GREYCORTEX

Solving the Everyday Challenges
of Your Network Security Team!

Proč útočníci vidí vaše ICS dřív než vy:
viditelnost jako základ ochrany kritické infrastruktur

Jiří Marek

GREYCORTEX MENDEL

Visibility

All the network communication, devices with inventory details, and user behavior

Detection

From misconfigurations, performance problems, or policy violations to undetected malware, ransomware, and hacker activities which are able to bypass existing security tools

Response

Rapid attack response, and incident investigation and management

+

SCADA/ICS Monitoring

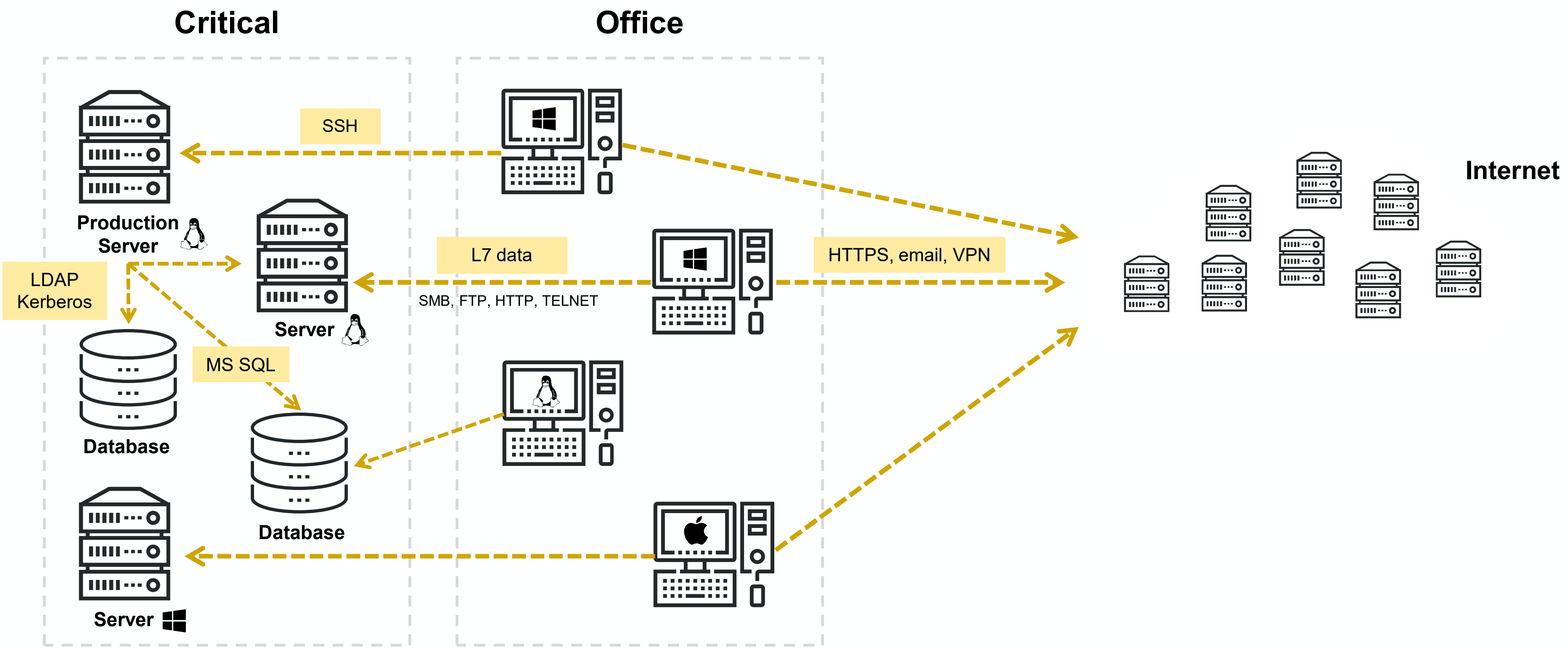
Application Performance Monitoring

Asset Inventory (2021)

Network Detection and Response

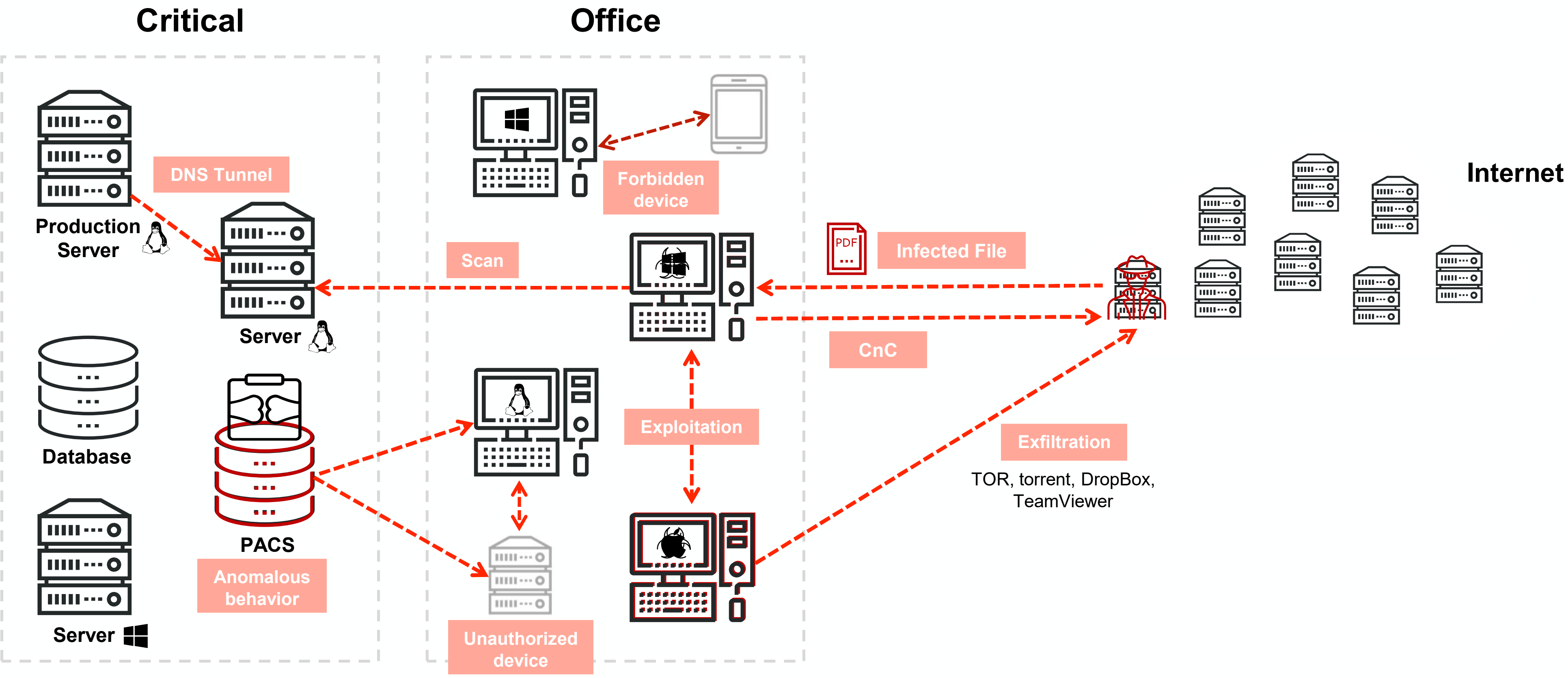
GREYCORTEX

Visibility

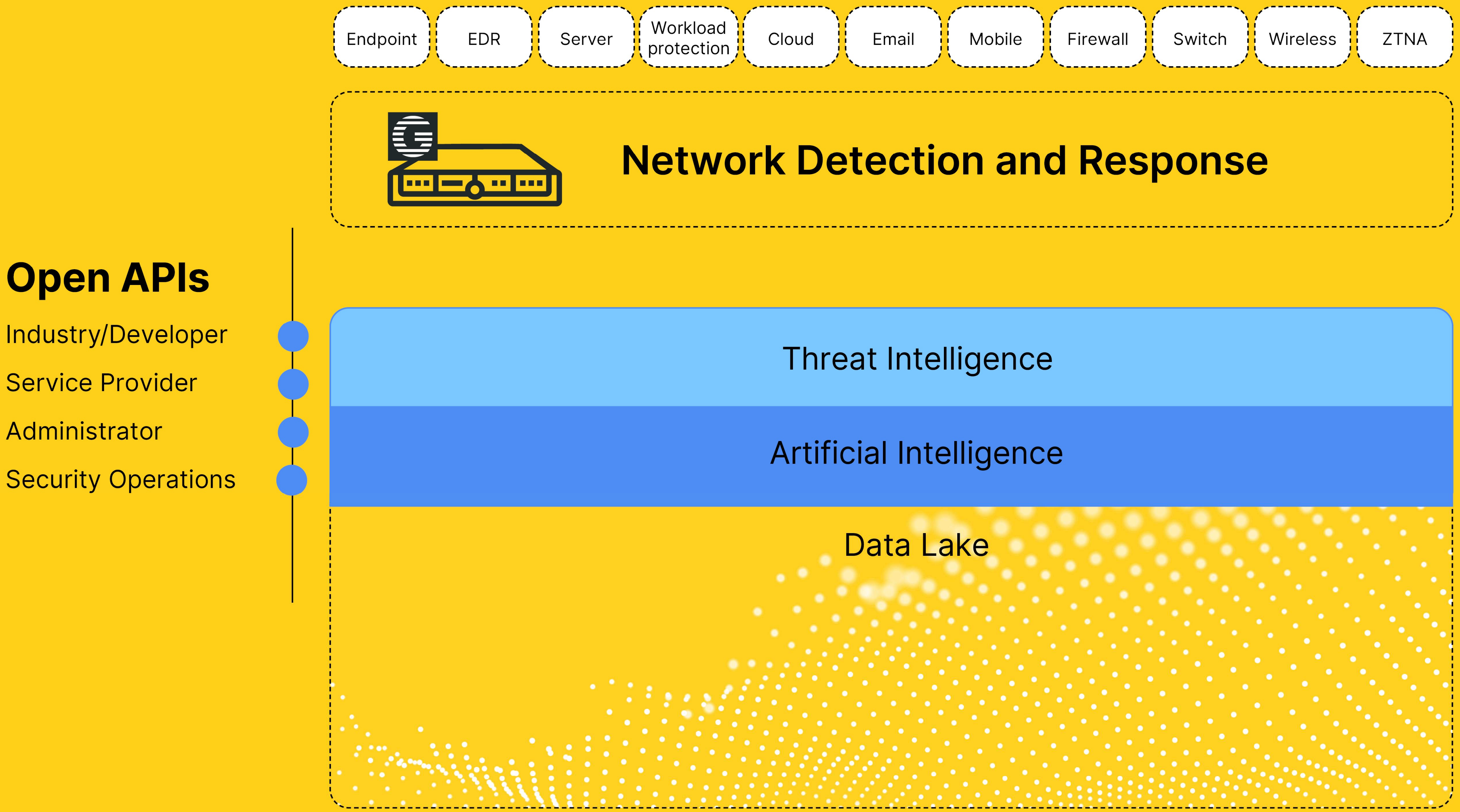


GREYCORTEX

Detection



GREYCORTEX



Endpoint

EDR

Server

Workload protection

Cloud

Email

Mobile

Firewall

Switch

Wireless

ZTNA

Network Detection and Response

Open APIs

Industry/Developer

Service Provider

Administrator

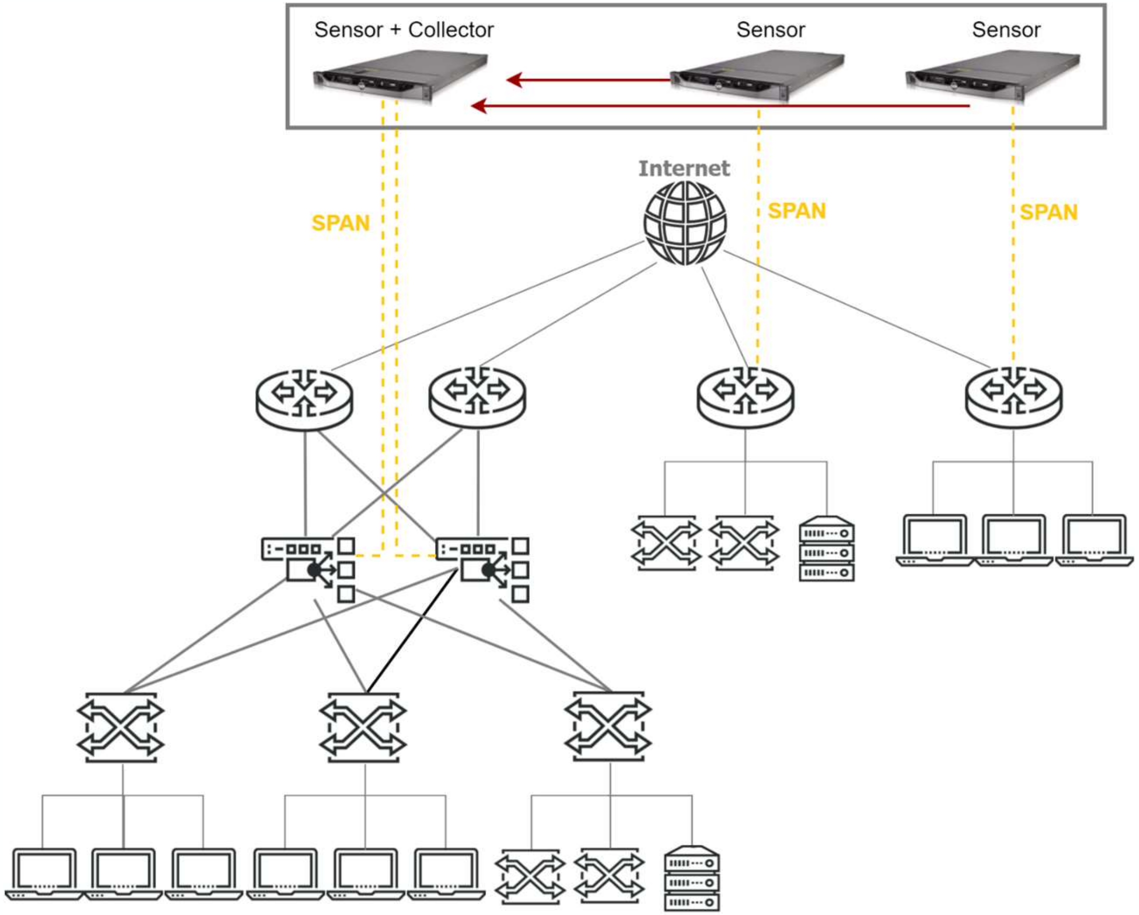
Security Operations

Threat Intelligence

Artificial Intelligence

Data Lake

Deployment



Sensors

- Port Mirroring (SPAN, RSPAN, ERSPAN)/TAP
- ASNM output (= 0,5% - 2% of traffic)
- Up to 100Gbps/sensor

Collectors

- 1 collector = 50+ sensors
- Aggregated input up to 100Gbps+
- Central collector for Events visualization

Devices

- Hardware
- Virtual (VMware ESXi, Hyper-V, KVM, …)
- Cloud (AWS, Azure, GCP)

ICS/SCADA

www.greycortex.com

Kde můžeme pomoci

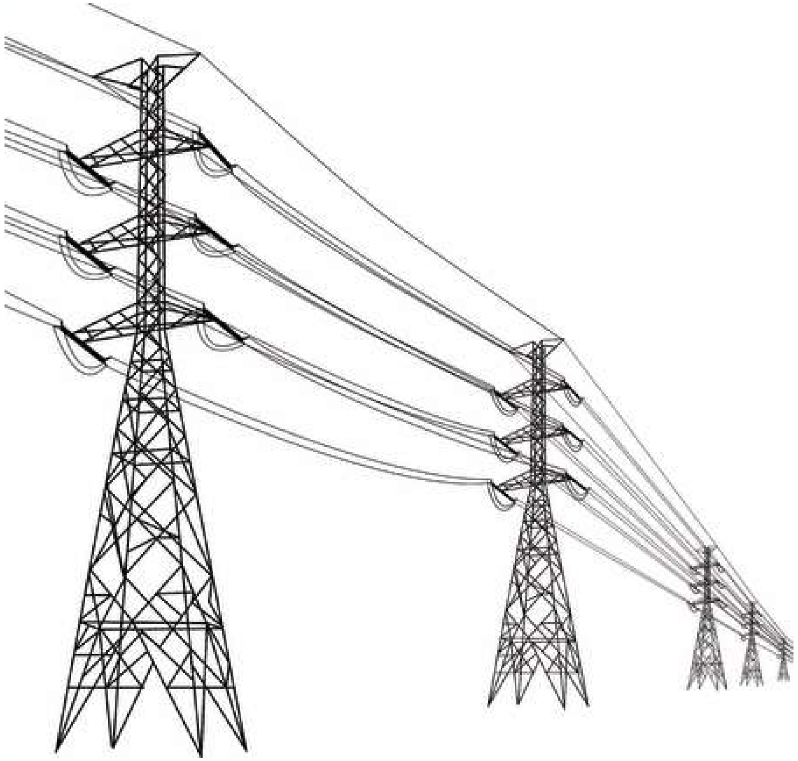
Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

VÝROBA A DISTRIBUCE ENERGIÍ

PRŮMYSLOVÁ VÝROBA

KRITICKÁ INFRASTRUKTURA

SPRÁVA BUDOV



Zpracovávané OT protokoly

- BACnet
- CoAP
- DLMS/COSEM
- DNP3
- ENIP
- EtherCAT
- GE SRTP
- HART-IP
- IEC 60870-5-104 (IEC-104)
- IEC 61850 GOOSE

- IEC 61850 MMS
- IEC 61850 SV
- Modbus
- MQTT
- OPC Parser
- Profinet
- Profinet IO DCE/RPC
- Siemens S7
- CC-Link
- Mitsubishi

Možné typy útoků

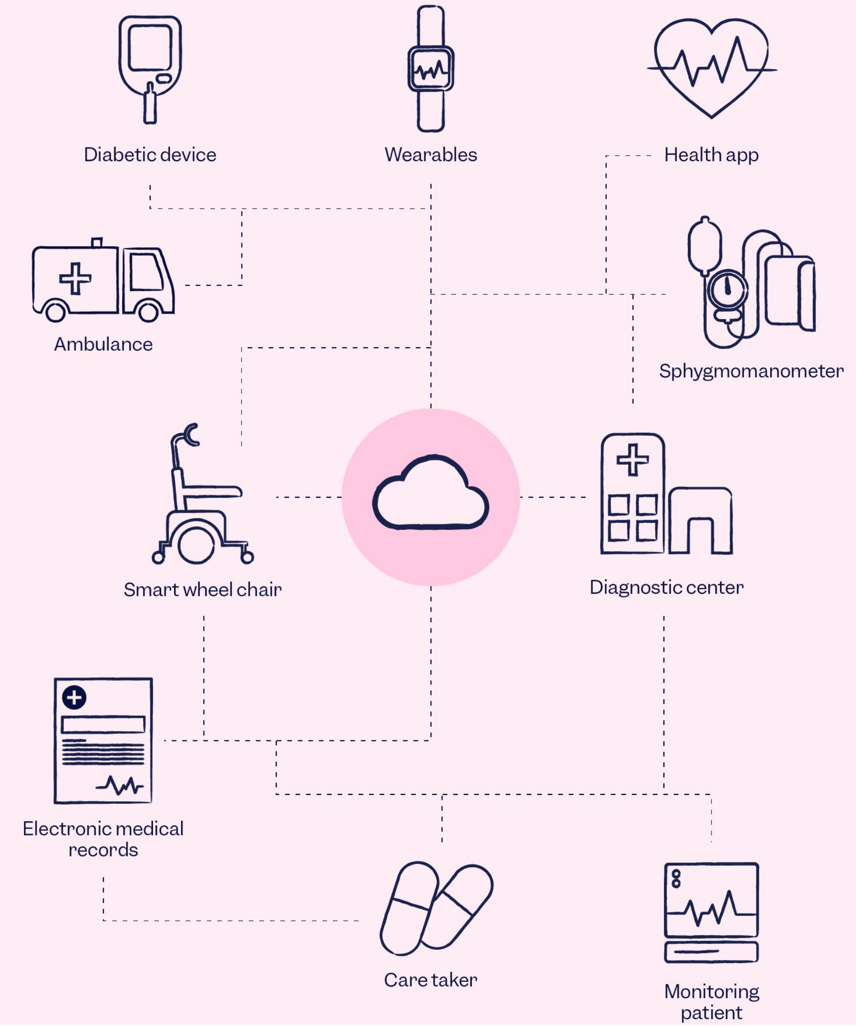
- Získání přístupu k jednotlivým zařízením
- Modifikace nastavení
- Restart jednotlivých zařízení
- Zápis neznámého registru
- Přehrávání smyčky provozu PCAP-loop
- Škodlivý update firmware
- Stažení konfigurace z neznámého zdroje

GREYCORTEX

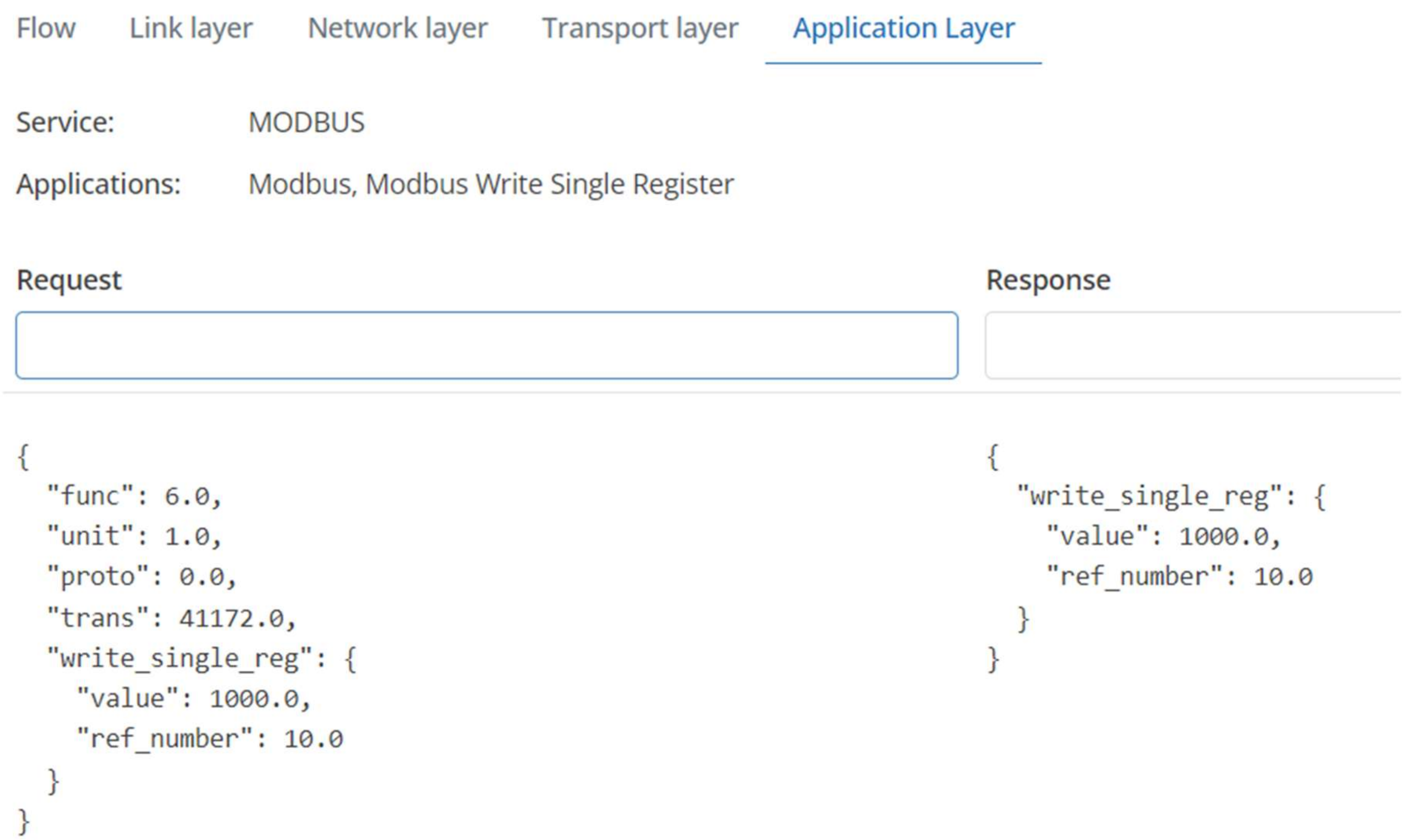
Internet of Medical Things

HL7® International

DICOM℠
Digital Imaging and Communications in Medicine



Zpracovávané OT protokoly



Service: MODBUS

Applications: Modbus, Modbus Write Single Register

Request

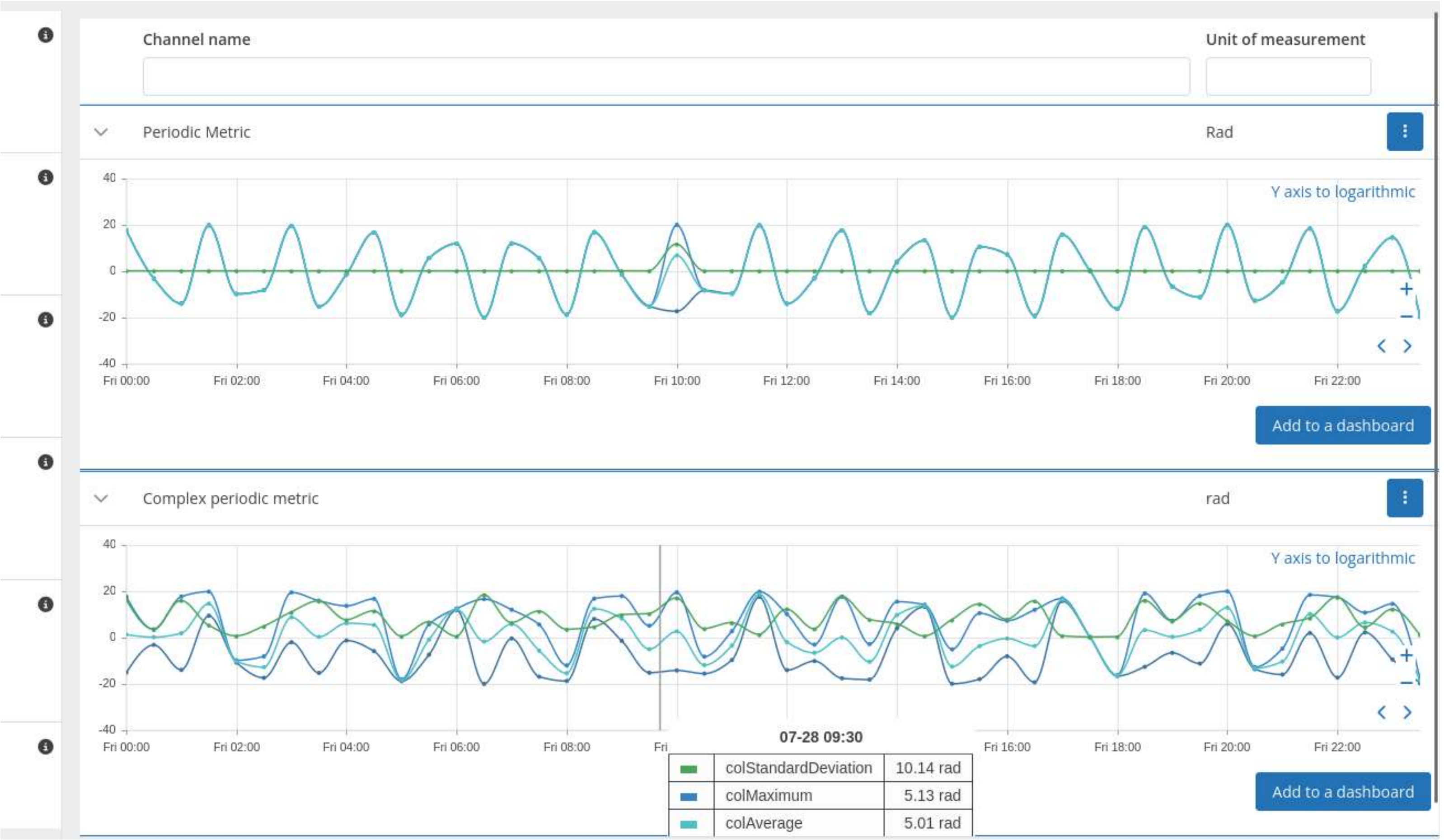
```
{
  "func": 6.0,
  "unit": 1.0,
  "proto": 0.0,
  "trans": 41172.0,
  "write_single_reg": {
    "value": 1000.0,
    "ref_number": 10.0
  }
}
```

Response

```
{
  "write_single_reg": {
    "value": 1000.0,
    "ref_number": 10.0
  }
}
```

GREYCORTEX

Zpracovávané OT protokoly



Channel name

Unit of measurement

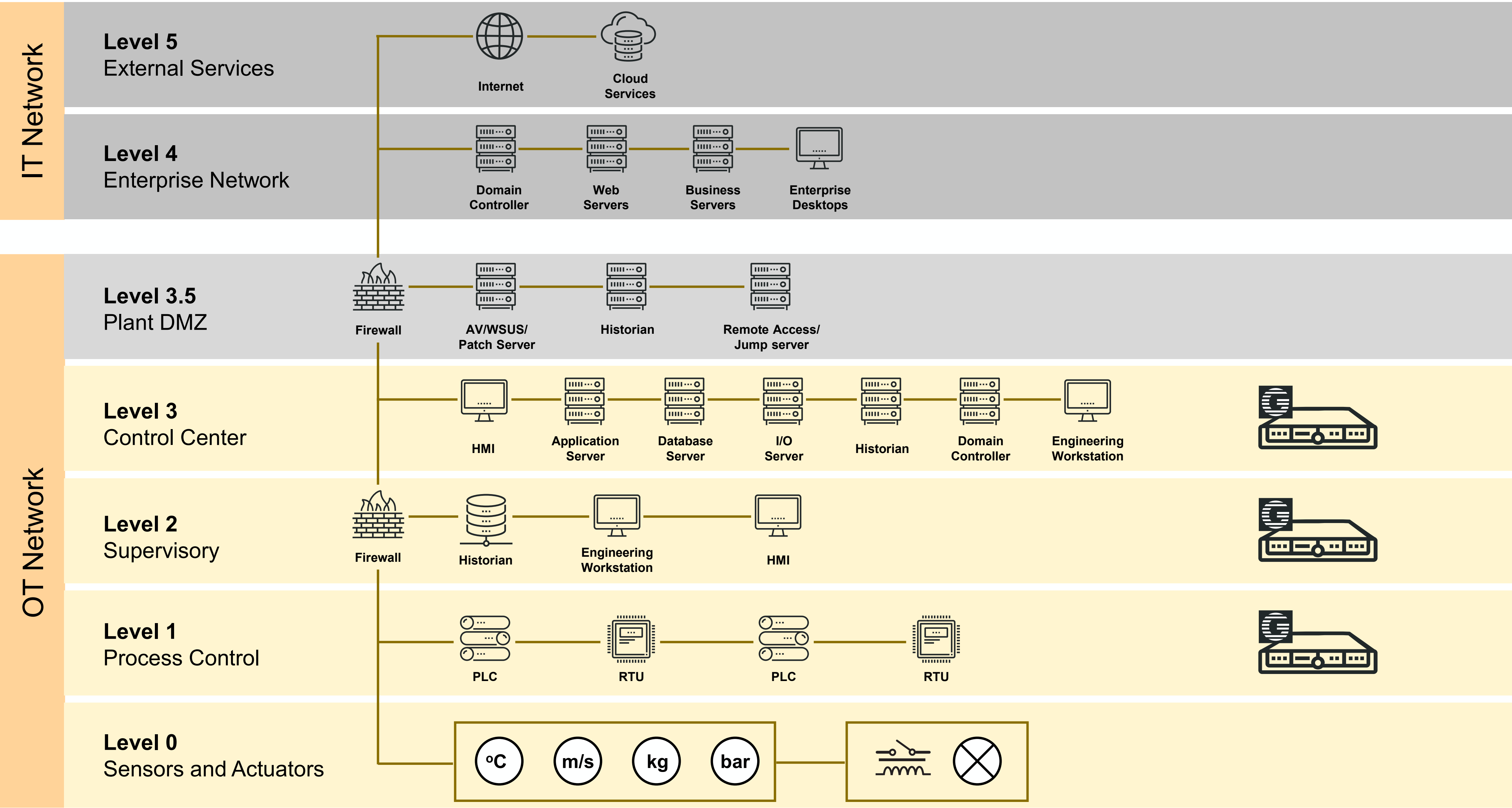
Periodic Metric — Rad

Complex periodic metric — rad

07-28 09:30

🟩	colStandardDeviation	10.14 rad
🟦	colMaximum	5.13 rad
🟦	colAverage	5.01 rad

GREYCORTEX



IT Network

Level 5
External Services

Internet
Cloud Services

Level 4
Enterprise Network

Domain Controller
Web Servers
Business Servers
Enterprise Desktops

OT Network

Level 3.5
Plant DMZ

Firewall
AV/WSUS/ Patch Server
Historian
Remote Access/ Jump server

Level 3
Control Center

HMI
Application Server
Database Server
I/O Server
Historian
Domain Controller
Engineering Workstation

Level 2
Supervisory

Firewall
Historian
Engineering Workstation
HMI

Level 1
Process Control

PLC
RTU
PLC
RTU

Level 0
Sensors and Actuators

°C
m/s
kg
bar

GREYCORTEX

HW specification based on roles

All-in-One

- from HW-SC-XS to HW-SC-2XL
- from 100Mbit to 25Gbit

Collector

- from HW-C-S to HW-C-3XL
- from 1Gbit to 100Gbit

Sensor

- from HW-S-XS to HW-S-3XL
- from 100Mbit to 100Gbit

Dell R360

Dell R760

Advantech UNO-127

DELL Edge 5200

LIVE DEMO

www.greycortex.com

GREYCORTEX

www.greycortex.com