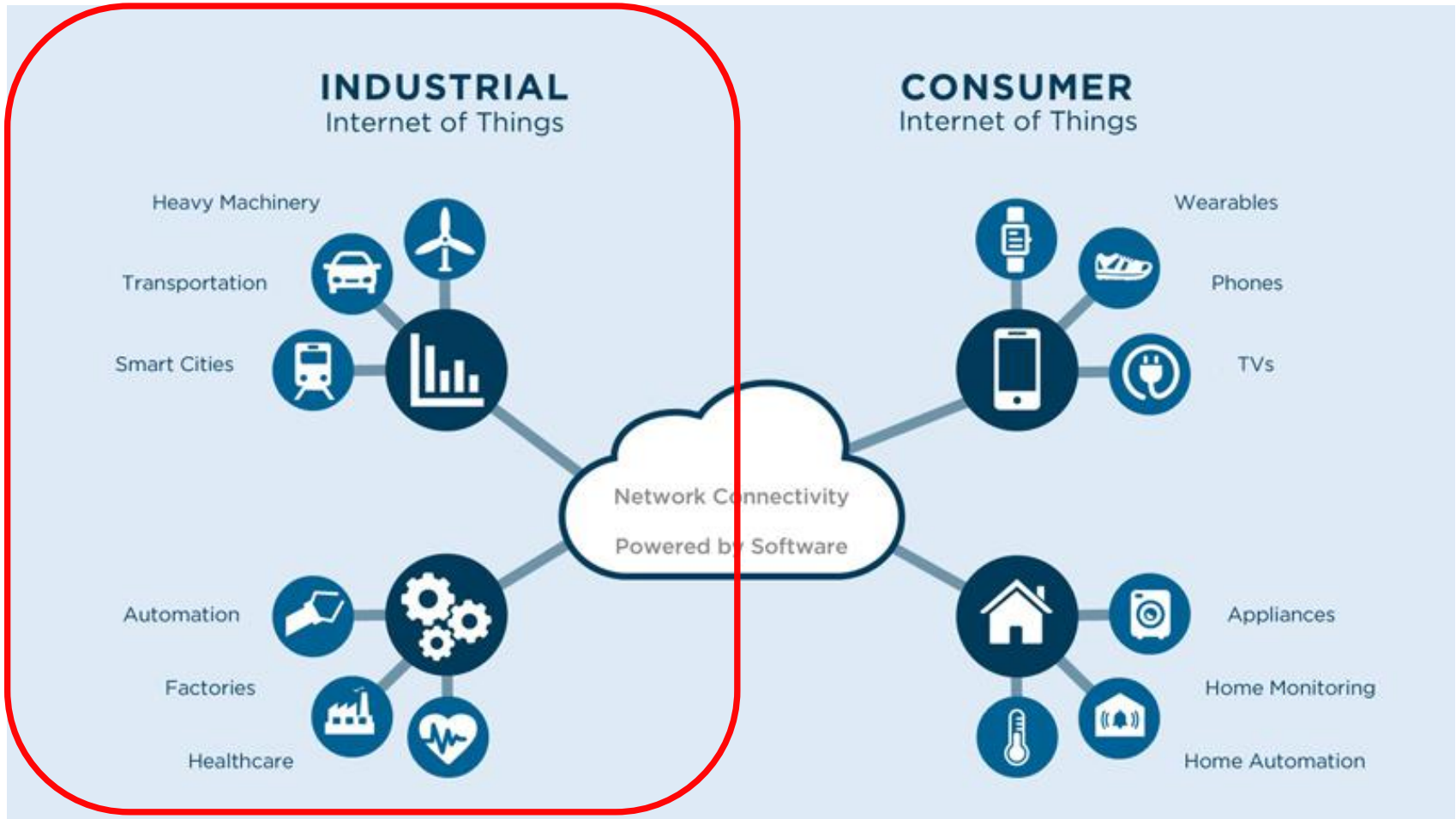
Posun v chápání rozdílů mezi ICT a ICS – současná situace.

Jiří Kasner, kasner.jiri@colaut.cz

COLSYS AUTOMATIK

HIRSCHMANN
A BELDEN BRAND

ICS a jeho pozice



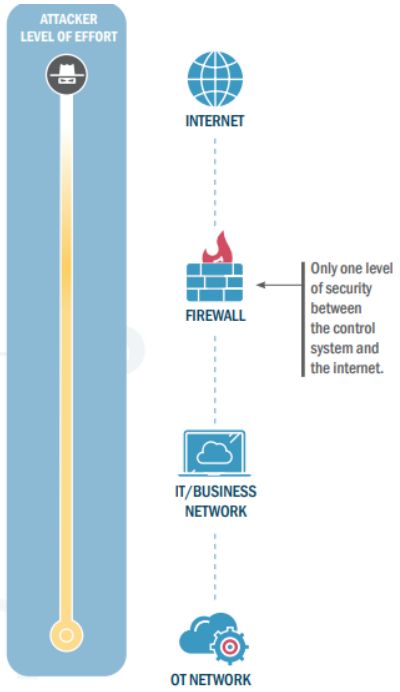
COLSYS AUTOMATIK

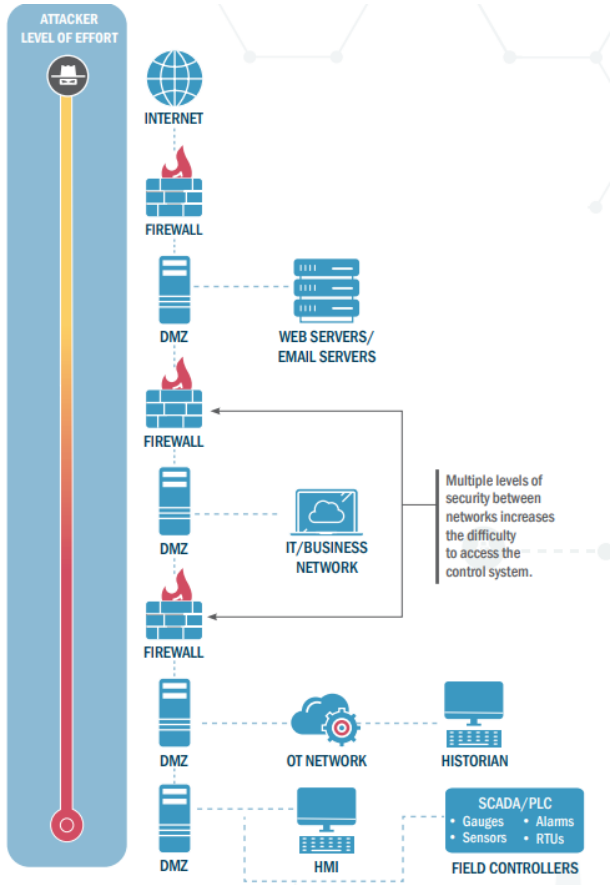
HIRSCHMANN
A BELDEN BRAND

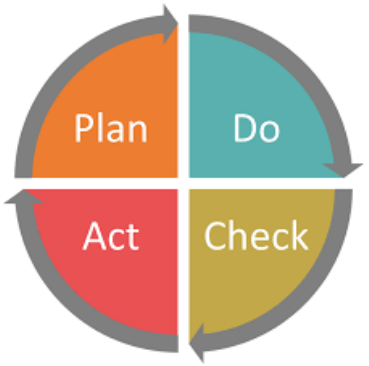
Porovnání ICT a ICS

	ICT	ICS
• Požadavky na výkonnost *odezva* *průchodnost*	mimo reálný čas *konzistentní* *vysoká*	v reálném čase *okamžitá* *střední*
• Požadavky na dostupnost *redundance*	se zpožděním *není nutná*	vysoká *nutná*
• Požadavky na řízení rizik	důvěrnost a integrita	maximální dostupnost
• Požadavky na bezpečnost	ochrana aktiv	ochrana procesů
• Komunikace	standardní protokol	vícero protokolů
• Operační systémy	standardní	proprietární
• Doporučená technická podpora	různá	jeden dodavatel
• Životnost komponent	3 – 5 let	15 – 20 let

Bezpečnostní cyklus + segmanetace ICS.







UNSEGMENTED IT AND OT NETWORKS INCREASE RISK[2]:

- OT networks are exposed to vulnerabilities in connected IT networks.
- Easier for threat actors to move laterally after breaching the IT network.
- Detecting threat actors is more difficult due to increased volume of network traffic.

BENEFITS OF SEGMENTING BETWEEN IT AND OT NETWORKS:

- Segmented zones isolate and protect high-value assets and data.
- Malicious traffic is easier to detect, prevent, and contain.
- Threat actors must negotiate multiple firewalls and other protocols to access the OT environment.

COLSYS AUTOMATIK

HIRSCHMANN
A BELDEN BRAND

Industrial cyber security – step-by-step

5 zásad kybernetické bezpečnosti v OT/ICS

Zásada 1: Provádět komplexní řízení rizik prostředí OT
Zásada 2: Zajistit, aby technici a provozovatelé zařízení OT nesli odpovědnost za kybernetickou bezpečnost OT.
Zásada 3: Sjednotit se s vrcholovým vedením organizace, týmy strategického plánování a třetími stranami, aby se bezpečnost podle návrhu stala skutečností.
Zásada 4: Zajistěte, aby standardy kybernetické bezpečnosti a osvědčené postupy byly smluvně vymahatelné u partnerů a dodavatelů s cílem vytvořit kyberneticky bezpečné prostředí OT.
Zásada 5: Provádějte společná Table Top cvičení, abyste zajistili připravenost pro případ skutečného incidentu.

COLSYS AUTOMATIK

HIRSCHMANN
A BELDEN BRAND

Technologie a služby ICS

Cyber-Physical Security and Operational Systems Health	• Data Manipulation and Data Injection • OT/ICS Asset-Signal Integrity and OT Anomaly Detection • Predictive Maintenance
Identity and Access Management (IAM)	• Identity Governance Across Assets and Users • MFA, Passwordless, and SSO • Policy and Role Management • Privileged Access Management (PAM)
Industrial IoT (IIoT) Device Security	• Continuous Vulnerability Management • Embedded IoT Agent-IIoT Inventory • Hardware/Software • Secure and Validate Device Updates
Network Discovery, Monitoring and Threat Detection	• Asset Intelligence - IT/OT/IIoT • Attack Path Management • Automated Network Inventory • Monitor, Alert, and Report • Network Anomaly and Threat Detection • Network Asset Discovery and Mapping
Operational IT/OT Endpoint Security and Patch Management	• Industrial IT Endpoint Protection, EDR/xDR/EPP • Device-level Zero-Trust • Firmware, Configuration, and Patch Management • OT Endpoint
Perimeter Security, Segmentation, and Zone Enforcement	• Data Diode/Unidirectional Gateways • Industrial Firewalls • Soft/Virtual/Micro-Segmentation • USB/Removable Media Sanitization
Product, Software, and Supply Chain Security	• Monitoring and Remediation • Product Security and SDLC • SBOM/HBOM Analysis, VEX, File Integrity • Third-party Risk Management • Vulnerability Management
Risk Management, Governance, and Compliance	• Exposure Reduction and Vulnerability Prioritization • Industrial Threat Intelligence • Risk Exposure Analysis and Reporting • Risk Management and Mitigation
Secure Remote Access	• Access Control: ABAC/DAC/MAC/BAC • Audit and Compliance: Session Logging/Recording/Termination • Jump box, VPN Access, Converged SRA platform • Privileged SRA, Zero-Trust, and Identity
Social Engineering and Phishing Prevention	• Inbox Cyber Security and Phishing Deterrence • Training Platforms, Behavioral Modification/Interactive Training, CBT/Video • Network Prevention/Enforcement • Secure Email Gateways

COLSYS AUTOMATIK

HIRSCHMANN
A BELDEN BRAND

Technologie a služby ICS

Assessments and Testing

- Asset Discovery, Inventory Hygiene, and Diagnostic Assessments
- Conduct Gap, Vulnerability, and Risk Assessment/Audit
- Governance, Policy, and Procedure Review
- Network Architecture Evaluation
- Penetration Testing
- Readiness Assessment
- Social Engineering and Phishing Testing/ Assessments
- Technology Efficacy and Efficiency Evaluation

Deployment, Implementation, and Managed Services

- Acceptance Testing: Backup and Recovery
- Configuration and Patch Management
- Managed SOC and Monitoring
- Network Design and Segmentation
- Network Hardening
- Platform Integration
- SIEM/SOAR, EDR/XDR, Network, Identity, Asset, Cloud
- Systems Hardening
- Endpoint, Appliance, and Device

Incident Planning, Response, and Recovery

- Contingency and crisis planning
- Manage and remediate cybersecurity incidents
- Playbooks and Response Procedures
- Post-incident Forensics
- Threat Hunting and Investigation
- Threat Modeling and Visualization

Program Development

- Cyber Risk Management
- IIoT cybersecurity strategy/plan
- Network Architecture and Design Planning
- Program Development, Review, and Management
- Regulatory Compliance
- Security Framework and Standards Adoption
- Social Engineering and Security Awareness Program

Supply Chain and Product Security

- Continuous Monitoring
- File and Patch Integrity Service
- Product Assessment
- SBOM/HBOM Analysis
- Secure System Design, Implementation, and Development
- Third-party Risk Management
- Vulnerability Management

Train and Educate

- Cyber Range: Simulation Training
- Cybersecurity Skills Development
- OT/IT Alignment Program
- Red vs. Blue training
- Security Awareness Training
- Tabletop exercises

COLSYS AUTOMATIK

HIRSCHMANN
A BELDEN BRAND