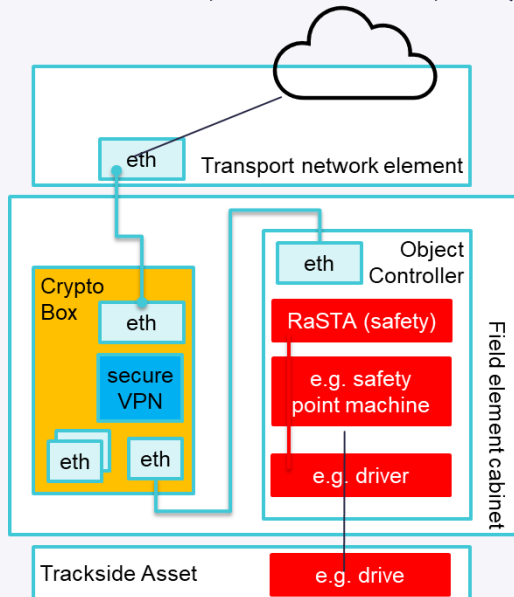
Trennung Safety und Security, aber...

Die Trennung von Safety und Security stellt sicher, dass:

- Security Updates ohne Kompromittierung der Safety Zertifizierung erfolgen kann
- Normenkonformität hergestellt werden kann (EN 50129, TS 50701, ...)

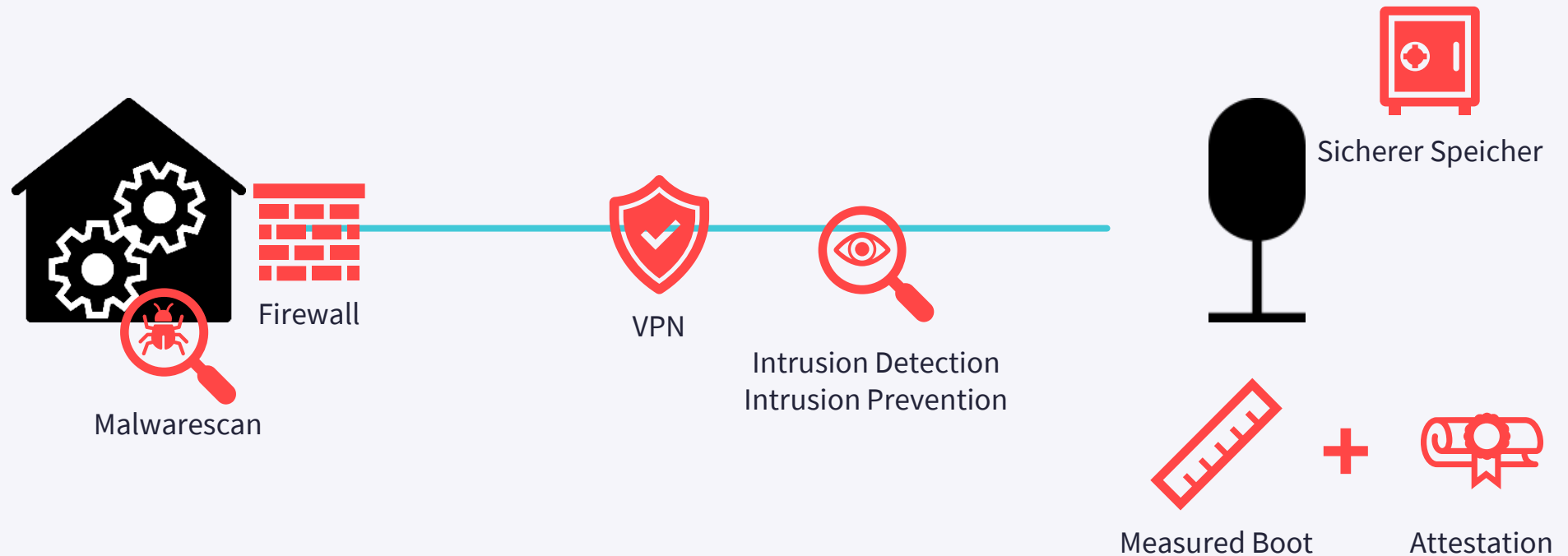
ABER: Eine stärkere Integration in einer Hardware ist unabdingbar, um:

- Den Schutz des Endpunktes sicher zu stellen
- Den Betrieb (LCC) zu vereinfachen



Evolution

Die Security-Schale setzt das Defense-in-Depth-Konzept um





Dr.-Ing. Markus Heinrich
Expert IT Security
Schaumainkai 91
60596 Frankfurt am Main

www.incyde.com
markus.heinrich@incyde.com
+49 160 4381583

Für Fragen stehe ich gerne zur Verfügung!

