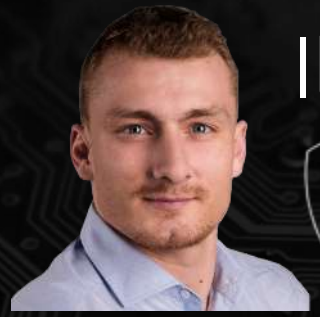
KYBERNETICKÁ BEZPEČNOST V PRŮMYSLOVÉM PROSTŘEDÍ

Pokročilé metody kybernetické bezpečnosti pro průmysl a kritickou infrastrukturu

Ilja David ☆ Kamil Kosour ☆ Communication Security ☆ Praha ☆ 2024

KDO JSME



Ilja David

IRON OT
Secure The Industry Future

Více než 10 let zkušeností s průmyslovou kybernetickou bezpečností obsahuje praktické projekty v klíčových průmyslových odvětvích, jako je letecký, námořní, potravinářský, energetický, ropný a plynárenský, farmaceutický, chemický a to ve společnostech Airbus Defence and Space, DNV a Nestlé, kde byl mmj. regionální manažer IT bezpečnosti pro 130 továren v 62 zemích.

Kamil Kosour

COMGUARD
cyber security masters

V IT oboru se pohybuje od r. 2001 na obchodních pozicích, aktuálně pracuje již 14. rokem ve společnosti COMGUARD a.s. na pozici seniorního obchodníka a vendor managera pro produkty SOPHOS, Ekran a Honeywell (SCADAfence).

IRON OT

O NÁS

Iron OT je první společnost v České republice zabývající se výhradně kybernetickou bezpečností průmyslových provozních technologií. Náš tým je dynamický, plný zkušených nadšenců do kybernetické bezpečnosti a průmyslu jako takového.

Nabízíme kybernetickou bezpečnost jako službu a také rozsáhlou sadu špičkových specializovaných řešení, která dokážeme upravit na míru konkrétní organizaci.

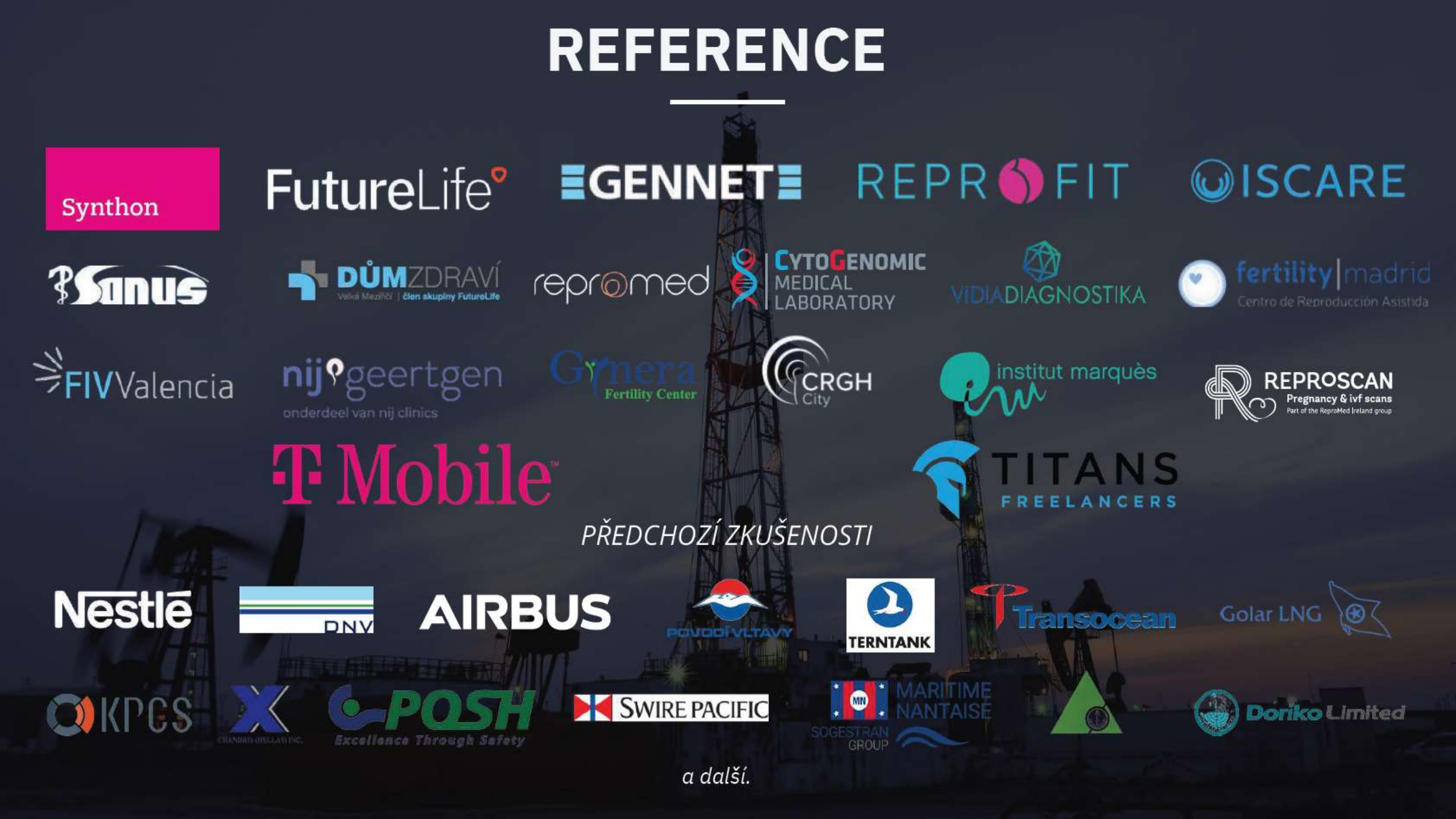
Specializujeme se na implementaci, kontrolu a dlouhodobou udržitelnost systémů řízení kybernetické bezpečnosti v organizacích spadajících pod kritickou infrastrukturu a průmyslové podniky.

V této prezentaci Vám krátce představíme naši firmu. Neváhejte se na nás obrátit v případě zájmu o další informace či o podrobnou nabídku.

Těšíme se na spolupráci
Tým Iron OT

Naše certifikace, červen 2024

REFERENCE



a další.

Obsah

1# OT Cyber Incident

2# Operational Technologies

3# Standardy IEC 62443

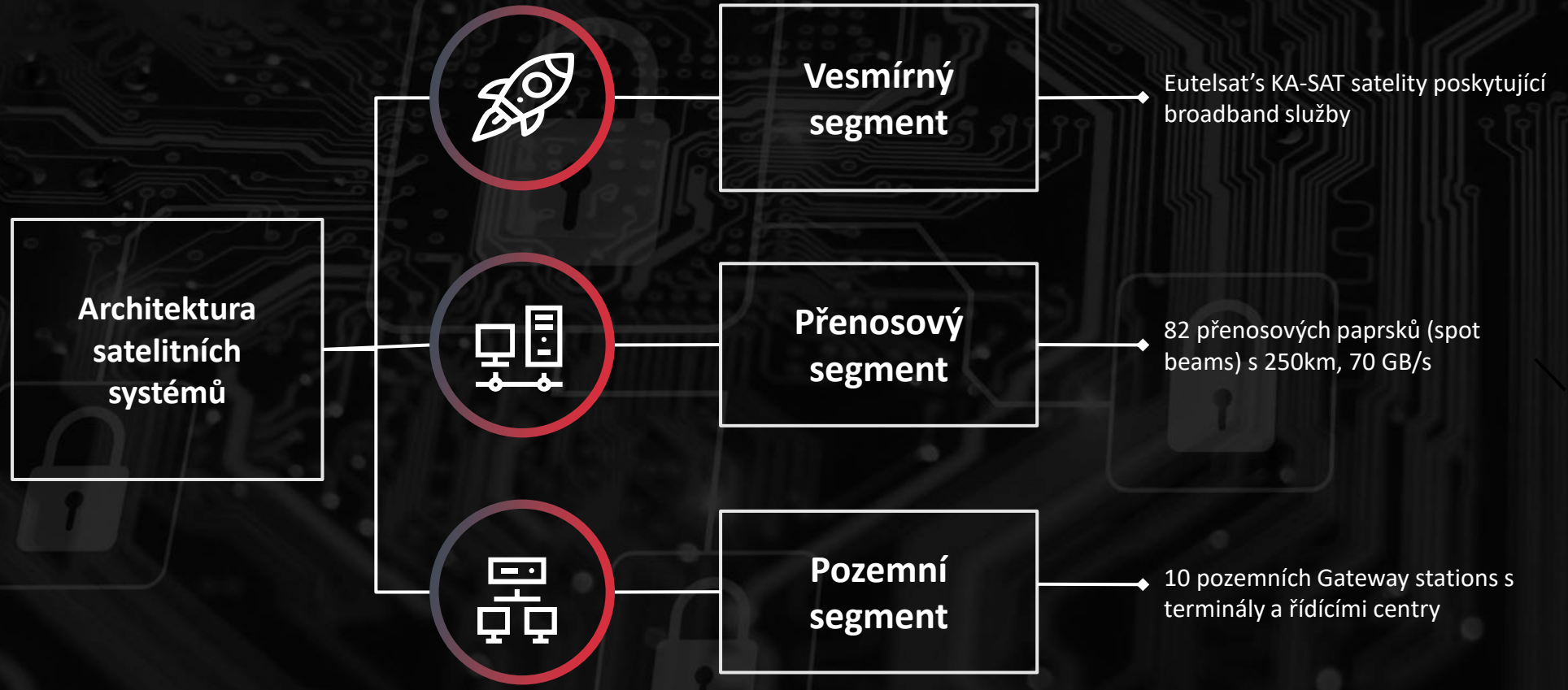
4# Bezpečná architektura

5# Shrnutí

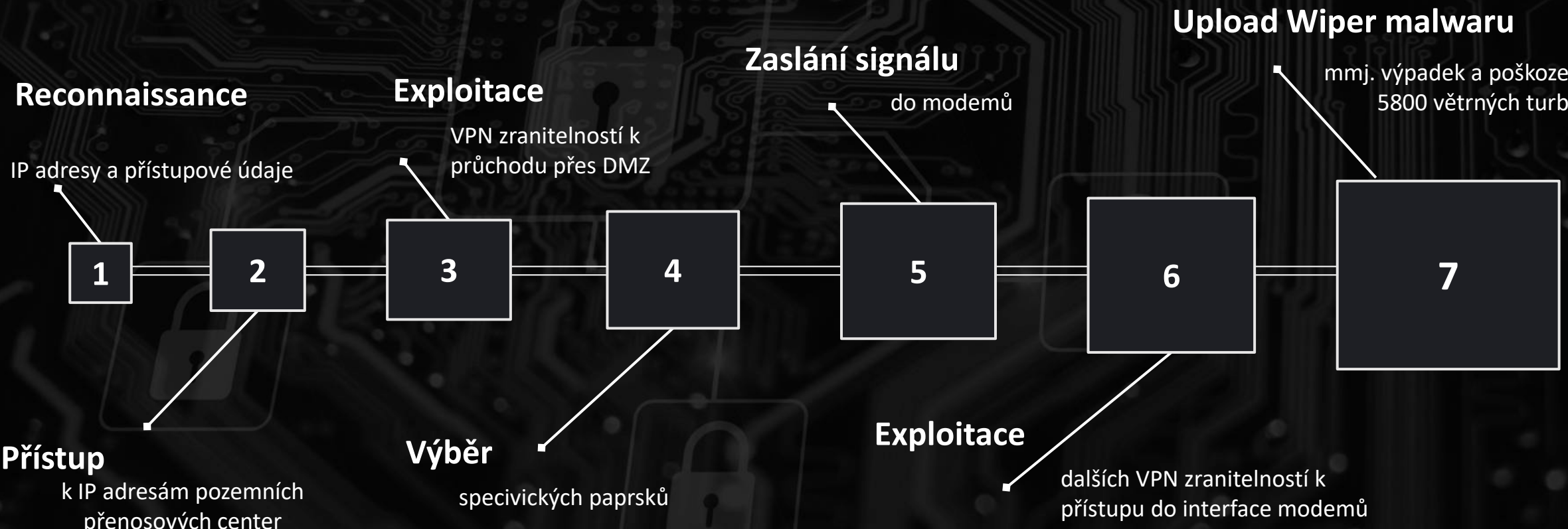
1# Cyber Incident

Ponaučení z kybernetického incidentu na spol. Viasat

Viasat Cyber Incident



Viasat Cyber-Attack Chain



~5800

nefunkčních větrných turbín

Viasat Cyber-Attack Lessons Learned

Supply Chain Management

Absence znalosti zapojení třetích stran

Absence řízení rizik „dual-use“ tech.

Žádné audity třetích stran

Proaktivní monitoring

Zranitelná zařízení nebyla monitorována

Předchozí úniky dat nebyly zjištěny

Nedefinovány kritické komponenty

Patch management

Nepatchovaná zařízení

Software i firmware

Nekonzistence patch procesu

Incident response

Absence redundance

Žádný incident response proces

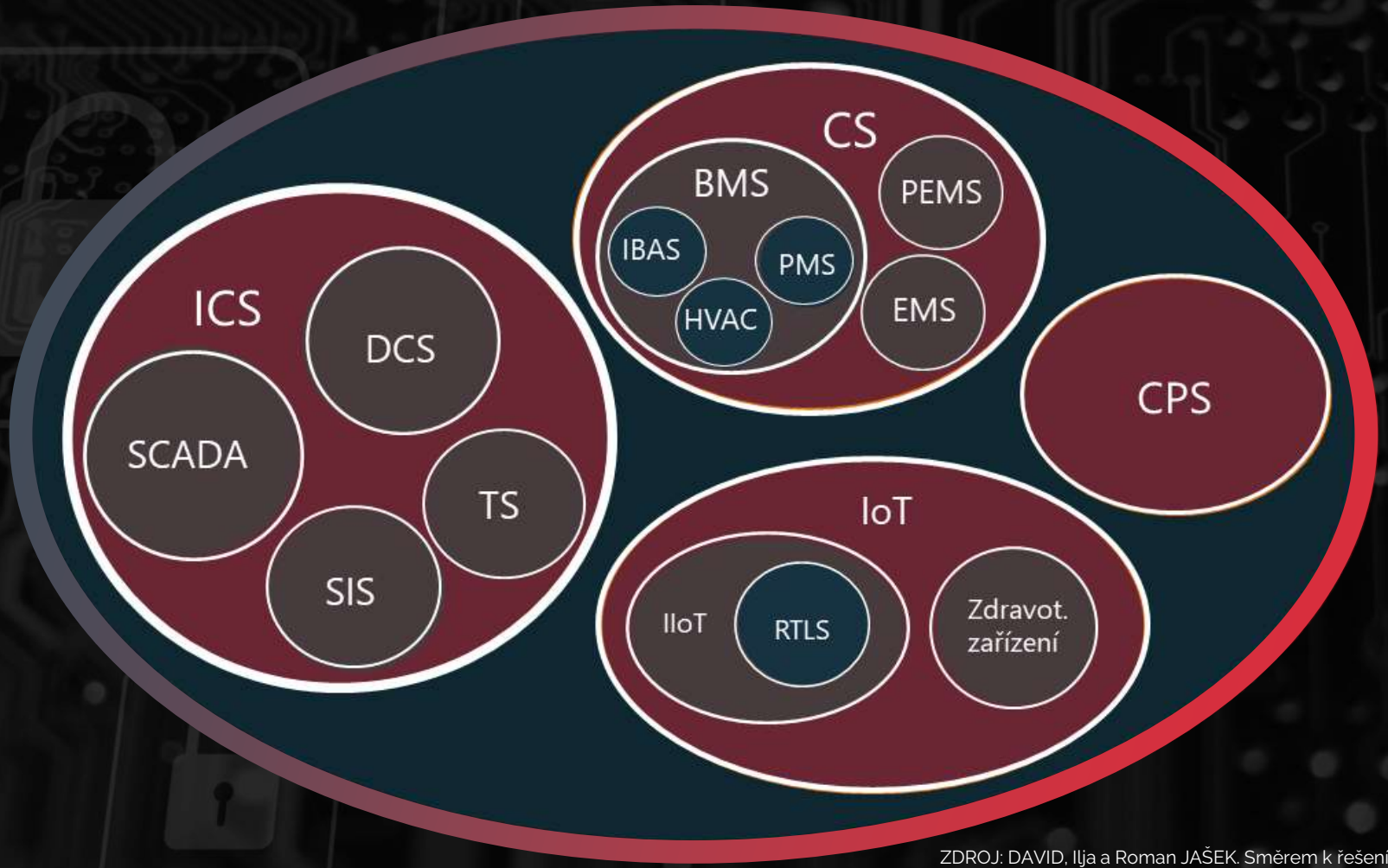
Absence BCP

2# Operational Technologies

Provozní technologie a jejich rozdíl od technologií informačních

Operational Technologies (OT)

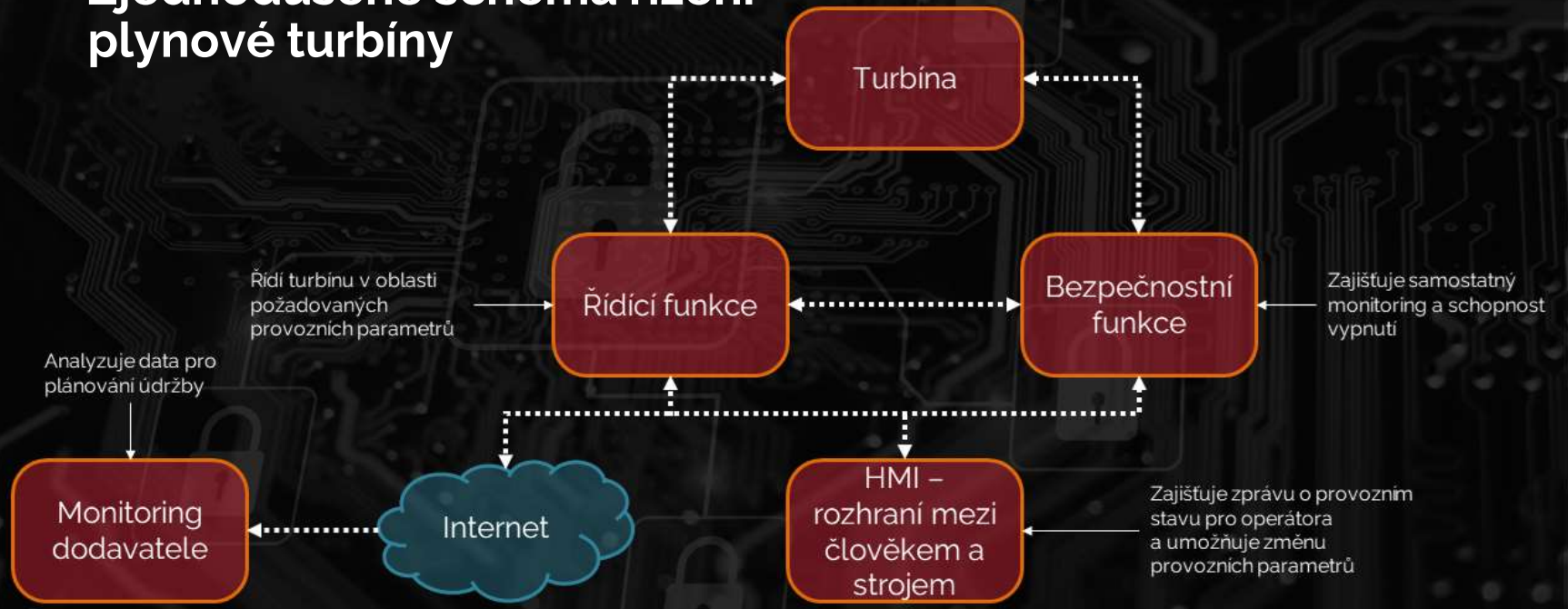
- Provozní technologie
- Zahrnují širokou škálu programovatelných systémů a zařízení, které interagují s fyzickým prostředím
- Široká definice
- Mnoho skupin a podskupin
- Vzájemné prolnutí
- Neustálý vývoj, konvergence i obohacení o IT
- V nZkb jako průmyslová, řídicí a obdobná specifická technická aktiva (dále jen jako „OT)

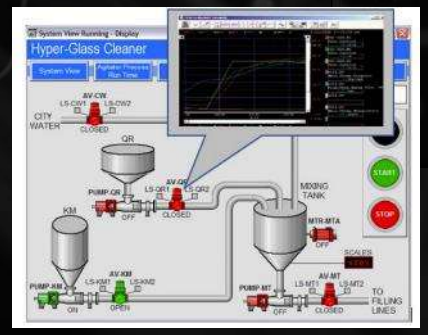


ZDROJ: DAVID, Ilja a Roman JAŠEK. Směrem k řešení OT kybernetické, Data Security Management., 10. ISSN 2336-6745

Architektura OT systému

Zjednodušené schéma řízení plynové turbíny



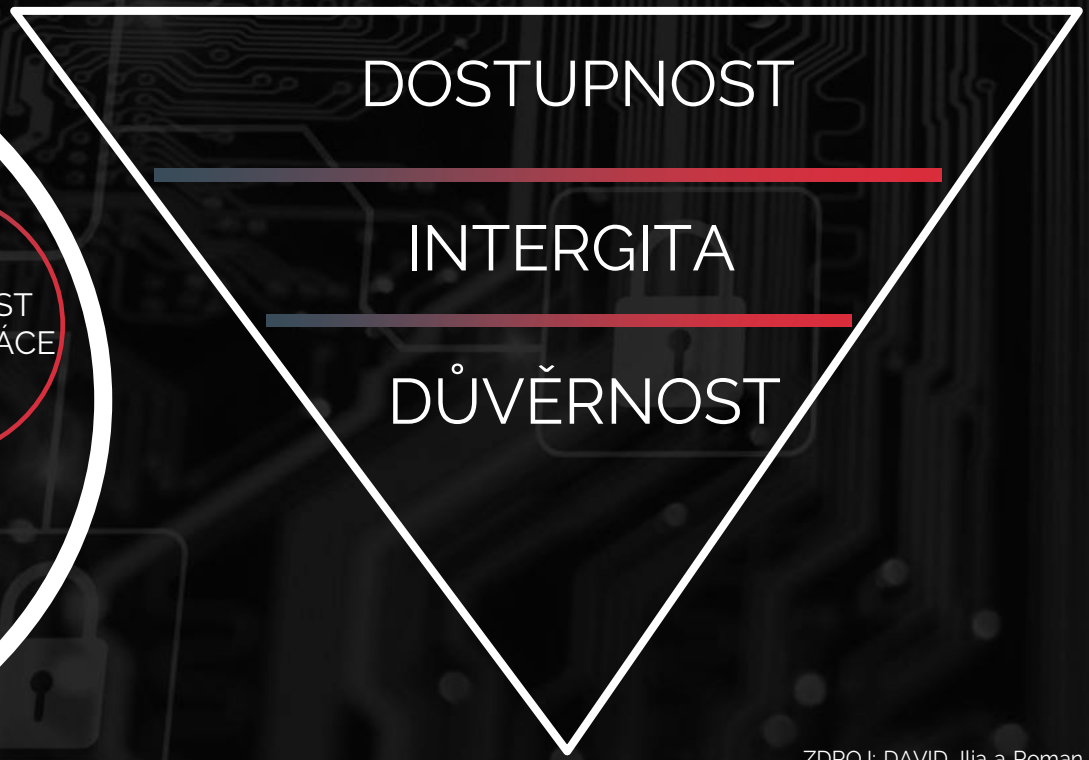


ZDROJ: XXXXXX

IT a OT divergence

z pohledu řízení bezpečnosti

ZDRAVÍ & BEZPEČÍ



ZDROJ: DAVID, Ilja a Roman JAŠEK. *Konvergence a divergence OT a ICT technologií ve vztahu ke kybernetické bezpečnosti.* Data Security Management. ISSN 2336-6745

Layers of Protection

Mitigation

Disaster Protection

Collection Basin

Overpressue Valve, Rupture Disk

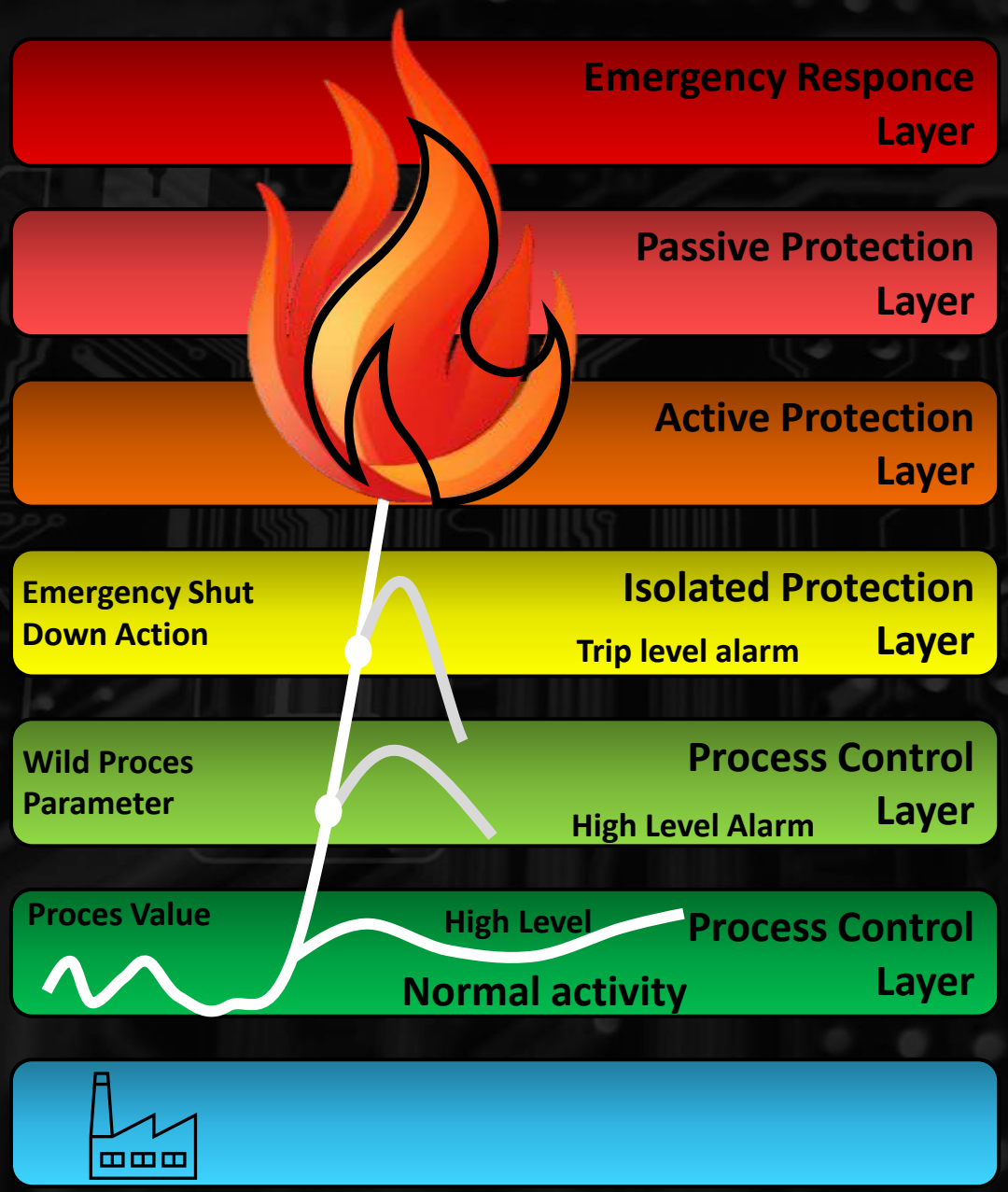
Prevention

Safety System (automatic)

Operaton Intervention

Basic Process Control System

Plant Design



IT a OT divergence

z pohledu řízení bezpečnosti

ZDROJ: DAVID, Ilja a Roman JAŠEK. *Konvergence a divergence OT a ICT technologií ve vztahu ke kybernetické bezpečnosti*. Data Security Management. ISSN 2336-6745

ISO 27001

Systém řízení informační bezpečnosti (ISMS)

IT Informační bezpečnost

Opatření pro řízení a administrativu procesů

Nedostatek technických řešení

OT není ani zmíněno

Vhodné k řízení kybernetické bezpečnosti OT?

NE

IEC 62443

Systém řízení kybernetické bezpečnosti (CSMS)

OT Kybernetická odolnost

Opatření pro řízení a technická bezpečnostní opatření

PERA model pro OT architektury

Kompenzační opatření

Vhodné k řízení kybernetické bezpečnosti OT?

ANO

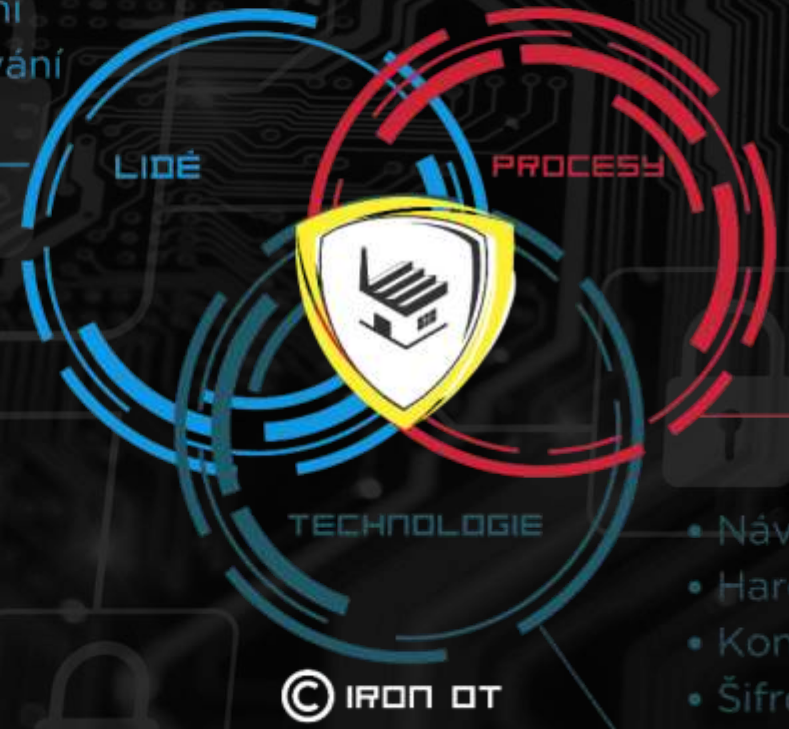
3#

IEC 62443

Praxí ověřená série standardů

3# Řízení průmyslové kybernetické bezpečnosti

- Školení a informovanost
- Odborné dovednosti a kvalifikace
- Bezpečnostní cvičení
- Autorizace a ověřování
- Fyzická bezpečnost



- Systémy řízení
- Legislativní rámce
- Politiky, standardy, procedury
- Smlouvy s třetími stranami
- Auditní režimy

- Návrh systému
- Hardening systémů
- Konfigurace softwaru
- Šifrovací protokoly
- Detekce a monitorování

> **IEC6 2443** poskytuje **ucelený systém standardů** pro **výrobce**, **provozovatele**, **systémové integrátory** a **poskytovatele služeb** souvisejících s OT

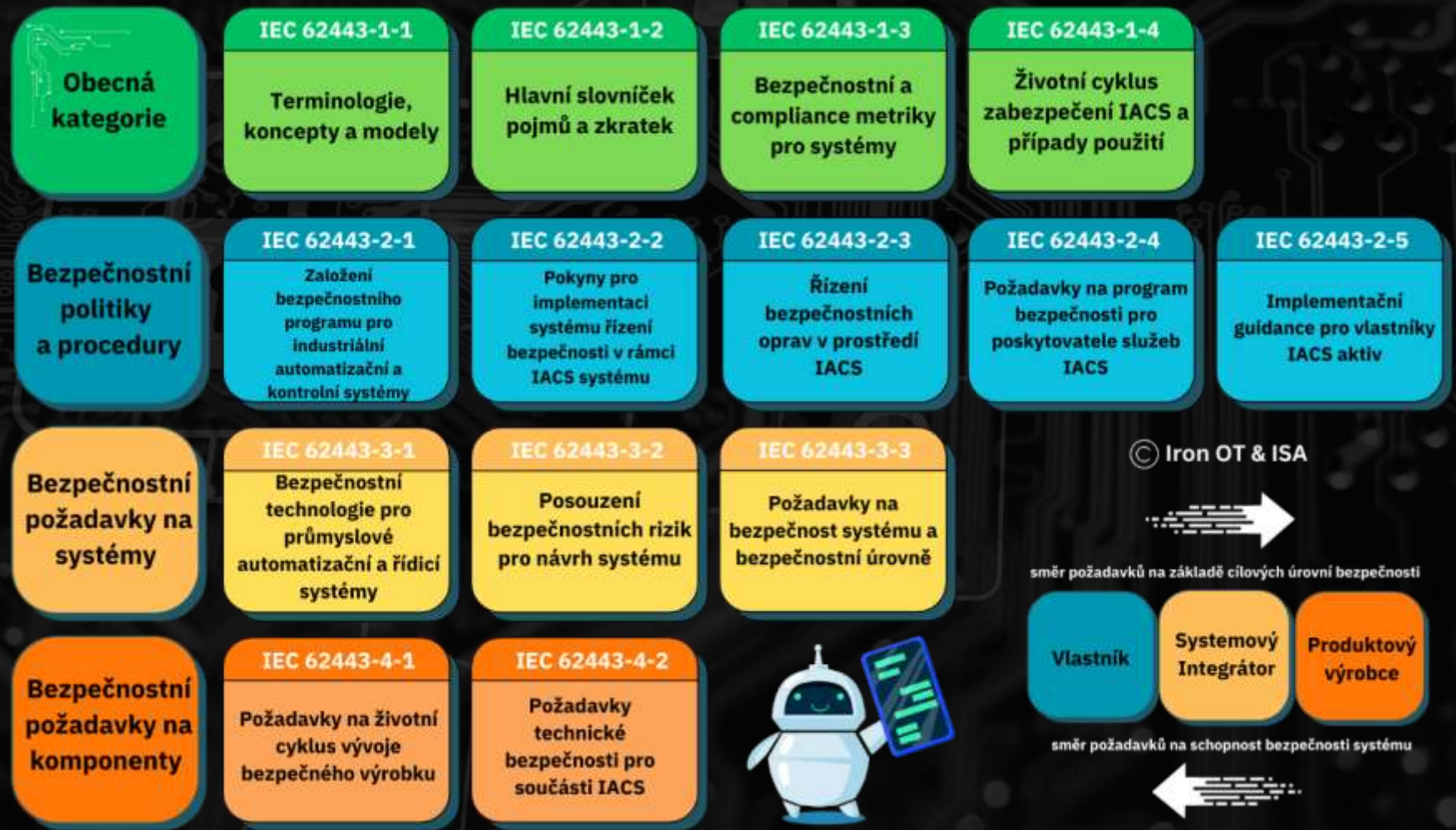
> Cílem je řešit **technologie**, **procesy** a **lidský element** současně

> Kombinace **správných procesů** a **správných technologií** je **klíčová**

ZDROJ: DAVID, Ilja a Luděk LUKÁŠ. *Řešení kompenzačních opatření kybernetické bezpečnosti dle norem IEC 62443.* Data Security Management, ISSN 1211-8737.

IEC 62443 ucelený přehled

- Ucelený systém standardů IEC6 2443 existuje přes 20 let, poskytuje pro **výrobce**, **provozovatele**, **systémové integrátory** a **poskytovatele služeb** souvisejících s OT
- Cílem je řešit technologie, procesy a lidský element současně (holistický přístup), **neustálý rozvoj**, vznikají další odnože (např. pro rozvodny či železnice).



Obrázek: Série standardů IEC 62443

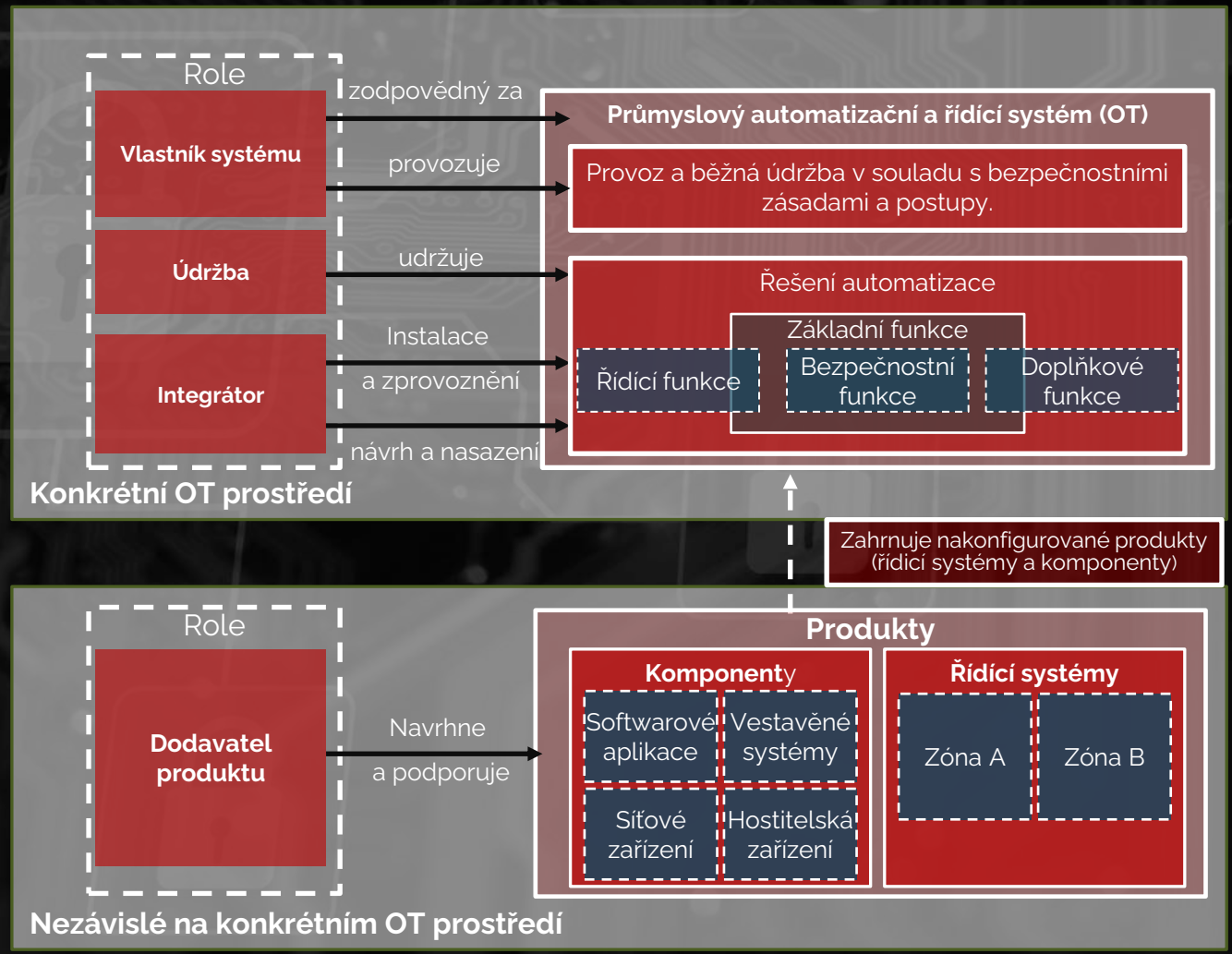
IEC 62433 - Životní cyklus výrobku

Životní cyklus návrhu produktu	Životní cyklus systémů průmyslové automatizace a kontrolních systémů	
	Návrh a integrace	Provoz a údržba
IEC 62443-1-1 Terminologie, koncepty a modely		
	IEC 62443-2-1 Založení bezpečnostního programu pro industriální automatizační a kontrolní systémy	
	IEC 62443-2-2 Pokyny pro implementaci systému řízení bezpečnosti v rámci IACS systému	
IEC 62443-2-3 Řízení bezpečnostních oprav v prostředí IACS		
	IEC 62443-2-4 Požadavky na program bezpečnosti pro poskytovatele služeb IACS	
	IEC 62443-3-2 Posouzení bezpečnostních rizik pro návrh systému	
IEC 62443-3-3 Požadavky na bezpečnost systému a bezpečnostní úrovně		
IEC 62443-4-1 Požadavky na životní cyklus vývoje bezpečného produktu		
IEC 62443-4-2 Požadavky technické bezpečnosti pro součásti IACS		

Tabulka: Vztah norem IEC 62443 k životnímu cyklu OT systémů

Vztah mezi rolemi, produkty, a OT systémy v rámci IEC 62443

- Ucelený systém standardů IEC 62443 existuje přes 20 let, poskytuje pro **výrobce**, **provozovatele**, **systémové integrátory** a **poskytovatele služeb** souvisejících s OT



Obrázek: Integrace jednotlivých rolí zodpovědných za životní cyklus OT systémů dle standardů IEC 62443

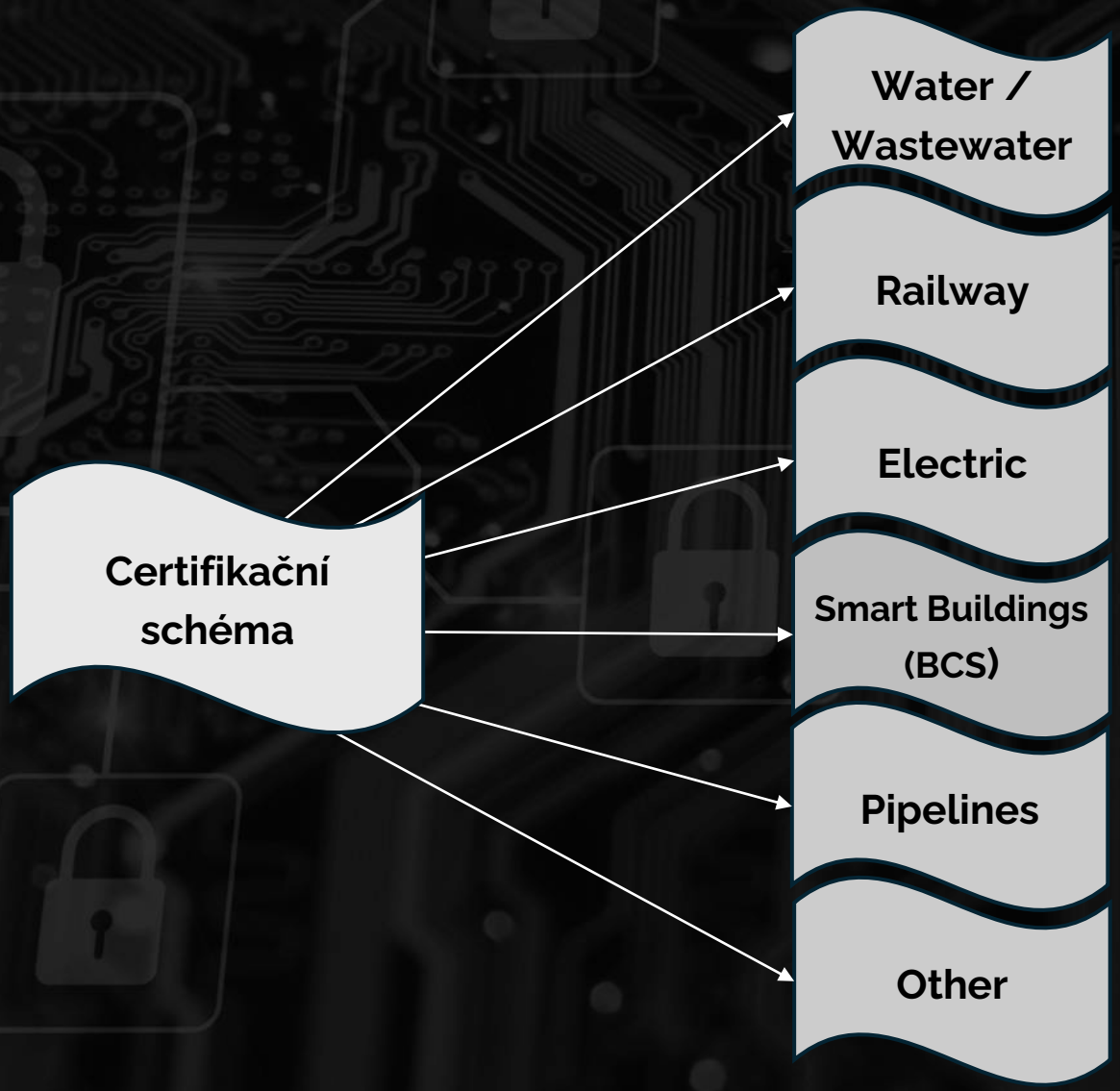
Vybrané významné části IEC 62443

Obecná kategorie	**IEC 62443-1-1**	Poskytuje **obecný přehled a definice** používané v celé sérii IEC 62443. Cílem je zajistit pochopení celého standardu ve správném kontextu. Zaměřuje se na základní principy jako je integrita, dostupnost a důvěrnost dat v průmyslových systémech
Bezpečnostní politiky a procedury	**IEC 62443-2-1**	Je zaměřena na požadavky a směrnice pro **řízení bezpečnostních politik a procedur v rámci organizace**, klade důraz na správu a implementaci bezpečnostních prvků, jako jsou identifikace rizik, management bezpečnostních událostí a školení zaměstnanců.
Bezpečnostní politiky a procedury	**IEC 62443-2-4**	Požadavky na **program bezpečnosti, které musí splňovat poskytovatelé služeb** v oblasti průmyslových automatizačních a řídicích systémů (IACS), aby zajistili ochranu před kybernetickými hrozbami.
Bezpečnostní požadavky na systémy	**IEC 62443-3-3**	Pokrývá požadavky na **bezpečnostní opatření a postupy na úrovni systému**. Zaměřuje se na návrh a implementaci bezpečnostních architektur, včetně segmentace sítě a aplikace bezpečnostních mechanizmů. Každý z těchto požadavků je přiřazen k jedné ze čtyř úrovní zabezpečení (SL1 až SL4), které určují, jak komplexní a odolné proti útokům musí být zabezpečení.
Bezpečnostní požadavky na komponenty	**IEC 62443-4-2**	Věnuje se bezpečnostním **požadavkům pro softwarové a hardwarové komponenty systému**. Obsahuje směrnice pro vývoj, údržbu a zajištění bezpečnosti komponentů během celého jejich životního cyklu.

Tabulka: Podrobnější popis hlavní IEC 62443 norem

IEC TS 62443-1-5 – Schémata pro IEC 62443 bezpečnostní profily (Security Profiles)

- Technická norma je v současné době ve fázi návrhu
- Některé jsou již hotové
- Profil: sada a podmnožina charakteristik ze společného definovaného rámce pro specifické aplikace
- Klíčové koncepty:
  - 62443-1-5 Tabulka A.1 definuje obsah profilu minimálního zabezpečení
    - Může být založen na jedné nebo více normách 62443
    - Výběry na základě vyhodnocení bezpečnostních rizikKontextové mapování pro konkrétní aplikační doménu
    - Žádné nové požadavky či jejich úprava požadavků, pouze jejich aplikace na konkrétní odvětví
    - Může vybrat minimální úroveň zabezpečení a/nebo úroveň splatnosti
    - Publikováno jako technická zpráva




4#
Bezpečná
architektura
Kybernetická bezpečnost OT je proveditelná
IRON OT
COMGUARD

Základní kroky k ochraně OT systémů

Krok 1.

- Analýza stávajícího stavu organizace a systémů

Krok 2.

- Posouzení kybernetických rizik OT organizace a systémů

Krok 3.

- Zjištění rozdílu mezi aplikovanými bezpečnostními požadavky a požadovaným stavem
- Implementace chybějících bezpečnostních požadavků

Krok 4.

- Zajištění dlouhodobého udržitelného řízení
- Pravidelné vyhodnocování s cílem zlepšení

- Iterace k vyřešení rozdílu

Obrázek: Zjednodušený souhrn základních kroků implementace OT kybernetické bezpečnosti

Identifikace kritických systémů

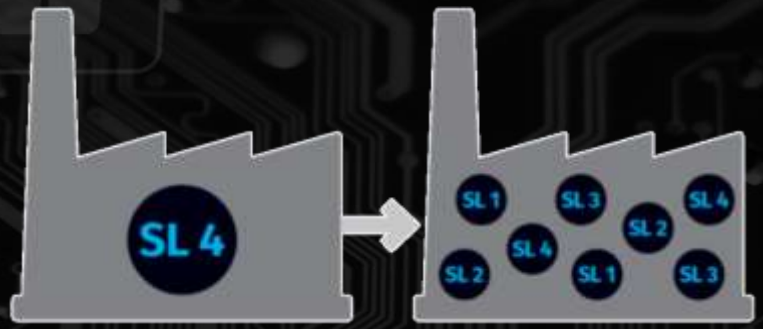
- **Inventarizace systémů**
- Co je **kritické** pro závod, zařízení, továrnu, prvek KI atd.
- Co chránit a s jakým rozsahem **bezpečnostních požadavků**
- **Rozlišit OT od IT systémů** (seskupení pro jednoduchost)
- Konektivita, přístupnost, CIA elementy
- **Scénáře nejhorších případů** (kritičnost)
- Výsledkem je **seznam systémů** s hodnocením kritičnost
- Poté definice **bezpečnostních zón** a zaměřit se dále na to, co je pro organizaci nejkritičtější

System	Location	Vendor	Connected with other systems?	Remote connection?	Possibility to update/upgrade ?	Physical accessibility?
System A	Location 1	Vendor X	Y	Y	Y	Y
System B	Location 2	Vendor Y	N	Y	N	N

ZDROJ: DAVID, Ilja a Luděk LUKÁŠ. *Řešení kompenzačních opatření kybernetické bezpečnosti dle norem IEC 62443.* Data Security Management, ISSN 1211-8737.

Bezpečnostní úrovně

- Úroveň bezpečnosti nastavuje rozsah aplikovaných bezpečnostních požadavků na OT systémy (nebo efektivněji na **bezpečnostní zónu**)
- Tímto přístupem lze dosáhnout bezpečnosti pro různé **systémy od více dodavatelů**, starší systémy atd.
- Organizace si může vytvořit **vlastní definici úrovní bezpečnost**i vč. vlastního mat, výpočtu pro každou úroveň
- Doporučují se alespoň **3 úrovně bezpečnosti** (organizace může tento počet zvýšit)
- IEC 62443 pracuje s pěti úrovněmi a **třemi stavy** (SL-T, SL-A, SL-C)



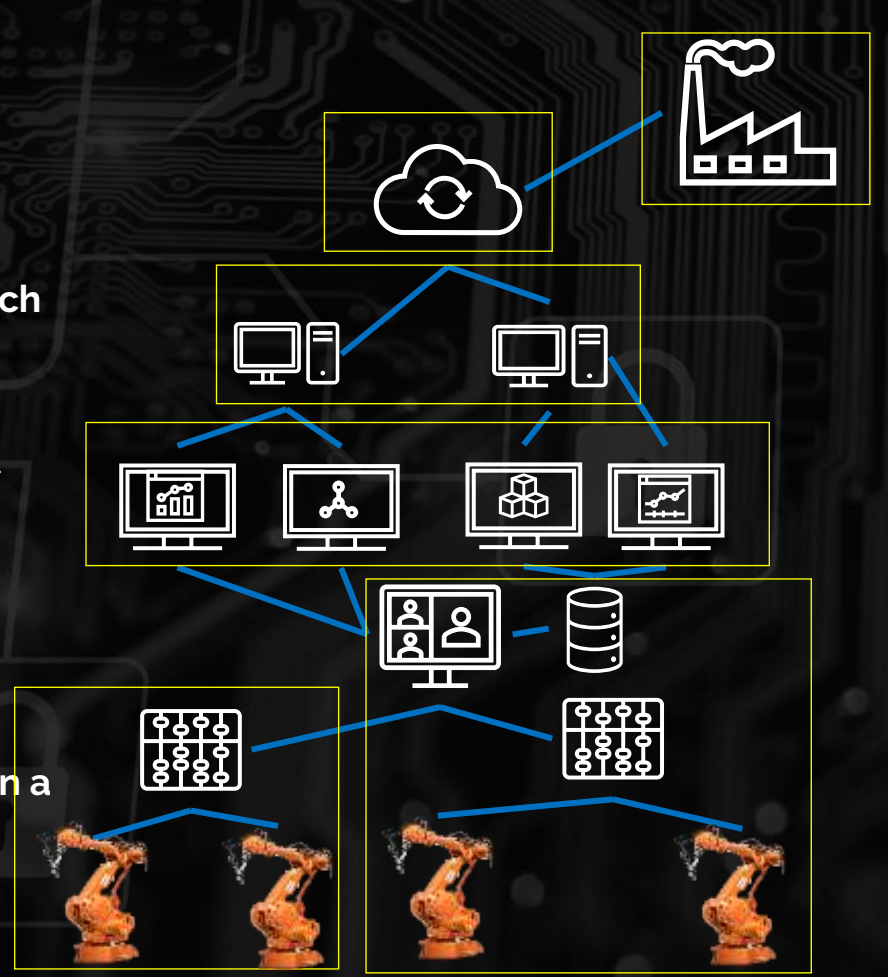
Security Level	Ochrana proti	Skilly	Motivace	Prostředky	Zdroje
SL-0	Nejsou nutné žádné zvláštní požadavky ani bezpečnostní ochrana				
SL-1	Příležitostné popř. náhodné porušení	Žádné útočné dovednosti	Spíše chyby	Neúmyslné	Indivudální
SL-2	Cybercrime, Hackeři	Obecné	Nízké	Jednoduché	Nízké (isolovaný jedinec)
SL-3	Hacktivisté, Teroristé	OT specifické	Střední	Sofistikované (Útok)	Střední (Hackerská skupina)
SL-4	Národní státy	OT specifické	Vysoká	Sofistikované (APT, kampaň)	Veliké (multidisciplinární týmy

ZDROJ: DAVID, Ilja a Luděk LUKÁŠ. *Řešení kompenzačních opatření kybernetické bezpečnosti dle norem IEC 62443*. Data Security Management, ISSN 1211-8737.

Bezpečnostní zóny a konduity

- Bezpečnostní **zóny seskupují systémy**, **komponenty**, **zařízení**, **procesy** atd., které sdílejí **stejnou úroveň** bezpečnosti
- Zóny mají definované **úrovně zabezpečení**
- Pro každou úroveň platí jinak **veliká sada bezpečnostních požadavků**
- Cílem je segmentovat různé systémy uvnitř IT/OT sítě a vytvořit **architekturu s prvky a procesy kybernetické bezpečnosti**
- **Modulární**, **škálovatelný** a **flexibilní** systém
- Mělo by být popsáno ve **speciálním nákresu** (nákres **zón a konduitů** – Zones and Conduits drawing)

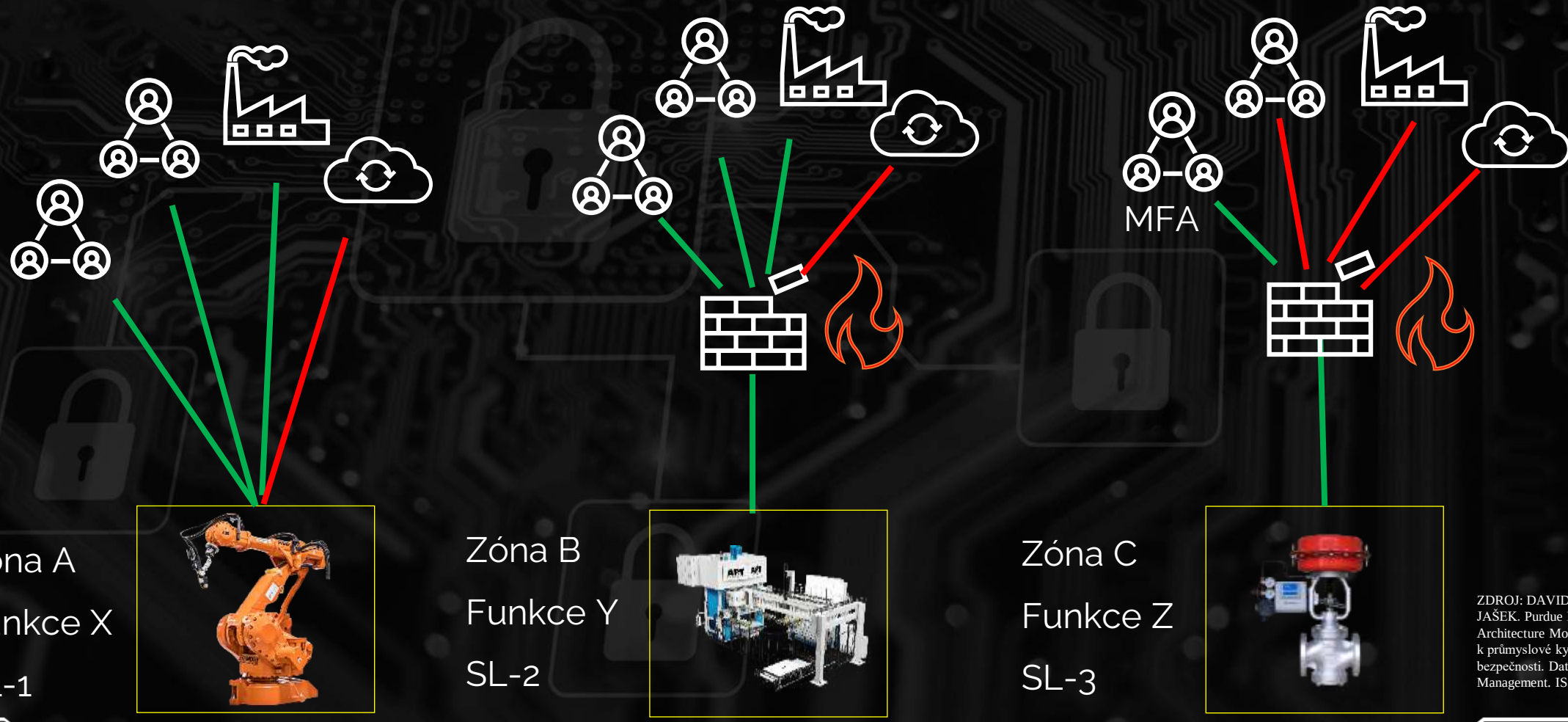
Note: Educational example



ZDROJ: DAVID, Ilja a Roman JAŠEK. Koncept zón a konduitů pro zajištění bezpečnosti provozních technologií (OT) - část 1. Data Security Management. ISSN XXXX

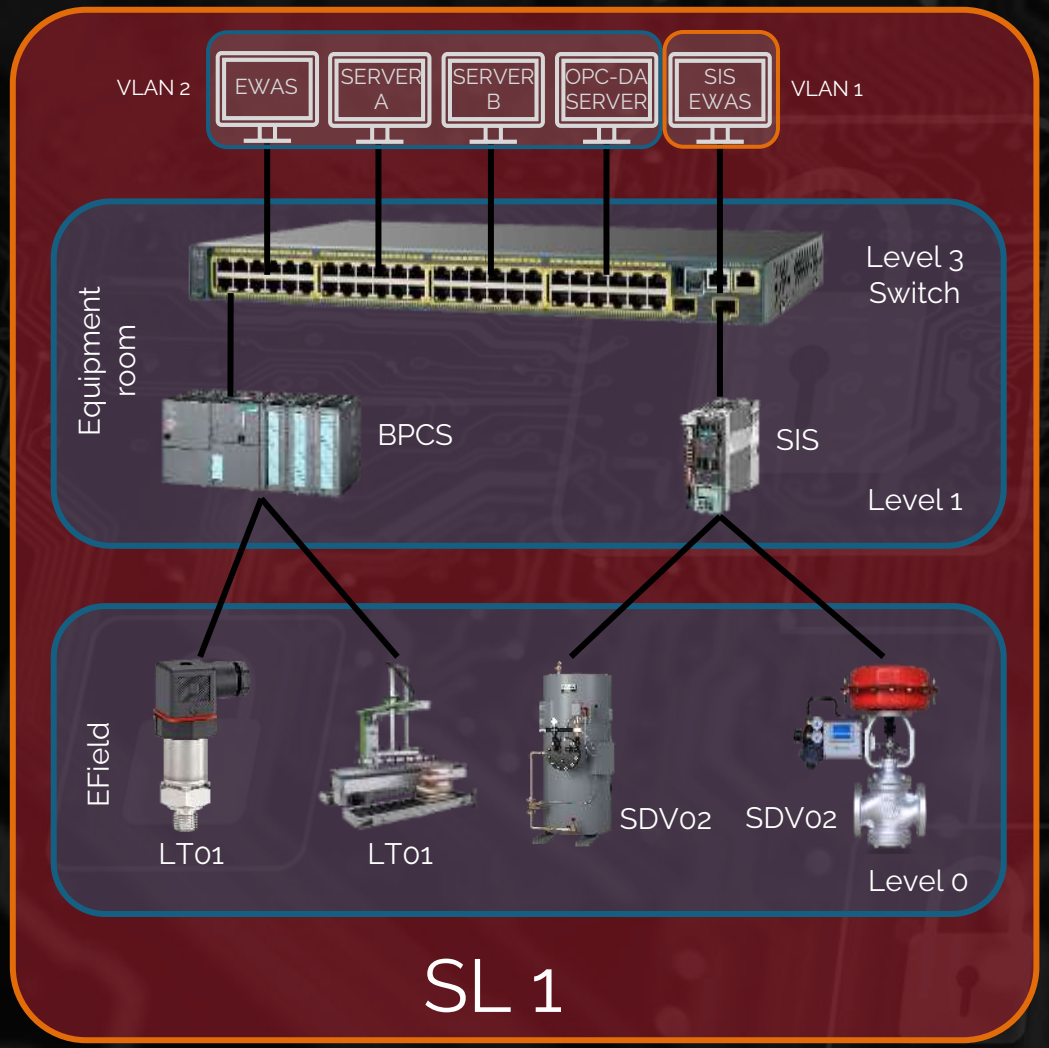
Aplikace bezp. požadavků

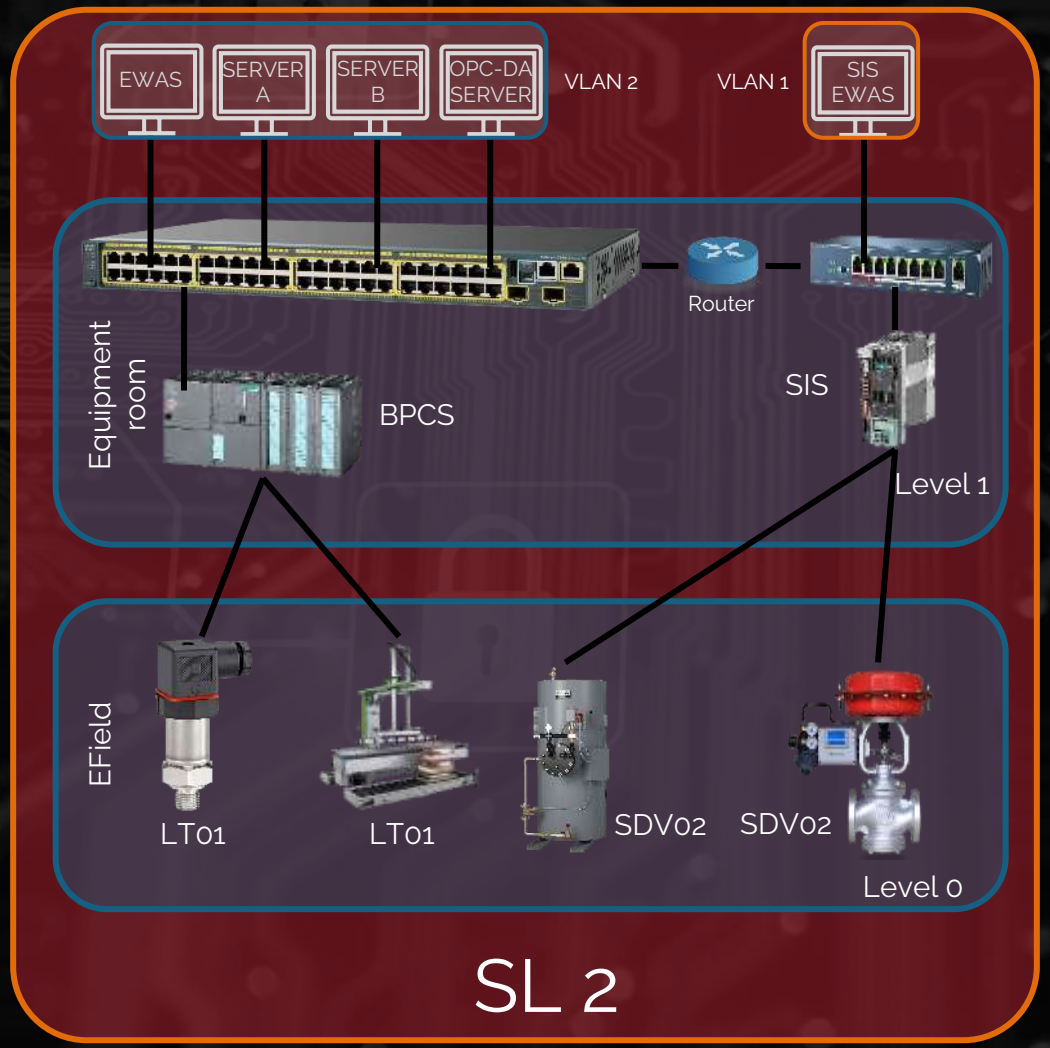
Note: Educational example



ZDROJ: DAVID, Ilja a Roman JAŠEK. Purdue Enterprise Architecture Model ve vztahu k průmyslové kybernetické bezpečnosti. Data Security Management. ISSN 2336-6745

Aplikace bezp. požadavků

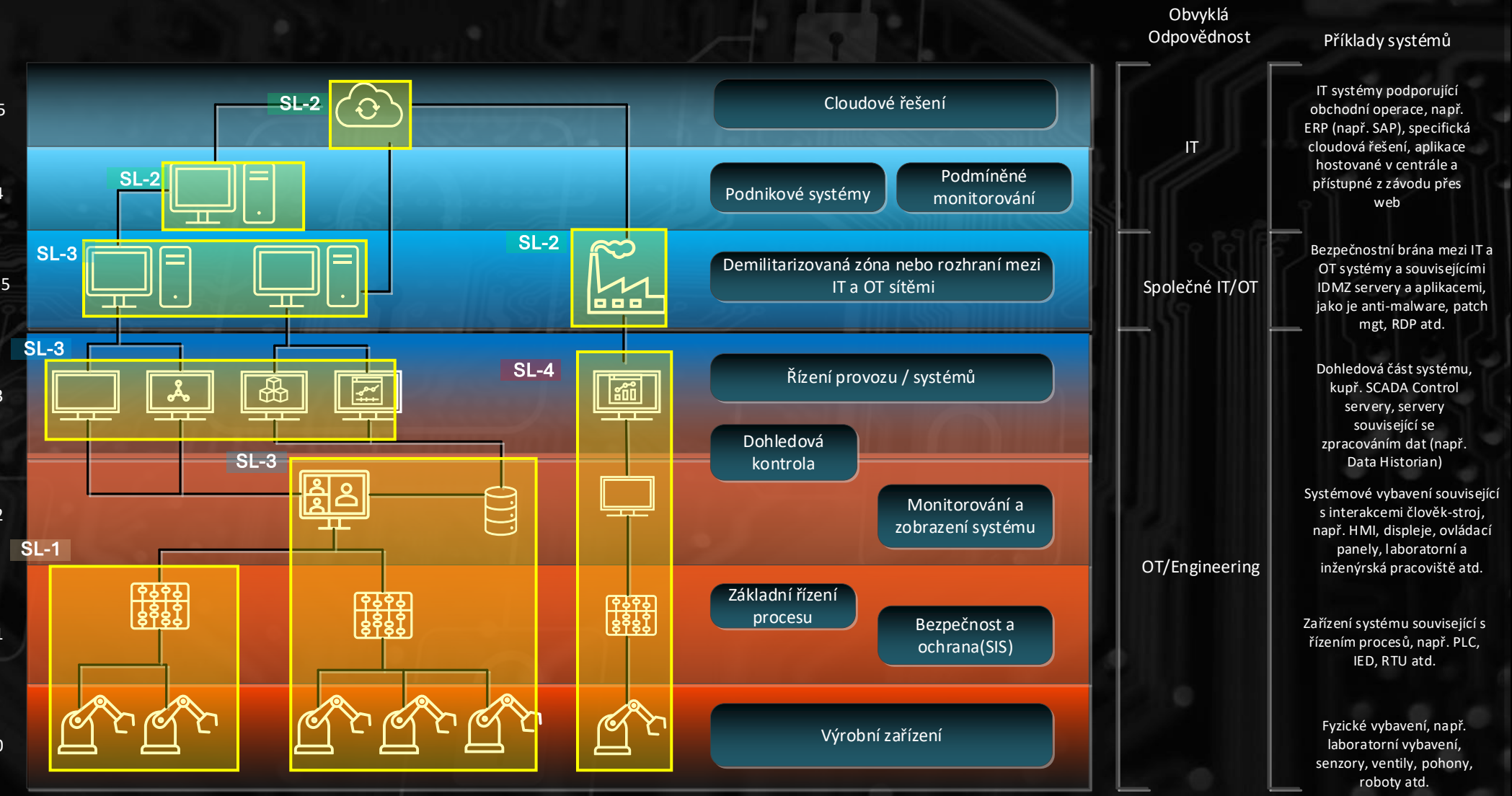




ZDROJ: Iron OT

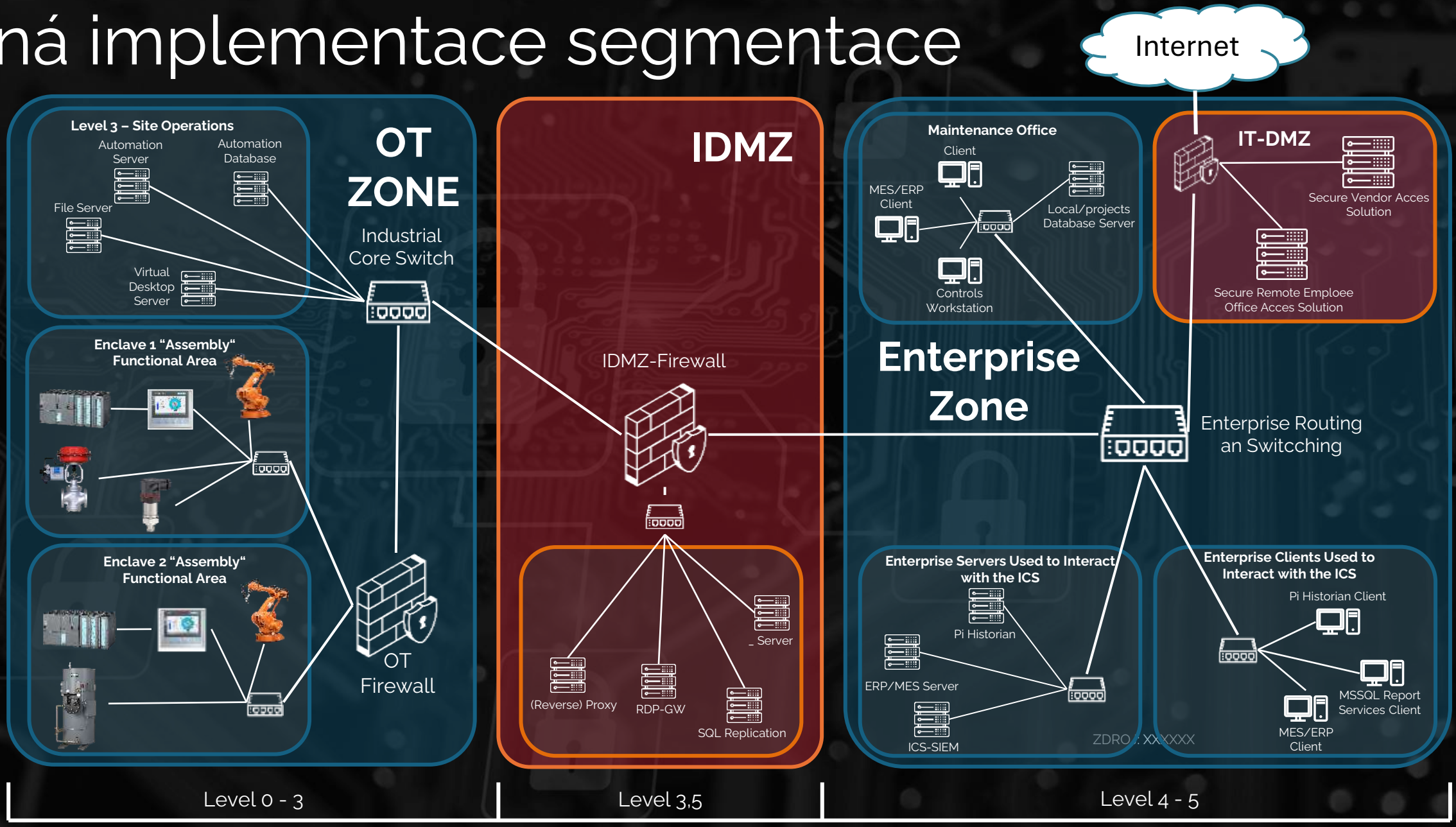
Řešení OT kybernetické bezpečnosti IEC 62443

- Zobrazení bezpečné architektury na základě IEC 62443 v modelu PERA
- Tzv. nákres Zón a konduitů
- Přehled nad architekturou a systémy = přehled nad bezpečností



Obrázek: Bezpečná architektura dle IEC 62443 v modelu PERA (ukázkový příklad)

Reálná implementace segmentace sítě



5#
Shrnutí

Shrnutí: implementační strategie OT bezpečnosti

- Na základě předchozích informací lze určit **strategické kroky vpřed** pro zajištění OT bezpečnosti:
  - Krok 1: **posoudit kybernetická rizika** OT systémů, určit které jsou kritické, určit bezpečnostní úrovně a rozdíl mezi stávajícím a očekávaným stavem
  - Krok 2: vytvořit **nákresy zón a konduitů**
  - Krok 3: vytvořit či zlepšit **politiku kybernetické bezpečnosti** IT/OT a související procesy (např. dle IEC 62443);
  - Krok 4: **redesign sítí** a **implementace bezpečnostních zařízení** na ochranu kritických OT systémů
  - Krok 5: zajistit **dlouhodobé řízení**, **monitorování** a **školení** uplatňované bezpečnostní politiky a souvisejících opatření.
- Pokud je to možné, měly by být některé bloky rozděleny podle osvědčených postupů do dvou částí:
  1. **Modelový závod či modelová zóńa (nová výrobní linka, retrofit projekt atp.**
  2. **Zbytek závodů či zón**

NAPIŠTE NÁM, JSME TU PRO VÁS

Neváhejte nám dát vědět, pokud budete potřebovat cokoliv dovysvětlit.

Jsme tu pro Vás a pomůžeme Vám, abyste s bezpečností měli jen minimum starostí.

KONTAKT:

email: info@ironot.io

telefon: +420 737 650 625

web: www.ironot.io

LinkedIn:

NAŠE VIZE

Již nyní se podílíme na ochraně organizací v České republice a Evropské unii, a tím na bezpečnosti celé naší lidské společnosti, a v tom bychom chtěli pokračovat, jak nejlépe dovedeme.

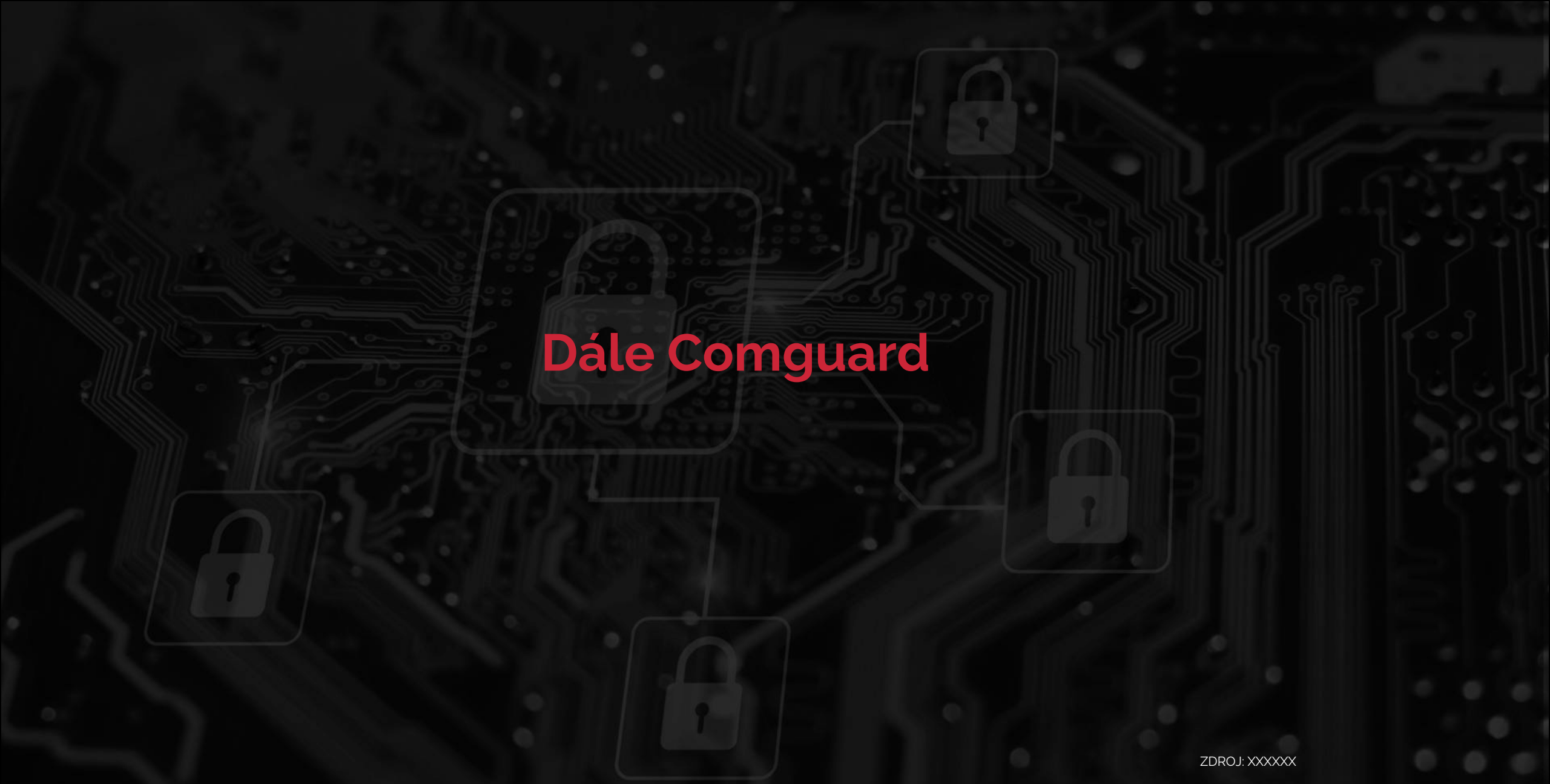
Primárně se zaměřujeme na kritickou infrastrukturu a průmyslové podniky. Dbáme na soulad bezpečnosti organizace s jejím provozem a zavádíme bezpečnostní opatření přesně úměrné rizikovému profilu organizace – ani více, ani méně, než je skutečně potřebné. Tímto jí tak pomáháme zajistit efektivní a bezpečný provoz nejen dnes, ale i v budoucnu.

Chceme, aby naše řešení byla jednoduchá, účinná a pro organizace snadno pochopitelná. Vše děláme s cílem dlouhodobé spolupráce a zachování vysoké úrovně důvěry a spolehlivosti.

No. 1 OT Security Company in Czech Republic

European Union Security Company

Dále Comguard



ZDROJ: XXXXXX

Honeywell SCADAfence

Monitoring OT sítě

- **Přehled o OT sítích**, komunikačních vzorcích, odhalení potencionálních útoků
- **Asset Management**
- **Monitoring síťového provozu**
- Proaktivně upozorňuje na **zranitelnosti** a **hrozby** v OT síti

- **Centrální management** pro více SCADAfence nebo pro sledování jednotlivých lokalit.
- Agregace informací z několika lokalit a sběr informace z ostatních bezpečnostních systémů
- **Reporting** - zobrazení real-time a generický reportů
- **Podpora standardů** a **legislativa** – IEC62443, NIS2

Reference:

TOYOTA

VESTEL

TARO

Ocenění:

Gartner COOL VENDOR

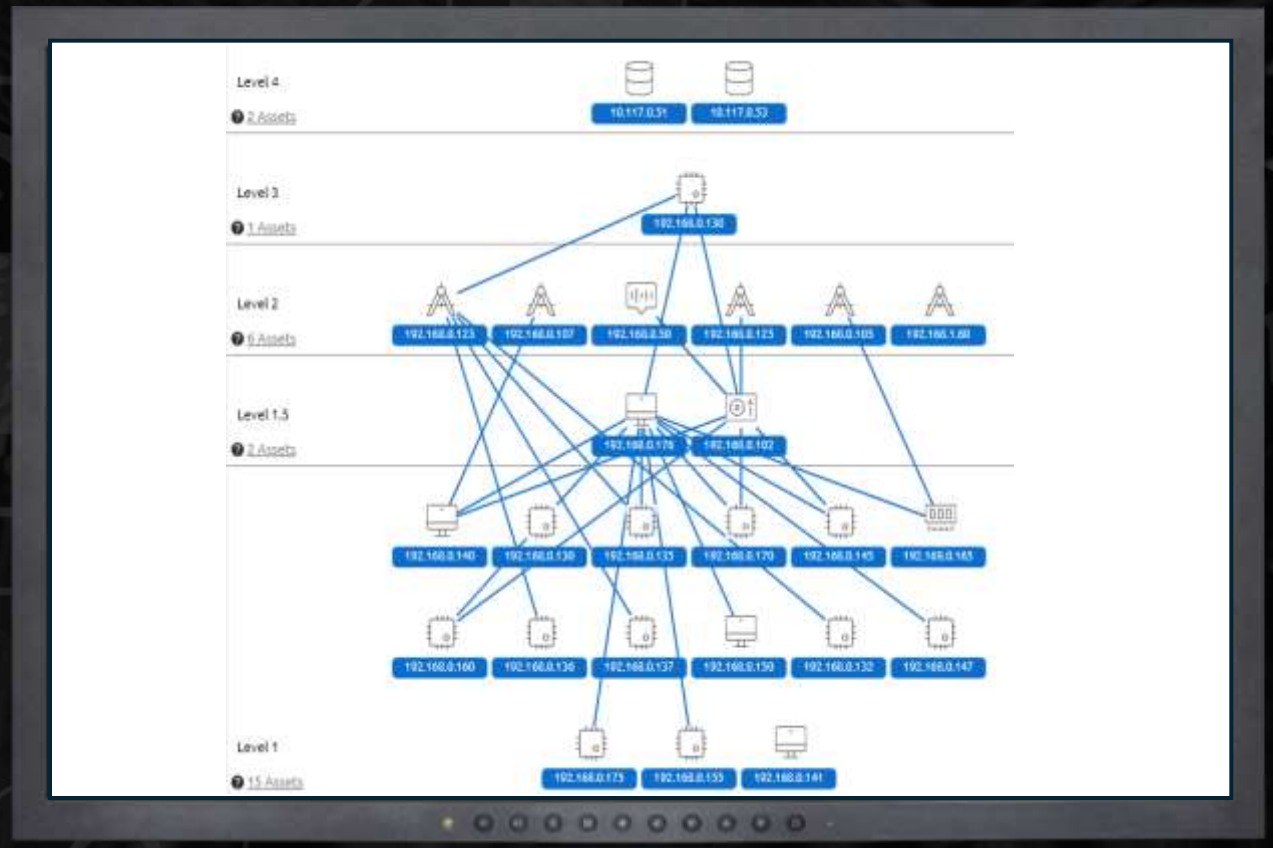
FROST & SULLIVAN

SCawards 2021 WINNER

ISG

Klíčové vlastnosti SCADAfence

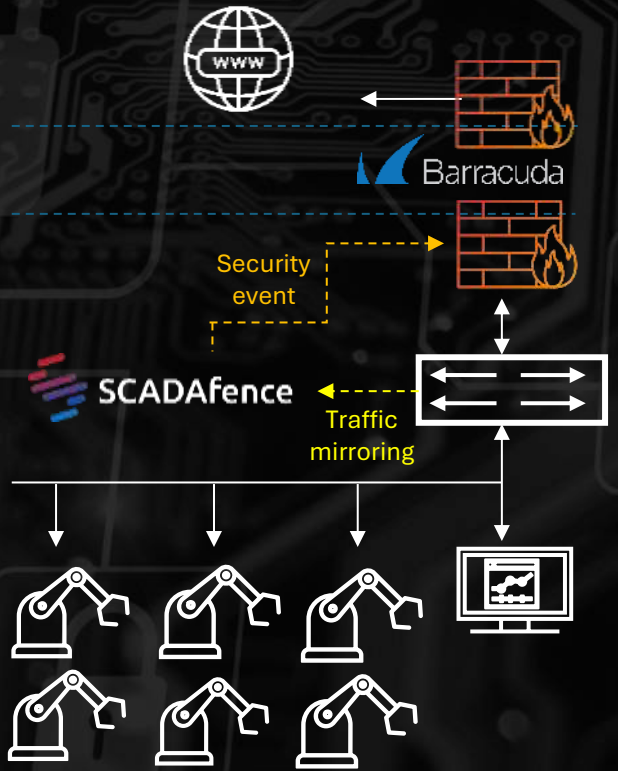
- > Detekce hrozeb
- > Podpora řízení rizik
- > Asset Management
- > Bezpečný vzdálený přístup
- > Integrace s dalšími nástroji
- > Agregace dat z více lokací



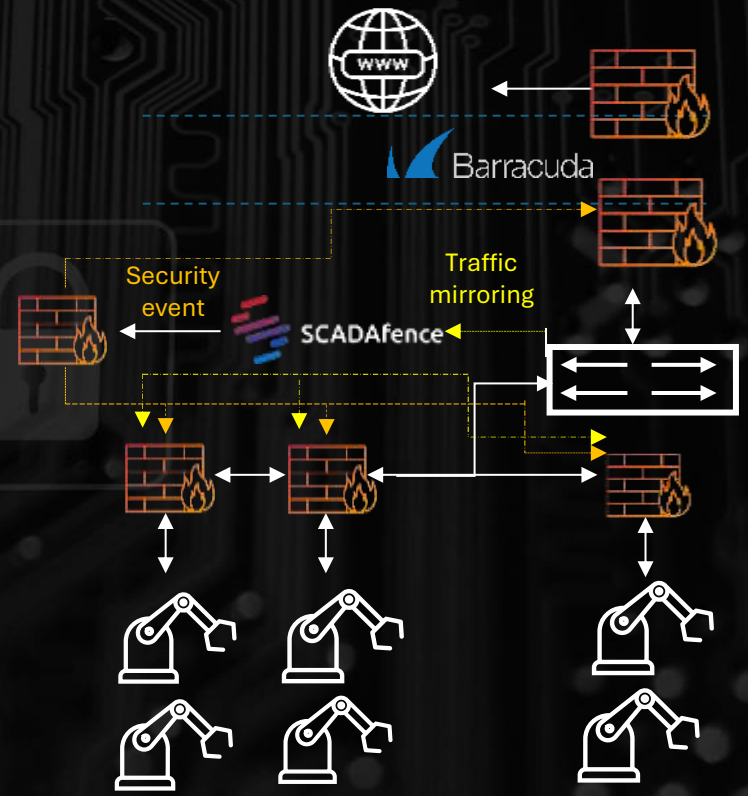
Barracuda Průmyslové firewally

- Hardwarové zařízení do průmyslového prostředí.
- Podpora průmyslových protokolů
- Segmentace průmyslových sítí
- Nativní Honeywell SCADAfence a Barracuda FW integrace
- Integrovatelnost také s jinými zařízení

Detekce hrozeb

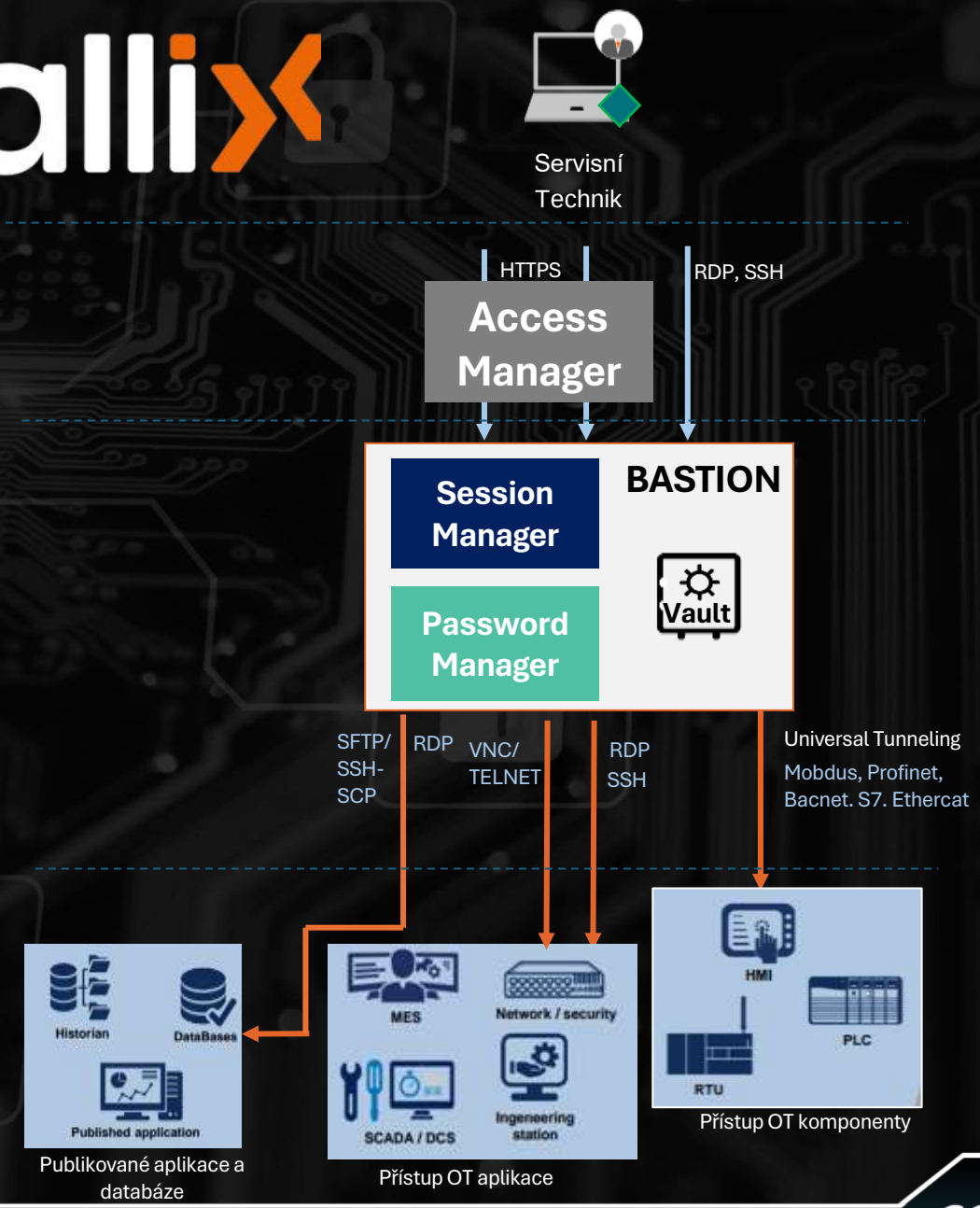


Mikrosegmentace



Řízení přístupů wallix

- Francouzská společnost s mezinárodní působnosti
- Leader v oblasti řízení přístupů PIM / PAM
- Silné zaměření na OT security
- Jednotné řešení pro řízení přístupů do často odlišných OT aplikací



Děkujeme za pozornost!

V oblasti OT Security jsme tu pro Vás

Ilja David

IRON OT
Secure The Industry Future

Ilja.david@ironot.io
+420 604 421 371
Ironot.io

https://www.linkedin.com/in/ilja-david/

Kamil Kosour

COMGUARD
cyber security masters

Kamil.kosour@comguard.cz
+420 602 129 569
Comguard.cz

IRON OT

Secure The Industry Future

Top Class Industrial Security, Resilience and Robustness

Iron OT je moderní bezpečnostní společnost nové generace specializující se v rámci Evropské unie na kybernetickou bezpečnost, odolnost a robustnost ochrany provozních technologií (OT) a souvisejících informačních technologií (IT).

- Kritická infrastruktura
- Všechny druhy průmyslů
- Zabezpečení SCADA, DCS, PLC, MES, robotů a další
- IT/OT konvergence
- Systémy řízení kybernetické bezpečnosti
- Posouzení a kompletní návrh řešení bezpečnosti
- Kompletní design bezpečnosti technologických celků
- Implementace frameworků IEC62443 / ISO27001 / NIS2 a mnoho dalších kategorií řešení:

The European Union Security Company

www.ironot.io

COMGUARD

cyber security masters

COMGUARD je Value Added Distributor (B2B) se specializací na IT bezpečnost. Působíme v České republice a na Slovensku. Naše komplexní řešení plně odpovídají potřebám velkých firem, včetně datových center, ale i menších a středních podniků.

- > Bezpečnost koncových stanic
- > Ochrana perimetru
- > Ochrana citlivých dat
- > Vyhodnocování potencionálních rizik
- > Kybernetická bezpečnost v průmyslovém prostředí
- > Správa privilegovaných uživatelů (PAM)
- > Penetrační testování
- > Security Operation Center (SOC)

Pro ochranu operačních technologií nabízí OT Guard, který spojuje několik technologií, které působí synergicky a dokážou pokrýt nejdůležitější oblasti v OT bezpečnosti.

Honeywell SCADAfence

Barracuda

wallix

www.comguard.cz


IRON OT
Secure The Industry Future