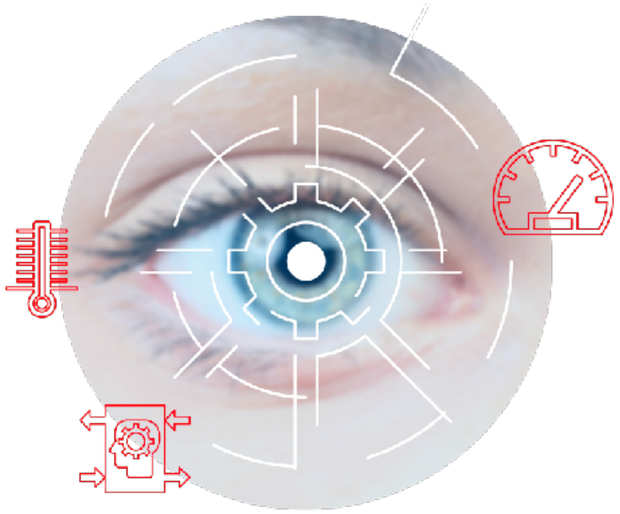
SCADA

AWARENESS LAB

„NESAHAT, HLAVNĚ ŽE TO FUNGUJE ANEB BEZPEČNOST”



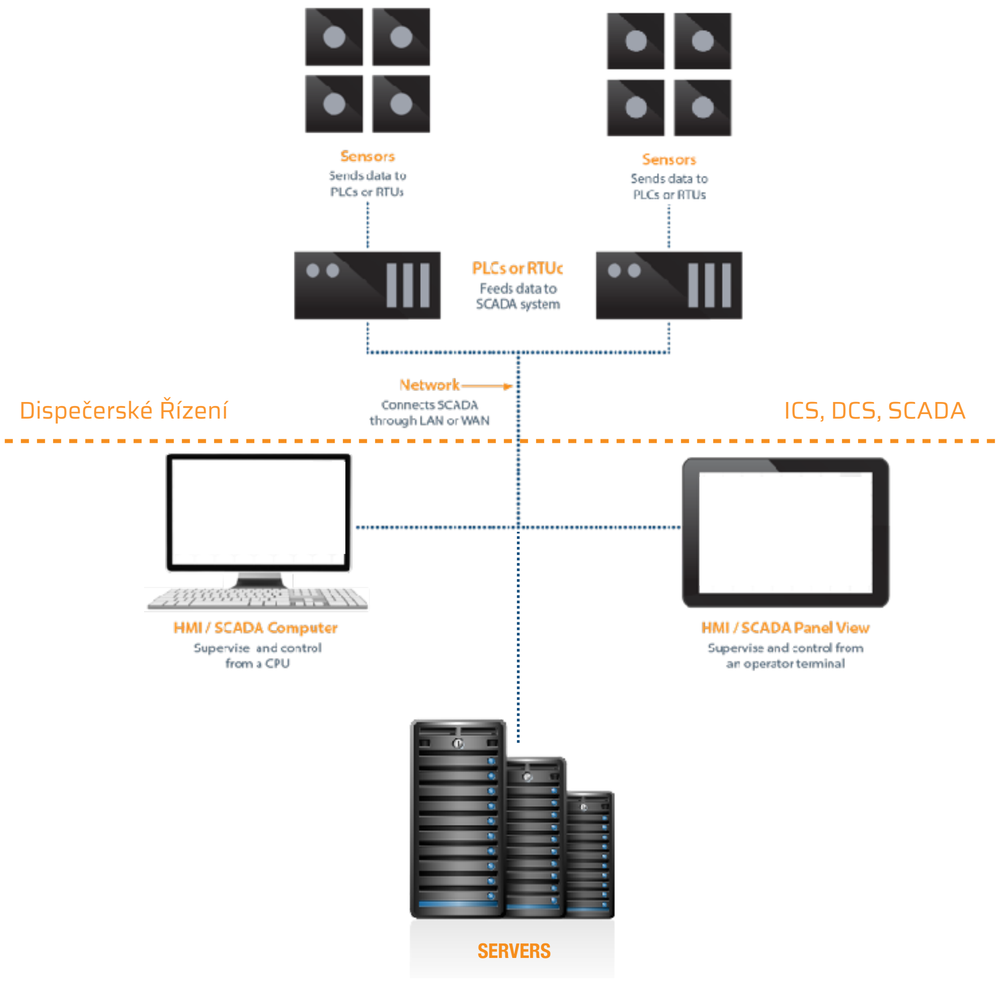
CORPUS SOLUTIONS A.S.

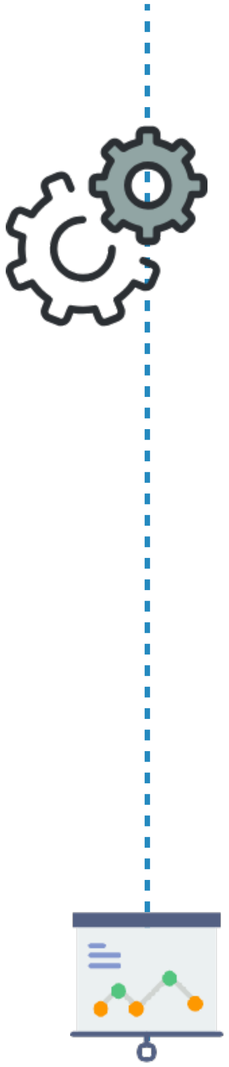
- Konzultační a technologická společnost
- Aplikovaná kybernetická bezpečnost
- Založena 1992
- Česká společnost
- Čeští akcionáři
- Dvě pobočky
- 60 zaměstnanců
- Určeni jako provozovatel KII

TF-CSIRT
Trusted Introducer
Accredited
since 24 Oct 2018

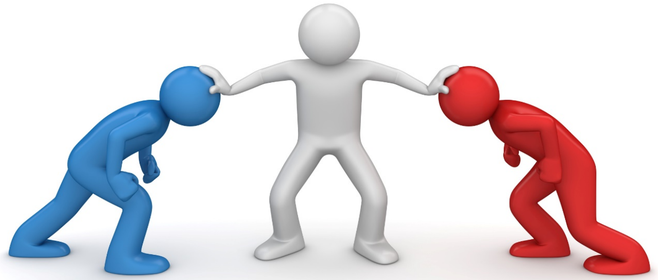
Corpus = Cybersecurity Experts

TYPICKÁ ARCHITEKTURA SCADA SYSTÉMU





IT - INFORMAČNÍ TECHNOLOGIE VS. OT - PROVOZNÍ TECHNOLOGIE

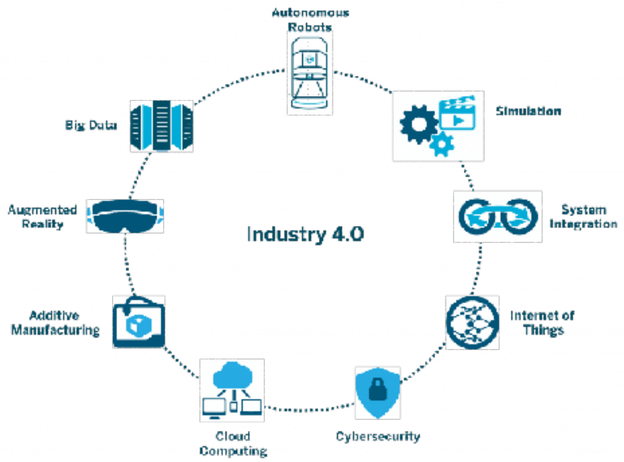


- C I A - důvěrnost, integrita, dostupnost
- Data Loss - Ztráta dat
- Moderní bezpečnostní technologie
- Životní cyklus : 5 let
- Vysoká segmentace sítě, správa aktiv
- Kryptovaná komunikace

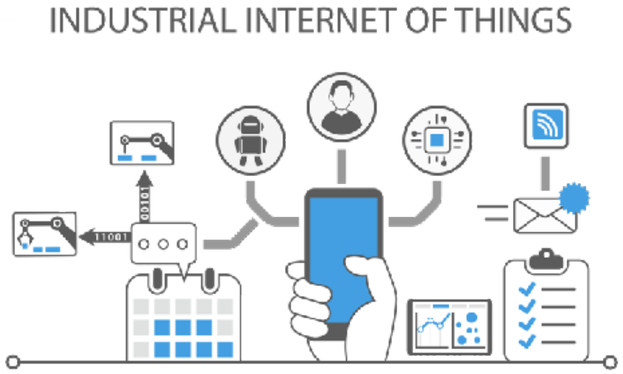
- A I C - dostupnost, integrita, důvěrnost
- Fyzické ztráty / škody
- Základní bezpečnostní technologie
- Životní cyklus : desítky let
- Slabá segmentace sítě a minimální správa aktiv
- Nezabezpečené komunikační protokoly

TRENDY V OT

- Industry 4.0



- IIoT - Industrial Internet of Things

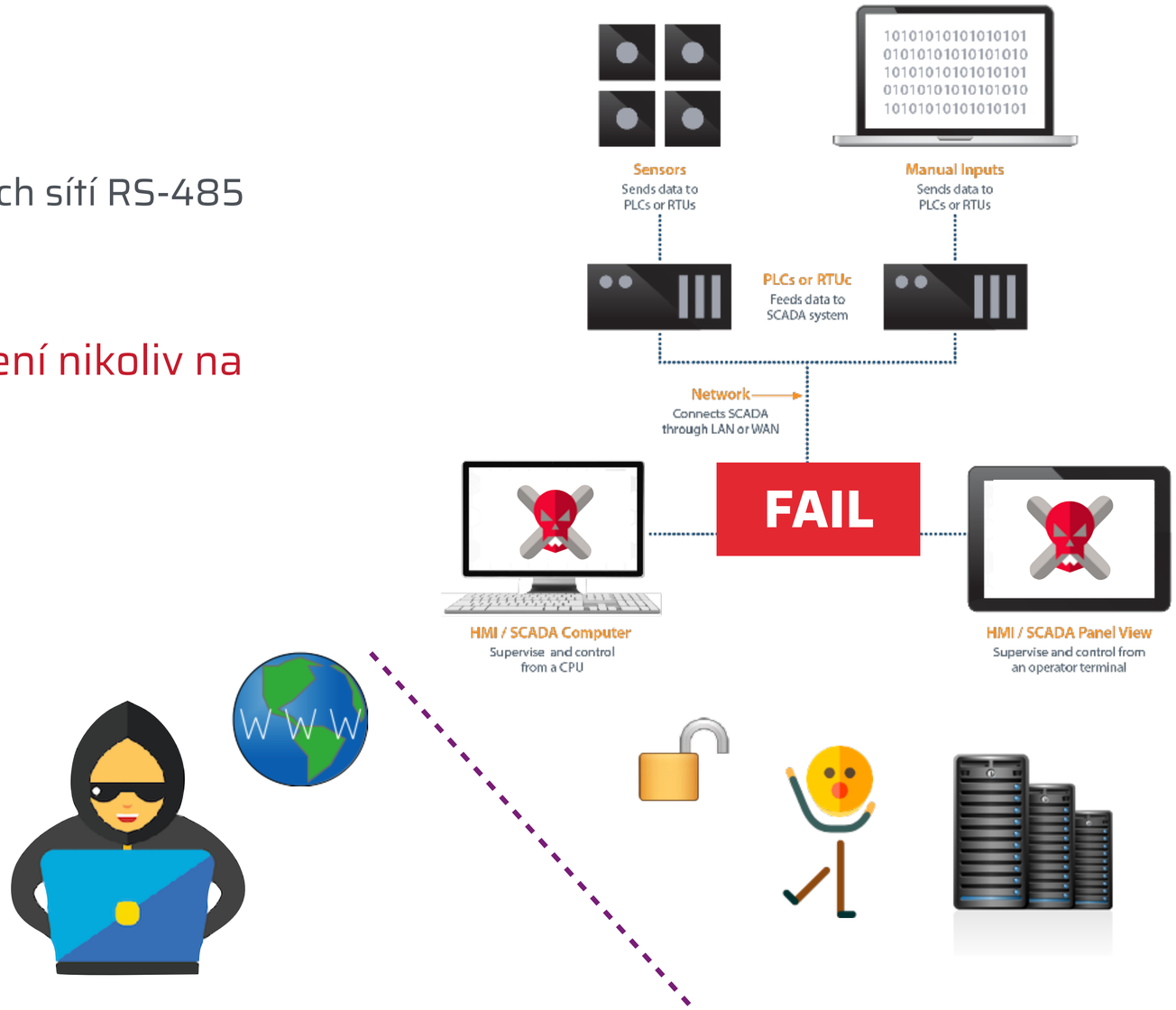


- PC based control IPC -> Server based control

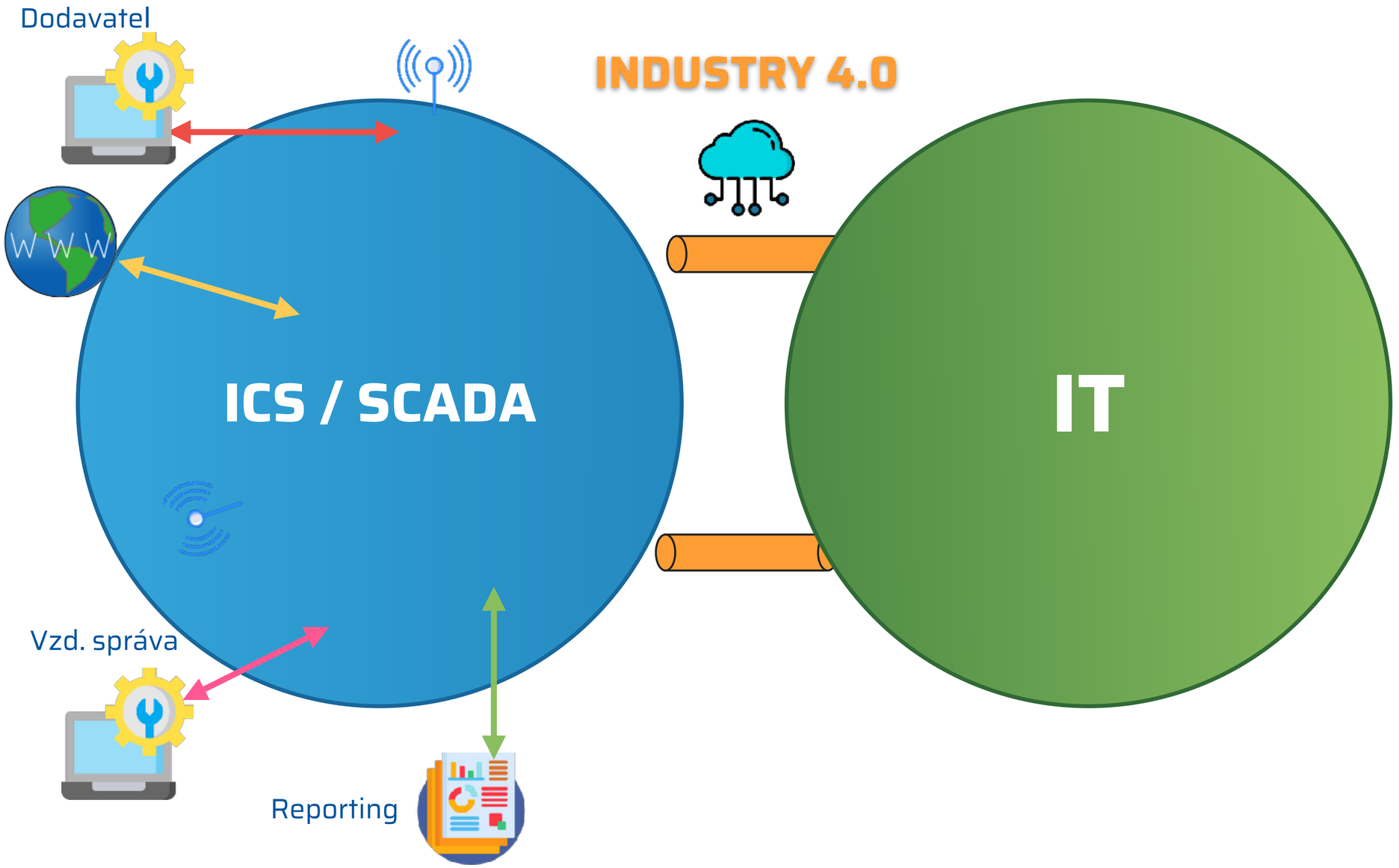
RADAR ICS - PRŮMYSLOVÉ SYSTÉMY S PŘÍSTUPEM DO INTERNETU

PROBLÉMY TRADIČNÍCH ICS PROTOKOLŮ

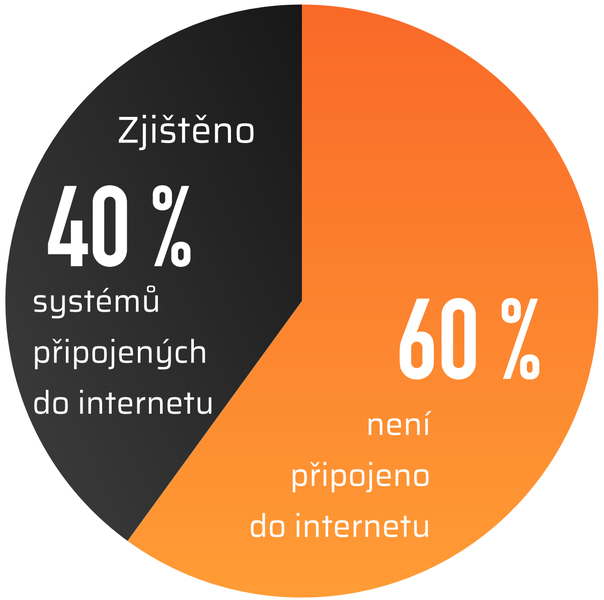
- Běží na vysloužilých technologiích
- Mnoho protokolů jsou derivátem předchozích sériových sítí RS-485
- Žádná autentizace , žádná datová integrita
- Návrh zaměřen na spolehlivost a dostupnost řízení nikoliv na bezpečnost komunikace
- Nezohledňují úskalí propojitelnosti s internetem



PROČ ICS NEZOHLEDŇUJÍ ÚSKALÍ PROPOJITELNOSTI S ?



MÝTICKÁ VZDUCHOVÁ MEZERA



zdroj : CyberX 2019 GLOBAL ICS & IIoT RISK REPORT

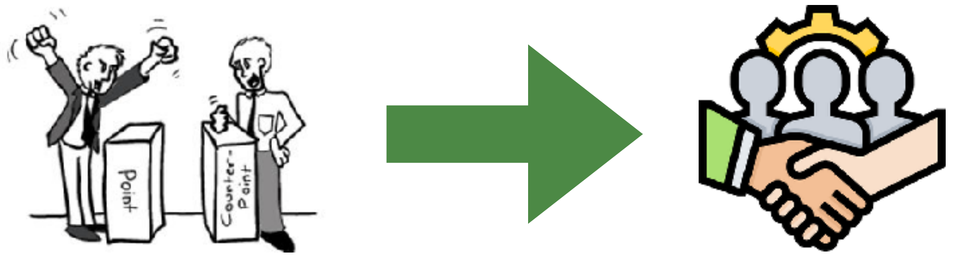
KLASIFIKACE INCIDENTŮ

- **Provozní** - narušení integrity systémů
  - Systémová porucha na zařízení
  - Hardwarová konfigurace
  - Konflikt na síti
  - Úprava Softwaru, nová verze Firmwaru

- **Bezpečnostní** - kybernetická hrozba
  - Mapování sítě, DoS
  - Únik / zneužití citlivých dat z provozu - Receptury, zranitelnosti
  - Kompromitování dat, komunikačních protokolů
  - Malware, kompromitované řízení

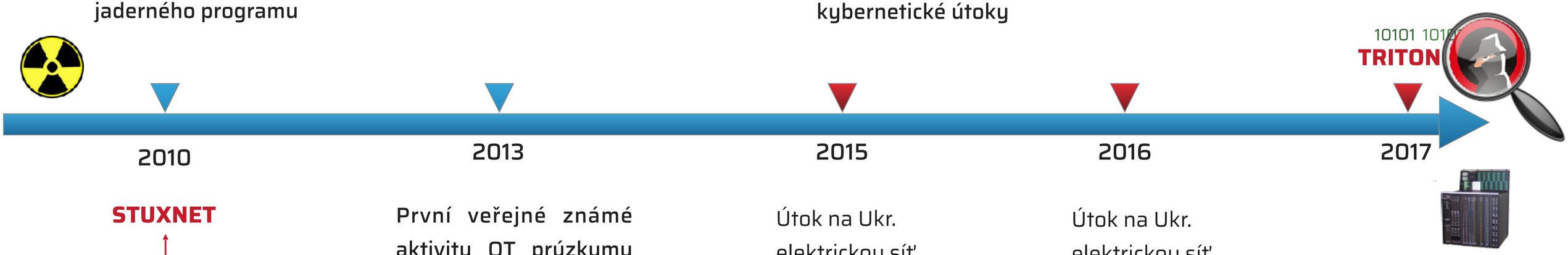
KLÍČOVÉ MOTIVÁTORY KE ZMĚNĚ PŘÍSTUPU

- **Legislativa** - Vyhláška / Zákon o kybernetické bezpečnosti, IEC 62443
- Zabezpečené technologie = Spolehlivější technologie = Vyšší konkurenceschopnost
- Lidské zdroje a procesy



Bezpečnost = Technologie x Lidský faktor x Procesy

NEBEZPEČÍ ICS ÚTOKŮ SE MĚNÍ A VYVÍJÍ



PROČ ANOMALY DETECTION ?

Čelit kybernetickým útokům po roce 2015 bez detekčních nástrojů je velmi obtížné. V pokročilých fázích prakticky nemožné.

VIZIBILITA PROVOZU

- ANALYTICKÉ NÁSTROJE A PROCESY (WireShark, Nmap, Komunikační GW, Diagnostický SW výrobce, Profinet, Ethernet/IP Analyzér ...)

- **PROVOZ POD DOHLEDEM UMĚLÉ INTELIGENCE**
  (Machine Learning, Neurónové sítě, Deep Packet Inspection)

MODERNÍ METÓDY DETEKCE PROVOZNÍCH / BEZPEČNOSTNÍCH INCIDENTŮ

- MACHINE LEARNING :
  - OT sítě periodický provoz
  - Znalostní báze pravidel, vzorů
  - Mód učení - Odposlech komunikace, interakcí, vytváření pravidel
  - Mód provozní - Aplikování naučené báze dat
  - Detekce anomálií, reakce uživatelů, učení v provozu

ADVANCED DETECTION SYSTEMS - AD

OT Protocols

- Modbus modicon:
  - Modsoft/Execload unity
- Siemens S7/S7-Plus
- Siemens P2
- EtherNet/IP + CIP (including Rockwell extension)
- PCCC/CPSv4
- GE SRTP
- Yokogawa VNet/IP
- Emerson Ovation DCS protocols
- Emerson DeltaV DCS protocols
- Melsec/Melsoft
- ABB 800xA DCS protocols
- MMS (including ABB extension)
- Sattbus
- OPC DA/AE/UA
- IEC104
- DNP3
- Profinet-DCP
- Bacnet
- Emerson ROC
- OMRON Fins

  ABB TotalFlow
- Triconex (TSAA, Tristation)
- Honeywell FTE
- CCC (Proconos)
- EGD
- Profibus
- Modbus RTU
- Lantronix
- CTI
- Bently Nevada

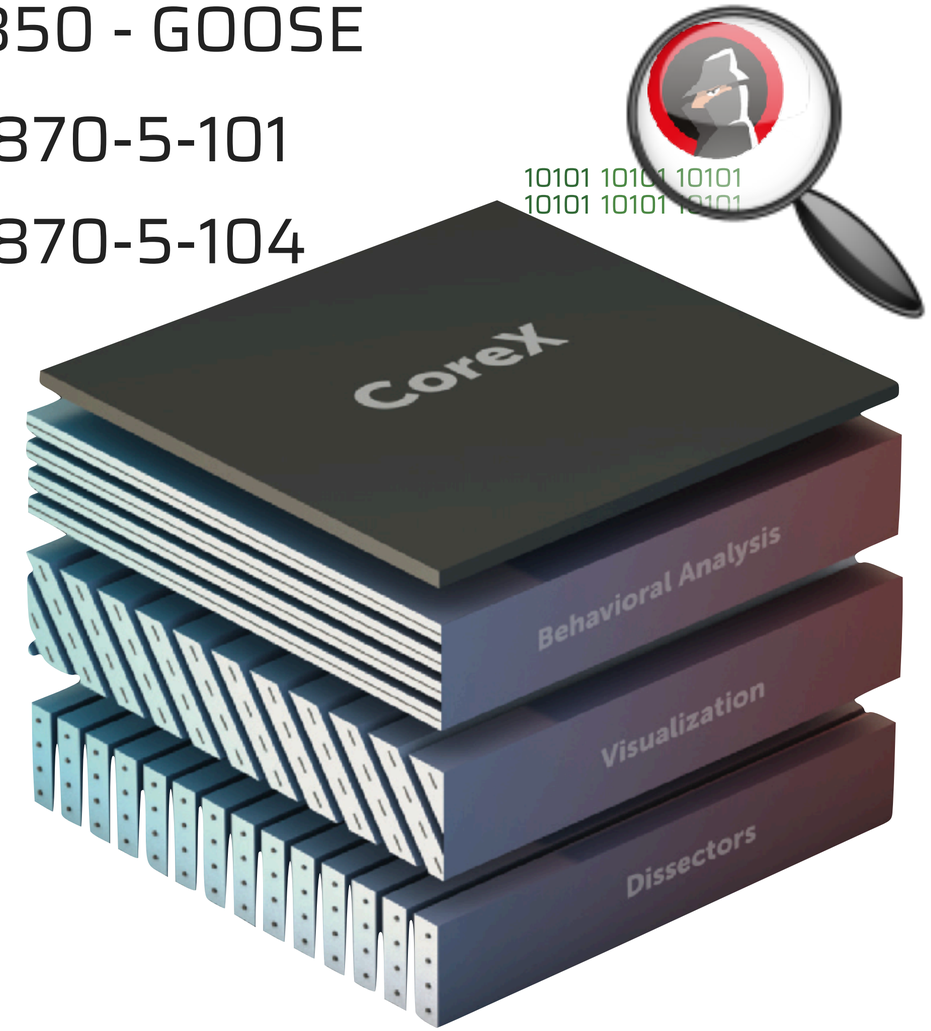
IT Protocols

- CDP
- LLDP
- DCE/RPC
- DHCP V4/V6
- ARP
- VNC
- TFTP
- NTP
- RDP
- SSL
- NTLMSSP
- ATSVC
- SMB-PIPE
- TCP/IP
- SNMP
- SSH
- HTTP / HTTPS
- Telnet
- FTP
- SMB / CIFS
- DNS
- ICMP
- IGMP
- Browser
- FTP
- SMB

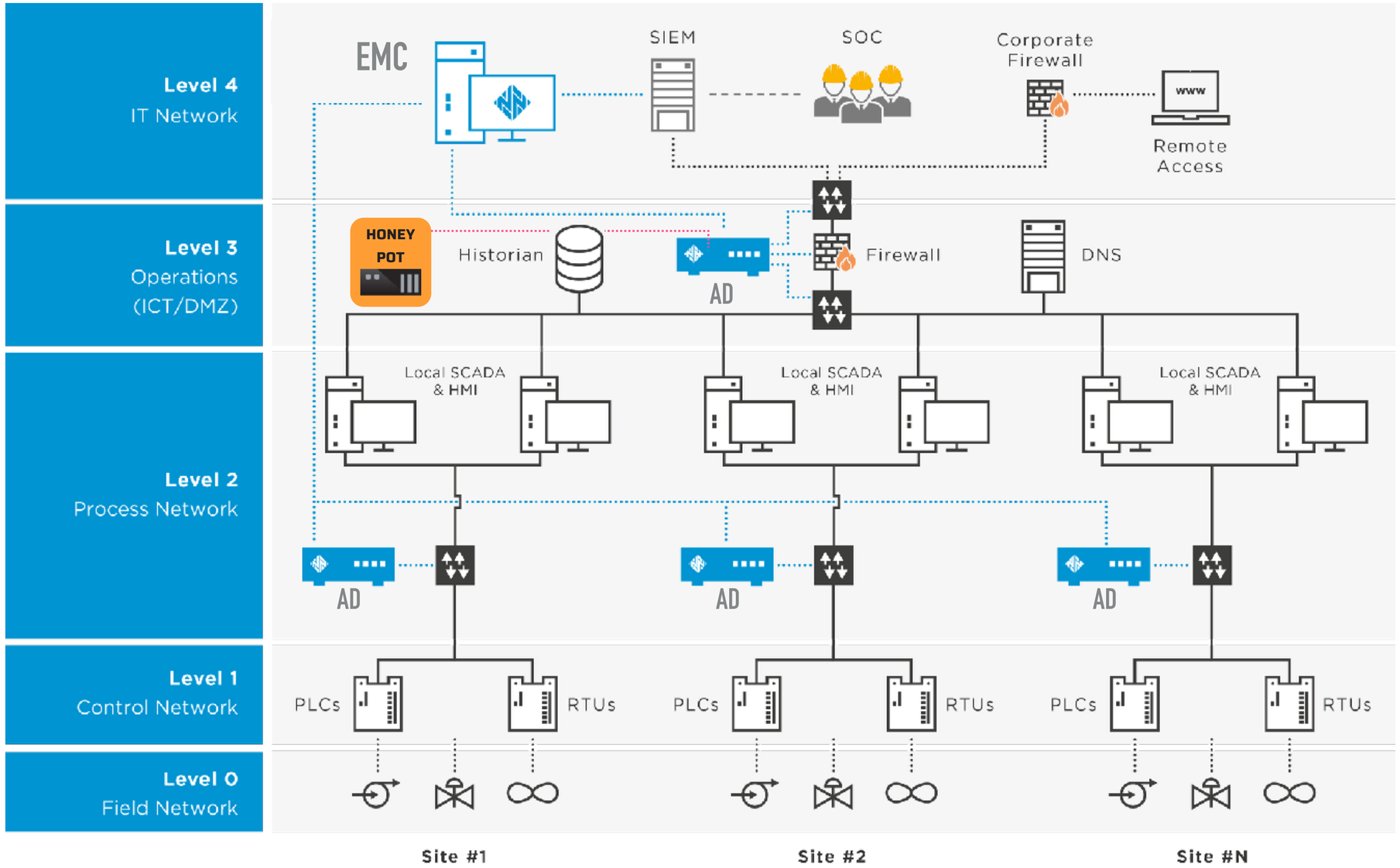
Vendors

ABB · GE · Honeywell · MITSUBISHI · OMRON · EMERSON · Rockwell Automation · Schneider Electric · YOKOGAWA · SIEMENS

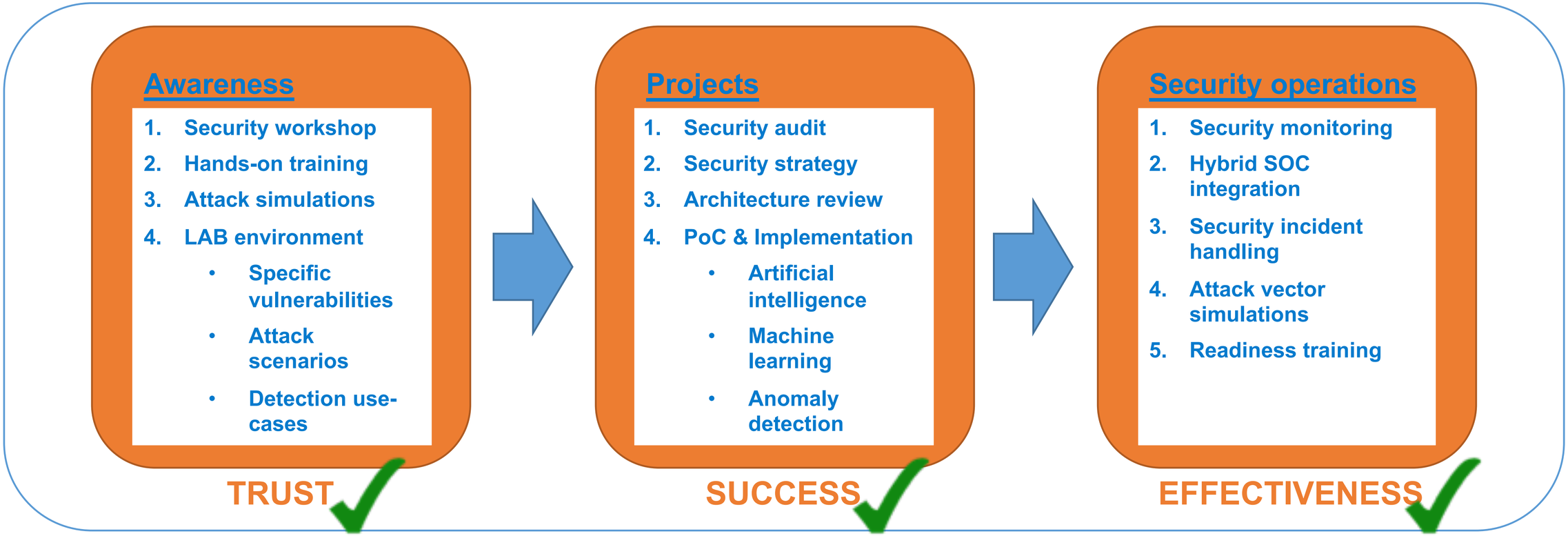
- 61850 - GOOSE
- 60870-5-101
- 60870-5-104



SYSTÉMOVÁ ARCHITEKTURA A INTEGRACE



PŘEDSTAVENÍ SPOLEČNOSTI - NÁŠ PŘÍSTUP



DEMONSTRACE ÚTOKŮ NA SCADA SOUSTAVU

ĎEKUJI ZA POZORNOST

??? OTÁZKY ???