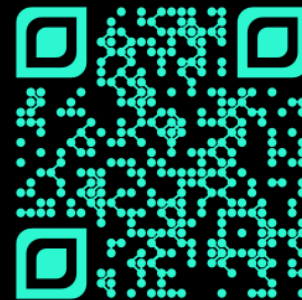


Útoky a zabezpečení OT systémů

14.5.2025





Kdo jsem?

Kdo jsem?

Jakub Alimov, CEH, CHFI



**Lead
Auditor**

architekt kybernetické bezpečnosti,
RANSOMWARE hunter,

konzultant informační bezpečnosti,

více jak 15+ let prokazatelných zkušeností s
kybernetickou bezpečností

<https://www.linkedin.com/in/jakub-alimov-332b1020/>



Kdo je Alinet?



Jsme progresivní IT firma se specializací na kybernetické útoky.

**DIGITAL FORENSICS AND INCIDENT
RESPONSE**





Jsme progresivní IT firma se specializací na kybernetické útoky.

DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ RANSOMWARE útoky
- ✓ Forezní vyšetřování kybernetických incidentů
- ✓ Krizové řízení
- ✓ AUDIT připravenosti na RANSOMWARE útok



Jsme progresivní IT firma se specializací na kybernetické útoky.

DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ RANSOMWARE útoky
- ✓ Forezní vyšetřování kybernetických incidentů
- ✓ Krizové řízení
- ✓ AUDIT připravenosti na RANSOMWARE útok

SLUŽBY KYBERNETICKÉ BEZPEČNOSTI



Jsme progresivní IT firma se specializací na kybernetické útoky.

DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ RANSOMWARE útoky
- ✓ Forenzní vyšetřování kybernetických incidentů
- ✓ Krizové řízení
- ✓ AUDIT připravenosti na RANSOMWARE útok

SLUŽBY KYBERNETICKÉ BEZPEČNOSTI

- ✓ NASTARTOVÁNÍ kybernetické bezpečnosti
- ✓ ARCHITEKT kybernetické bezpečnosti dle ZoKB
- ✓ Přehledové testy zranitelnosti
- ✓ ISO IEC 27001, ISO IEC 62443, NIST CSF, NIS2
- ✓ Zabezpečení kritické infrastruktury



Jsme progresivní IT firma se specializací na kybernetické útoky.

DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ RANSOMWARE útoky
- ✓ Forenzní vyšetřování kybernetických incidentů
- ✓ Krizové řízení
- ✓ AUDIT připravenosti na RANSOMWARE útok

SLUŽBY KYBERNETICKÉ BEZPEČNOSTI

- ✓ NASTARTOVÁNÍ kybernetické bezpečnosti
- ✓ ARCHITEKT kybernetické bezpečnosti dle ZoKB
- ✓ Přehledové testy zranitelnosti
- ✓ ISO IEC 27001, ISO IEC 62443, NIST CSF, NIS2
- ✓ Zabezpečení kritické infrastruktury

SLUŽBA DETEKCE KYBERNETICKÝCH UDÁLOSTÍ



Jsme progresivní IT firma se specializací na kybernetické útoky.

DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ RANSOMWARE útoky
- ✓ Forenzní vyšetřování kybernetických incidentů
- ✓ Krizové řízení
- ✓ AUDIT připravenosti na RANSOMWARE útok

SLUŽBY KYBERNETICKÉ BEZPEČNOSTI

- ✓ NASTARTOVÁNÍ kybernetické bezpečnosti
- ✓ ARCHITEKT kybernetické bezpečnosti dle ZoKB
- ✓ Přehledové testy zranitelnosti
- ✓ ISO IEC 27001, ISO IEC 62443, NIST CSF, NIS2
- ✓ Zabezpečení kritické infrastruktury

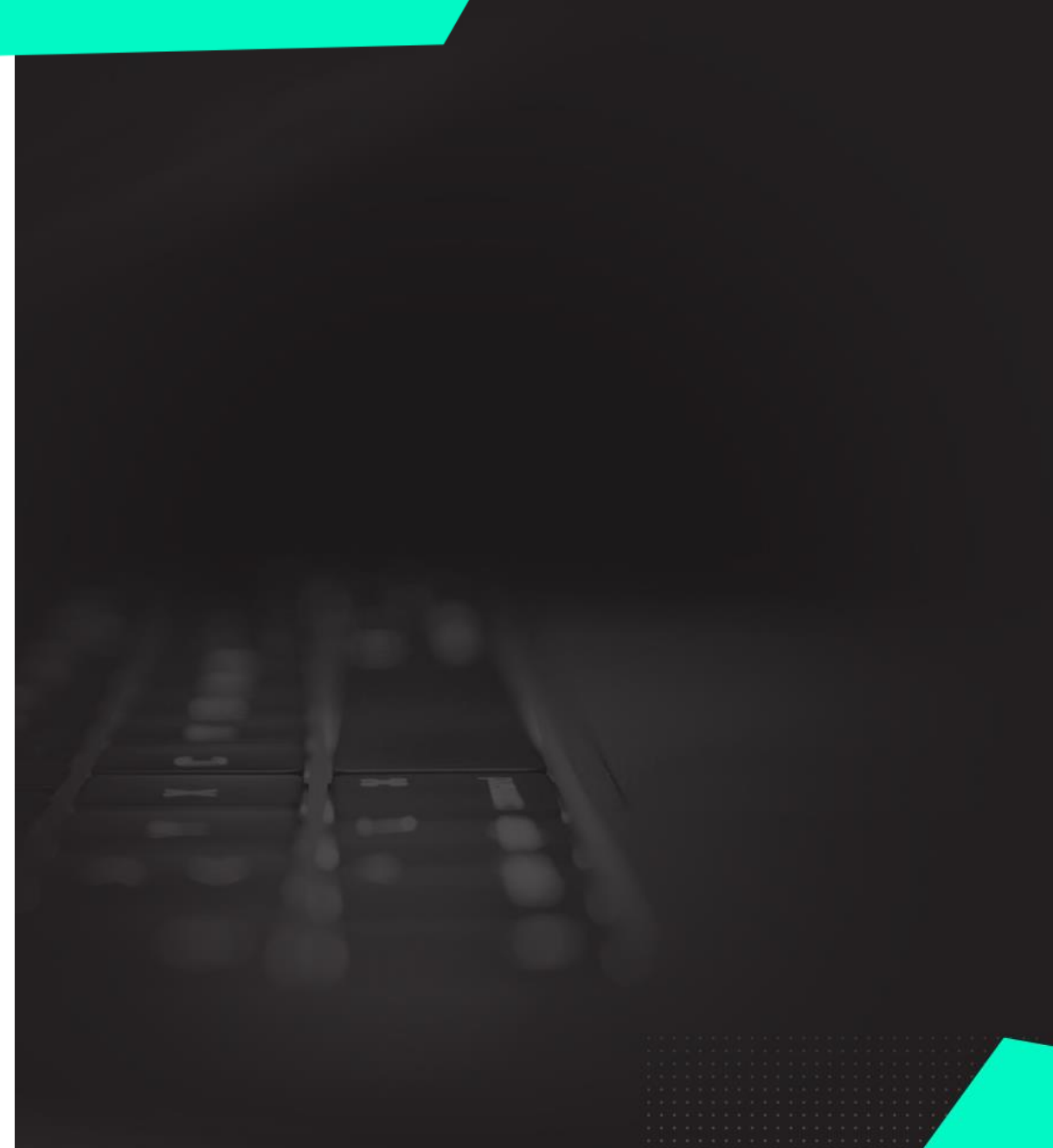
SLUŽBA DETEKCE KYBERNETICKÝCH UDÁLOSTÍ

- ✓ Proaktivní monitoring kybernetické bezpečnosti
- ✓ Dohled kritických assetů ve společnosti
- ✓ Visibilita co se děje
- ✓ Ochrana perimetru



Otázka na úvod?

Kdo je u Vás zodpovědný za provoz a údržbu OT systémů **z pohledu IT?**



Kdo je u Vás zodpovědný za provoz a údržbu OT systémů **z pohledu IT?**

IT Oddělení

X zařízení

Kdo je u Vás zodpovědný za provoz a údržbu OT systémů **z pohledu IT?**

IT Oddělení

X zařízení

OT Oddělení

3x zařízení

Kdo je u Vás zodpovědný za provoz a údržbu OT systémů **z pohledu IT?**

Oddělení
Kybernetické
bezpečnosti

IT Oddělení

X zařízení

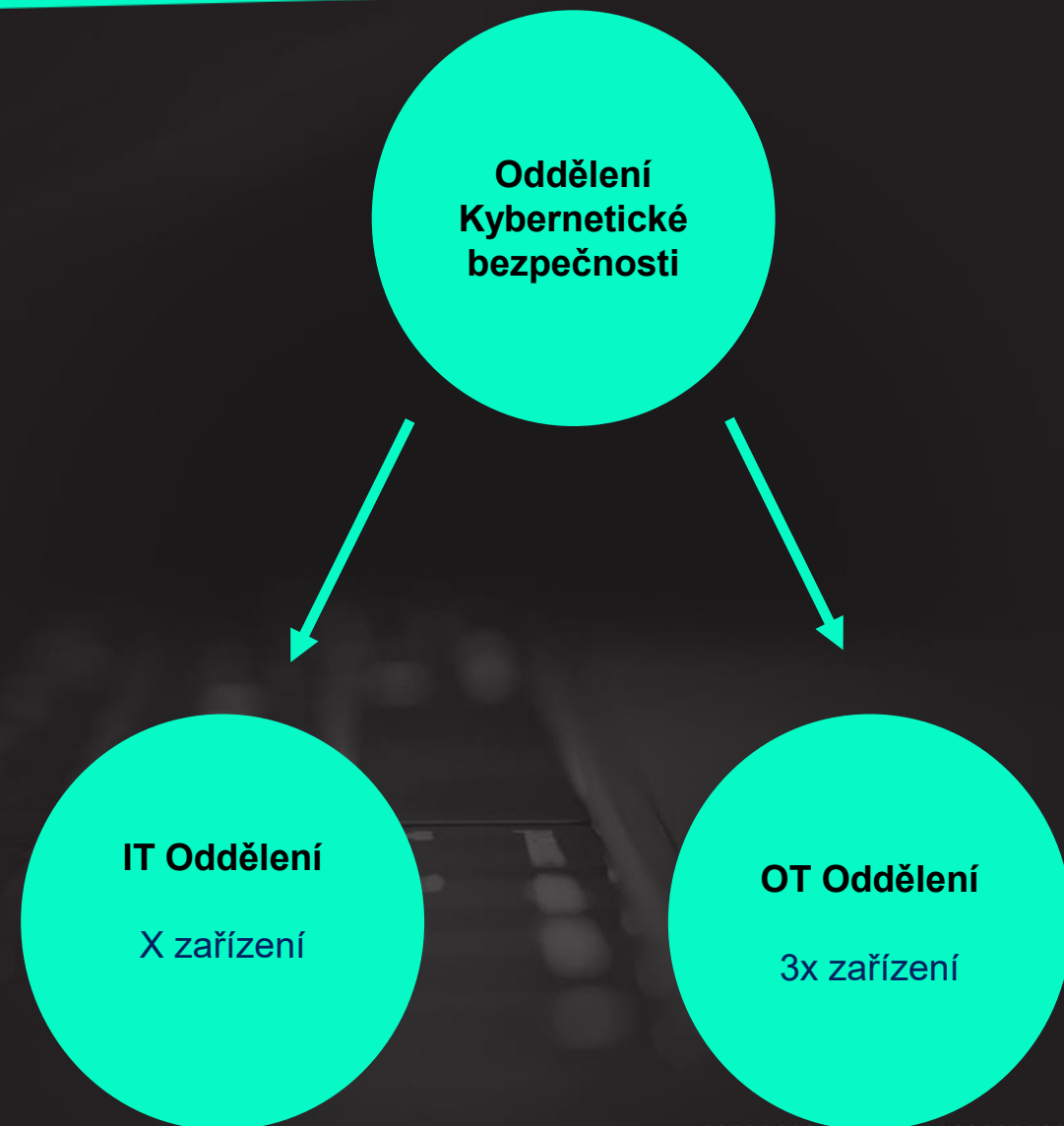
OT Oddělení

3x zařízení

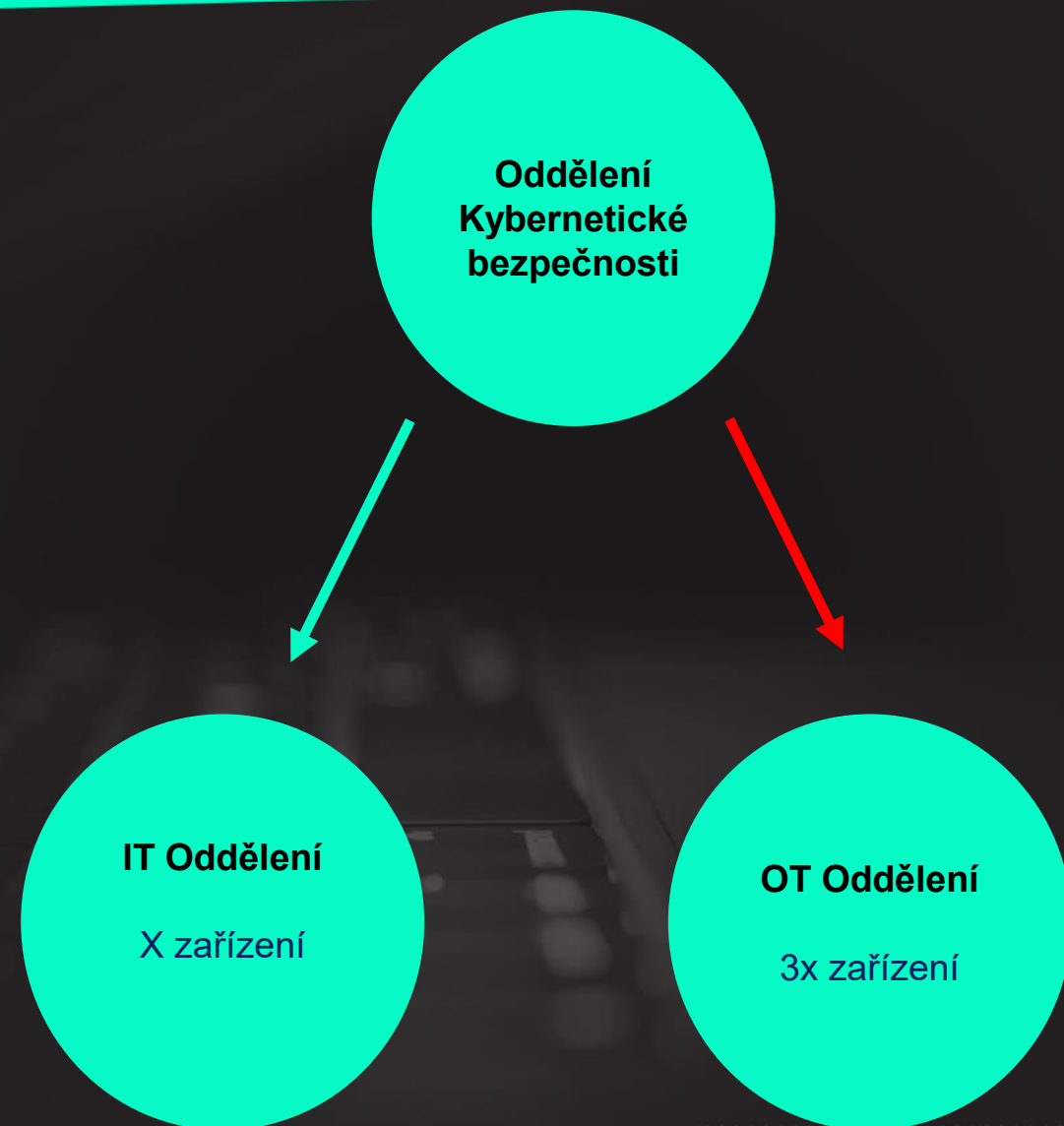
Kdo je u Vás zodpovědný za provoz a údržbu OT systémů **z pohledu IT?**



Kdo je u Vás zodpovědný za provoz a údržbu OT systémů **z pohledu IT?**



Kdo je u Vás zodpovědný za provoz a údržbu OT systémů **z pohledu IT?**





Útoky na Operační Technologie

OT útoky v roce 2024?

✓ **Každá 3** organizace hlásí více než 6 a více narušení OT systémů

zdroj: <https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-of-cybersecurity.pdf>

OT útoky v roce 2024?

✓ **Každá 3** organizace hlásí více než 6 a více narušení OT systémů

✓ **55%** OT organizací zaznamenalo **výpadek** systému s kybernetickým útokem

zdroj: <https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-of-cybersecurity.pdf>

OT útoky v roce 2024?

- ✓ **Každá 3** organizace hlásí více než 6 a více narušení OT systémů
- ✓ **55%** OT organizací zaznamenalo **výpadek** systému s kybernetickým útokem
- ✓ **43 %** OT organizací přišlo o kritický data

zdroj: <https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-of-cybersecurity.pdf>

Reálné útoky v roce 2024?

Chtěl bych se s Vámi podělit o několik skutečných příběhů z forenzního vyšetřování z minulého roku.

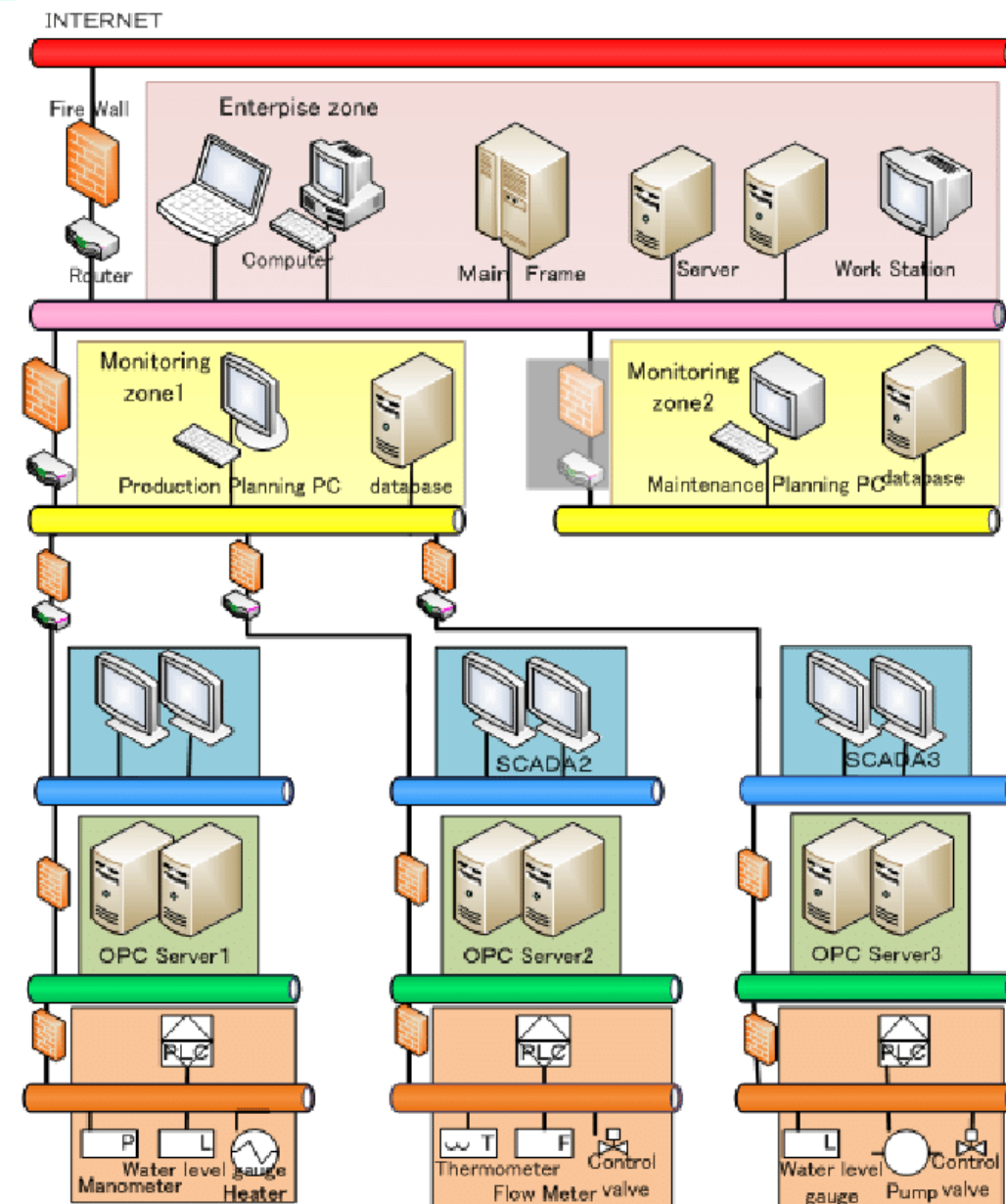
- ✓ Útok na nezabezpečené zařízení vzdálené správy OT zařízení, exploitace a následné proniknutí do jiné vrstvy podnikové sítě
- ✓ Neaktualizovaná webová služba umožnila přístup komukoliv do interní firemní sítě
- ✓ Sít'ově spojené IT a OT prostředí zašifrovalo výrobní společnost
- ✓ Dělali jsme audit IT prostředí OT prostředí audit nelze co kdyby náhodou to přestalo fungovat ? :)

Proč útoky na operační technologie?

- ✓ Protože OT systémy vždy byly navrženy pouze pro **funkčnost** nikoliv kybernetickou bezpečnost
- ✓ Protože životnost OT systému je **10-30 let!**
- ✓ Protože OT systémy je **heterogenní prostředí**, kde je peer systém dodavatel, peer dodavatel vlastní 5G mobilní připojení ideálně rovnou do sítě internet
- ✓ Protože hrozba útoku přes **dodavatelský řetězec** je velmi častá a bohužel i reálná
- ✓ Protože OT kybernetická bezpečnost DNES = IT kybernetická bezpečnost **před 15 ti lety!**
- ✓ Protože jsou zranitelnosti ve Firmware a Software update a je složitý někdy až **nemožný**

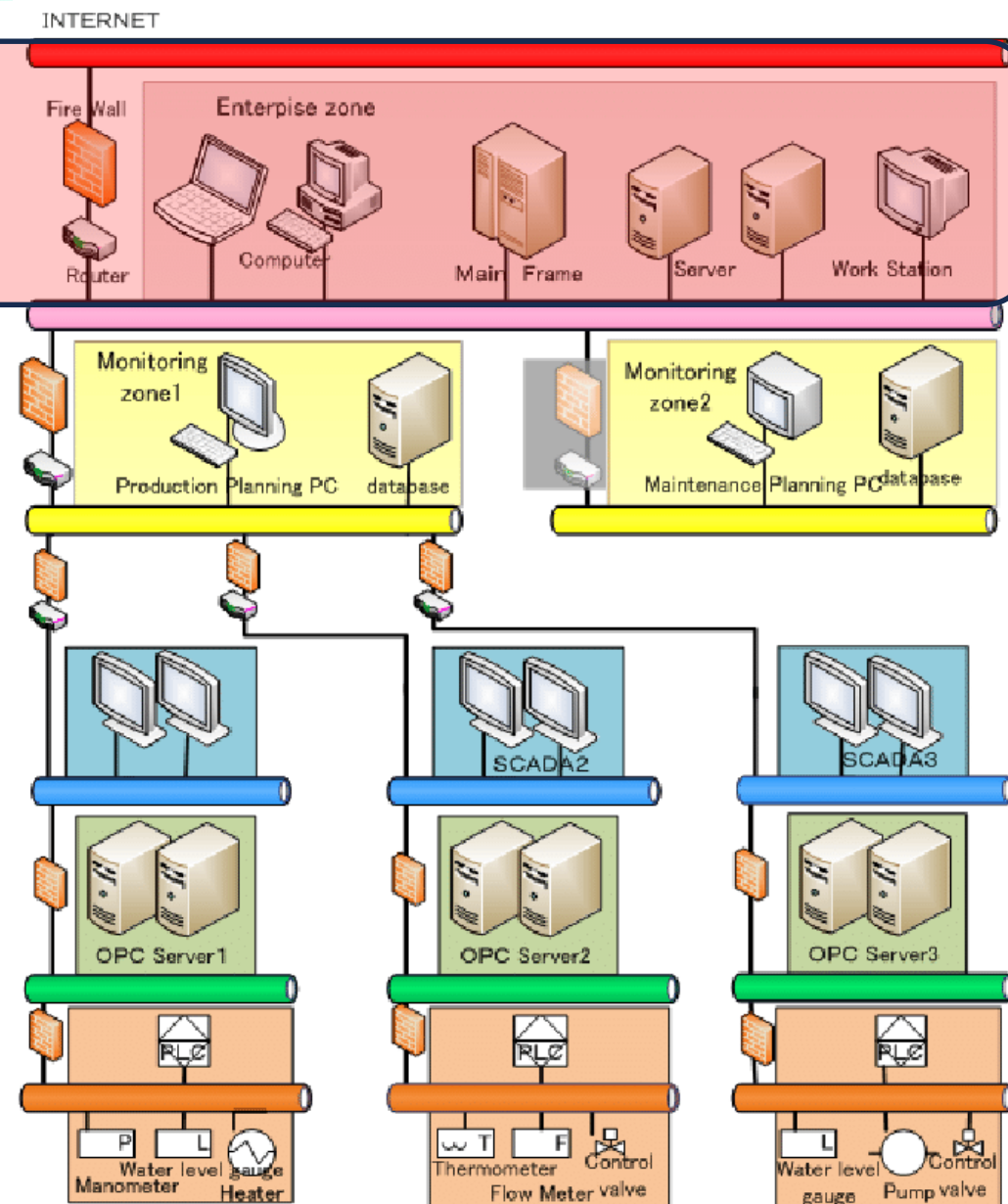


Jak by to mělo dnes vypadat?



Level 4

■ ENTERPRISE ZONE



Level 4

▪ ENTERPRISE ZONE

INTERNET

Fire Wall

Enterprise zone

Router

Computer

Main Frame

Server

Work Station

DMZ

▪ DMZ ZONE

Monitoring zone1

Production Planning PC

database

Monitoring zone2

Maintenance Planning PC

database

SCADA1

SCADA2

SCADA3

OPC Server1

OPC Server2

OPC Server3

PLC

PLC

PLC

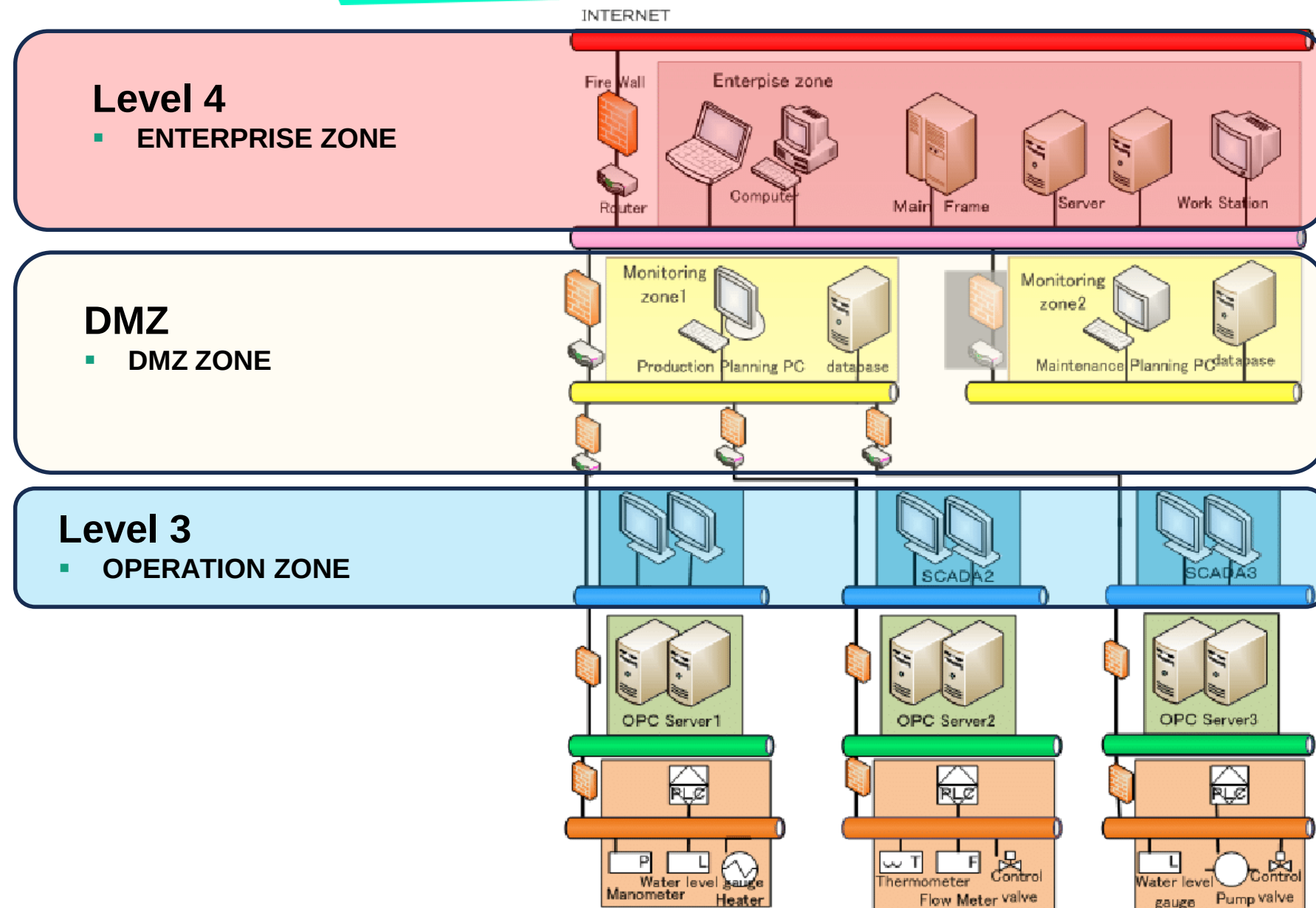
Water level gauge
Manometer

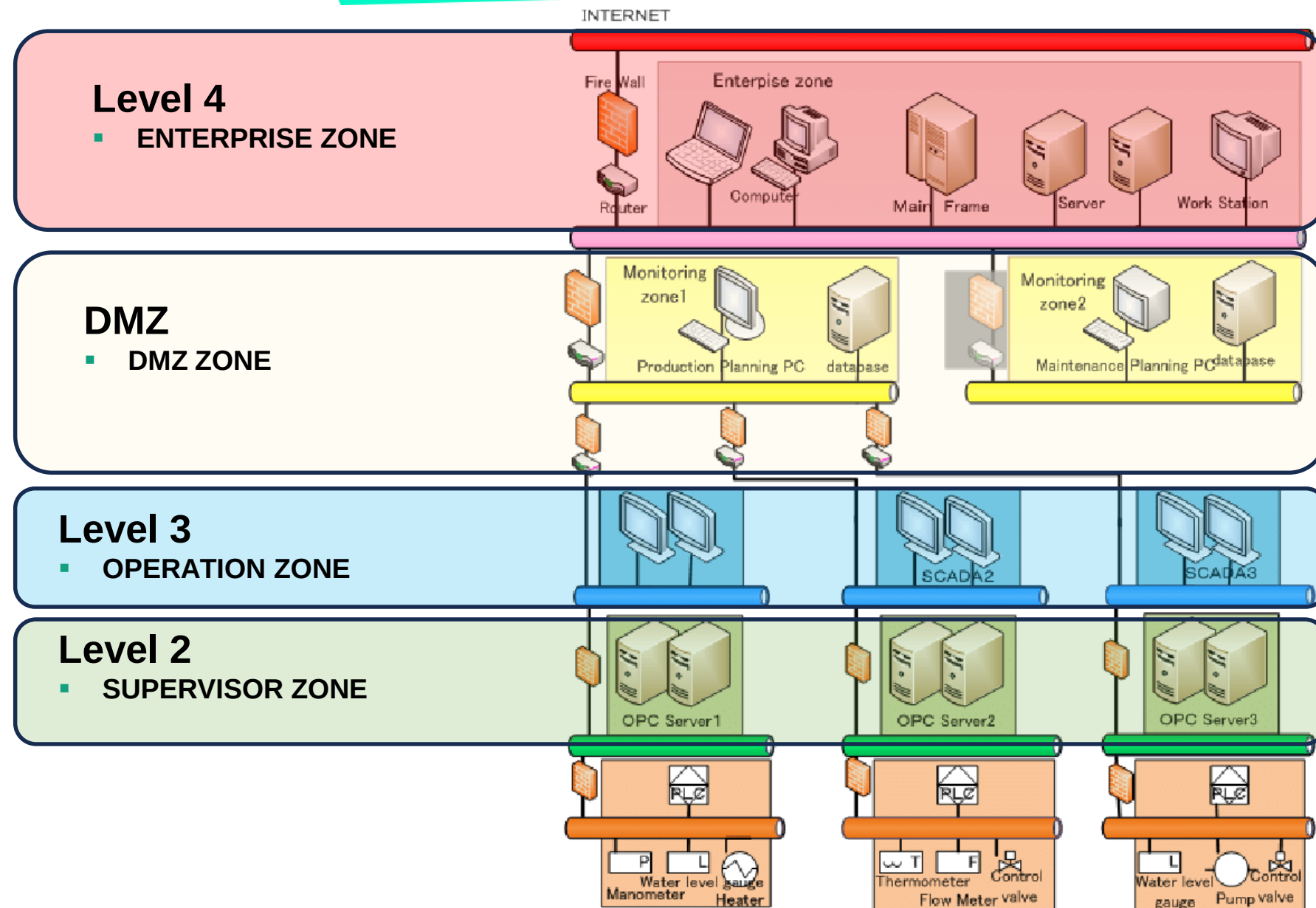
Heater

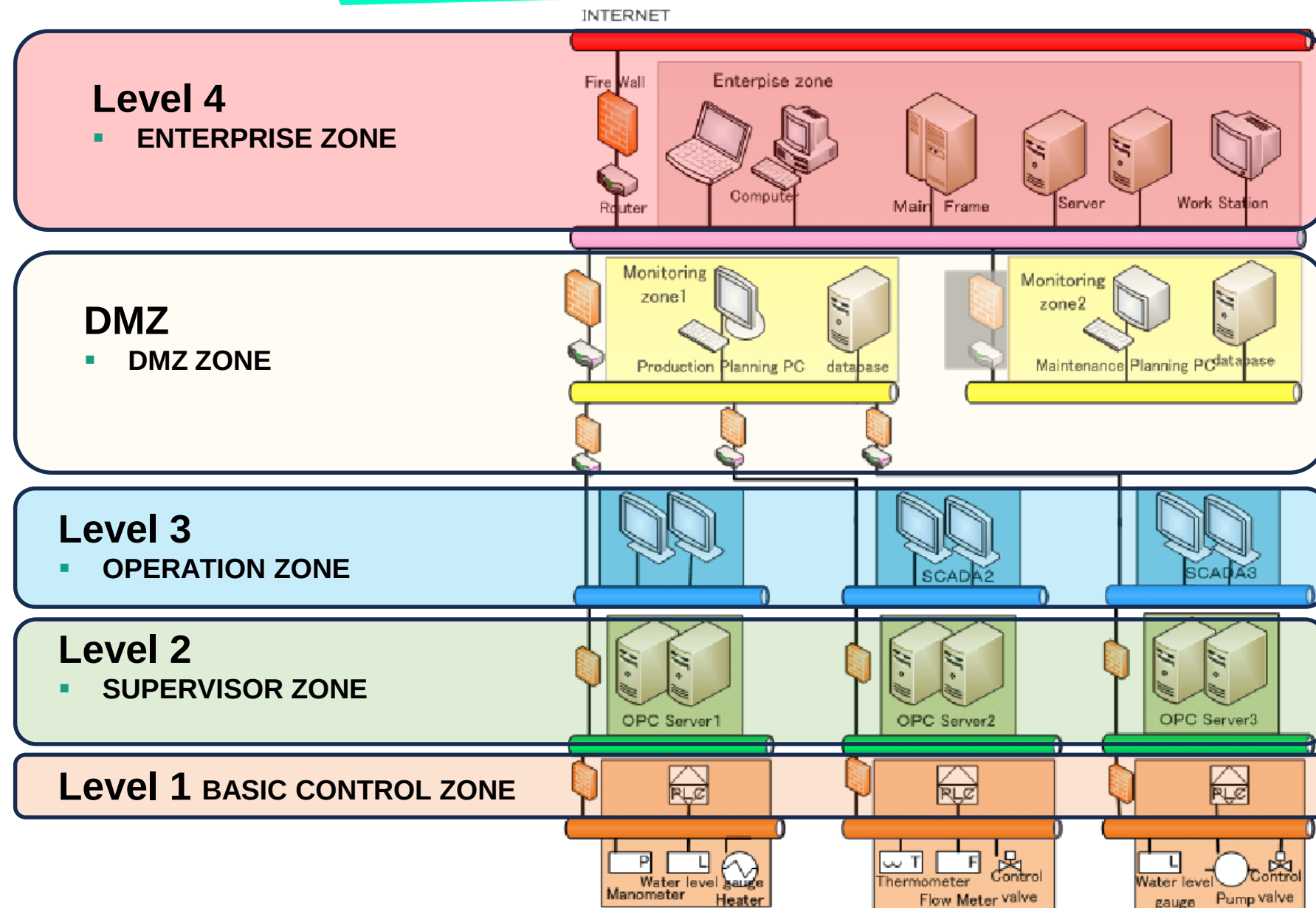
Thermometer
Flow Meter

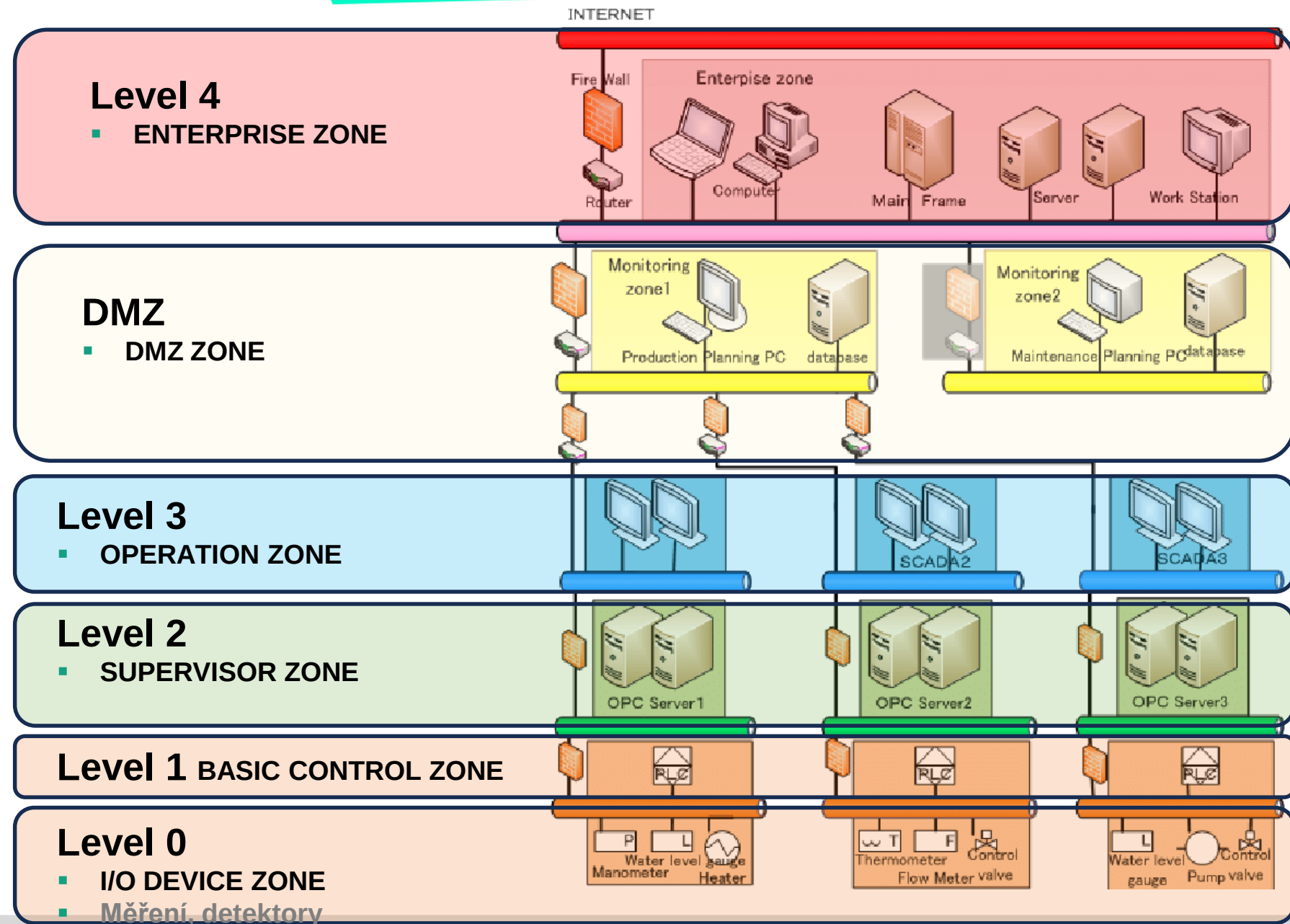
Control valve

Water level gauge
Pump valve





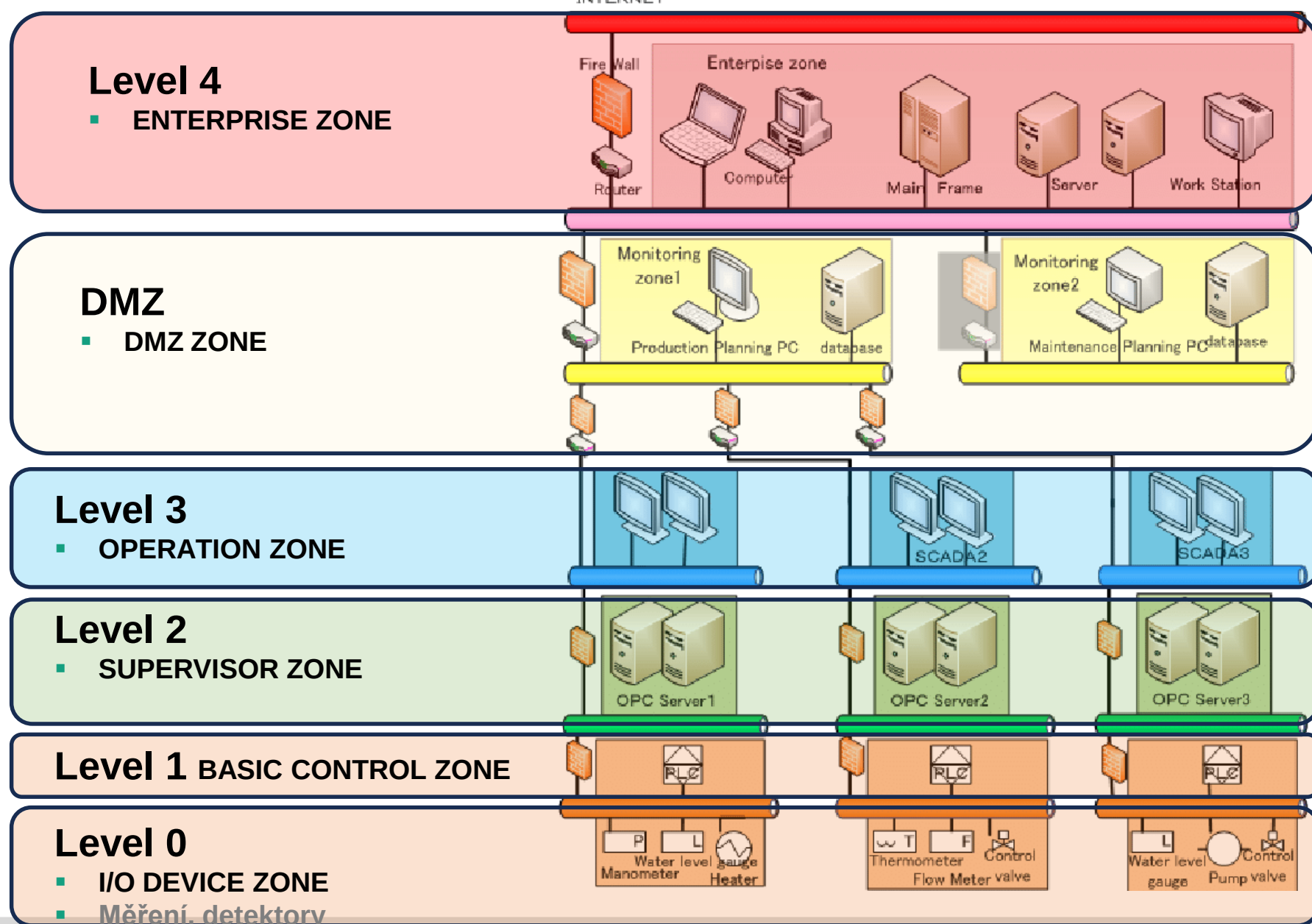




IT ZONE

DMZ ZONE

CONTROL ZONE

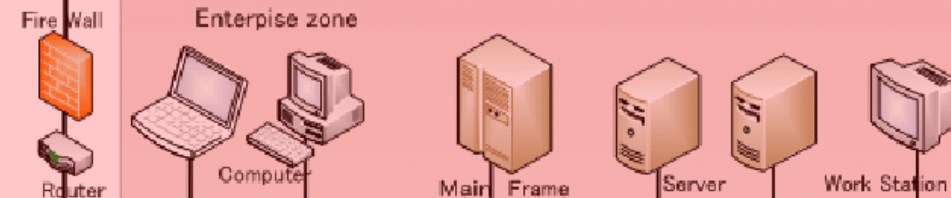


IT ZONE

Level 4

- ENTERPRISE ZONE

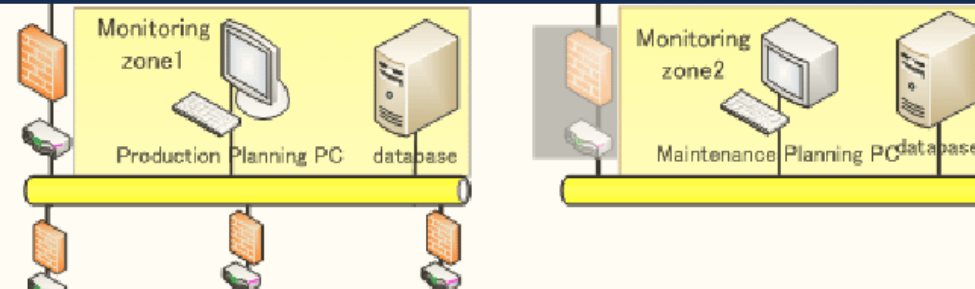
INTERNET



DMZ ZONE

DMZ

- DMZ ZONE



Level 3

- OPERATION ZONE



Level 2

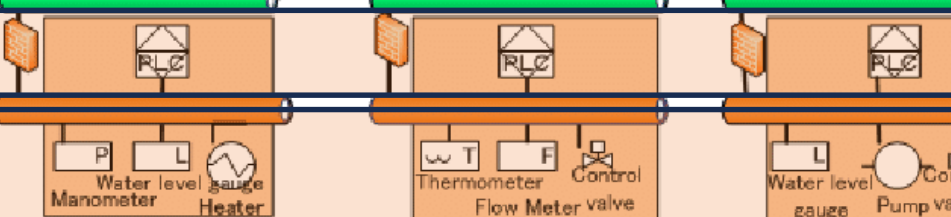
- SUPERVISOR ZONE



Level 1 BASIC CONTROL ZONE

Level 0

- I/O DEVICE ZONE
- Měření, detektory



Wide Area
Network

CONTROL ZONE



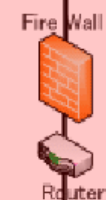
Alinet

IT
ZONE

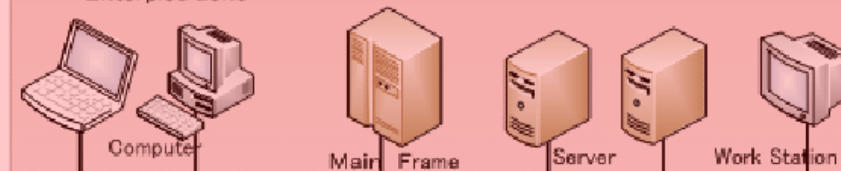
Level 4

- ENTERPRISE ZONE

INTERNET



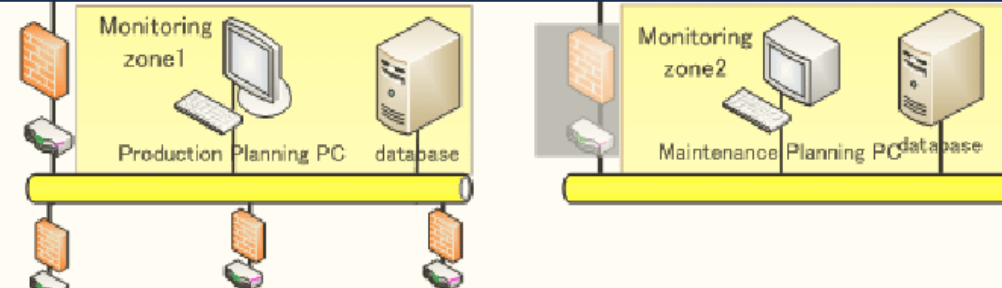
Enterprise zone



DMZ
ZONE

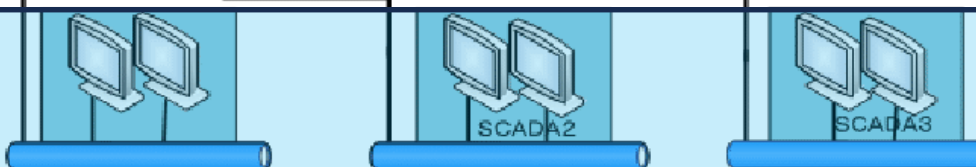
DMZ

- DMZ ZONE



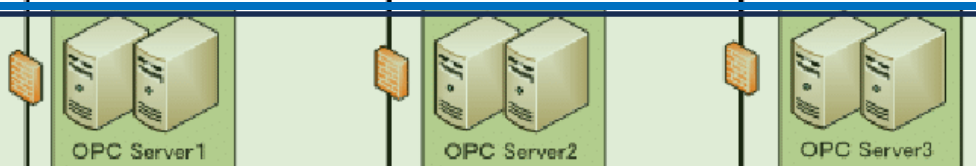
Level 3

- OPERATION ZONE



Level 2

- SUPERVISOR ZONE

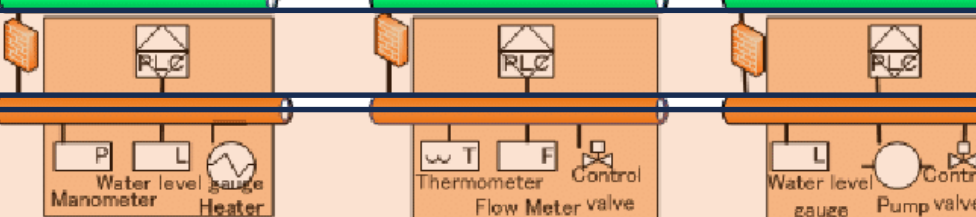


Level 1 BASIC CONTROL ZONE

Level 0

- I/O DEVICE ZONE

- Měření, detektory



Wide Area
Network

CONTROL
ZONE



Alinet

IT
ZONE

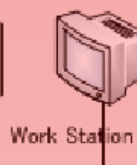
Level 4

- ENTERPRISE ZONE

INTERNET



Enterprise zone



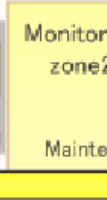
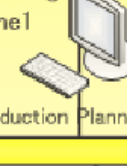
DMZ
ZONE

DMZ

- DMZ ZONE



Monitoring zone1



Level 3

- OPERATION ZONE



Wide Area
Network

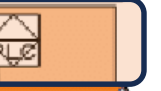
CONTROL
ZONE

Level 2

- SUPERVISOR ZONE



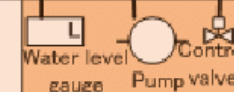
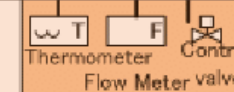
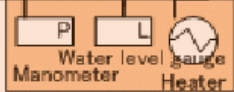
Level 1 BASIC CONTROL ZONE



Level 0

- I/O DEVICE ZONE

Měření, detektory





Jak začít ?

Jak začít ?

- ✓ **Identifikovat a klasifikovat** OT zařízení, díky které máte dostatečnou viditelnost
- ✓ **MIKROSEGMENTACE** sítě a síťových ZÓN
- ✓ **Začlenit OT systémy** do bezpečnostních operací a reakcí na bezpečnostní incidenty (SOC, DR a IR plány)
- ✓ Správně navržená **architektura OT**
- ✓ NEbýt REAKTIVNÍ ale **PROAKTIVNÍ**
- ✓ Ochrana zranitelností na perimetru **VŠECH** internetů
- ✓ **Přehledové testy zranitelností/penetrační testy**
- ✓ **Zálohy** konfigurací!



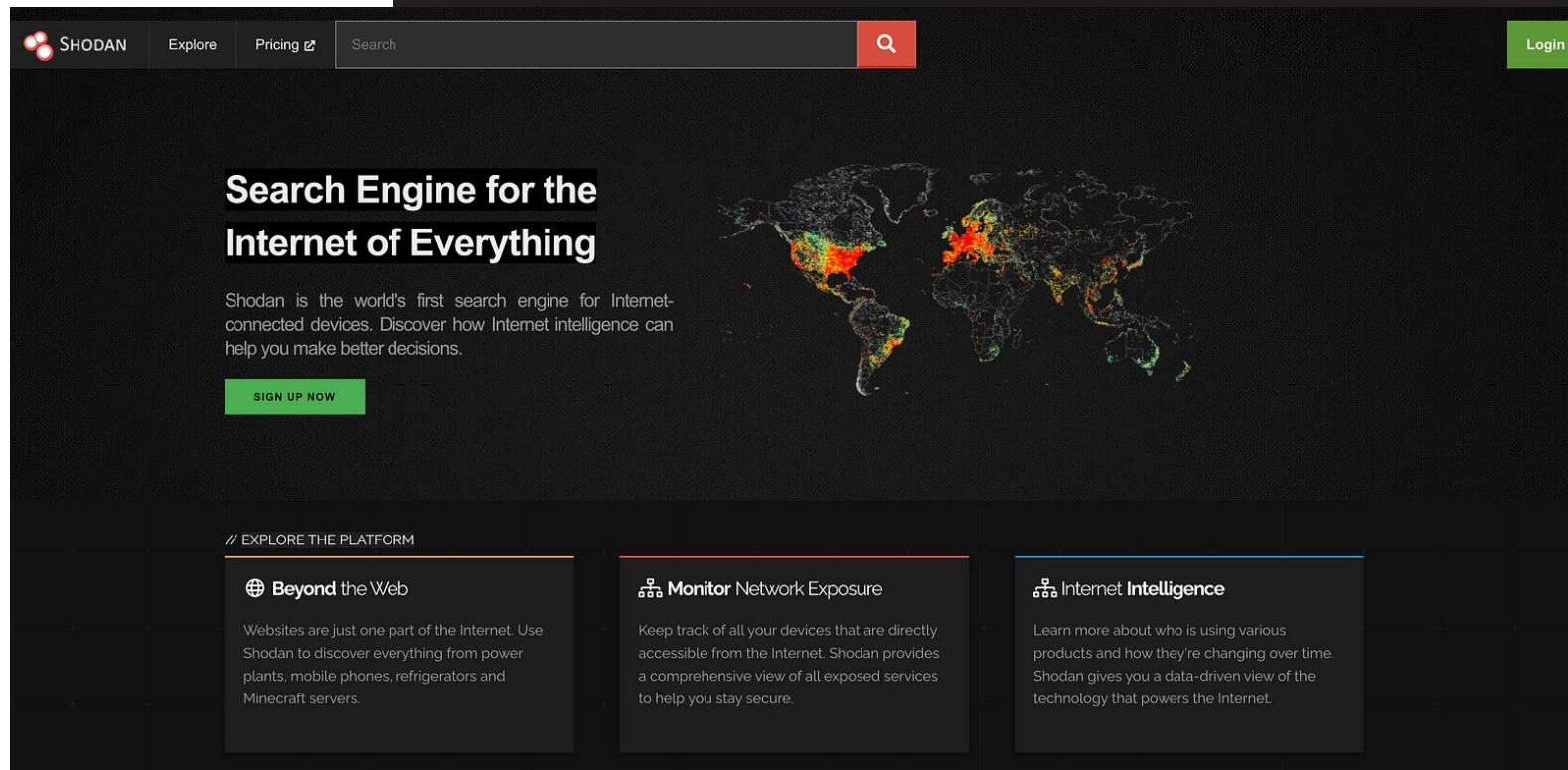
Jak **opravdu** začít ?



Ochrana perimetru



Shodan.io



The screenshot shows the Shodan.io homepage. At the top, there is a navigation bar with the Shodan logo, links for 'Explore' and 'Pricing', a search bar, and a 'Login' button. The main heading reads 'Search Engine for the Internet of Everything'. Below this, a paragraph states: 'Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.' A green 'SIGN UP NOW' button is positioned below the text. To the right of the text is a world map with glowing nodes representing internet-connected devices. Below the main content area, there is a section titled '// EXPLORE THE PLATFORM' with three columns. The first column, 'Beyond the Web', describes searching for power plants, mobile phones, refrigerators, and Minecraft servers. The second column, 'Monitor Network Exposure', describes tracking devices directly accessible from the Internet. The third column, 'Internet Intelligence', describes a data-driven view of the technology powering the Internet.

SHODAN Explore Pricing Search Login

Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

[SIGN UP NOW](#)

// EXPLORE THE PLATFORM

 **Beyond the Web**

Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.

 **Monitor Network Exposure**

Keep track of all your devices that are directly accessible from the Internet. Shodan provides a comprehensive view of all exposed services to help you stay secure.

 **Internet Intelligence**

Learn more about who is using various products and how they're changing over time. Shodan gives you a data-driven view of the technology that powers the Internet.

Zdroj: <https://www.shodan.io/>



Potřebujete pomoci ?

**Vyžádejte si s námi
schůzku již NYNÍ**

- ✓ Do chatu
- ✓ Napište klíčové slovo **ALINET** spojíme se s Vami
- ✓ Provedeme **SCAN PERIMETRU ZDARMA**
- ✓ Zkonzultujeme Vaše potřeby



Bezpečnostní upozornění na závěr

FORTINET®

15.1.2025

Password DUMP

Authentication
bypass

CVE-2024-55591

Zdroj: <https://www.heise.de/en/news/Unknown-group-releases-Fortinet-config-files-and-VPN-passwords-to-the-darknet-10244238.html>

- ✓ 15 474 Fortigate celý svět (**136 CZ a 11 SK**)
- ✓ Seznam je už z roku 2022 !!
 - ✓ založený na zranitelnosti CVE-2022-40684
 - ✓ Aktualizovaný 1/2024
 - ✓ Seřazen podle zemí RU
- ✓ Uživatelské jména
- ✓ Hesla (samozřejmě v plaintextu)
- ✓ Full config fortigate (včetně certifikátů)

FORTINET®

15.1.2025

Password DUMP

Authentication bypass

CVE-2024-55591

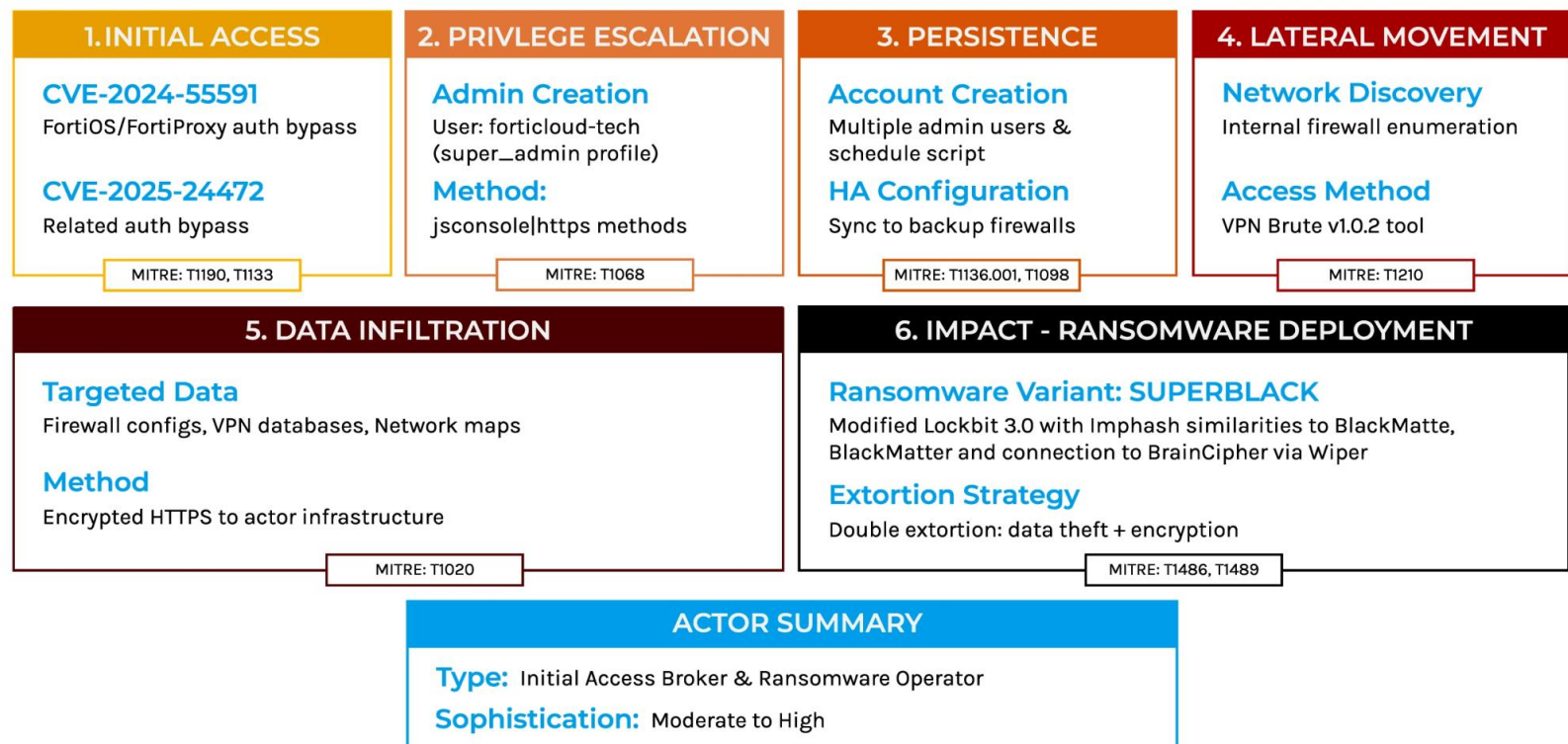
Zdroj: <https://www.heise.de/en/news/Unknown-group-releases-Fortinet-config-files-and-VPN-passwords-to-darknet-10244238.html>

MORA_001-THREAT ACTOR

TARGET: FORTINET's CVE-2025-24472 and CVE-2024-55591



ATTACK CHAIN



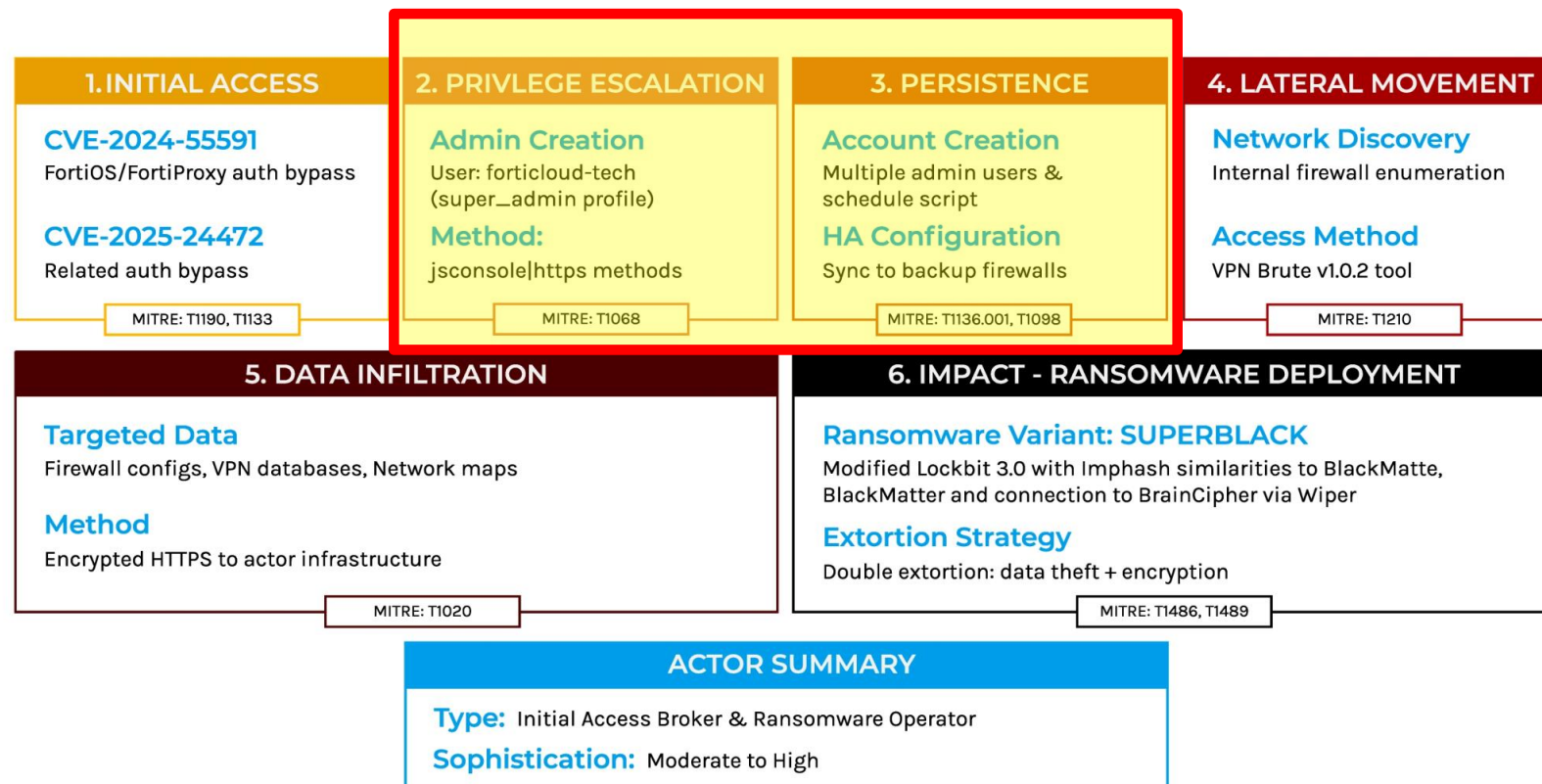
15.1.2025**Password DUMP****Authentication
bypass****CVE-2024-55591**

Zdroj: <https://www.heise.de/en/news/Unknown-group-releases-Fortinet-config-files-and-VPN-passwords-to-darknet-10244238.html>

MORA_001-THREAT ACTOR

TARGET: FORTINET's CVE-2025-24472 and CVE-2024-55591

ATTACK CHAIN





Alinet

Cyber Security, **Ransomware Incident Response**



Jakub Alimov

www.alinet.cz jakub.alimov@alinete.cz +420 774 077 108