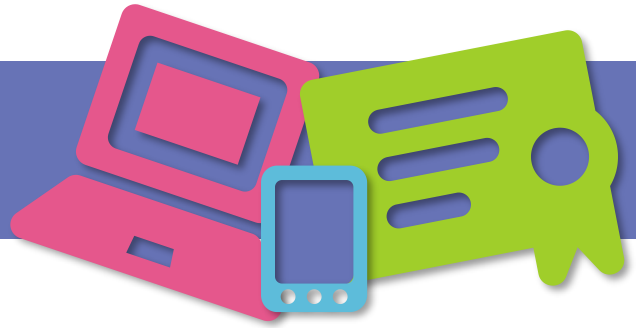
SECURITY 2015

23. ročník konference o bezpečnosti v ICT



SCADA? Jasně, to slovo znám …

Libor Kovář
CSO, ČEZ ICT Services, a. s.
Head of Corporate CyberSec Group

Pavel Hejduk
CSIRT Team Leader, ČEZ ICT Services, a. s.
CISO, Telco Pro Services, a. s.

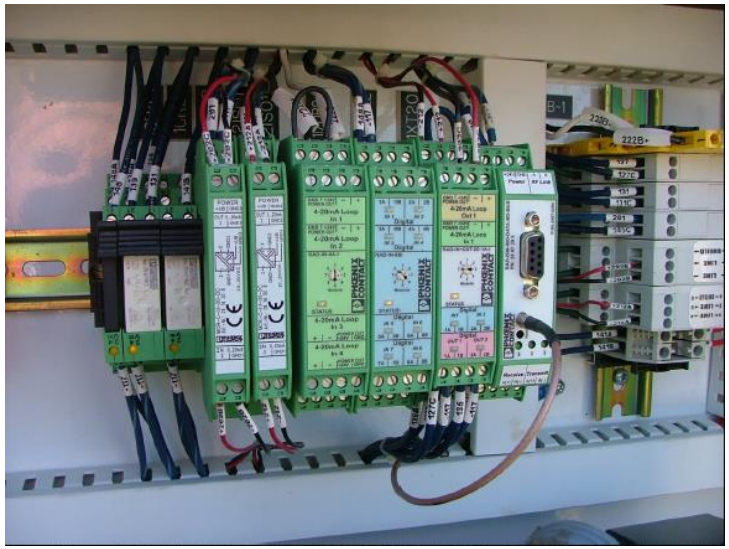
AGENDA

- Co je a co není SCADA
- Představy a realita o SCADA systémech
- Průmyslový malware – opakování
- SCADA schematicky, ale prakticky
- Testujeme SCADA
- Závěr, doporučení

Co není SCADA systém

- Bezpečnostní a kontrolní zařízení
- Elektrické / elektronické zařízení
- Single-box řešení / aplikace
- Uživatelské prostředí

RTU - Remote Terminal Unit



PLC – Programmable Logic Controller

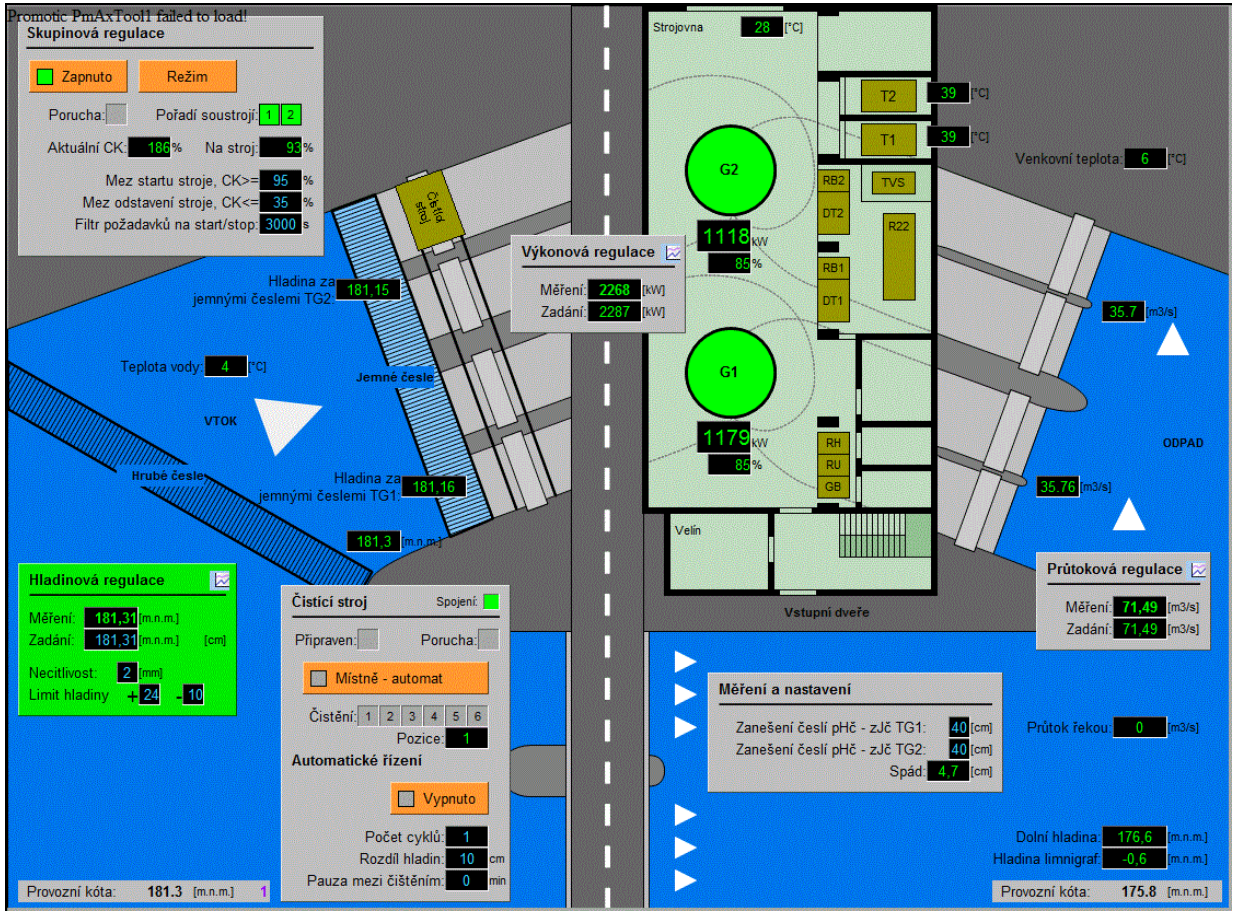
Zdroj: Internet

Co je SCADA systém

SCADA – „Supervisory control and data acquisition - Dispečerské řízení a sběr dat“

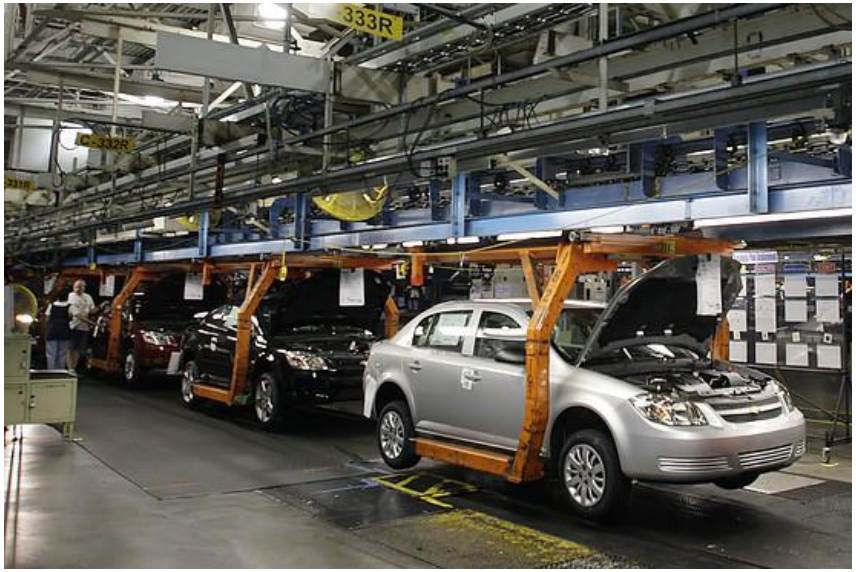
Jedná se o průmyslové řídící systémy (Indrustry control systems)

- Centrální monitoring a ovládání zařízení a procesů
- Ukládání historie dat
- Přenos dat do dalších zařízení / systémů
- Přesné měření technologických dat



Proč potřebuje SCADA výpočetní systémy

- Zařízení závisí na velmi rychlé odezvě
- Je nutné shromažďovat velký objem dat
- Stovky až tisíce zařízení jsou řízeny současně
- Jedná se o téměř nepřerušovaný provoz



Zdroj: Internet

Co se může stát v případě chyby?

Havárie ruské vodní elektrárny – 12 mrtvých zaměstnanců

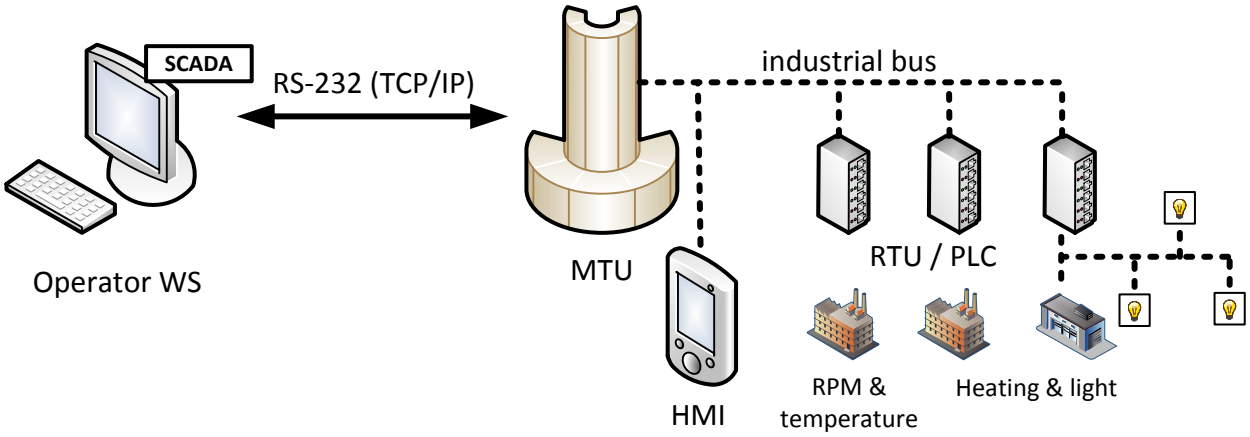
Havárie chemické továrny v Německu – stovky tun toxického odpadu v řekách

Exploze chemické továrny v Číně – 5 nezvěstných, 15 zraněných

Zdroj: Internet

Mylné představy o SCADA

- **SCADA sítě jsou izolovány a nemají prostupy na internet**
- **Používáme vlastní / upravené systémy, protokoly a zařízení, které nejsou napadnutelné**
- **HMI / kontrolní interface systémy mají omezenou funkcionalitu a/nebo omezení a tím pádem nemohou být napadnutelné**



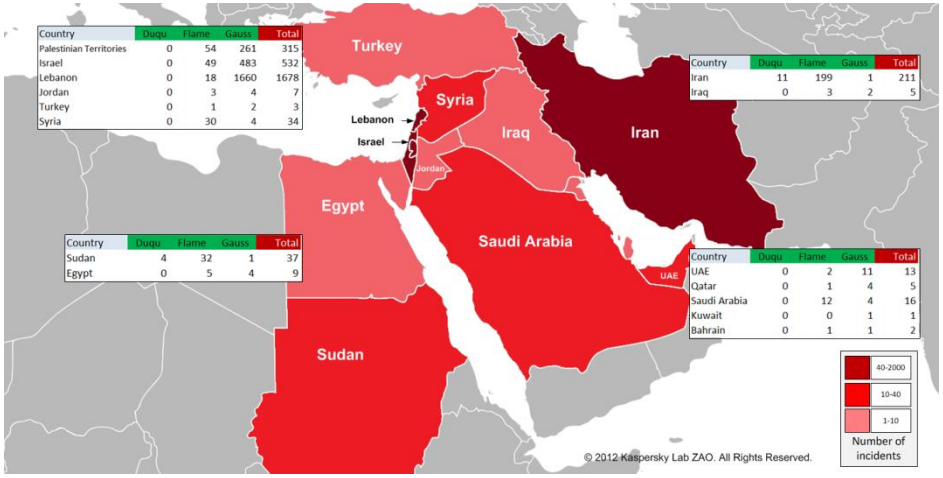
Realita SCADA systémů

- **Všechny průmyslové sítě jsou určitým způsobem napojeny na internet nebo korporátní síť**
  - Integrační software (ERP, údržba), telefon/modem/3G, špatná konfigurace síťových prvků (switche, routery, firewally), vyjímatelná média, vzdálený přístup
- **Většina sítí je provozováno operátory s nízkou IT znalostí**
  - Způsobují bezpečnostní incidenty, provádí nebezpečné činnosti během pracovní doby na výpočetních zařízení (hry, nebezpečné web stránky, stahování), informační bezpečnost je nezajímá, pouze chtějí dělat svou práci
- **Většina sítí a serverů je spravováno IT personálem**
  - Nízká znalost průmyslových řídících systémů, dopadů hackerských útoků, způsobují množství chyb při nastavení zařízení
- **99,9 % průmyslových zařízení je lehce „hackovatelných“**
  - Běžné OS (Windows/Linux), běžné / nezabezpečené protokoly (HTTP, Telnet, Modbus), neaktualizované aplikace, jednoduchá prolomitelná hesla, množství aplikačních zranitelností

Průmyslový malware - opakování

- **Stuxnet** (2010) – První známá kybernetická zbraň
  - továrna Natanz (obohacování uranu), Írán
  - Využíval zranitelnosti Siemens WinCC, PLC

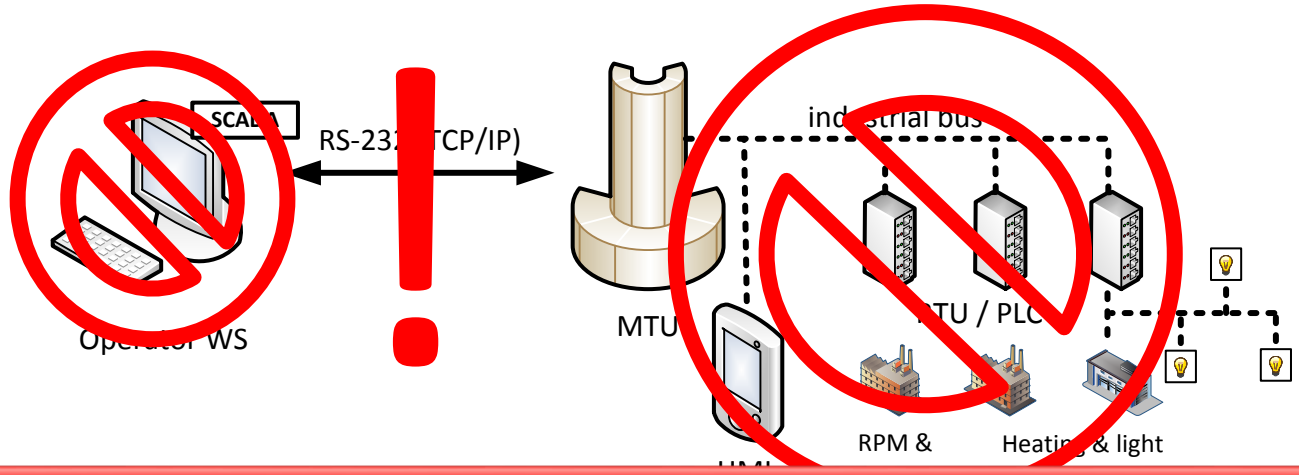
- **DuQu** (2011) – zaměřen na špionáž
  - SW a HW průmyslových řídících systémů po celém světě
  - Využíval jednu zranitelnost Microsoft



SCADA? Jasně, to slovo znám …

Je praxe skutečně taková?

SCADA schematicky



TAK TOHLE NEJDE ZABEZPEČIT!

SCADA key features:

- GUI
- Alarms
- Trends
- Scalability
- History data

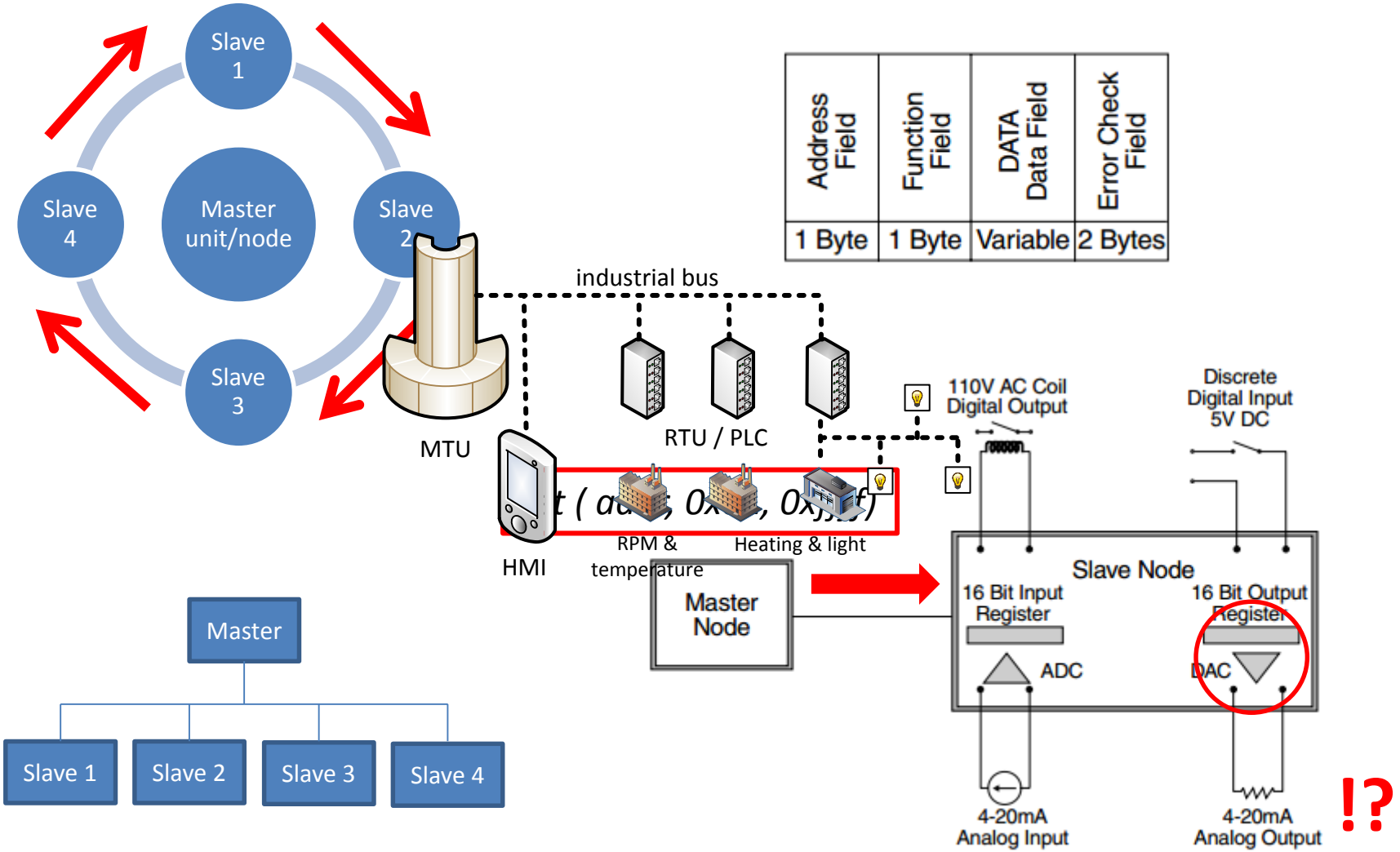
SCADA comm layers:

- RS232/RS422/RS485
- 20mA current loop
- Modems, radio
- Ethernet / WIFI

SCADA protocols:

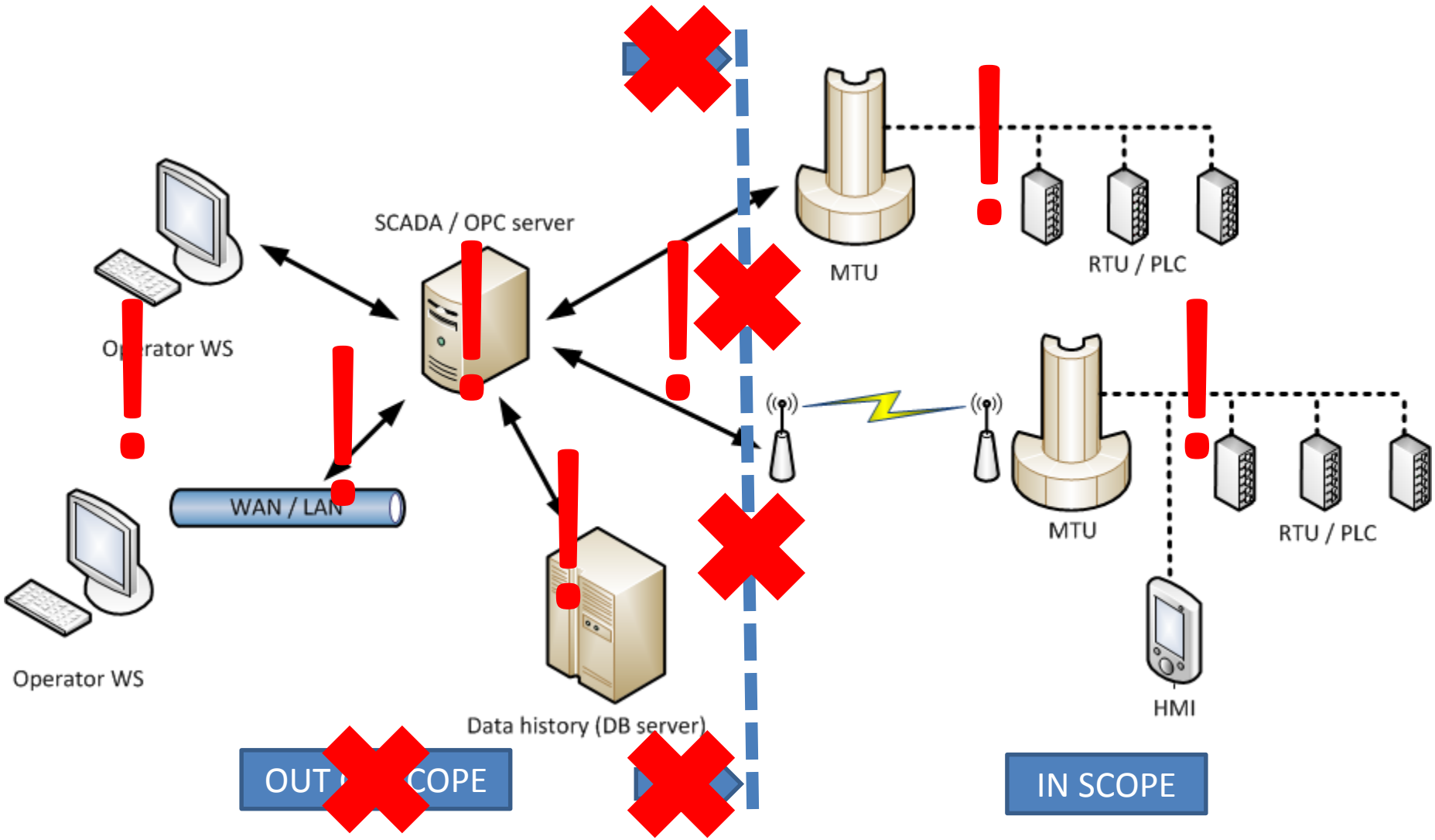
- HDLC
- MODBUS/ProfiBus
- BACnet
- DNP3, IEC60870, …

SCADA – MTU/RTU/PLC



Zdroj: https://www.fer.unizg.hr

SCADA schematicky & realisticky



Jak se (ne)stát SCADA testerem

Fiktivní příběh: Byl jednou jeden pracovní den …

… šéf vychází z kanceláře s telefonem na uchu a dokončuje hovor:

šéf: *„… jasně, kluci se na to přijedou mrknout … v klidu, to zvládnou …“*. Pokládá telefon. ***„Hoši, zbalte si fidlátka, pojedete testovat SCADU do elektrárny na severu …“***

geek: ***„Hmm, SCADA! Jasně, to slovo znám …“***.

Jakmile šéf zmizí, geek píše do Googlu:

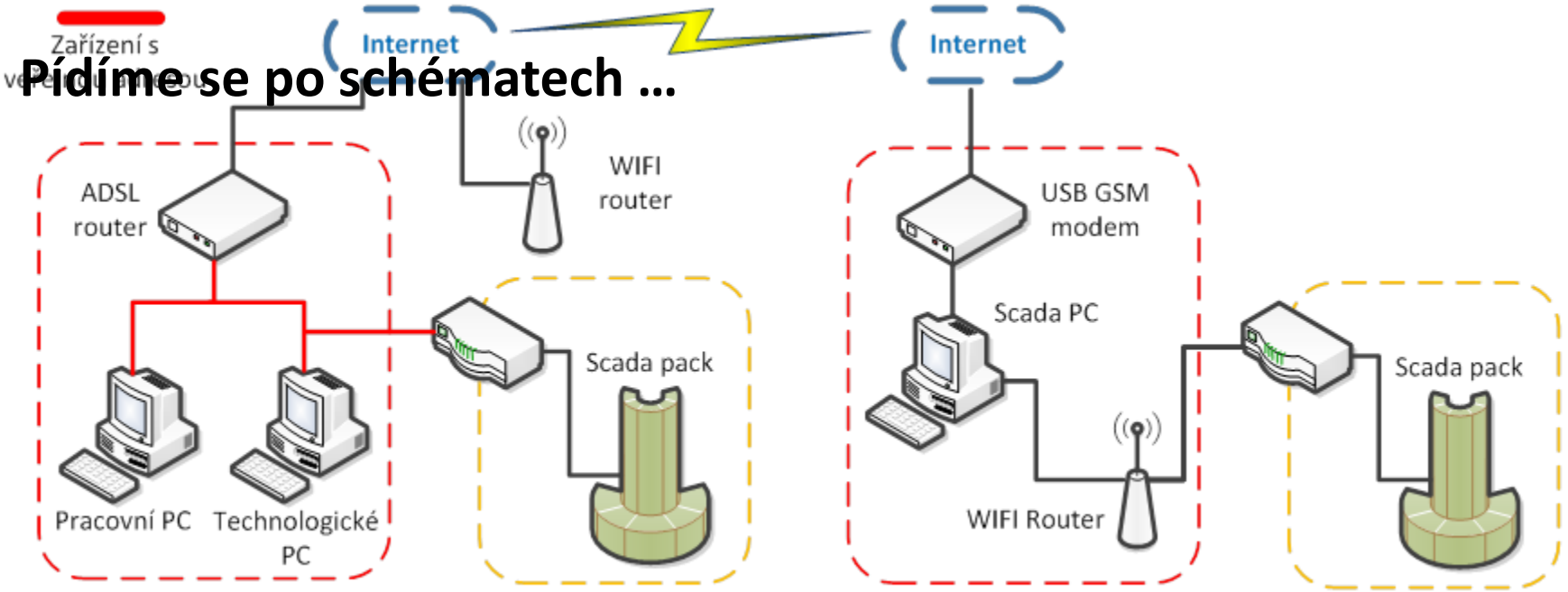
„S … C … A … D … A“

Nalezeno přibližně 21 300 000 záznamů

geek: „Hmm, to bude dlouhá noc ☹ … potřebuju víc kafe …“

SCADA poprvé

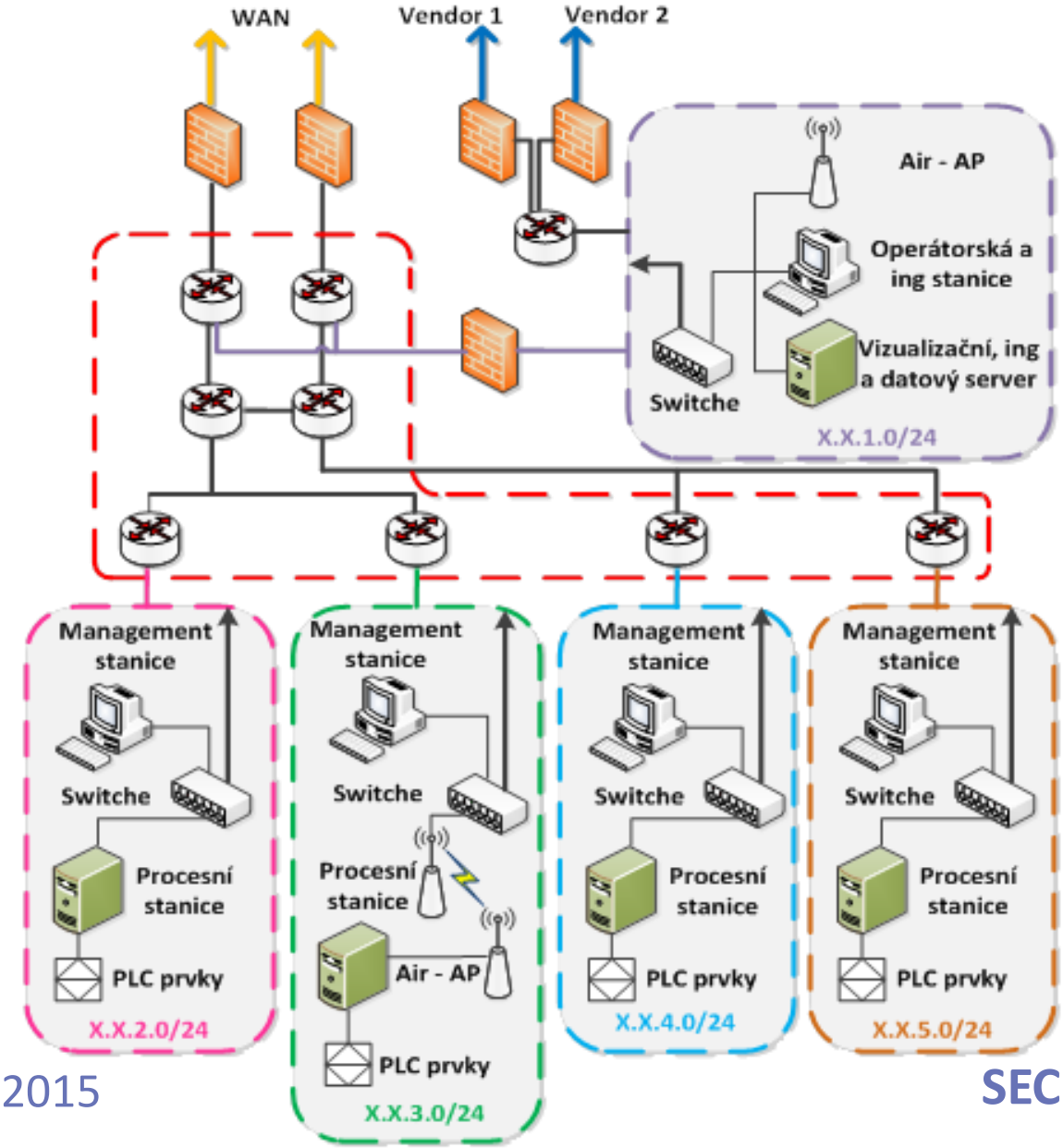
Pídíme se po schématech …



Bezpečnostní chyby „by design“

- Nesystematická architektura ICT infrastruktury
- Veřejná adresace PC
- Chybějící bariérová ochrana, preventivní opatření
- Remote site přes Internet bez VPN
- Vzdálené přístupy dodavatele bez VPN

SCADA podruhé



S čím začít, aneb testujeme SCADA

- Co to vlastně jdeme testovat?
  - PLC, MTU/RTU, Modbus, Profibus, …
  - Operátorské stanice (PC s Windows …)
  - Síťová infrastruktura (switche, routery, modemy ..)
  - Servery (Unix/WIN, DB, …)

- Co se na to hodí?
  - Běžné tooly (nmap, tcpdump, …)
  - Scannery se SCADA pluginy
  - Zdravý rozum …
  - Google ;-)

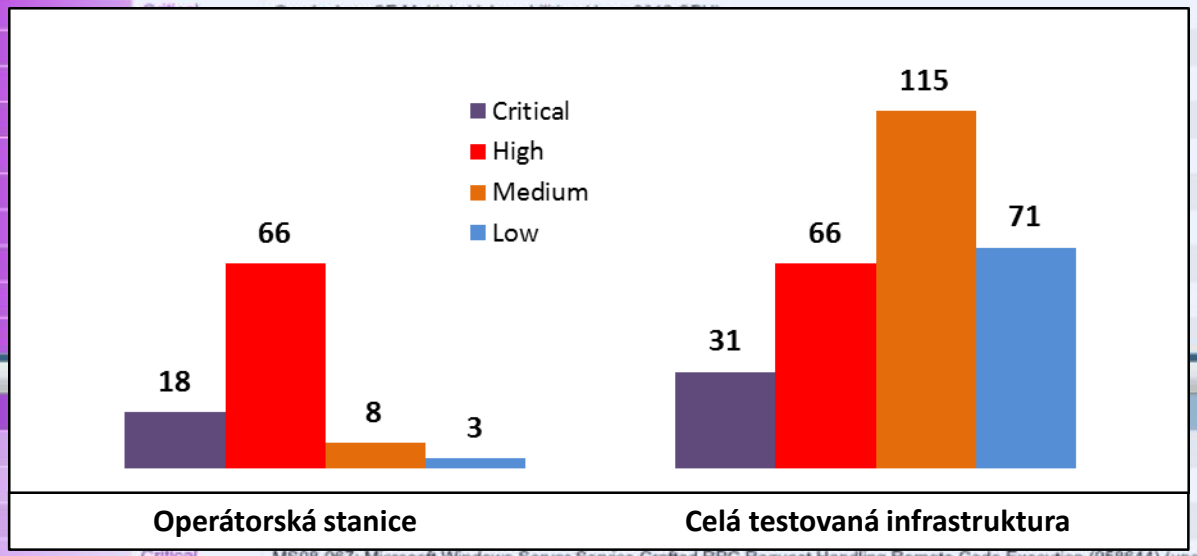
To není problém SCADA nebo ano?

První výsledky …

Rozsah	OS	Detekované služby
X.X.1.0/24	Windows XP	RPC, HTTP, FTP, NetBIOS
	Windows 7	RPC, HTTP, FTP, NetBIOS
	Windows 2003 server	RPC, HTTP, NetBIOS, Terminal services
	Síťové prvky (3Com, Cisco..)	HTTP, telnet, SSH
	PLC a automaty	HTTP, TMS
X.X.2.0/24	Windows 7	IRC, RPC, HTTP,
	Windows XP	RPC, NetBIOS,
	Windows 2003 server	RPC, NetBIOS, SQL, IRC
	Síťové prvky (Alied Telesyn, Moxa, 3Com)	HTTP, SSH, Telnet
X.X.3.0/24	Unix (HP-UX)	SMTP, FTP, Telnet, X11
X.X.4.0/24	Windows XP	RPC, PRINT server
	Unix (Linux)	FTP, SSH, Telnet, X11
X.X.5.0/24	Unix (HP-UX)	FTP, SSH, Telnet, NFS, POP3, SMTP
X.X.6.0/24	Unix (HP-UX)	FTP, SSH, Telnet, NFS, POP3, SMTP
X.X.7.0/24	Unix (HP-UX)	FTP, SSH, Telnet, NFS, POP3, SMTP, IMAP, X11

SCADA Windows komponenty

Plugin ID	Count	Severity	Name	Family
48405	1	Critical	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)	Windows
49996	1	Critical	Oracle Java SE Multiple Vulnerabilities (October 2010 CPU)	Windows
52002	1	Critical	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Windows
53503	1	Critical	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)	Windows
54997	1	Critical	Oracle Java SE Multiple Vulnerabilities (June 2011 CPU)	Windows
56213	1	Critical	Adobe Reader Unsupported Version Detection	Windows
56566	1	Critical	Oracle Java SE Multiple Vulnerabilities (Oct 2011 CPU)	Windows
57959	1	Critical	Oracle Java SE Multiple Vulnerabilities (Feb 2012 CPU)	Windows
59462	1			Windows
62593	1			Windows
64454	1			Windows
64790	1			Windows
65995	1			Windows
66932	1			Windows
70472	1			Windows
71966	1			Windows
73182	1			Windows
73570	1			Windows



Plugin ID	Count			Family
73182	21			Windows
11890	1			Windows
19948	1			Misc.
22194	1			Windows
34477	1	Critical	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)	Windows
35362	1	Critical	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)	Windows
47709	1	Critical	Microsoft Windows 2000 Unsupported Installation Detection	Windows
48405	1	Critical	MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214) (remote check)	Windows
53503	1	Critical	MS11-020: Vulnerability in SMB Server Could Allow Remote Code Execution (2508429) (remote check)	Windows
53514	1	Critical	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)	Windows
66349	1	Critical	X Server Unauthenticated Access: Screenshot	Misc.

Operátorské stanice

Typ zranitelnosti	Microsoft Windows Administrator Default Password Detection
Popis	Zjištěno defaultní (známé) heslo pro bulit-in účet „administrator“ v systému Windows
Důsledky a rizika	Útočník se může bez problémů přihlásit ke stanici a provádět úpravy v systému s plným oprávněním.
Doporučené řešení	Změna hesla pro účet „administrator“ v systému Windows

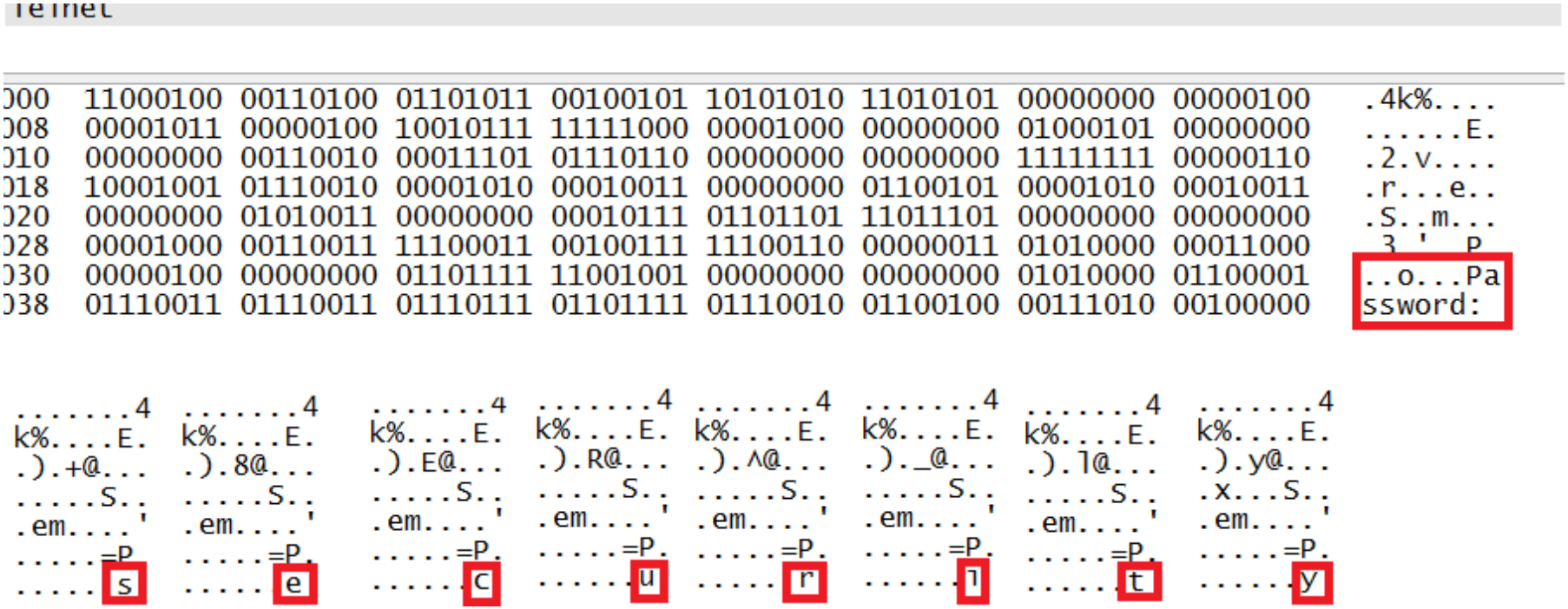
Typ zranitelnosti	Remote Code Execution – RPC, Buffer overflow, SMB, …
Popis	Stanice/systém je náchylná k zneužití, pomocí vzdáleného nebo lokálního spuštění kódu. To lze využít ke spuštění speciálního kódu, který nebude zjištěn AV ochranou.
Důsledky a rizika	Kód (skript) může provést např. eskalaci oprávnění uživatele nebo aktivovat na stanici malwarový program.
Doporučené řešení	Problém souvisí s neaktualizací OS a také používaných aplikací. Řešením je tedy aktualizace/vypnutí aplikací.

PLC / MTU / RTU …

- Příprava nutná …
  - Studujte dokumentaci … co vendor, to specifika
  - Věnujte se místním odlišnostem
  - Nezkoušejte plošné /exploring scany ani pakety s „větším“ payloadem
- Testujte pouze PLC odstavených technologií
- Typické zranitelnosti
  - „IP nestabilita“
  - Defaultní hesla, chybějící autentizace
  - Otevřené protokoly

A co switche … ?

„Dodavatel pouští telnet na switch … jaké je asi heslo???“



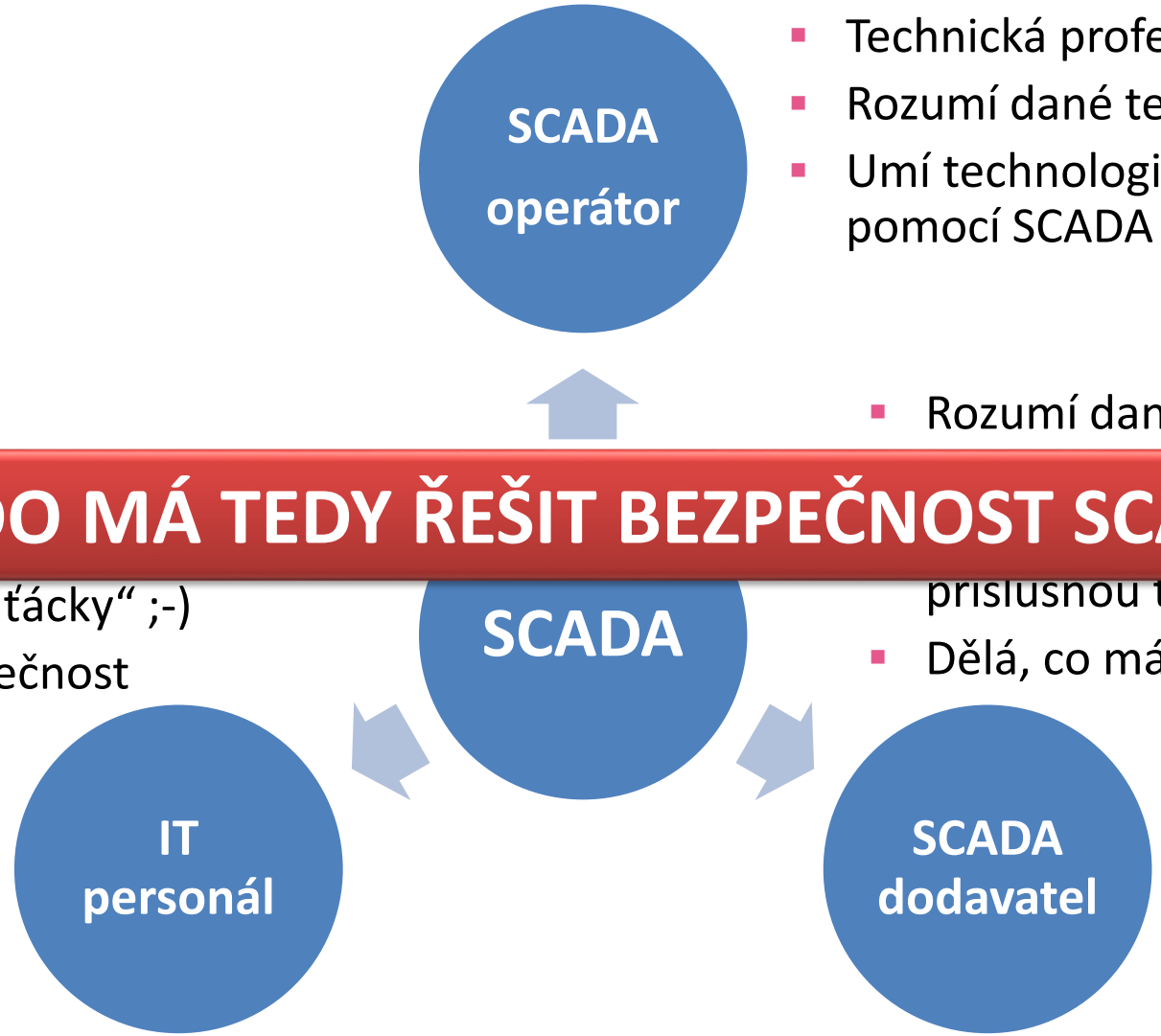
„Hmmm, … to jsem taky mohl vygooglit …“

Končím s testováním … zeptám se

Požadavek	Výsledek	Poznámka
Jednotný registr identity	NESOULAD	Neexistuje jednotné místo s uvedením všech účtů, které mají oprávněný přístupu do systému
Jednotná autentizace	SOULAD	
Správa identit	NESOULAD	Neexistuje centrální řízení správy identit
Autorizační koncept	NESOULAD	Neexistuje dokument s přesným popisem jednotlivých uživatelských či administrátorských účtů a rolí
Přidělování přístupů	NESOULAD	Neexistuje schvalovací workflow, které by proces přidělení přístupu/role řídilo.
Uložení hesel k admin účtům	NESOULAD	Hesla k účtům root či administrator nejsou uložena na zabezpečeném místě.
Minimální délka hesla	NESOULAD	Minimální délka hesla není vyžadována žádnými politikami či procesy
Komplexita hesla	NESOULAD	Komplexita hesla není vyžadována / vynucena.
Expirace hesla	NESOULAD	Maximální doba platnosti hesla není procesně vyžadována / vynucena.
Změny dočasných hesel	NESOULAD	Není zajištěno, že dočasná hesla se mění při prvním přihlášení
Vícefaktorová autentizace	N/A	
Volně přístupná hesla	SOULAD	
Hlášení ztrát autentizačních prostředků	SOULAD	
Záznam použití administrátorského hesla	SOULAD	
Pravidelný audit nastavení oprávnění	NESOULAD	Kontrola nastavených oprávnění není kontrolována pravidelně

Tak už dost … někde jsem tu měl security checklist

SCADA Babylon



Závěr, doporučení

- Stanovte odpovědnosti
- Stanovte politiku a pravidla
  - Pro operátory
  - Pro dodavatele
  - Pro ICT
- Nerezignujte na ověřené bezpečnostní principy
  - Řiďte rizika – chraňte to důležité
  - Volte správnou architekturu
  - Nebojte se segmentace, použijte bariérovou ochranu
  - Vyžadujte bezpečnost od dodavatele SCADA
  - Dbejte na bezpečnost infrastruktury, system hardening
  - …

SECURITY 2015

23. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Libor Kovář <libor.kovar@cez.cz>
ČEZ ICT Services, a. s.
Pavel Hejduk <pavel.hejduk@cez.cz>
ČEZ ICT Services, a. s.