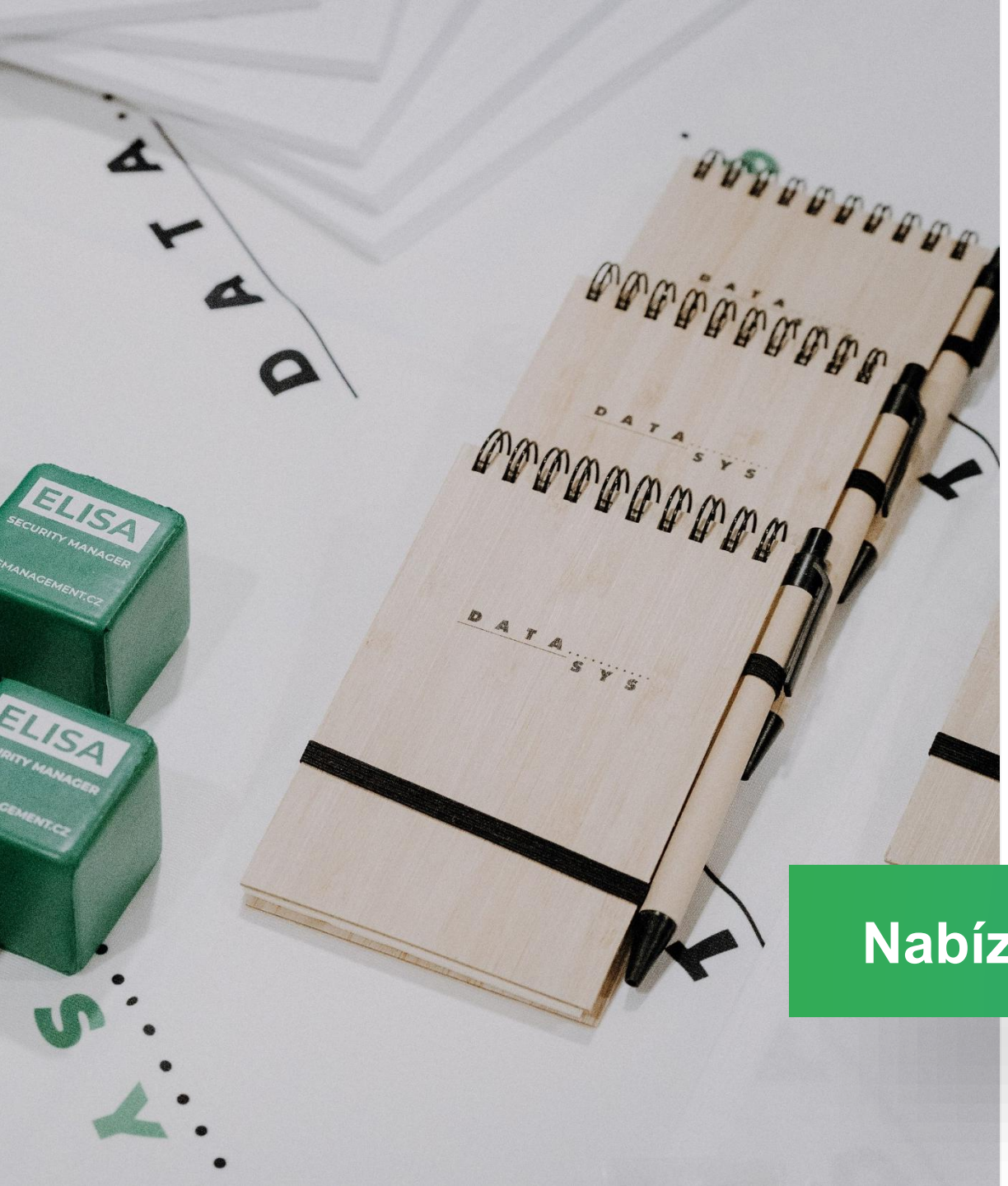
DATA SYS

Zálohy jsou jako Schrödingerova kočka Business Continuity pro provozní technologie

Igor STONAWSKI, Tomáš SLÍVA, Štěpán BÍNEK

+420 736 750 109 | stonawski@datasys.cz

+420 604 310 202 | sliva@datasys.cz



DATASYS

„Nejste v tom sami"

- Široké integrované portfolio řízených služeb.
- Dohledy, správa IT, SOC, outsourcing,
- Business Continuity Services
- 6 kroků k bezpečí Vašich dat

Nabízíme řešení, které fungují

DATA SYS

Realita zálohování

Stejně jako nelze dosáhnout 100% kybernetické bezpečnosti, nelze nikdy zaručit ani 100% úspěšnost obnovy.

- Zálohy jsou jako Schrödingerova kočka, nikdy nevíte, zda žijí, dokud krabici s nimi neotevřete.
- Pomůžeme Vám o ně pečovat a předcházet problémům.

CÍLEM NENÍ ZÁLOHA, CÍLEM JE OBNOVA

DATA SYS

Proč jsme tady?

- Máte Recovery nebo jen plán?
- Představíme řešení, které funguje
- Ukážeme, jak to reálně vypadá při přípravě OT prostředí na obnovu

KYBERNETICKÁ BEZPEČNOST NENÍ NIKDY 100%
PROTO JSOU ZÁLOHY A OBNOVA NEZASTUPITELNÉ

Víte kde všude máte OT zařízení
a na co mají vliv?

DATA SYS

Od ochrany dat k ochraně schopnosti fungovat

- Pozornost organizací se přesouvá od ochrany systémů k ochraně schopnosti poskytovat služby

Provozní technologie JSOU často kritičtější než samotné IT

- Ať už vyrábíte, léčíte, přepravujete nebo dodáváte energie – klíčová otázka zní:

  Jak rychle dokážete obnovit klíčovou službu po incidentu?

DATA SYS

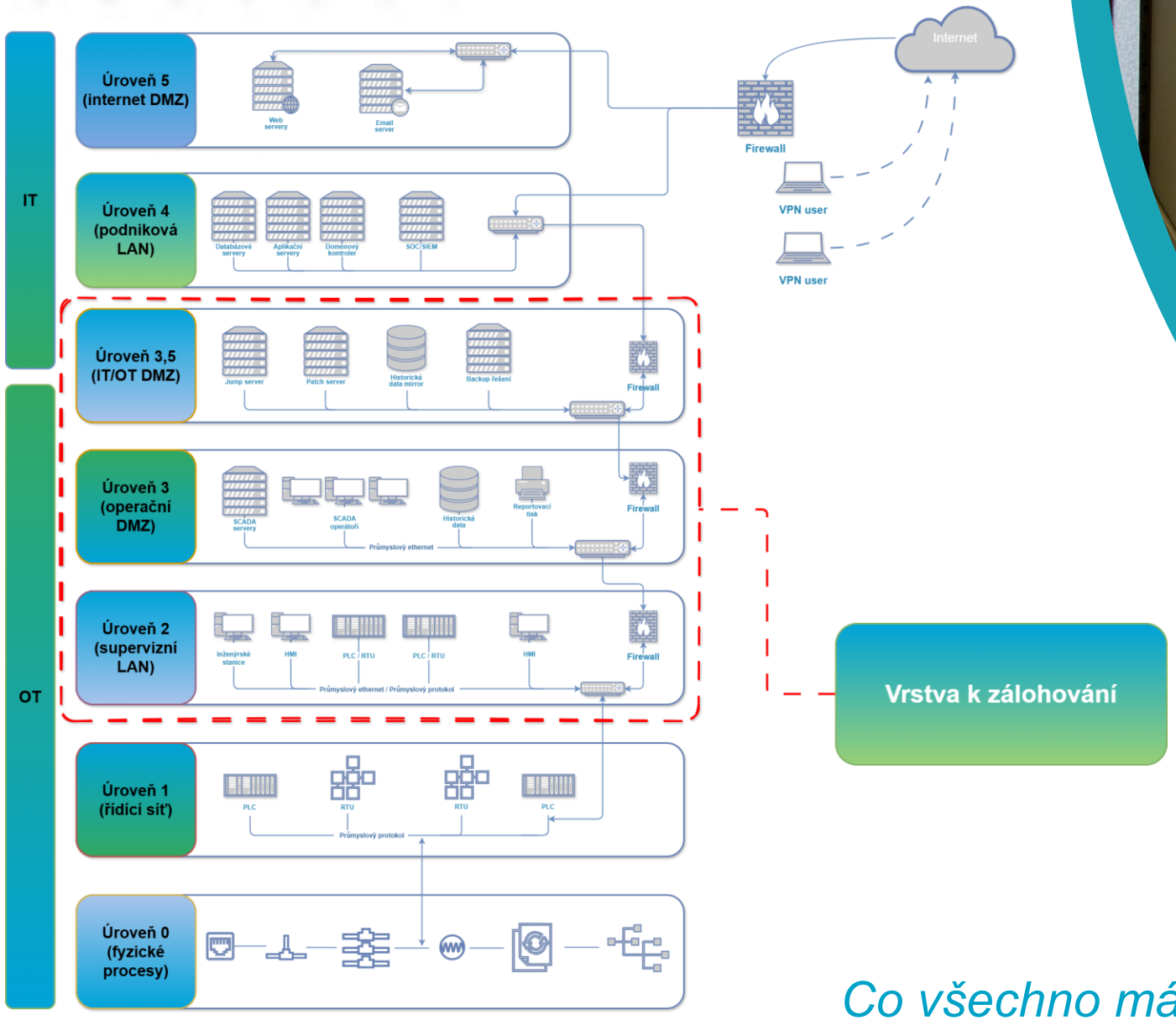
Funkčí obnova je základ

- Zákon č. 264/2025 Sb. (transpozice NIS2) přímo ukládá povinnost chránit klíčové služby a jejich aktiva
- § 4 se týká prakticky každého odvětví: veřejná správa, energetika, výrobní/potravinářský/chemický průmysl, vodní a odpadové hospodářství, doprava, digitální infrastruktura, finanční trh, zdravotnictví, věda/výzkum/vzdělávání, poštovní služby, obranný a vesmírný průmysl
- Rozdíl mezi „máme zálohu" a „dokážeme obnovit provoz" se ukáže přesně ve chvíli, kdy na tom nejvíc záleží

DATA SYS

Purdue Model – Tomáš Slíva

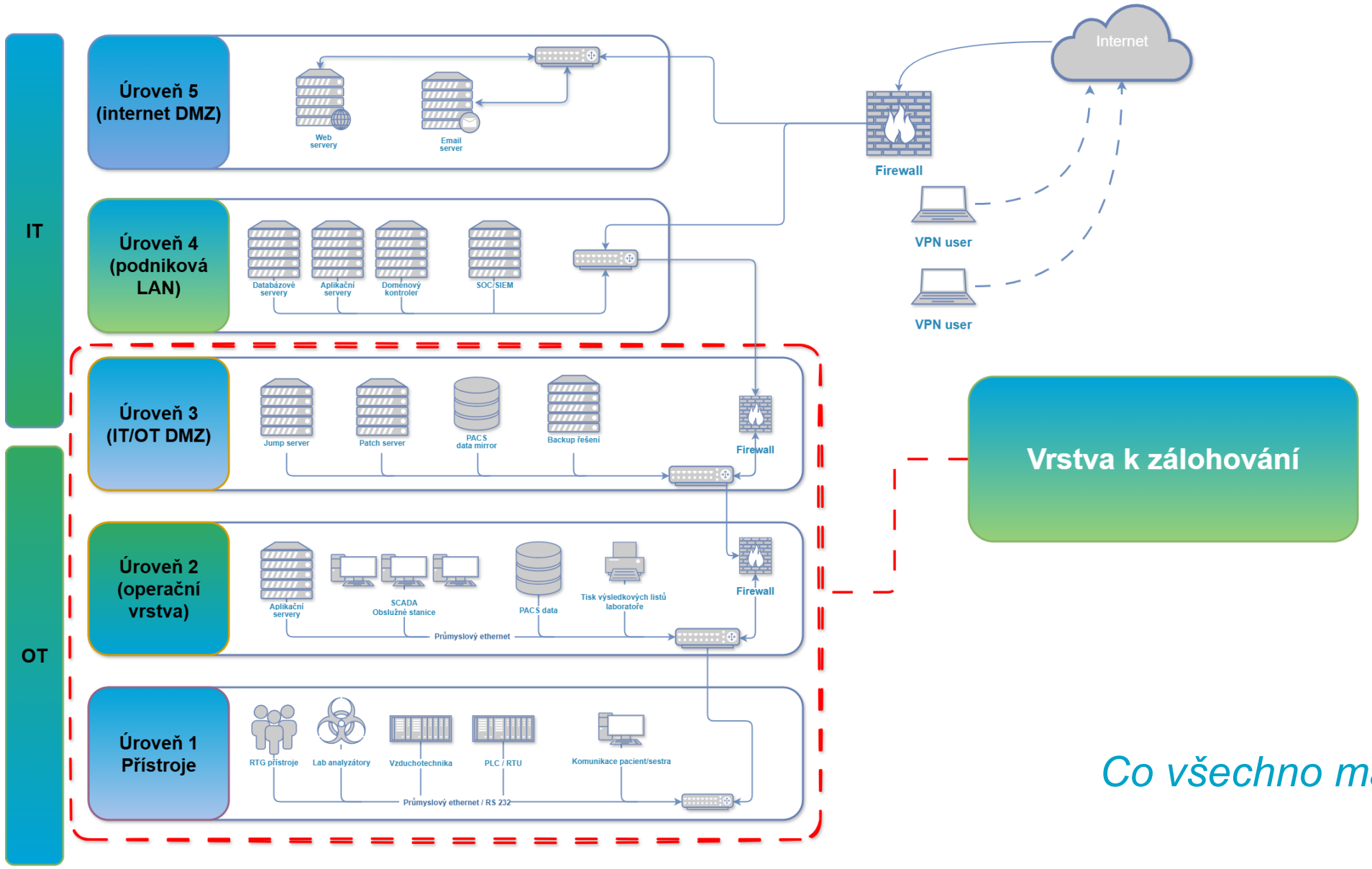
Základní schéma - průmysl



Co všechno máte v OT – víte to?

DATA SYS

Základní schéma-nemocnice



Co všechno máte v OT – víte to?

DATA SYS

Jak na to – Štěpán Bínek

Praktické dopady

Analýza - příklad dle prostředí

- Analýza OT aktiv & identifikace kritičnosti
  - *Kompletní mapování zařízení (PLC, HMI, SCADA, řídicí rozvaděče, řídící stanice)*
  - *Stanovení kritičnosti procesů z pohledu kontinuity výroby a obnovy po havárii*
- Sběr dat & pasivní analýza provozní sítě
  - *Nedestruktivní (pasivní) monitoring síťového provozu bez rizika ovlivnění výroby*
  - *Detekce nezdokumentovaných zařízení a probíhající komunikace (LoRa, GSM, RS232)*
- Vstupní workshop & Audit provozu
  - *Propojení klíčových rolí (IT, výroba, údržba)*
  - *Prohlídka fyzického prostředí a kontrola řídicích a operátorských stanic*
- Klíčové výstupy pro zálohování‘
  - ***Katalog OT aktiv** včetně prioritizace pro disaster recovery*
  - ***Návrh segmentace sítě** a prioritizovaná **roadmapa bezpečnostních opatření***

DATA SYS

Nejen „Co zálohovat?“, ale i „Kdo zodpovídá?“

- Předmět OT zálohování (Více než jen IT data)

  - Zálohovat je nutné konfigurace řídicích systémů (PLC), receptury a provozní nastavení, ne jen běžné databáze a systémy.
  - Je vyžadována důkladná analýza procesů a všech technologických vstupů.

- Specifika a limity OT prostředí

  - Nelze aplikovat běžné IT postupy – neuvážená aktualizace OS může odstavit celé řešení.
  - Historické vazby a architektura často znemožňují přímou obnovu na nový, moderní hardware.

- Odpovědnost a Shadow OT

  - Kdo má zálohy reálně na starosti? IT, provoz (zdravotní technika), nebo vnější dodavatel?
  - Riziko dodavatelských zásahů: Připojování zařízení do sítě bez vědomí IT oddělení.

DATA SYS

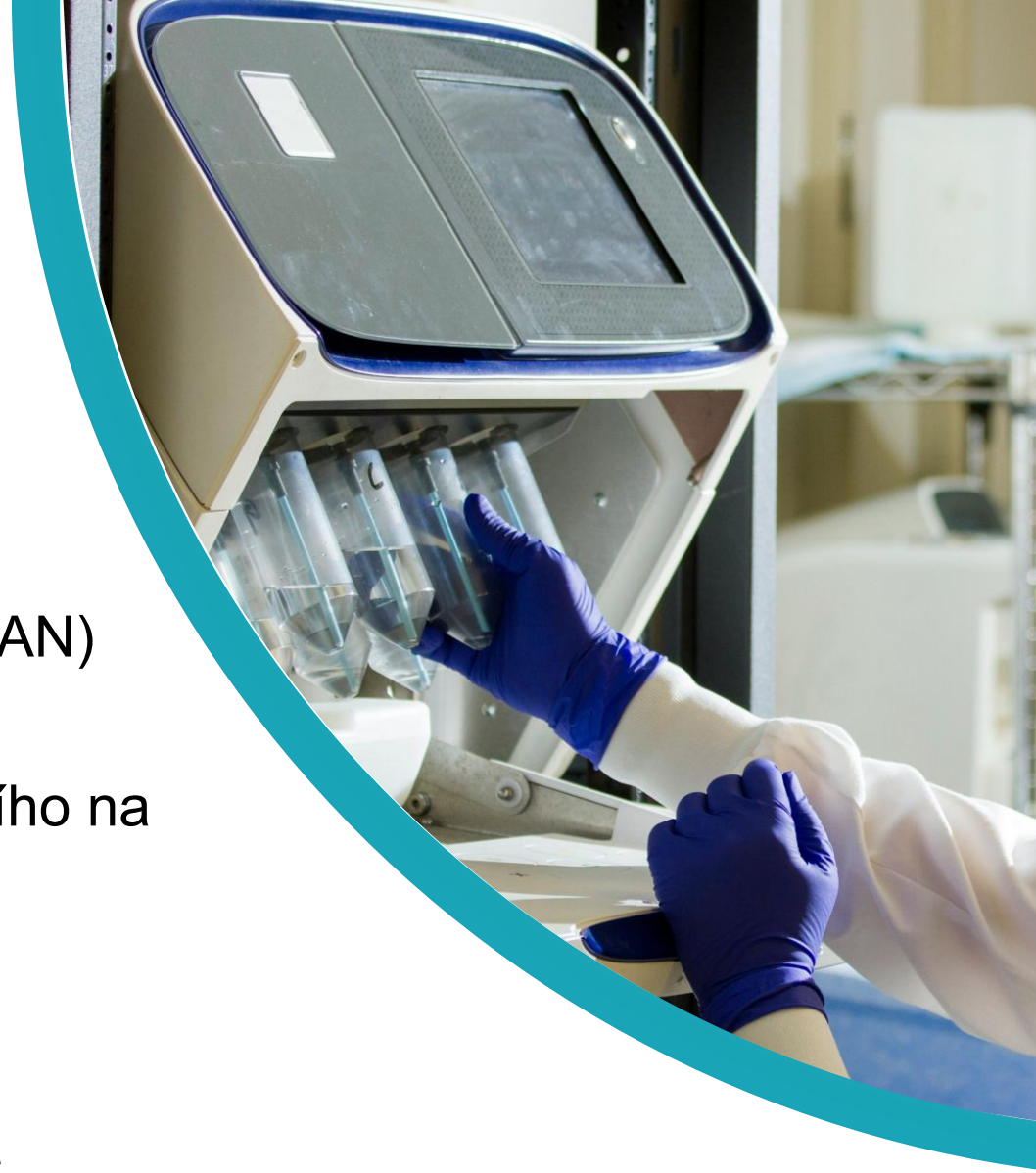
Jak přistupovat k cílovému prostředí?

- Definice prostředí dle typu zařízení
  - Volba vhodné strategie obnovy na základě specifik daného OT hardwaru a softwaru.
- RTO řízené potřebami výroby, ne IT normami
  - Stanovení doby obnovy (RTO) musí vycházet z reálné kritičnosti provozu, nikoli ze šablon běžného IT.
- Příprava virtualizace s podporou legacy systémů
  - Zajištění platformy schopné emulovat nebo podporovat starší generace hardwaru i OS.
- Riziko fyzických „skladových záloh“
  - Nespoléhat na staré kusy HW – hrozí jejich nefunkčnost, opětovné selhání v krátkém čase či nedostupnost náhradních dílů.

DATA SYS

Příklad incidentu

- Výpadek řídicího PC s Wind XP v nemocniční laboratoři připojeného k laboratornímu analyzátoru přes sériovou linku (RS232)



Řešení

- Převod sériové komunikace na síťovou (RS232 > LAN) pomocí IP převodníku
- Náhrada fyzického PC pomocí restore image běžícího na virtualizovaném serveru

Přínos

- Vyšší dostupnost, snadné zálohování a nezávislost na zastaralém HW

Nutnost mít předem připravené prostředí (případný HW a virtualizační platformu)

DATA SYS

Testování: Jediná záruka funkční obnovy

- Pravidelnost místo jednorázovosti
  - Obnovu je nutné testovat dle DR plánu ve stanovených intervalech, ne jen při prvotním nastavení.
- Správa verzí a změn (Version Control)
  - Bez průběžného sledování změn v OT konfiguracích selže i ten nejlepší BCP/DR plán.
- Proaktivní odhalení chyb
  - Testování musí odhalit nedostatky a úzká hrdla dříve, než k nim dojde při reálné havárii.
- Integrované funkce Acronis
  - Součástí zálohovacího procesu v Acronisu je integrovaná detekce malwaru, která zajišťuje 100% bezpečnost ukládaných i obnovovaných dat

DATA SYS

Zničení fyzického aktiva

- Riziko neopravitelného poškození
  Disaster Recovery (DR) i Business Continuity (BC) plány musí počítat s kompletní ztrátou zařízení (výrobní linka, rentgen, CNC stroj).
- Mapování dodavatelských vztahů
- Přesná identifikace dodavatelů klíčových komponent a zařízení.
- Smluvně garantované reakční doby a podmínky dodání náhradního HW (SLA).
- Prověření reálné dostupnosti náhradních dílů na trhu.

DATA SYS

KLÍČOVÉ POZNATKY

Testování záloh

- **Mít zálohu nestačí, pokud** nemáte kam obnovovat a pravidelně netestujete obnovu.

Prioritizace je kritická

- Bez jasného seznamu kritických systémů obnova trvá výrazně déle.

Síť je stejný bottleneck jako servery

- **Zničené komunikační prostředky = nefunkční prostředí**
- DR plán musí zahrnovat všechno důležité pro obnovu i networking.

Musí existovat plnohodnotný DR scénář

- automatizace failoveru
- připravená DR lokalita
- dostatečná kapacita

DATA SYS

Doporučení

- Mít **dostatečnou kapacitu** pro DR scénáře
- Stanovené odpovědnosti a kompetence
- Připravené náhrady HW, včetně případného virtualizačního prostředí (v dnešní době nepříliš nákladné)
- DR plán testovaný v praxi
- Dokumentovanou prioritizaci systémů
- Redundantní síťovou infrastrukturu

DATA SYS

JAK VÁM MŮŽEME POMOCI

DATASYS - Backup & Recovery Services

6 kroků k bezpečí OT

1. Klasifikace OT aktiv
2. Audit současného stavu OT
3. Scénáře řízené obnovy
4. Realizace nápravných opatření
5. Provozní dohled (L3)
6. Obnova po incidentu

DATA SYS

Klasifikace aktiv a informací

Proč?

- Ne všechna aktiva mají stejnou hodnotu
- Často chybí přehled o kritických aktivech
- Obnova se pak zaměřuje na špatná místa

Co uděláme?

- Určíme klíčová zařízení
- Priority ochrany i obnovy
- Navrhneme požadavky na obnovu

Váš benefit

✅ Přehled o kritických aktivech
✅ Smysluplnější investice

DATA SYS

Scénáře obnovy

Proč?

- Při incidentu rozhoduje čas.
- Obnova zahrnuje řadu navazujících činností a vazeb.
- Priority a postupy obnovy je vhodné připravit předem.

Co uděláme?

- Identifikujeme klíčové scénáře obnovy.
- Stanovíme priority obnovy systémů, služeb a procesů.
- Připravíme postupy, role a odpovědnosti pro zvládnutí incidentu.

Váš benefit

✅ Jasný postup při obnově provozu.
✅ Lepší koordinace činností během incidentu.
✅ Omezení dopadů výpadků a incidentů.

DATA SYS

Provozní dohled (L3)

Proč?

- Infrastruktura a požadavky organizace se v čase mění.
- Backup prostředí vyžaduje průběžnou kontrolu a vyhodnocování.
- Odchylky a problémy je vhodné odhalit dříve, než při incidentu.

Co uděláme?

- Budeme průběžně sledovat stav backup prostředí.
- Ověřovat průběh zálohování, obnovy a využití kapacit.
- Identifikovat odchylky, rizika a doporučovat opatření.

Váš benefit

✅ Přehled o skutečném stavu zálohování.
✅ Včasné odhalení problémů a změn.
✅ Vyšší jistota připravenosti na obnovu.

DATA SYS

Obnova po incidentu

Proč?

- Bez zkušeností a koordinace roste chaos i dopad na byznys
- V kritické situaci nemá management čas řešit technické detaily
- Potřebujete partnera, který už řešil podobné situace v praxi

Co uděláme?

- Poskytneme podporu při řešení incidentu a obnově provozu??
- Pomůžeme koordinovat obnovu systémů a služeb??
- Podpoříme rozhodování a prioritizaci dalších kroků??

Váš benefit

✅ Zkušený partner v krizové situaci.
✅ Lepší koordinace obnovy provozu.
✅ Efektivnější zvládnutí incidentu.

DATA SYS

Plný outsourcing B&R

- Převezmeme odpovědnost za návrh, provoz, dohled a průběžné zlepšování backup & recovery prostředí.
- Propojíme klasifikaci aktiv, audit současného stavu, realizaci opatření, scénáře obnovy, provozní dohled i podporu při incidentu do jedné služby.
- Cílem není jen zálohovat data, ale dlouhodobě udržovat schopnost organizace obnovit klíčové systémy a provoz v situaci, kdy na tom opravdu záleží.

DATA SYS


Harmonogram zálohování
- poslední aktualizace 2012
Mon.
Tue
Wed
Thu
Fri
Zálohování systému: Díl 1 (1993-2023)
Umění ruční rekonstrukce databáze
JEDINÉ ZNÁMÉ SYSTÉMOVÉ ZÁLOHY

DATA SYS

DATA SYS

Pokud Vás naše prezentace zaujala, napište nam na obchod@datasys.cz

DĚKUJEME ZA POZORNOST

Acronis

Cyber Protect pro prostředí Operational Technology (OT)

Štěpán Bínek

Business Unit Manager Acronis

SB@zebra.cz +420 777 008 462

https://www.linkedin.com/in/stepanbinek/

Ochrana OT systémů je náročná

- **Real-time řízení běží na starých počítačích**
  - Staré počítače a OS po end-of-support (Win XP, 2003)
  - Zranitelné vůči malware, bez podpory moderního AV
- **Patche a updaty jsou problematické**
  - Specifické požadavky dodavatelů automatizace
    - Podpora heterogenních řešení
    - Nekompatibilní požadavky na patching
    - Oborové compliance standardy (GxP a EU GMP Annex 11, NERC CIP, NIS2, TISAX, ISO 27001/27019)
- **Backup windows jsou nákladná**
  - Obnova od nuly nebo z backupu je obtížná

Onsite IT v produkci obvykle chybí

- Air-gap blokuje remote management tools

Acronis podporuje legacy OS, které konkurence již opustila

Legacy OT systémy musí být řízeným rizikem

Pokud technické aktivum již není podporováno, musí být evidováno a chráněno bezpečnostními opatřeními zajišťujícími obdobnou nebo vyšší úroveň bezpečnosti.

Vyhláška č. 409/2025 Sb., § 24 odst. 2; vyhláška č. 410/2025 Sb., § 12 písm. b)

Industry best coverage of various OSes and hypervisors

Windows
- Windows Server 2003 SP1, R2 and later, 2008, 2008 R2, 2012/2012 R2, 2016, 2019, 2022 except Nano Server
- Windows Small Business Server 2003/2003 R2, 2008, 2011
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows XP Professional SP1, SP2, SP3
- Windows 7 , 8/8.1, 11 (all editions), 10, – all editions, except Windows RT

Microsoft SQL Server
- 2022, 2019, 2017, 2016, 2014, 2012, 2008 R2, 2008, 2005

Microsoft Exchange Server
- 2019, 2016, 2013, 2010, 2007

Hypervisors

VMware vSphere
- 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Microsoft Hyper-V Server
- 2022, 2019, 2016, 2012/2012 R2, 2008/2008 R2

Citrix XenServer/Citrix Hypervisor
- 8.2 - 4.1.5

Linux KVM
- 8 - 7.6

Scale Computing Hypercore
- 8.8, 8.9, 9.0

Red Hat Enterprise Virtualization (RHEV)
- 3.6-2.2

Red Hat Virtualization
- 4.0, 4.1, 4.2, 4.3, 4.4

Virtuozzo
- 7.0.14 - 6.0.10

Virtuozzo Infrastructure Platform
- 3.5

Nutanix Acropolis Hypervisor (AHV)
- 20160925.x through 20180425.x

MacOS
- **OS X** Mavericks 10.9, Yosemite 10.10, El Capitan 10.11
- **macOS** Sierra 10.12, High Sierra 10.13, Mojave 10.14, Catalina 10.15, Big Sur 11, Monterey 12, Ventura 13, Sonoma 14

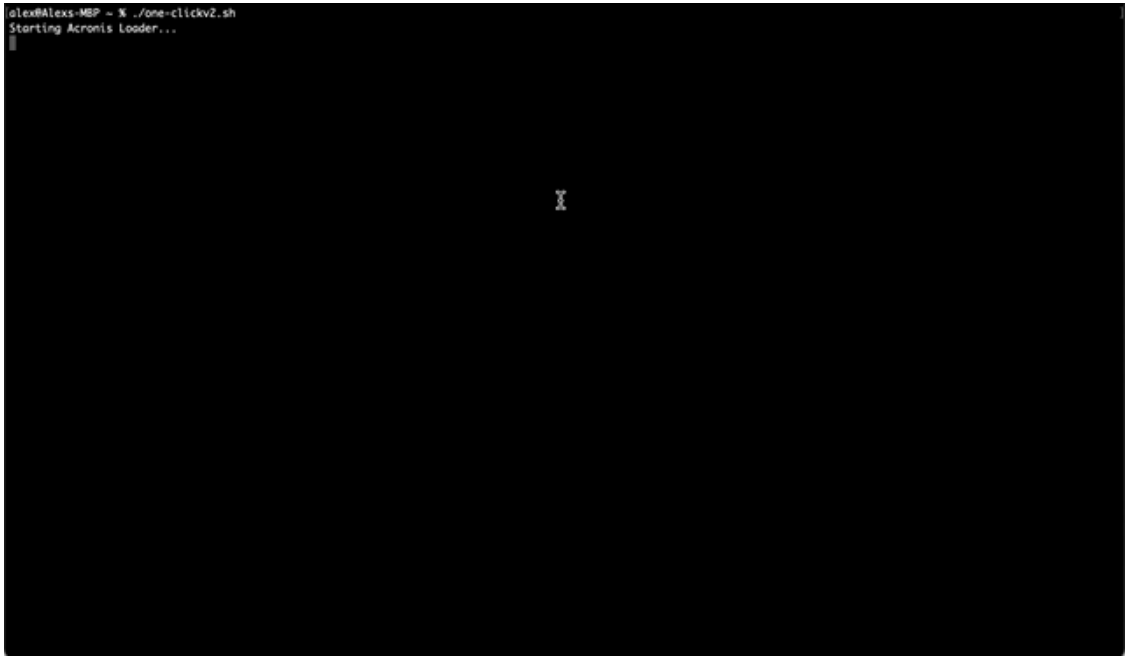
Linux: Kernel 2.6.9 to 5.19
- RHEL 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10 - 23.04
- Fedora 11 - 31
- SUSE Linux Enterprise Server 10, 11, 12, 15
- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4-7.7, 8.0-8.8, 8.11, 9.0- 9.8, 10.x, 11.x
- CentOS 5.x, 6.x, 7.x, 8.x*, Stream 8*,9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*,9.0*, 9.1*, 9.2*, 9.3*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

Acronis chrání real-time OT systémy

- **Bez plánovaných odstávek a restartů**
  - Live installation a backups bez restartů
- **Zjednodušuje a automatizuje backup**
- **Výrazně zrychluje backup**
- **Přesouvá IT administrační úlohy mimo OT systémy**
- **Zajišťuje spolehlivou a rychlou recovery konzistentně napříč lokalitami**
- **Nenarušuje Purdue Model**
  - **Jednosměrné datové toky backupu**
- **Přidává volitelné zabezpečení: EDR, endpoint anti-malware, ransomware protection**
- **Chrání také back-office a front-office systémy**

Acronis umožňuje self-service recovery OT systémů

- Acronis One-Click Recovery umožňuje místnímu pracovníkovi bez IT specializace obnovit OT systém bez pomoci IT
- Kritické pro vzdálené lokality, kam může IT podpora dorazit až za několik hodin
- Nezbytné v air-gapped prostředích bez remote management tools
- Zkracuje odstávky výroby při selhání OT systémů z hodin na minuty



Acronis One-Click Recovery umožňuje mimořádně rychlou a jednoduchou obnovu OT systému z backupu

Acronis v průmyslové praxi: ABB a Toyota Manufacturing

CASE STUDY

Acronis

ABB chooses **Acronis** Cyber Protect to ensure maximum security for its customers' facilities

The Acronis solution means that ABB customers can avoid costly business interruptions by restoring the functions of any system in a matter of seconds.

COMPANY OVERVIEW

Founded in 1988 following the merger of Swedish company ASEA and Swiss company Brown Boveri, ABB is a technology company operating in more than 100 countries around the world. Its electrification, automation, robotics and motion offering serves the utilities, industrial, transport and infrastructure sectors. Technological excellence, a global presence, application knowledge and strong local skills make up the hallmark of a complete portfolio of products, systems and services that enable all customers to improve their businesses in terms of energy efficiency, network reliability and industrial productivity. In Italy, ABB has acquired the experience and skills of many brands in the Italian electromechanical sector over the years. This includes major companies that

INDUSTRY

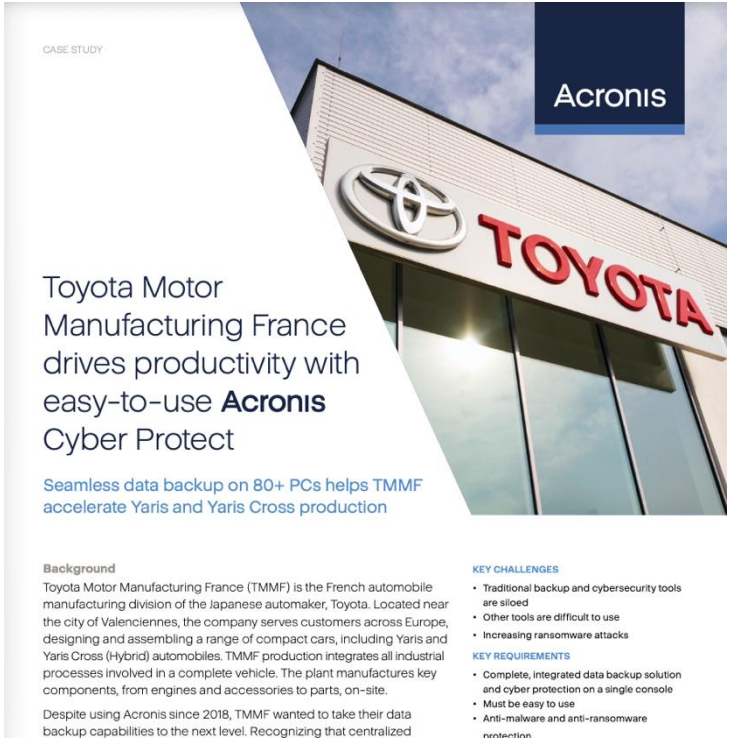
- Electrotechnical

KEY CHALLENGES

- Poor standardization in terms of recovery operations
- Difficult to automate backups
- Complex management systems

KEY REQUIREMENTS

- Automatic bare metal recovery
- Universal restore
- Maximum reliability



CASE STUDY

Acronis

TOYOTA

Toyota Motor Manufacturing France drives productivity with easy-to-use **Acronis** Cyber Protect

Seamless data backup on 80+ PCs helps TMMF accelerate Yaris and Yaris Cross production

Background

Toyota Motor Manufacturing France (TMMF) is the French automobile manufacturing division of the Japanese automaker, Toyota. Located near the city of Valenciennes, the company serves customers across Europe, designing and assembling a range of compact cars, including Yaris and Yaris Cross (Hybrid) automobiles. TMMF production integrates all industrial processes involved in a complete vehicle. The plant manufactures key components, from engines and accessories to parts, on-site.

Despite using Acronis since 2018, TMMF wanted to take their data backup capabilities to the next level. Recognizing that centralized

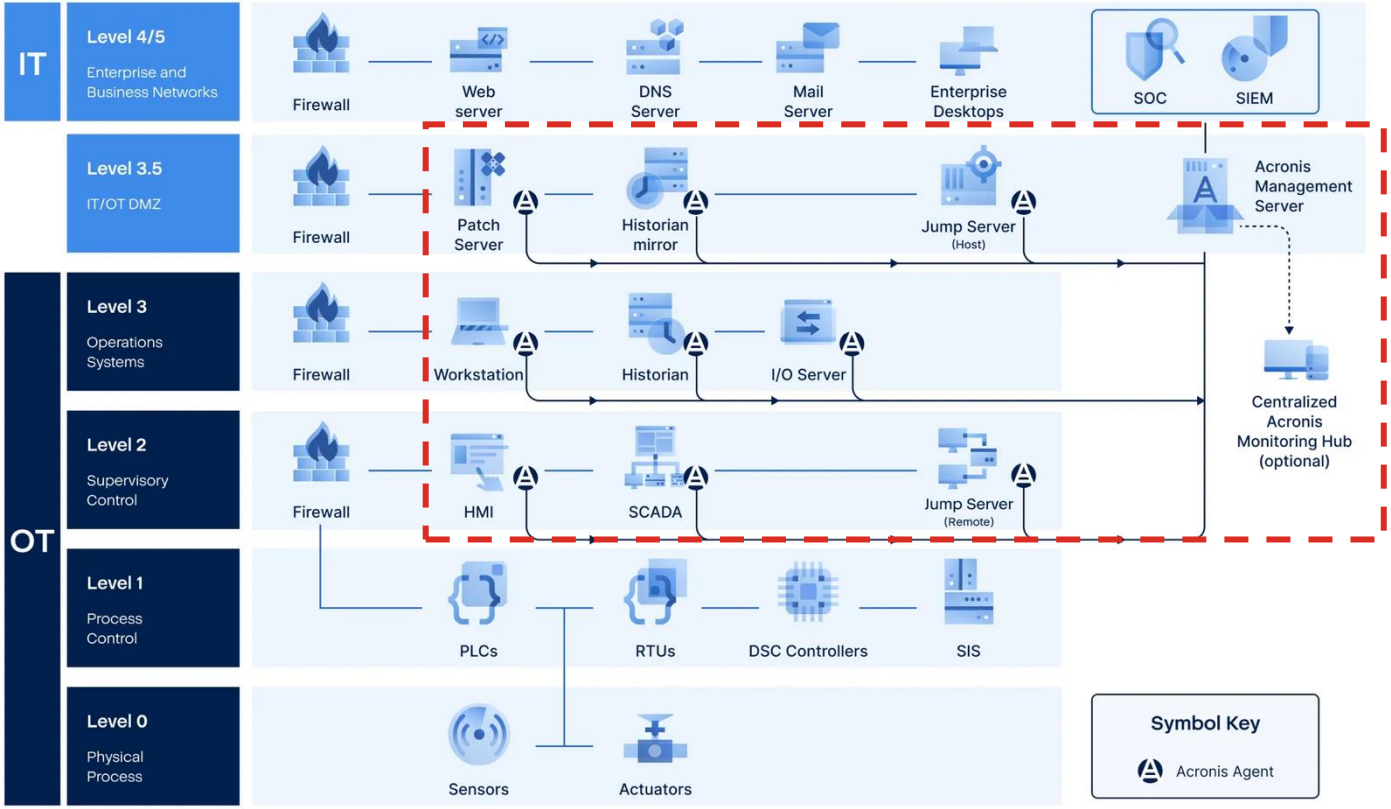
KEY CHALLENGES

- Traditional backup and cybersecurity tools are siloed
- Other tools are difficult to use
- Increasing ransomware attacks

KEY REQUIREMENTS

- Complete, integrated data backup solution and cyber protection on a single console
- Must be easy to use
- Anti-malware and anti-ransomware protection

Role Acronis v Purdue Model



*List of protected systems not exhaustive

Acronis chrání OT systémy napříč lokalitami

Funkce

- ✓ Snapshoty aktuálních dat
- ✓ Historický pohled
- ✓ Vysoce přizpůsobitelné dashboardy
- ✓ Více datových zdrojů
- ✓ Monitoring a analytické dashboardy
- ✓ Data drill-down a filtry
- ✓ Alerts podle datových thresholds
- ✓ Integrace s third-party systémy