



**RELAX,  
WE CARE**

**SICHERUNG VON OT-UMGEBUNGEN:  
EFFEKTIVE UMSETZUNG VON NETWORK ACCESS  
CONTROL (NAC)**

25.02.2025 | Kapfenberg

# NETWORK ACCESS CONTROL



- Kontrolliert Netzwerk Zugriff im LAN und WLAN
- Authentisiert oder klassifiziert Endpoints
- Abgestufter Zugriff anhand zusätzlicher sicherheitsrelevanter Kriterien möglich
- Im IT Bereich weitgehend etabliert, im OT Bereich noch kaum vorhanden
- Bestehende (Teil-)Lösungen für OT ungeeignet

# OT UMGEBUNG

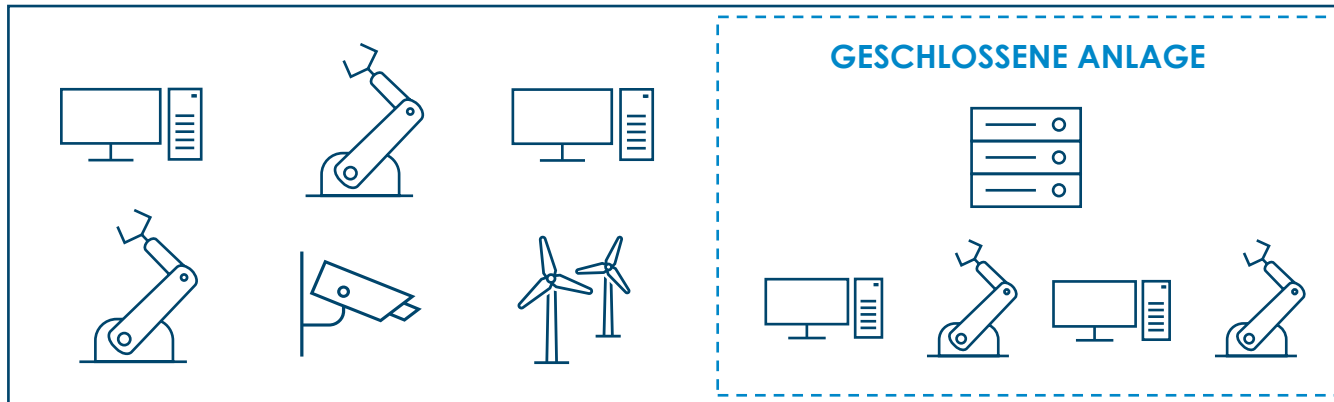
Oft unsegmentiert

Oft keine direkte Kontrolle über Geräte

Viele verschiedene Hersteller

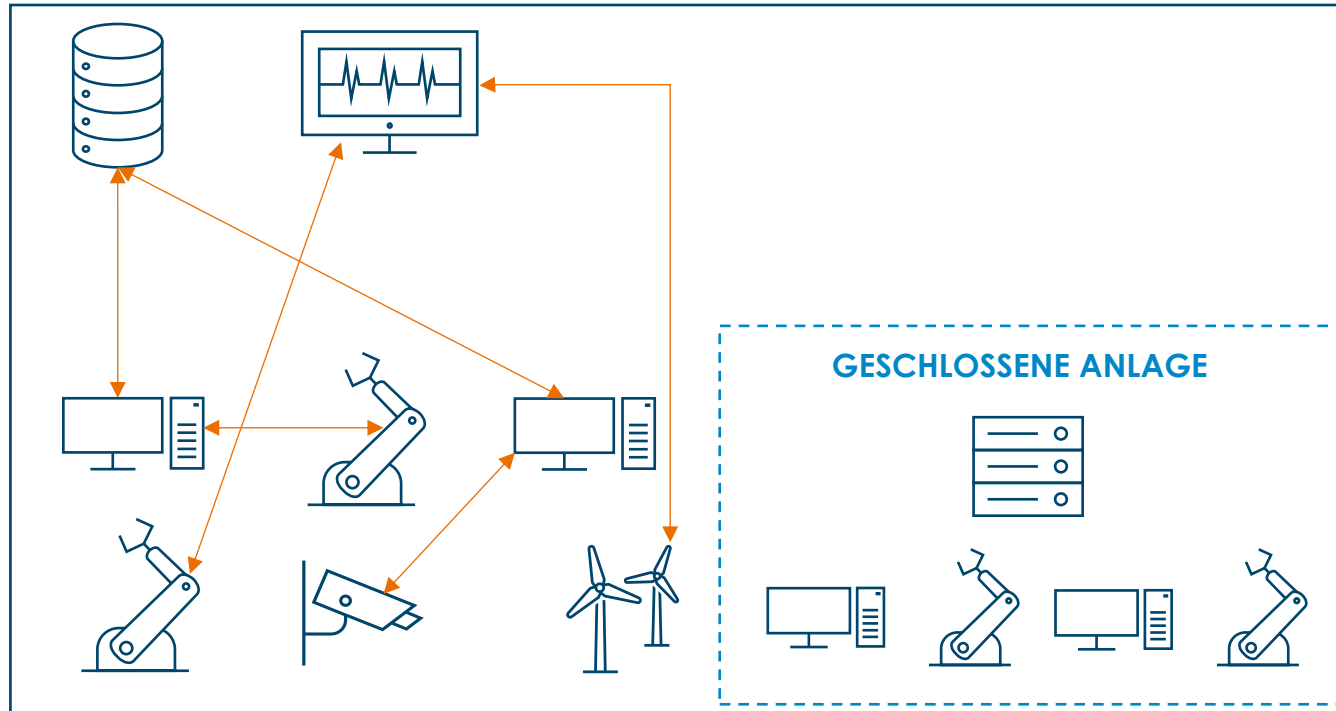
Lange Lebensdauer der Geräte

## UNSEGMENTIERTES NETZWERK



# LEGACY OT UMGEBUNG

Air Gapped / Kein Internet Zugriff

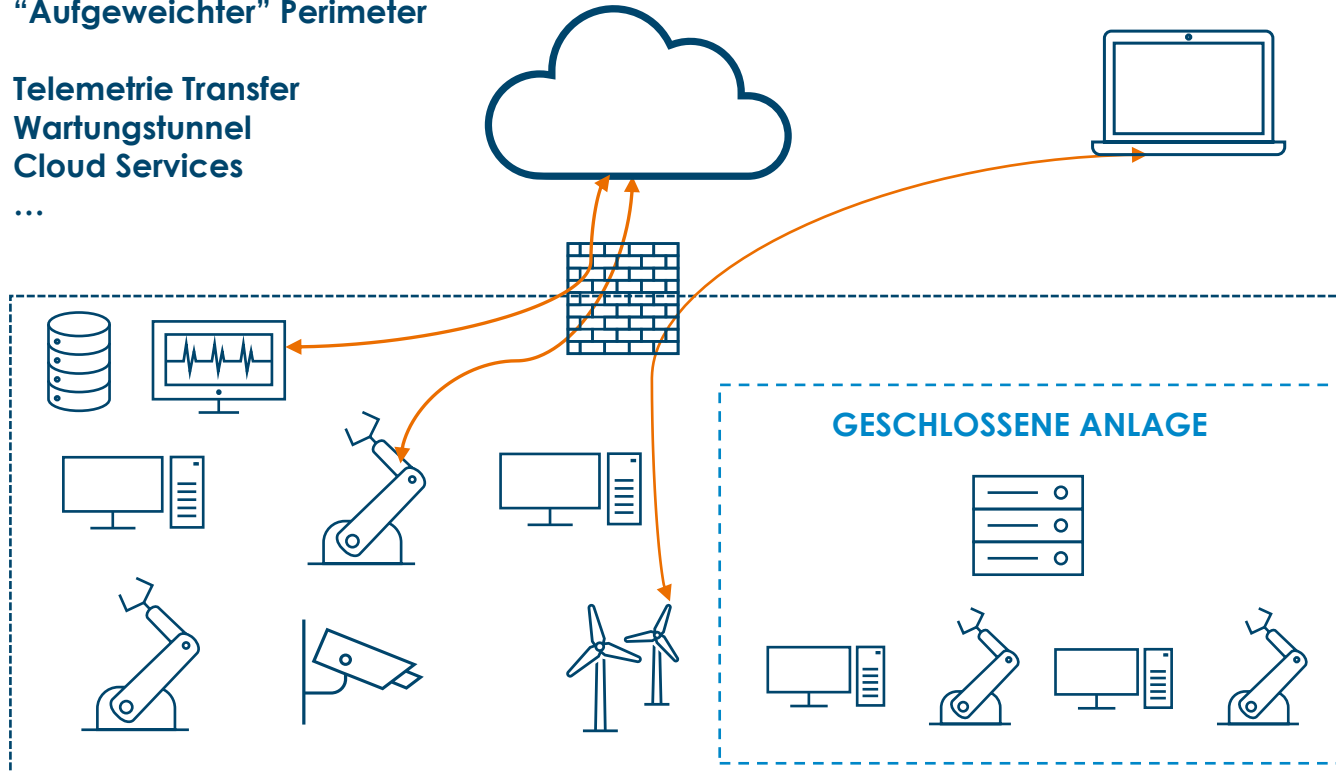


# MODERNE OT UMGEBUNG

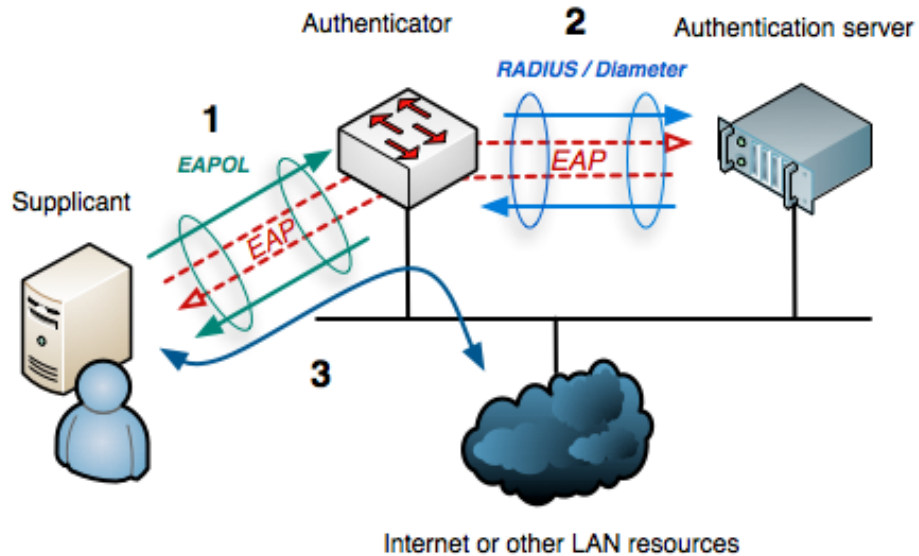
“Aufgeweichter” Perimeter

Telemetrie Transfer  
Wartungstunnel  
Cloud Services

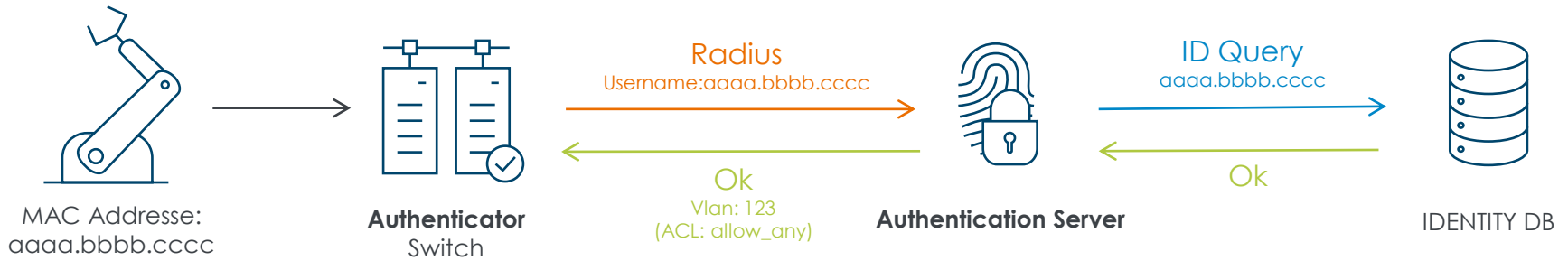
...



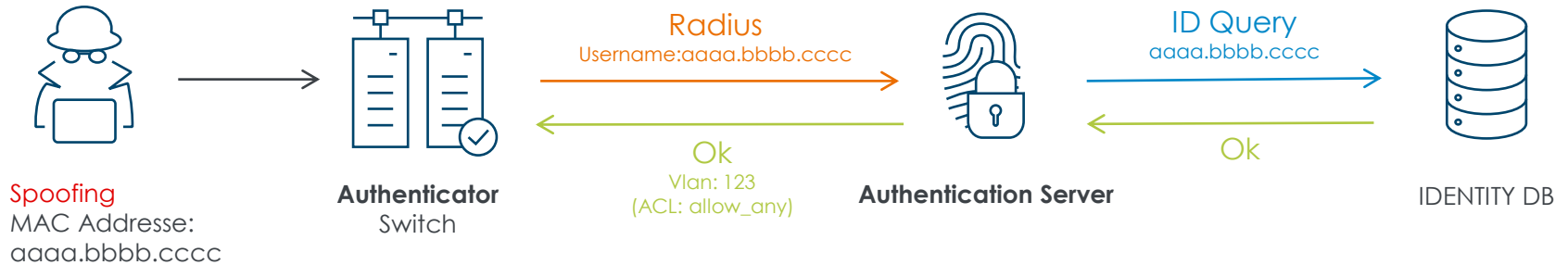
# 802.1X / EAPOL AUTHENTICATION



# MAB (MAC AUTHENTICATION BYPASS)

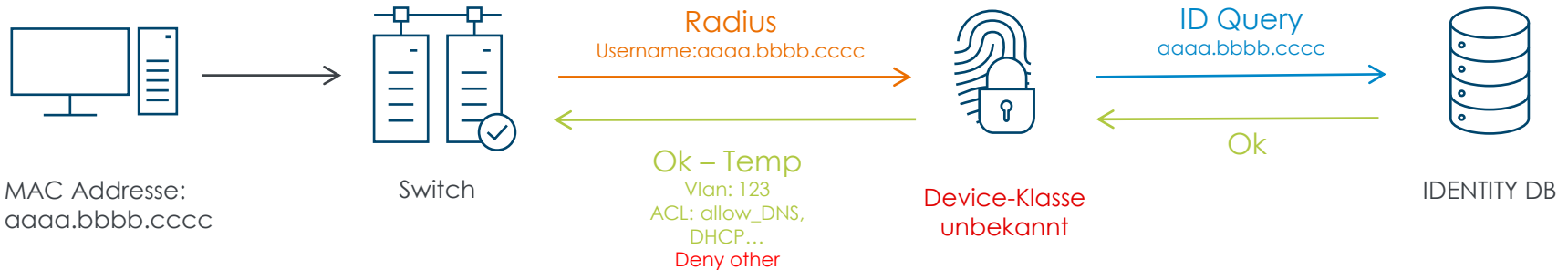


# MAB (MAC AUTHENTICATION BYPASS)

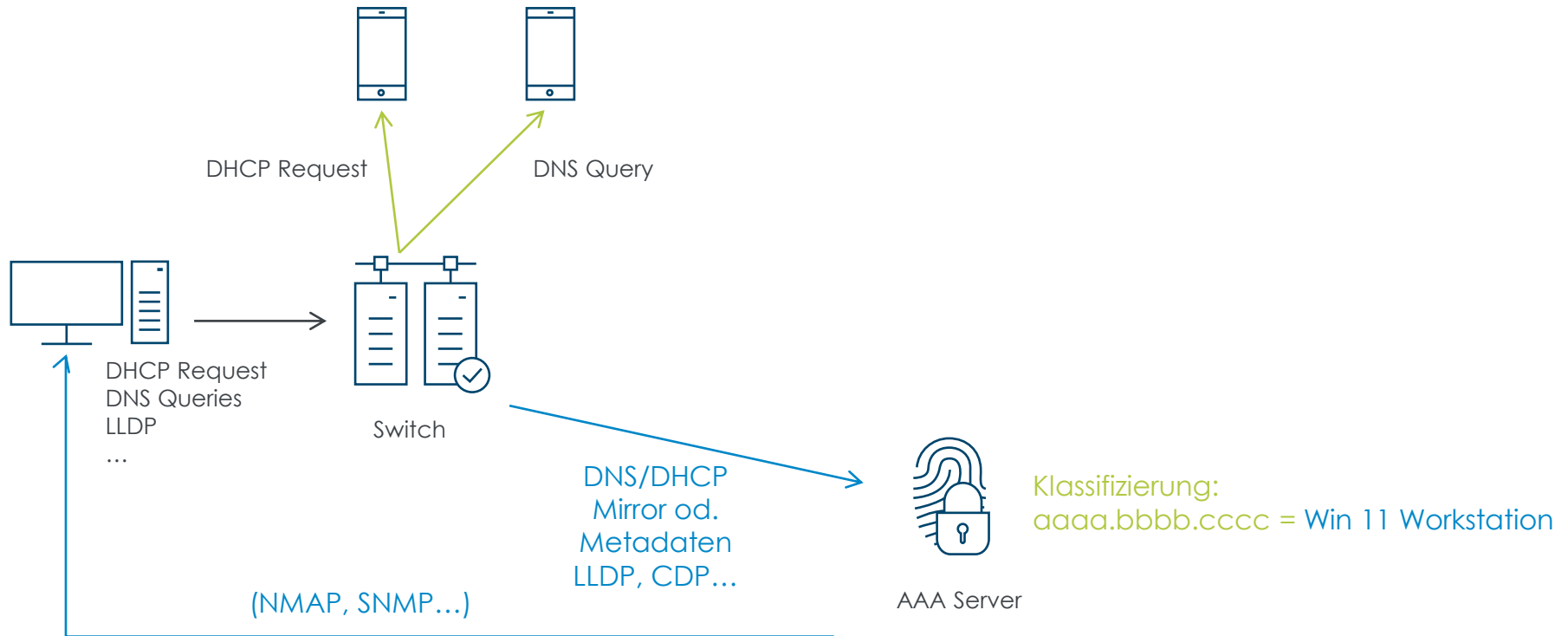




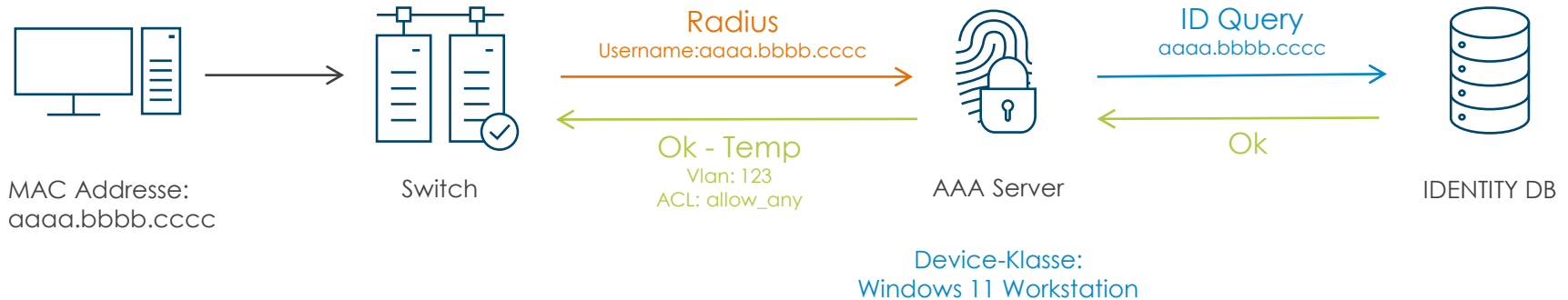
# ZUSÄTZLICHE STUFE: PROFILING - 1



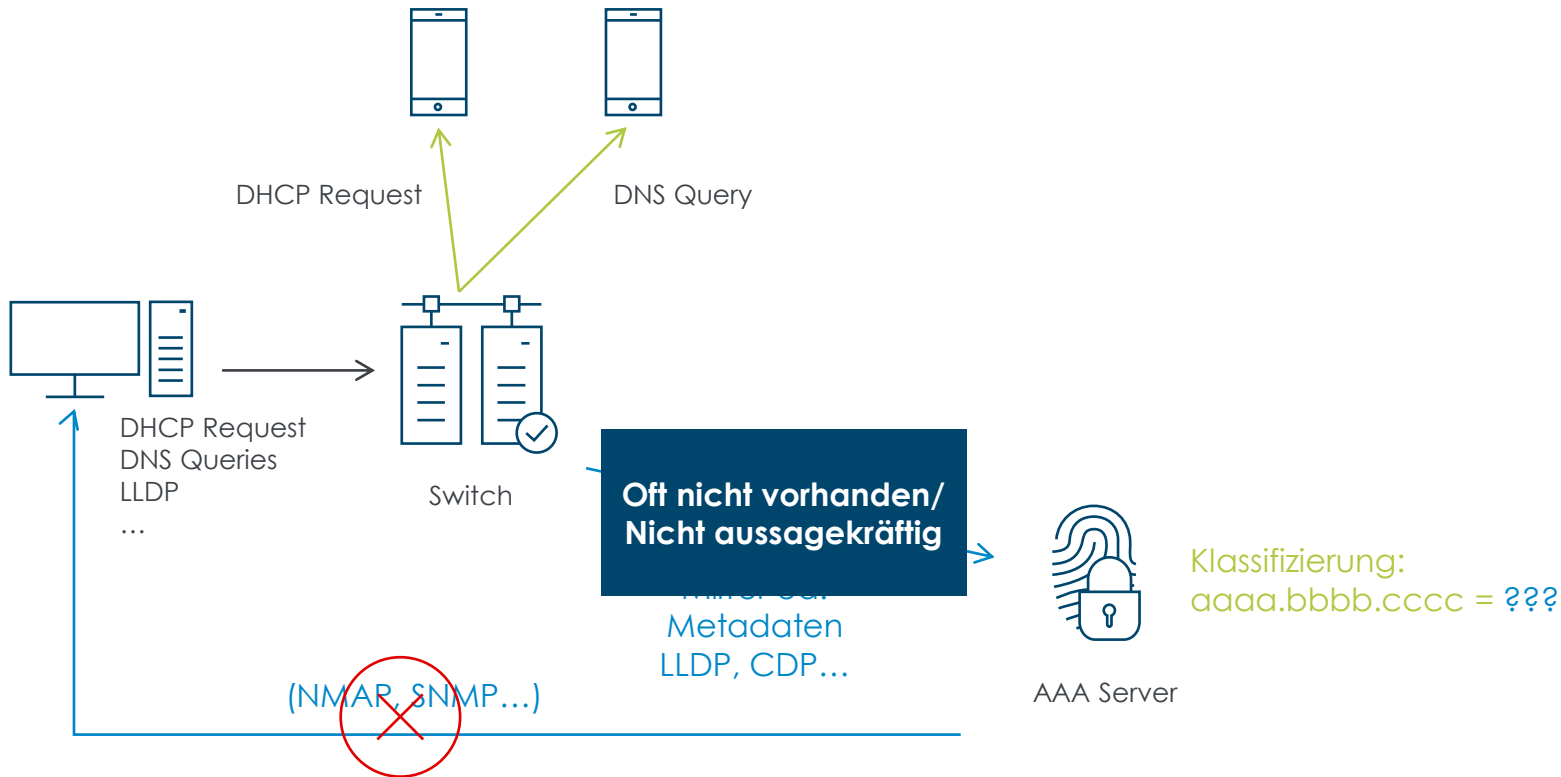
# ZUSÄTZLICHE STUFE: PROFILING - 2



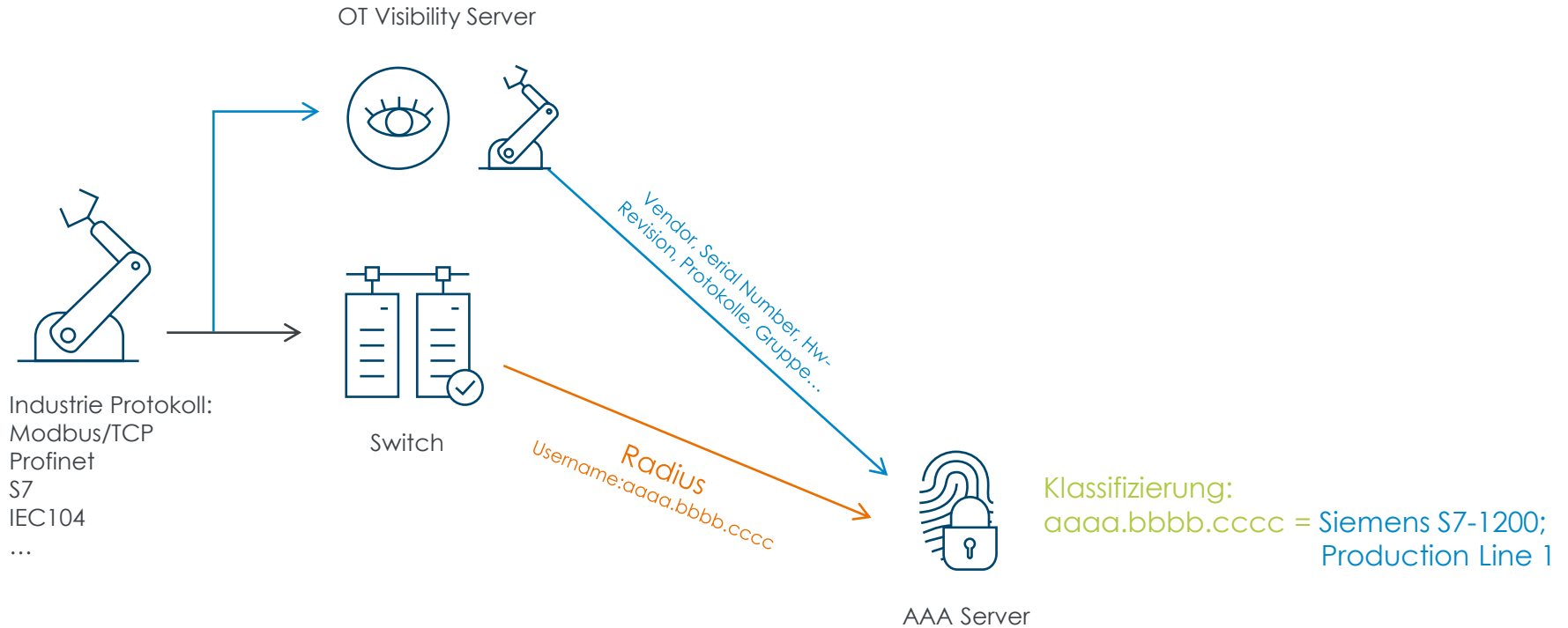
# ZUSÄTZLICHE STUFE: PROFILING - 3



# PROFILING IN OT UMGEBUNGEN



# PROFILING IN OT UMGEBUNGEN



# MAB + OT KONTEXT

OT Visibility Solution liefert spezifischen Kontext.

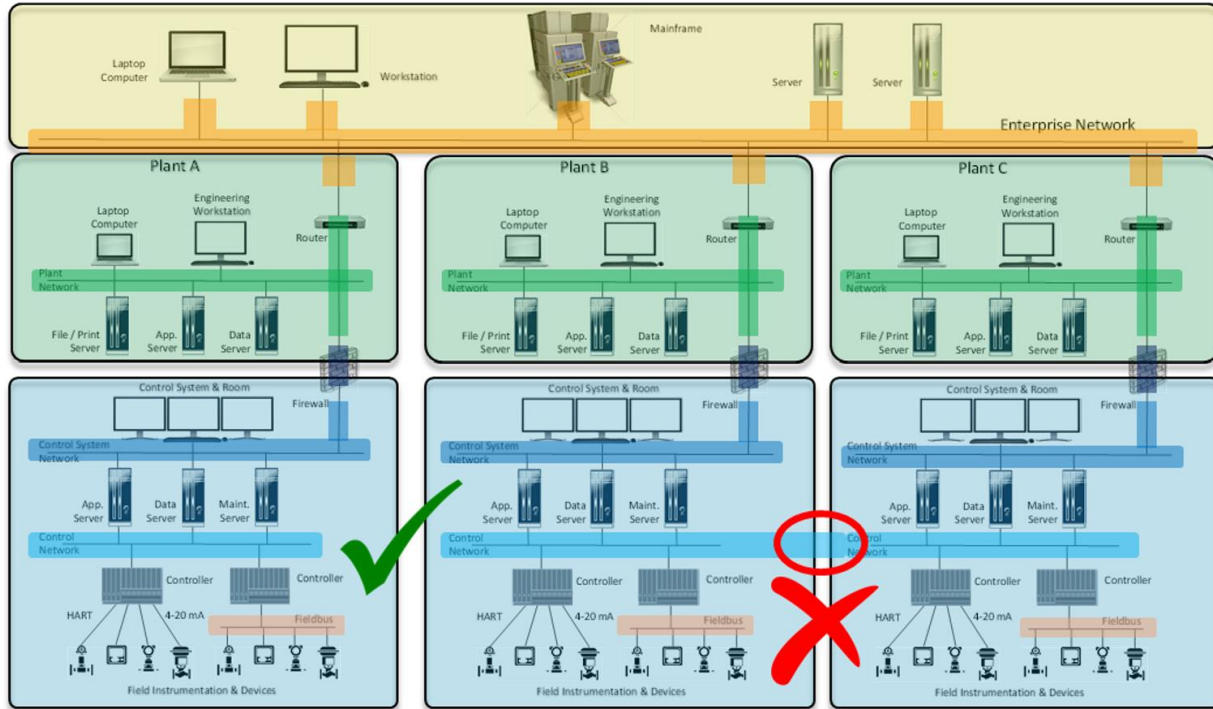
z.B. Device-Typ, Modell, Seriennummer, Firmware Version

Nutzung dieser Attribute in der NAC Policy

Keine echte Authentication mit Username/Pw oder Zertifikat.

Einfaches MAC Spoofing nicht mehr ausreichend, Verhalten muss ebenfalls gespoofed werden -> Benötigt tieferes Know-How, ABER nicht unmöglich.

# ISA99 / IEC62443 ZONIERUNG



# ISA99 / IEC62443 ZONIERUNG

OT Engineer gruppiert Geräte auf dem OT Visibility Server nach Zonen

Attribute werden zum Authentication Server übertragen

Authentication Server steuert Netzwerkzugriff

OT Engineer benötigt keinen Zugriff und Know-How für Authentication Server

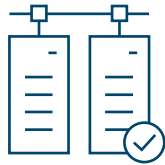
Vereinfacht Klassifizierung, Wartungszugang und Geräte-Tausch



# CISCO LÖSUNGEN

**OT Visibility Server**  
Cyber Vision

In-line Sensoren



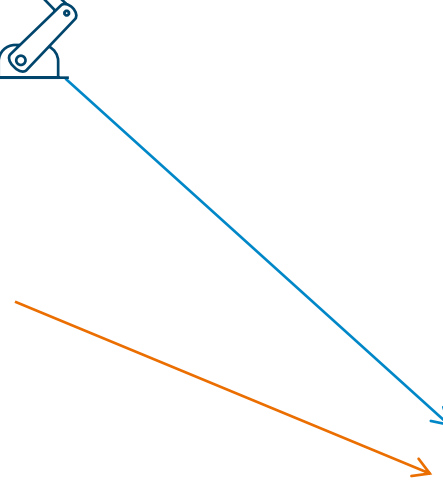
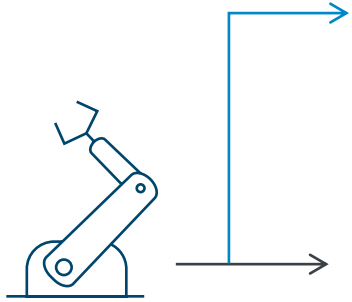
**Switch**  
Catalyst  
IE Switches

CV Sensor  
on board



**AAA Server**  
ISE - Identity Services Engine

pxgrid



The logo consists of the letters 'NTS' in a bold, white, sans-serif font, centered within a white square with rounded corners. The 'N' and 'T' are connected at the top, and the 'S' is positioned to the right of the 'T'.

**NTS**

**RELAX,  
WE CARE**