Zukünftige Security Anforderungen für die Energieautomatisierung

Christoph Ruland

Vortrag beim VDE Kassel

23. Mai 2019

IT-Security für die Energieversorgung

- Security for Operational Technology (OT)
- Security für verteilte Prozesssteuerung
- Security for Industrial Automation and Control Systems
- Industrial Security
- Industrial Information and Communication Security

IT- Security vs. OT - Security

Datenverarbeitung (Banken, Büro, Versicherungen, Verwaltung, Buchungssysteme, Forschung)

- Sicherheitsanforderungen
  1. Vertraulichkeit
  2. Datenunversehrtheit
  3. Verfügbarkeit
- Hoher Durchsatz
- Schäden können repariert/ausgeglichen werden
- Rollback- und Backupmöglichkeiten

Produktionssteuerung, Industrie 4.0, Smart Manufacturing, Smart Grids, Smart Cities, Autonomes Fahren

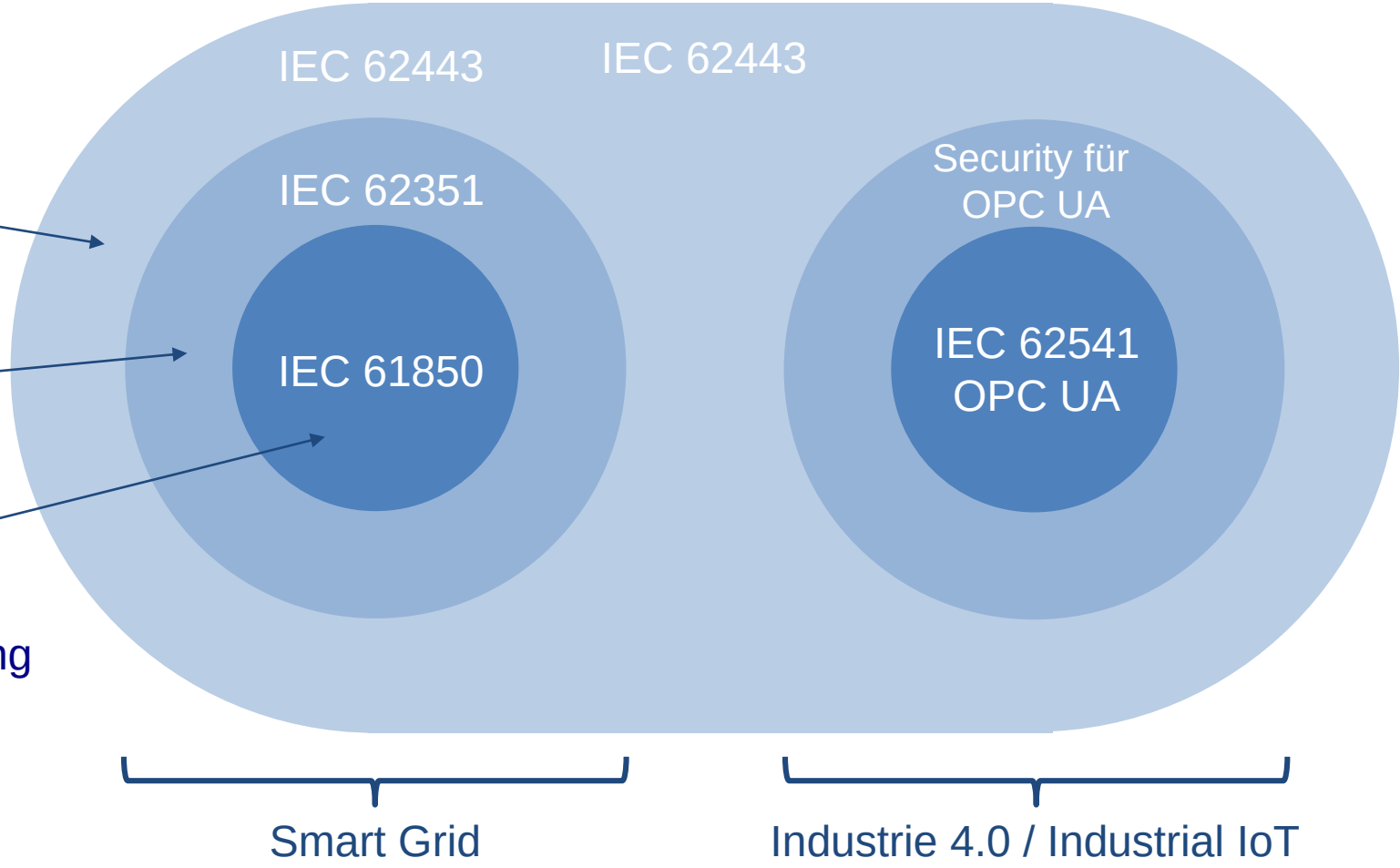
- Sicherheitsanforderungen
  1. Verfügbarkeit
  2. Datenunversehrtheit (Authentisierung, Autorisierung, Zugangs-/Zugriffskontrolle
  3. Vertraulichkeit
- Kurze Reaktionszeiten (< 3 ms)
- Schäden sind nicht reparierbar
- Auswirkungen auf die Safety
- Schäden für Menschen, Investitionen und Umwelt
- Berücksichtigung von Notfallsituationen
- Langlebige Produktzyklen

Standardisierungshintergrund

Industrielle Kommunikationsnetze –
IT-Sicherheit für Netze und Systeme

Energiemanagementsysteme und
zugehöriger Datenaustausch –
IT-Sicherheit für Daten und
Kommunikation

Kommunikationsnetze und
-systeme für die Automatisierung
in der elektrischen Energieversorgung

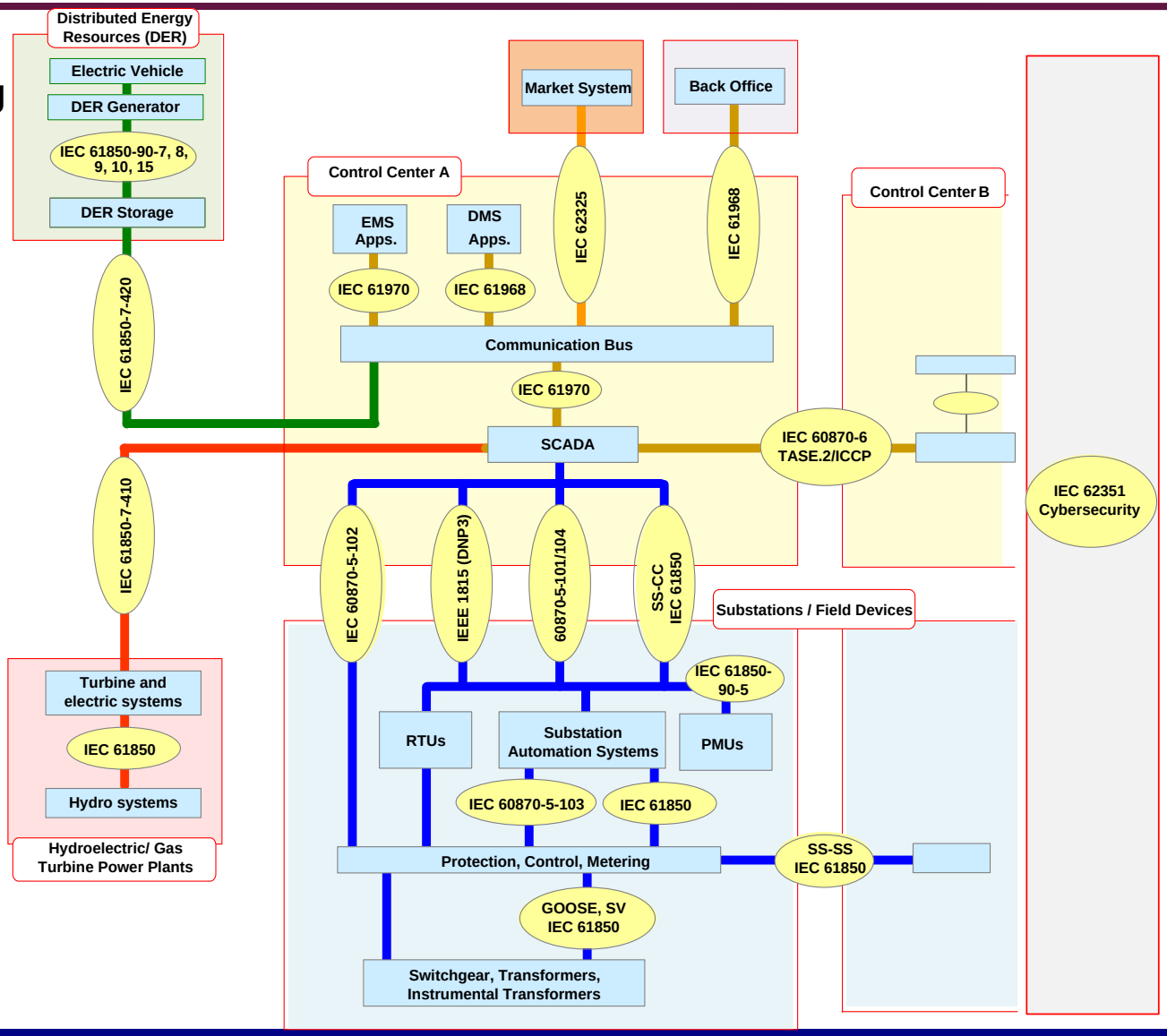


Übersicht über sicherheitsrelevante Standards and Guidelines in der Energieautomatisierung

IEEE 1686 – IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities	• High-level view on security requirements and measures, especially for Intelligent Electronic Devices in Power Systems.
ISO/IEC 27001/27002/27019	• Information and Security Management Systems (ISMS) in general (ISO/IEC 27001/27002) and domain-specific application for ISMS in power systems (ISO/IEC 27019)
NIST SP 800-82r2 Guide to Industrial Control Systems (ICS) Security	• Guideline for IACS security, Categorization of information systems, also see FIPS 199 or NIST SP 800-60. • Example security categorization for sensor data: (confidentiality: NA, integrity: high, availability: high).
NERC Critical Infrastructure Protection (CIP)	• Developed by the North American Electric Reliability Corporation, consists of several parts and defines security requirements that have to be met for systems that are part of critical infrastructures.
NISTIR 7628 Guidelines for Smart Grid Cyber Security	• Guideline for Smart Grid Cyber Security published by NIST. Contains detailed security considerations for different applications in the smart grid. Contains comprehensive considerations of security requirements and measures.
BDEW Whitepaper	• Published by the BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. Contains a comprehensive view on security requirements for communication and control in Smart Grids
IEC 62443 - Part 3-3: System security requirements and security levels	• Security Requirements for Industrial Automation and Control Systems (IACS). A classification scheme for different security levels and corresponding security measures.

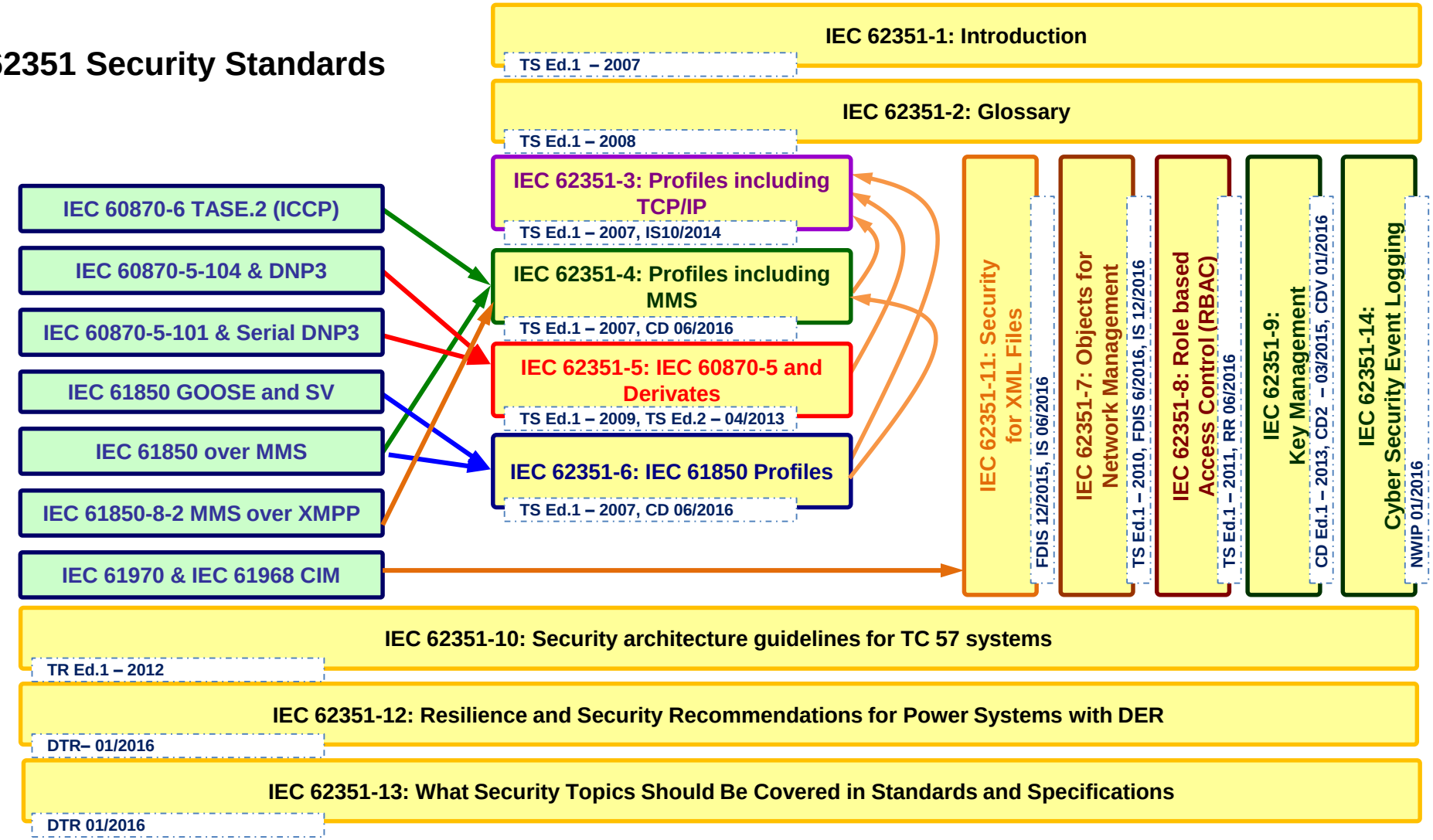
TC 57 Standards in der Energieversorgung

- **IEC 61970 / 61968**
  Common Information Model (CIM)
- **IEC 62325**
  Market Communication using CIM
- **IEC 61850**
  Substation & DER Automation
- **IEC 60870**
  Telecontrol Protocols
- **IEC 62351**
  Security for Smart Grid



Quelle: TC 57 WG 15

IEC 62351 Security Standards

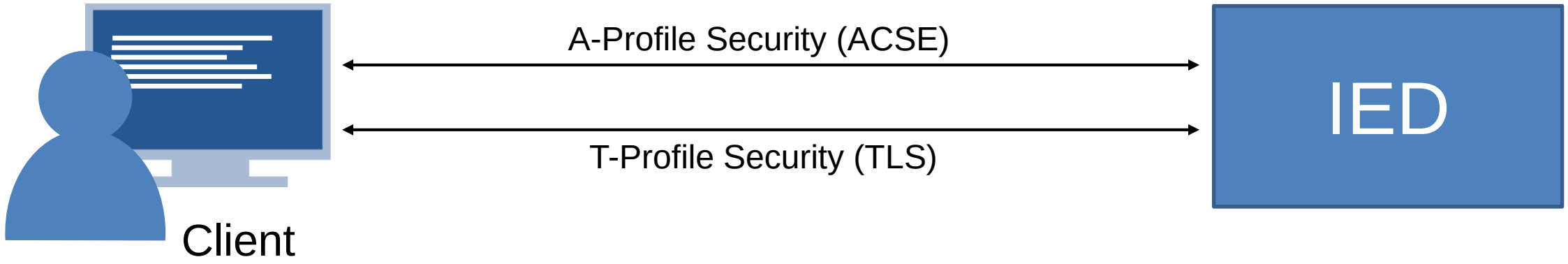


T-Profil

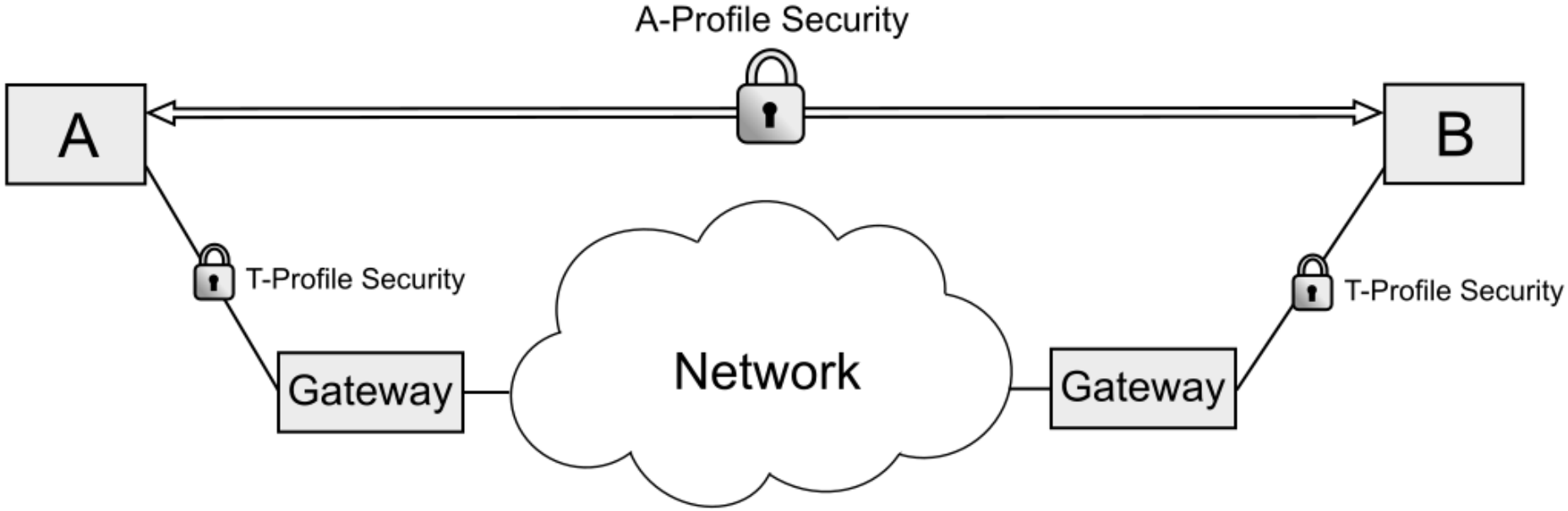
- Definiert in IEC 62351, Part 3: Profiles Including TCP/IP
- Verwendet TLS für Vertraulichkeit, Authentikation und Gewährleistung der Datenunversehrtheit

A-Profil

- Security für MMS-Protokoll (IEC 62351-4)
- Authentication beim Aufbau einer Association über ACSE (Association Control Service Element)
- Association Authentication Request/Reponse (AARQ/AARE)



Security: T-Profil verglichen mit A-Profil



T-Profil Security: schützt TCP-Verbindungen abschnittsweise (mit TLS)
Probleme: sequentielle TLS Verbindungen, unsicheres Netz hinter dem Gateway, unsichere Gateways

A-Profil Security: schützt die Association unabhängig vom T-Profil auf Anwendungsebene
Probleme: Authentisierung nur beim Setup, nicht der Daten

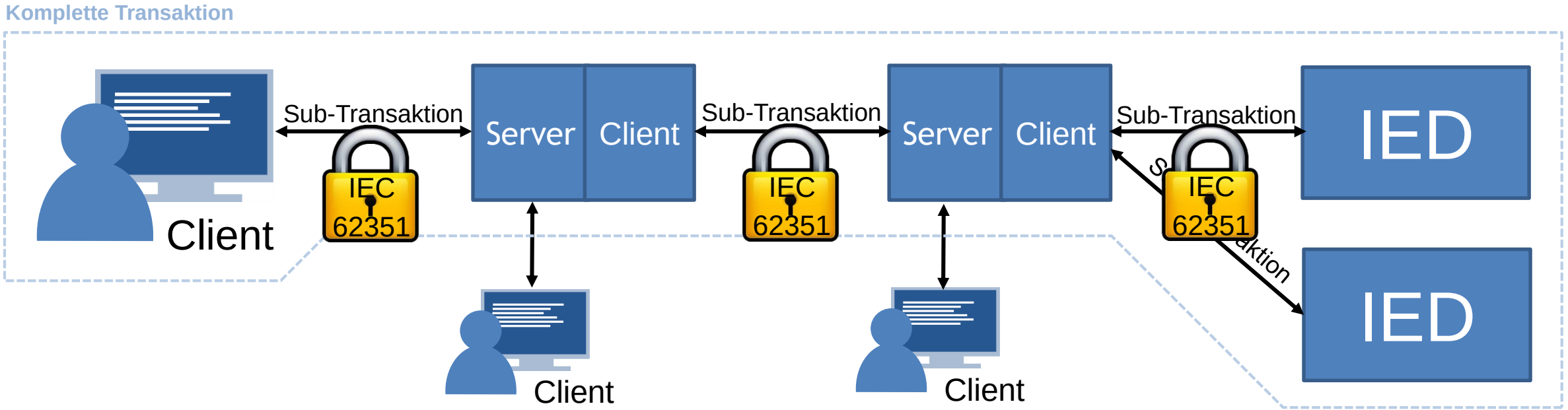
Stand der Technik – Erweitertes Szenario mit End-to-End Security

- IEC 62351-4: Verbesserte Sicherheit auf Anwendungsebene, geeignet für Einsatz über Gateways

- E2E-Protokoll, optional auch ohne TLS, da Verschlüsselung und Gewährleistung der Datenunversehrtheit „wirklich“ end-to-end

Neues Szenario - Transaktionsketten

Authentication, Non-Repudiation, Traceability?

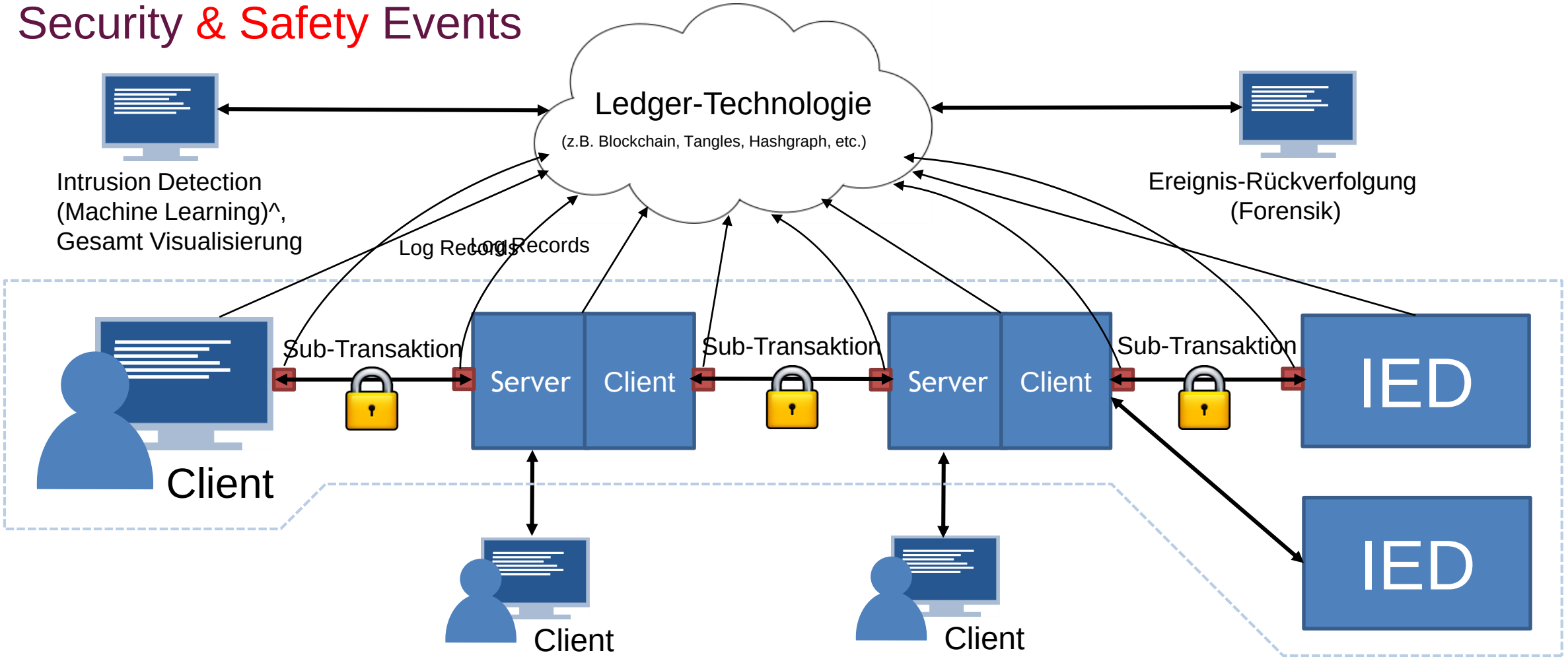


Offene Anforderungen - IEC 62443

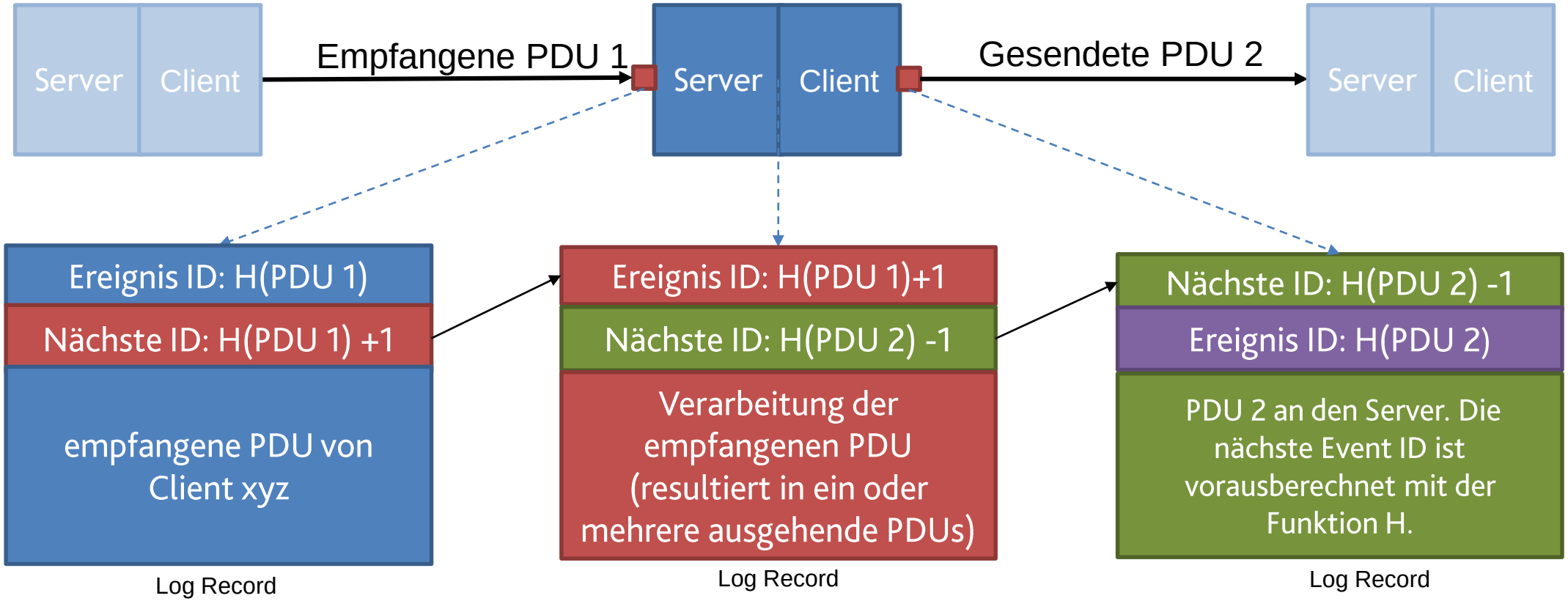
- Non-Repudiation (Nachweisbarkeit) auf Anwendungsebene
- Doppelte Zustimmung bei kritischen Operationen
- Logging und Monitoring

- Lösungsansatz
  - Erweiterung der IEC 62351-4 (End-to-End Security Protocol)
  - XML-Security für XER-kodierte Datenpakete (XMPP, IEC 61850-8-2)
  - Mehrfache digitale Signaturen

Logging und Monitoring von Security & Safety Events

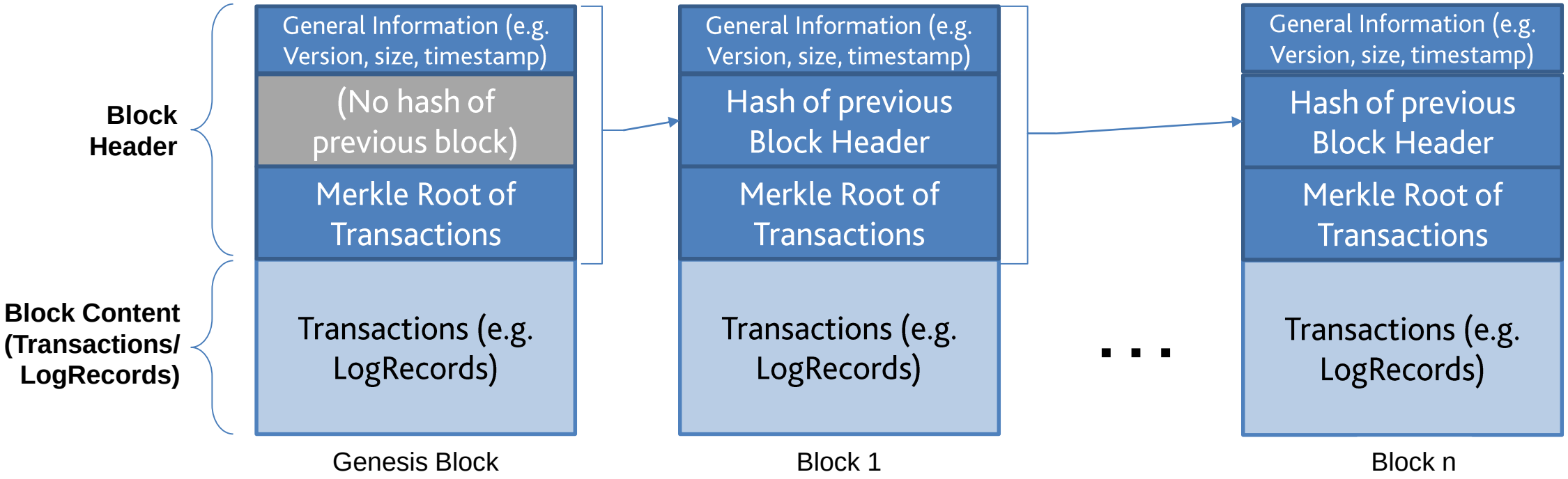


Kette von Teil-Transaktionen

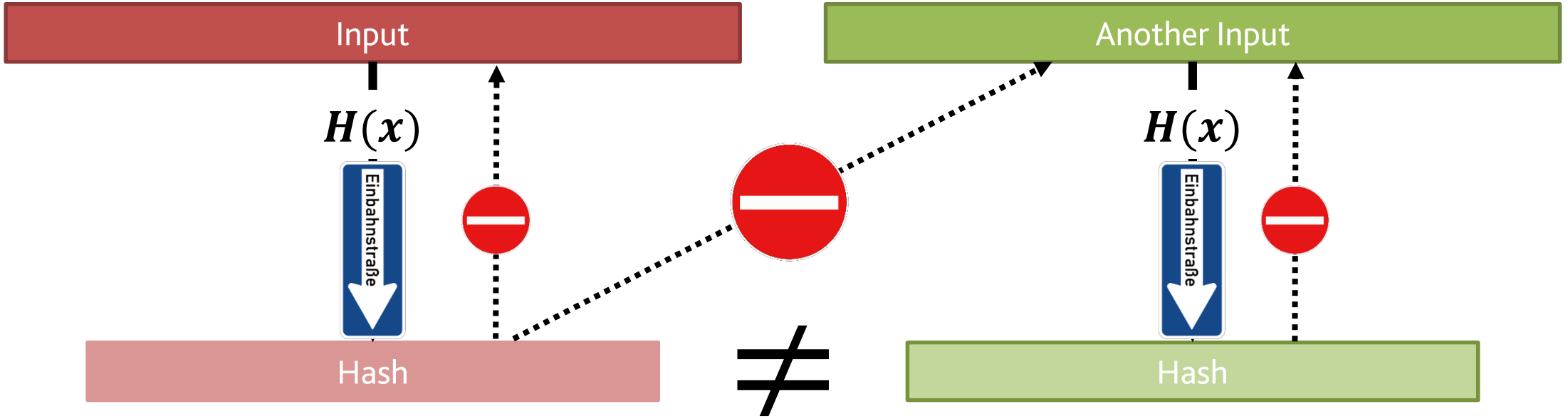


- H ist eine Funktion, die eine eindeutige Ereignis ID berechnet, abhängig von der nächsten PDU

Distributed Ledger Technologies - Blockchain



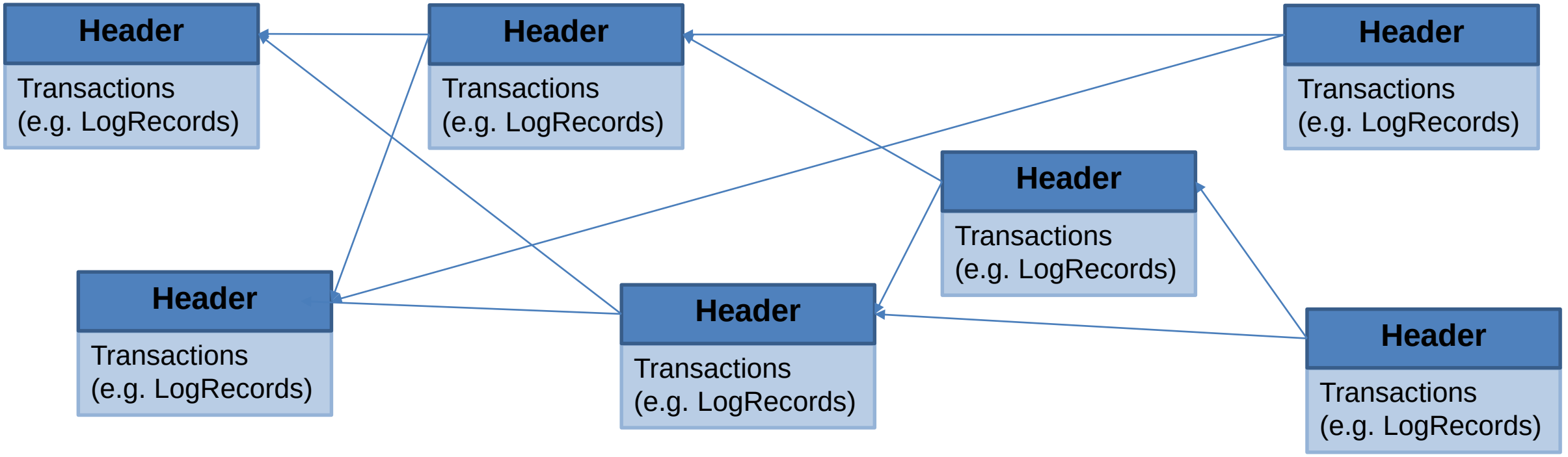
Hash Funktionen



Eine Hash Funktion bildet einen Input variabler Länge auf einen Output fester Länge ab, z.B. 256 Bits

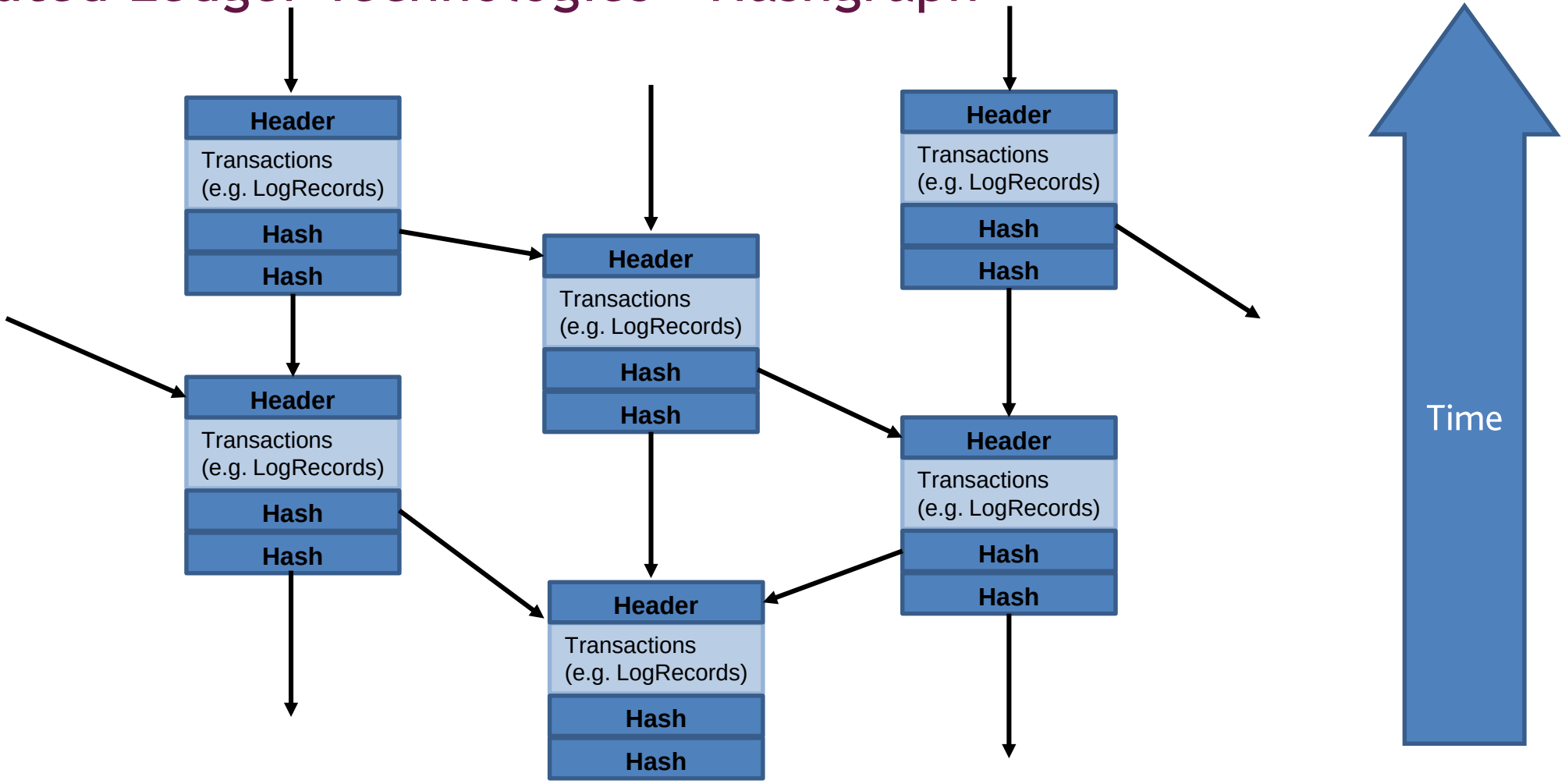
- Kryptographische Hashfunktionen sind Einweg-Funktionen, bei denen zu einem gegebenen Output kein passender Input gefunden werden kann
- Es gibt keine Möglichkeit, einen zweiten Input zu finden, wenn ein Input mit Output bekannt sind
- Es gibt keine Möglichkeit, ein Pärchen von Inputs zu finden, die denselben Output ergeben

Distributed Ledger Technologies – Tangles

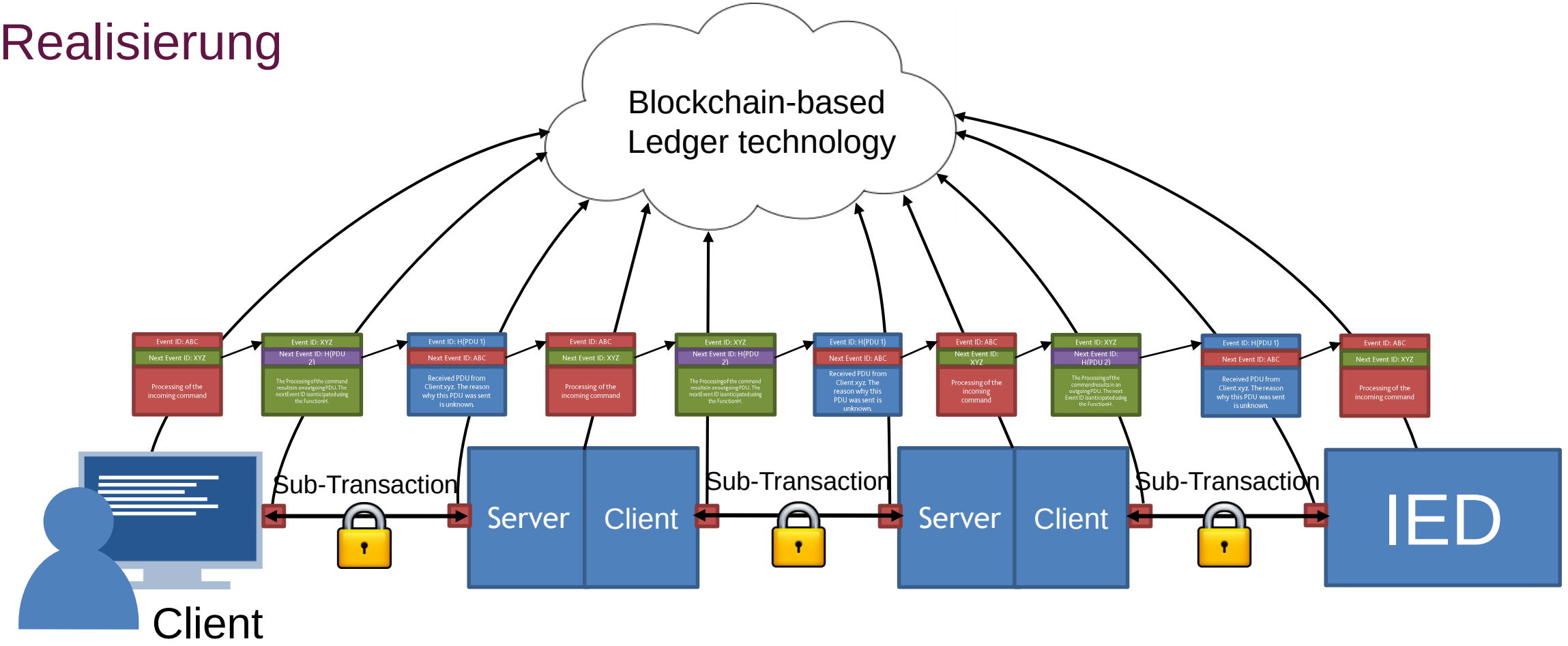


Jede Transaktion zeigt auf zwei vorhergehende Transaktionen (parents), die überprüft wurden (child).

Distributed Ledger Technologies – Hashgraph

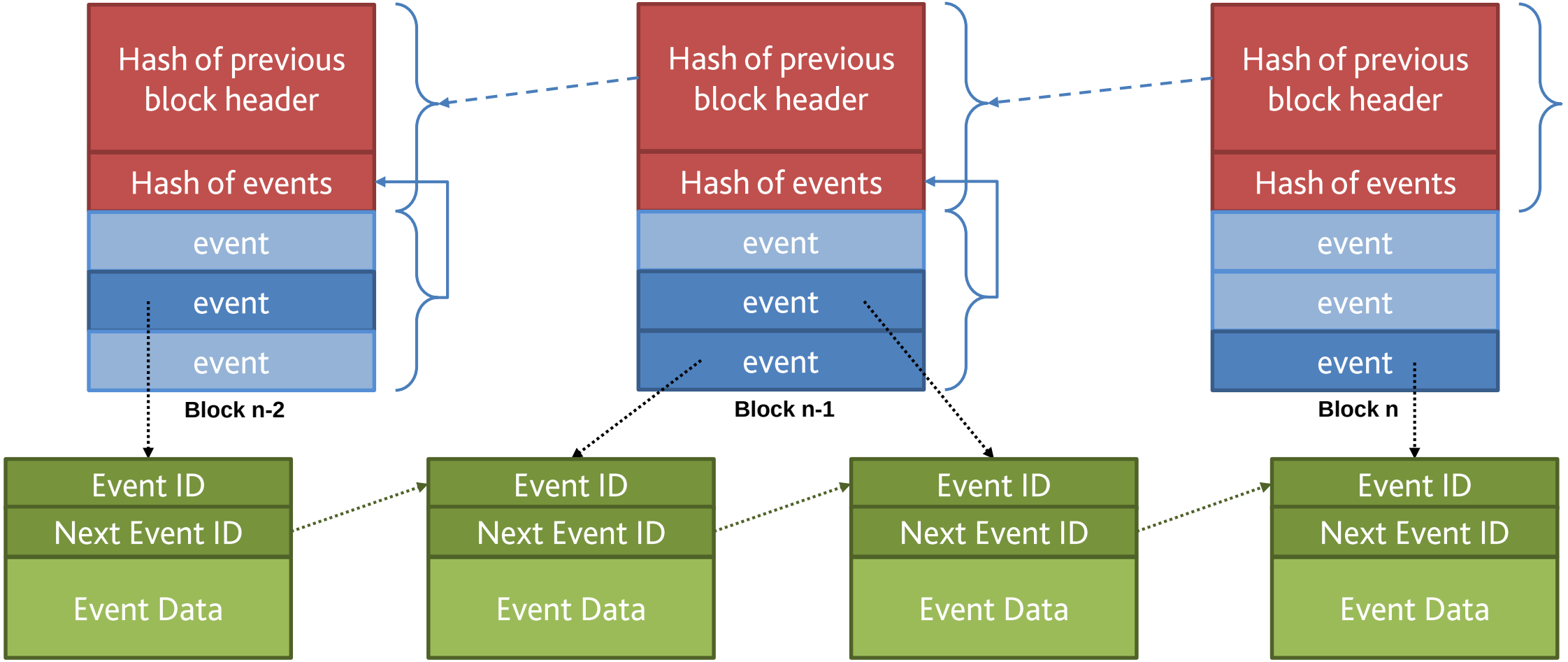


Realisierung

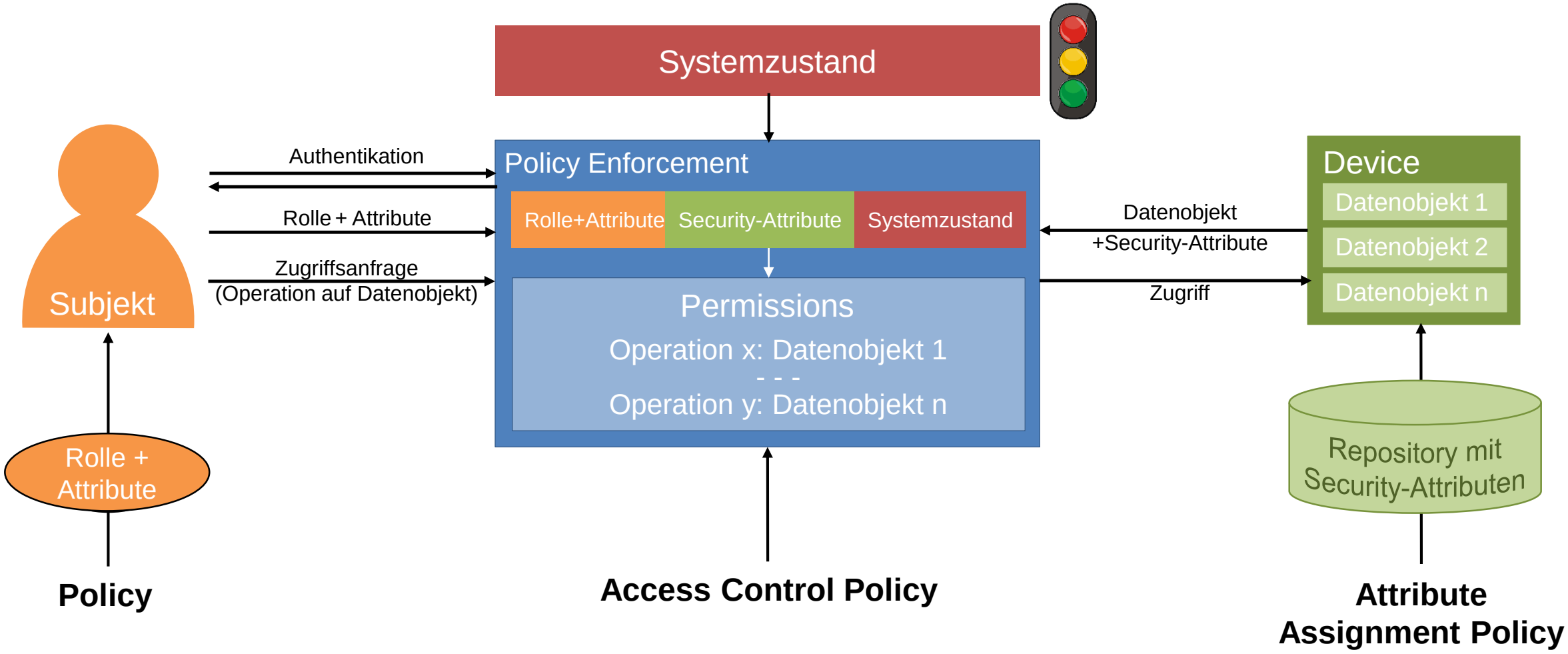


Jedes Log Record wird digital signiert, bevor es in die zentrale Blockchain eingefügt wird

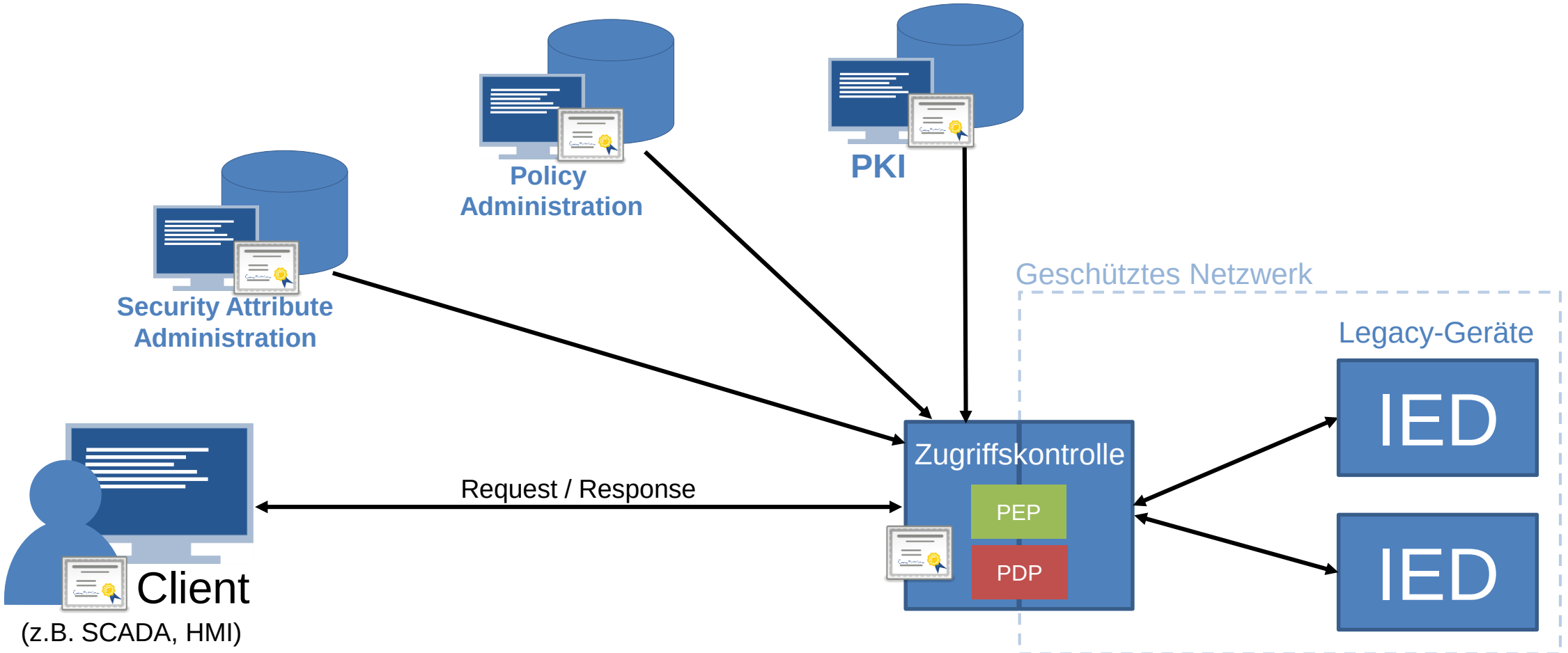
Speicherung der Ereignisse in der Blockchain



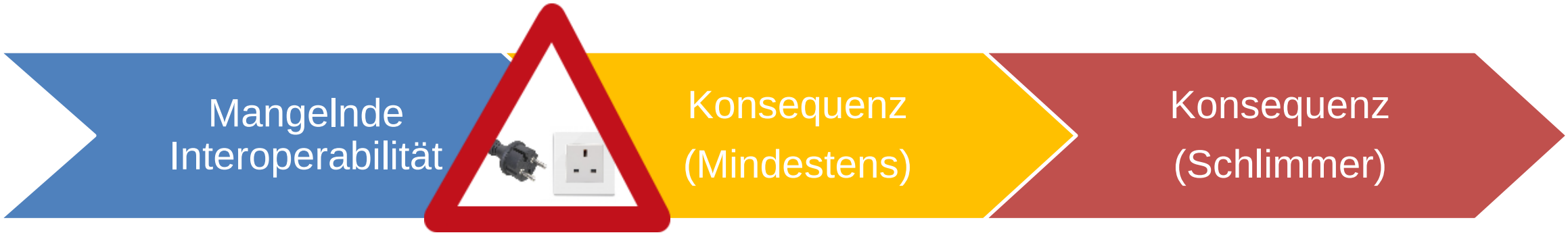
Zugriffskontrolle: Rollenbasiert zu Attributbasiert



Voraussetzung: Sicherheitsinfrastruktur



Sicherheitsanforderung: Interoperabilität



- (Sicherheits-) Protokolle sind meist nur in Textform und nicht vollständig spezifiziert

- Im Fehlerfall: Undefinierte Dauer bis zum erfolgreichen Wiederaufbau einer Verbindung/Association
- Realzeitverhalten wird verletzt

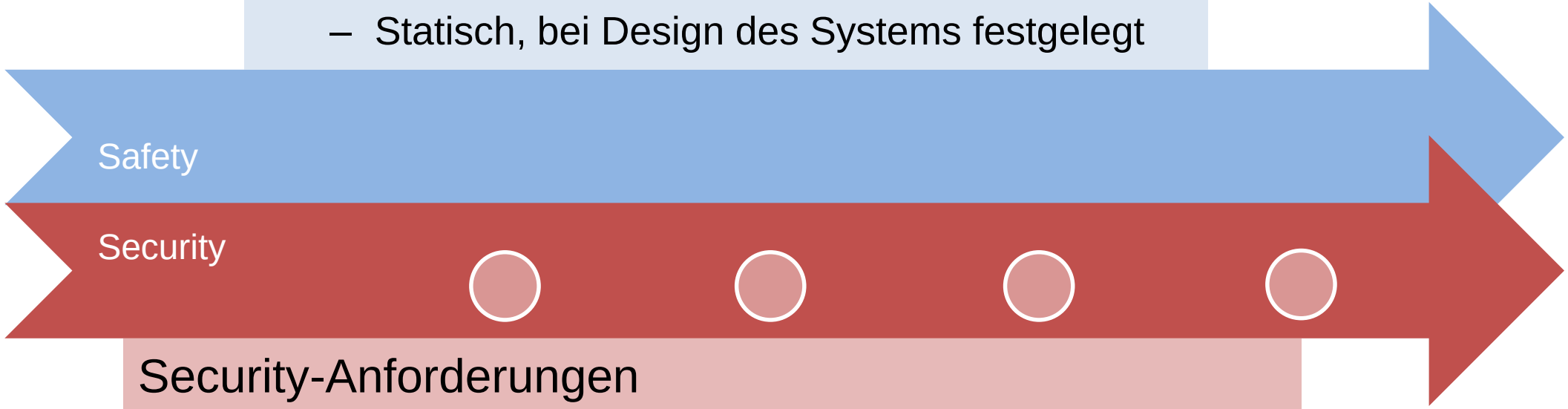
- Fehlersituation kann nur durch Eingriff von außen geklärt werden
- Beeinträchtigung der funktionalen Sicherheit
- MangeInde Interoperabilität kann für Angriffe genutzt werden

Sicherheitsanforderung: Flexibilität der IACS-Security

Safety-Anforderungen

- Statisch, bei Design des Systems festgelegt

Lange Lebensdauer der eingesetzten Geräte (>10 Jahre)



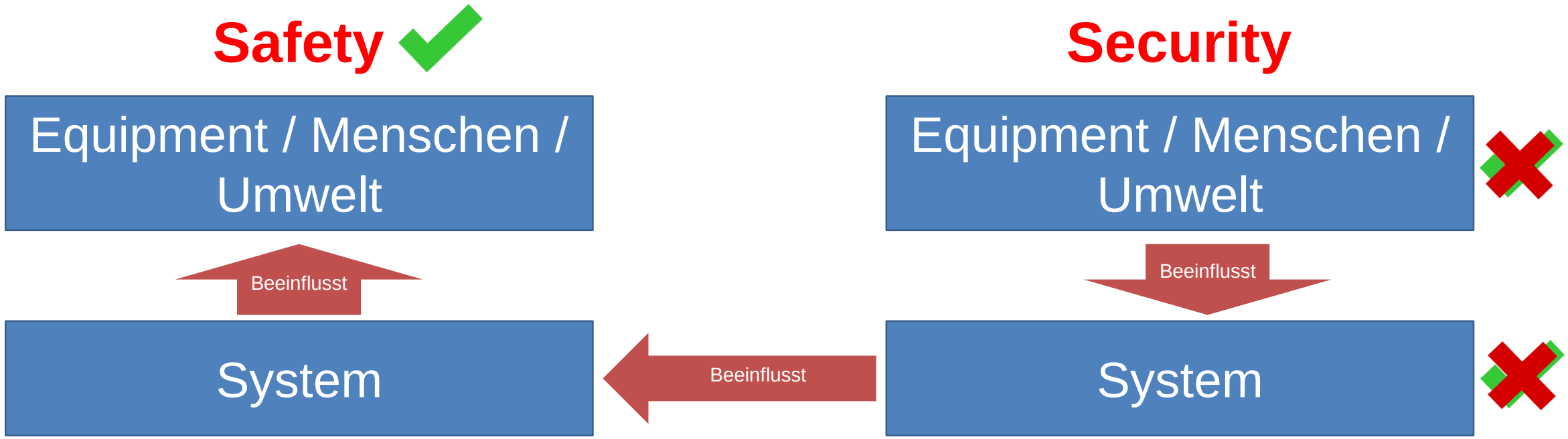
Security-Anforderungen

- Werden beim Design des Systems als bekannt angenommen
- Neue Angriffsmöglichkeiten während des Betriebs

→ Flexibilität und Erweiterbarkeit

+ Größeres Gewicht auf sicherer Hardware / Security Module
+ Security by Design

Gewährleistung der Funktionalen Sicherheit



- "There is no Safety without Security"
  - Aber: Gewährleistung der Safety auch bei Ausfall der Security-Mechanismen
  - Safety darf nicht durch Blockierung des Security Systems beeinträchtigt werden

Zusammenfassung

Industrial Security in der Energieversorgung

- **Konzentriert sich auf**
  - Anwendungsprotokolle (IEC 61850), Dateninhalte und ihre Bedeutung

Benötigt

- Nachweisbarkeit und Rückverfolgbarkeit von komplexen Transaktionen
- Rollenbasierte und datenobjekt-basierte Zugriffskontrolle, auch gegen Insiderattacken
- Geeignete Sicherheits-Infrastruktur
- Sichere, flexible, interoperable und robuste Implementationen
- Konfliktfreies Zusammenspiel von OT-Sicherheit und funktionaler Sicherheit
- Forschung, Entwicklung, Standardisierung und Zulassungsregelungen


Bundesministerium
für Wirtschaft
und Technologie
EENERGY
Smart Grids
made in Germany
www.e-energy.de