

# Kybernetická bezpečnosť v priemysle

Bratislava 05/2023

# Kontakt

---

Štefan KÖRÖSI

+421 910 955 388

stefan.korosi@actemium.sk

ProCS, Kráľovská 8, 927 01 Šaľa

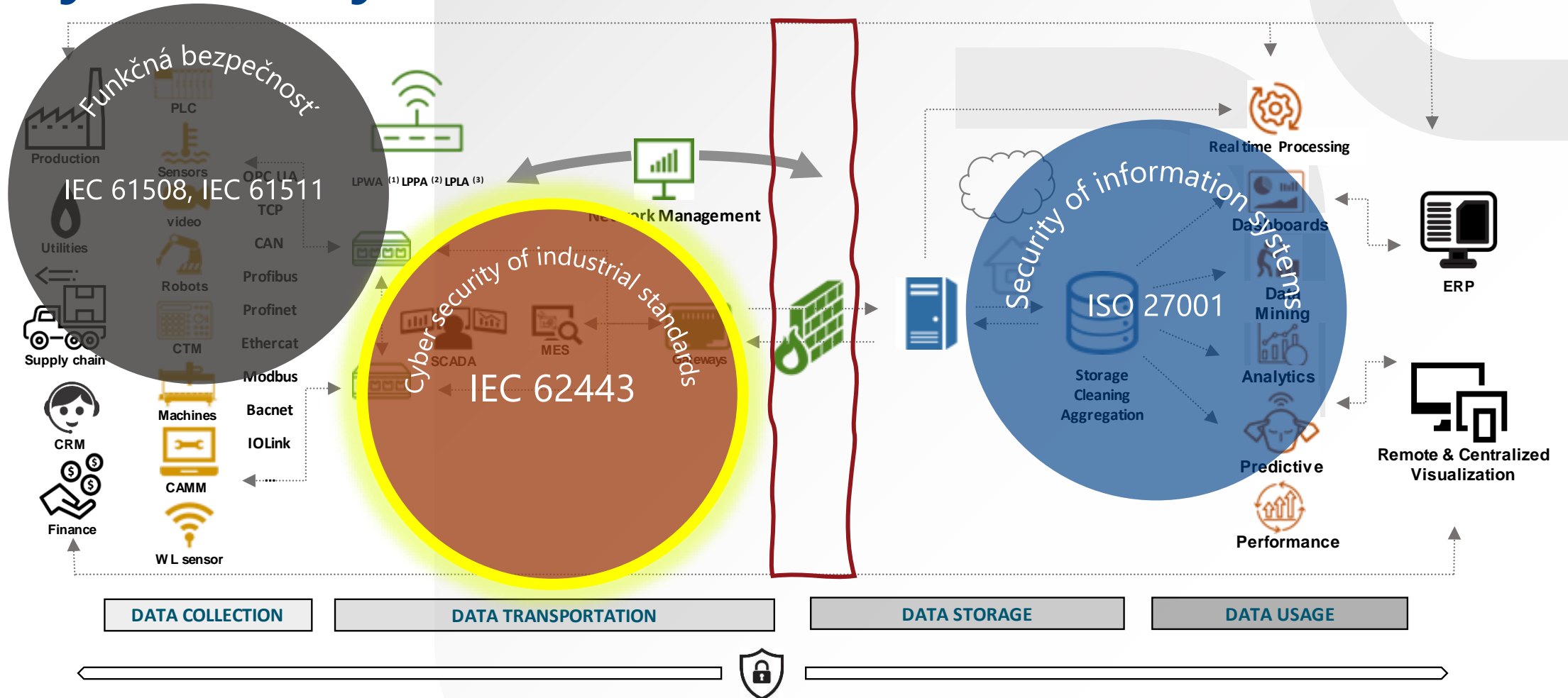
---



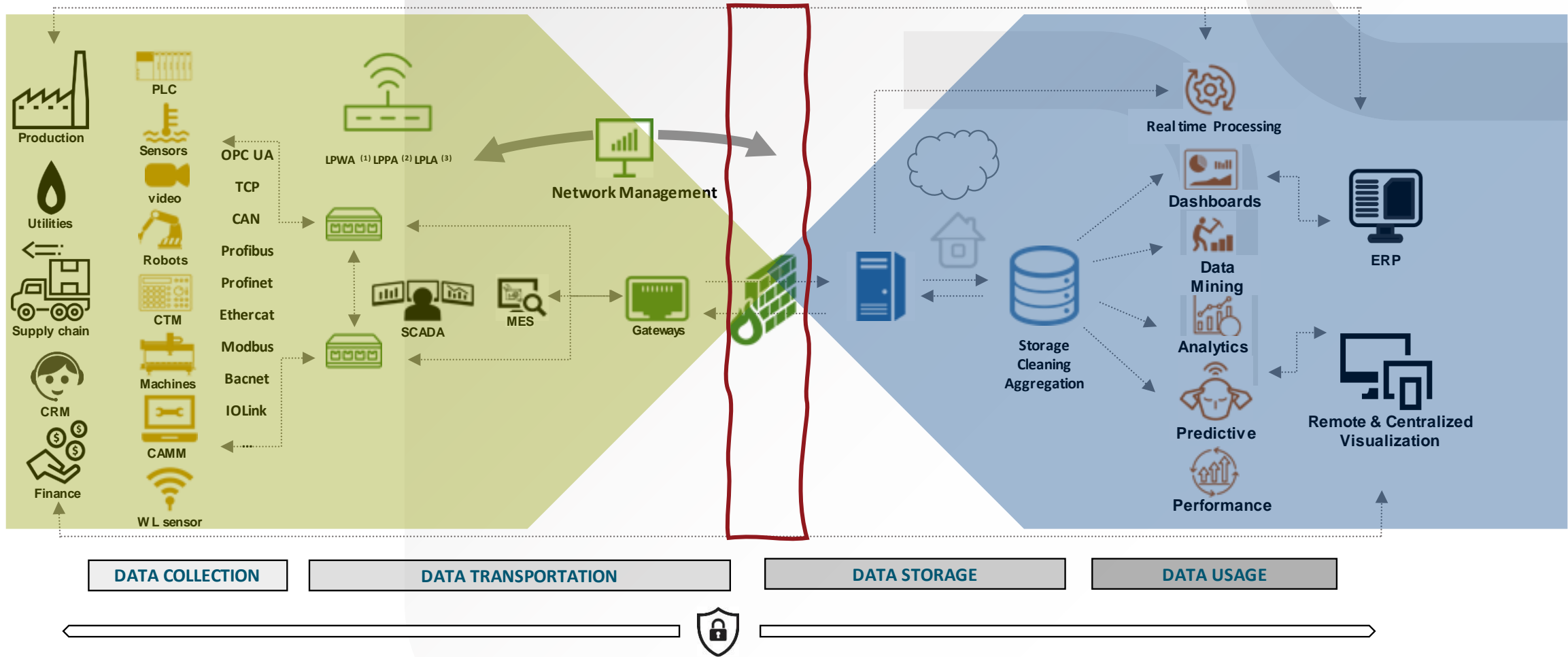
# Safety / Security



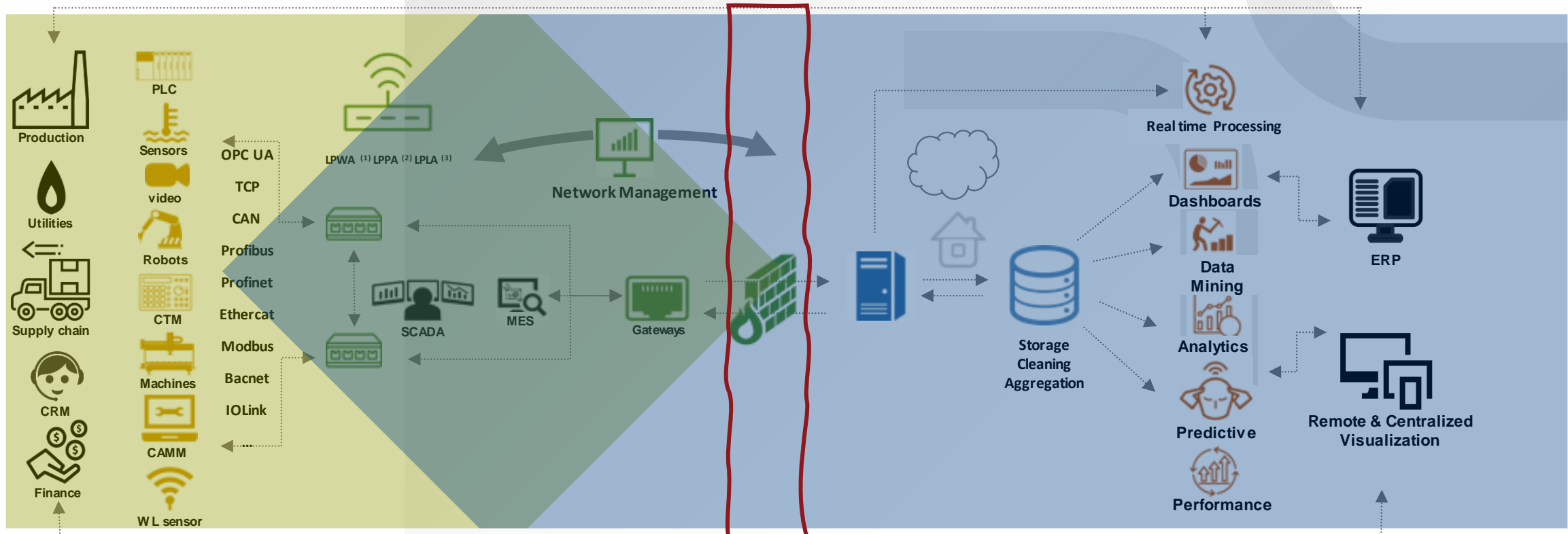
# Safety / Security



# OT / IT



# OT / IT



**DATA COLLECTION**

**DATA TRANSPORTATION**

**DATA STORAGE**

**DATA USAGE**



# Rozdiely v požiadavkách kybernetickej bezpečnosti medzi IT a OT

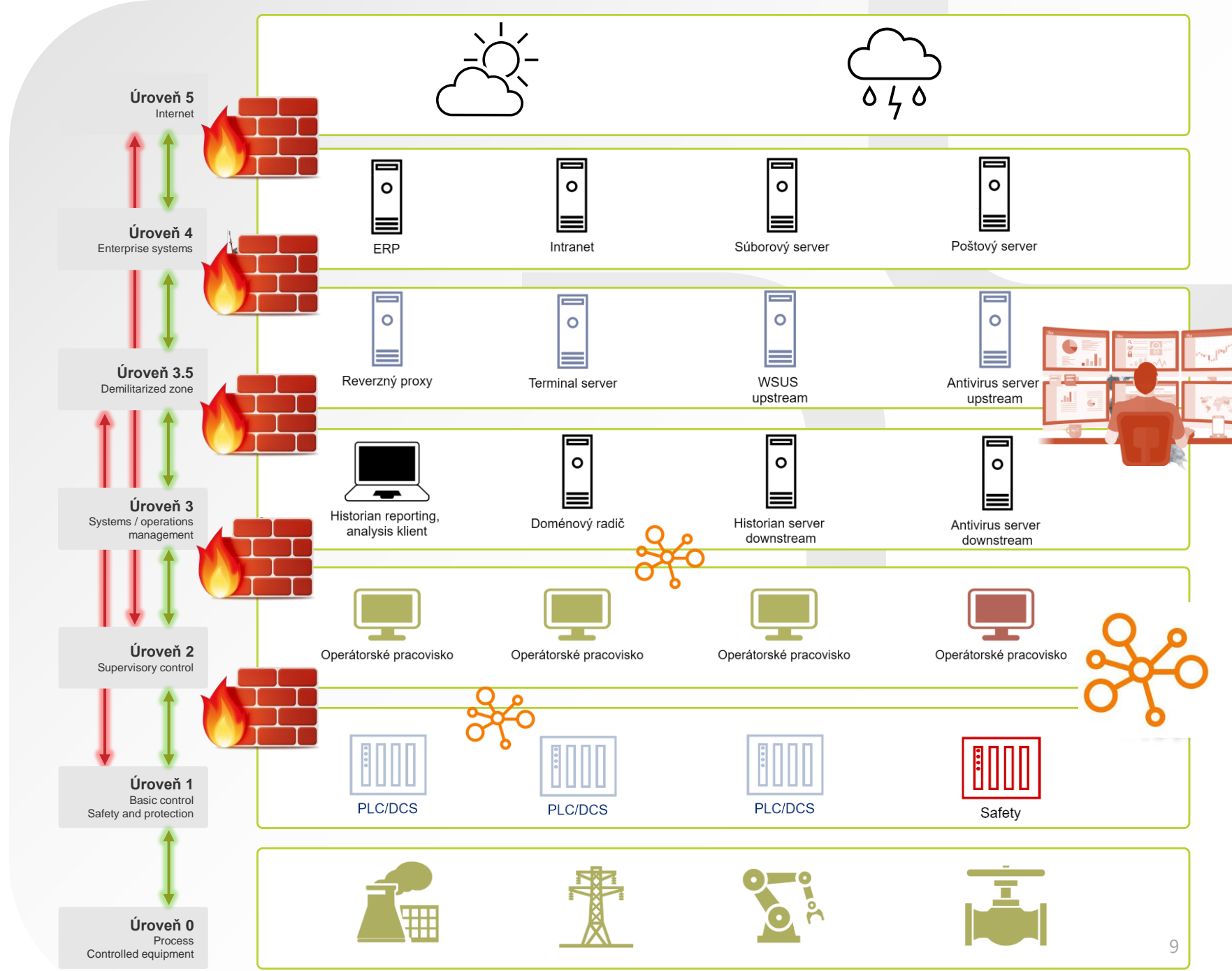
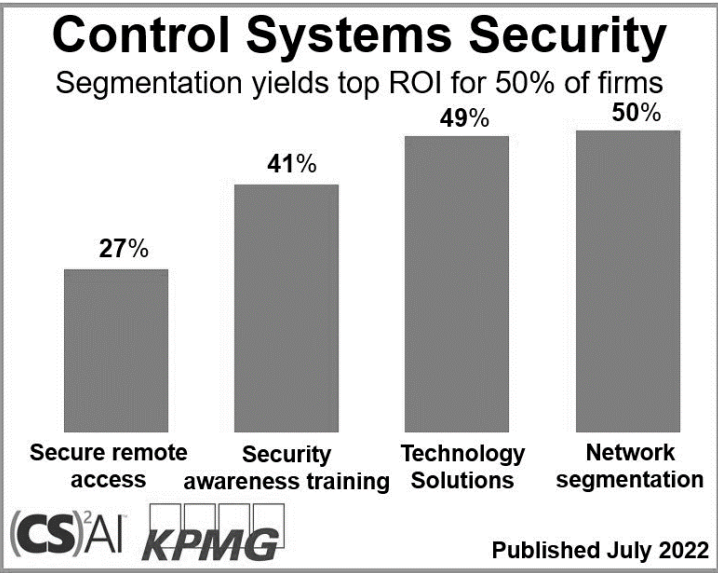
	Informačné technológie	Prevádzkové technológie
Požiadavky na kybernetickú bezpečnosť	dôvernosť integrita dostupnosť	dostupnosť integrita dôvernosť
Predmet ochrany	informácie	fyzické procesy
Riziká	únik informácií, financie	bezpečnosť, zdravie, životné prostredie, financie
Životnosť systémov	3 – 10 rokov	5 – 25 rokov
Požiadavky na dostupnosť	95 % a viac	99,9 % a viac
Zameranie bezpečnosti	servery, dátové úložiská	stabilita riadiacich systémov
Riešenie problémov	reset	odolnosť proti chybám, online oprava
Operačné prostredie	transakcie	reálny čas

# Stredoveká segmentácia





# Segmentácia siete podľa ISA/IEC 62443



# Smernica Európskeho parlamentu NIS 2

opatrenia sa uplatňujú od  
**18. októbra 2024**

**69/2018** Z. z. Zákon o kybernetickej  
bezpečnosti

Vyhláška č. **362/2018** Z. z. Vyhláška  
NBÚ, ustanovuje obsah  
bezpečnostných opatrení, obsah a  
štruktúru bezpečnostnej  
dokumentácie a rozsah  
všeobecných bezpečnostných  
opatrení

ODVETVIA S VYSOKOU ÚROVŇOU KRITICKOSTI

INÉ KRITICKÉ ODVETVIA



doprava



energetika



zdravotníctvo



priemysel



bankovníctvo



infraštruktúra  
finančných trhov



pitná voda



odpadová voda



verejná správa



vesmír



riadenie IKT



poštové a kuriérske  
služby



odpadové  
hospodárstvo



výroba a distribúcia  
a chemických látok



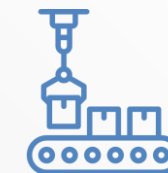
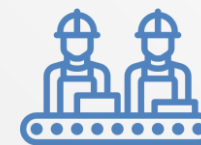
výskum



výroba a distribúcia  
a spracovanie  
potravín



poskytovatelia  
digitálnych služieb



výroba (zdravotnícke pomôcky, počítačové, elektronické a optické  
výrobky, elektrické zariadenia, stroje a zariadenia, motorové vozidlá,  
návesy, prívesy, ostatné dopravné prostriedky...)

# Projekt kybernetickej bezpečnosti

Názov p

Účinný koncept zabezpečenia zohľadňuje zlepšenie bezpečnostných riešení, ktoré sú súčasťou implementácie. Okrem toho sa zameriava na faktor. Takýmto spôsobom je možné zvýšiť účinnosť rôznych ochrany, keď jedna vrstva zlyhá počas kybernetického incidentu.

IACS sú často zraniteľné z dôvodu nedostatku aktualizácií siete a spĺňať požiadavku trvalej dostupnosti. Komplexné pokrytie z uvedeného dôvodu nevyhnutnosťou.

Hlavným cieľom stratégie obrany do hĺbky je znížiť plochu bezpečnosti v rámci stratégie obrany do hĺbky zvyšujúcej bezpečnostných opatrení:

- fyzická bezpečnosť - ochrana IACS pred neoprávneným prístupom (napr. ploty, zámky, zamknuté dvere),
- fyzická konektivita - ochrana IACS pred neoprávneným pripojením k systému svojej
- bezpečnosť komunikácie - ochrana IACS pred neoprávnenými používateľmi/softvérom videli ale
- bezpečnosť používateľov - nastavenie a aktualizácia oprávnení (k čomu majú používatelia p

## Bezpečnostné požiadavky

Norma IEC 62443 definuje tri základné role:

- Dodávateľ produktu
- Systémový integrátor
- Vlastník aktív.

Každá z rolí je zodpovedná za definovanú oblasť podľa súboru noriem IEC 62443.

**Dodávateľ (výrobca) produktu** je zodpovedný za vývoj a testovanie IACS a jeho komponentov, PLC, DCS, firewally, smerovače, operátorské stanice, inžinierske stanice atď., ktoré spoločne alebo subsystém definovaný v normách IEC 62443 3-3, IEC 62443 4-1, IEC 62443 4-2.

**Systémový integrátor** je zodpovedný za integráciu a uvedenie produktu do prevádzky pomocou postupov v súlade s normami IEC 62443 2-4, IEC 62443 3-2, IEC 62443 3-3.

**Vlastník aktív (konečný používateľ)** je zodpovedný za prevádzku a údržbu pomocou postupov v normách IEC 62443 2-1, IEC 62443 2-3 a IEC 62443 2-4.



## The Scope of

- 1-1: Terminol
- 1-2: Master
- 1-3: System
- 1-4: IACS
- 2-1: Rec
- 2-2: In
- 2-3: P
- 2-4: P
- 3-1: Ap
- 3-2: P
- 3-3: P
- 3-4: P

## 2.1 Obrana do hĺbky

Jedným zo základných bezpečnostných konceptov Armáda používala túto stratégiu na obmedzenie opatrenie. V prípade IACS existujú okrem cieľov obmedziť implementáciu hĺbkovej obrany.

Obr. č. 1 Všeobecný model úrovni bezpečnosti



# ĎAKUJEME ZA POZORNOSŤ

---

ProCS, s.r.o.  
Kráľovská ulica 8/824  
927 01 Šaľa  
Tel.: +421 31 7731111

[info@actemium.sk](mailto:info@actemium.sk)

[www.actemium.sk](http://www.actemium.sk)

[linkedin.com/company/actemium-slovakia](https://www.linkedin.com/company/actemium-slovakia)