INTERNATIONAL FORUM FOR CLEAN ENERGY TECHNOLOGIES

ЕПС ДИСТРИБУЦИЈА

ENERGETSKA DIGITALNA PERSPEKTIVA SRBIJE

PRETNJE I TIPSKA REŠENJA BEZBEDNIH INDUSTRIJSKIH MREŽA

Slavko K. DUBAČKIĆ
Aleksandar M. BOŠKOVIĆ
Đorđe Ž. VLADISAVLJEVIĆ

Novi Sad, 29-30. oktobar 2019.

ЕПС ДИСТРИБУЦИЈА

UVOD

- **Šta su OT sistemi?**

  Operativne tehnologije (OT) čine sistemi namenjeni nadzoru, kontroli i upravljanju uređajima u industrijskim sistemima, transportu, komunalnim sistemima

- **IT – OT konvergencija**

  Povezivanje korišćenjem IT tehnologija omogućuje bolje praćenje sistema, mogućnost daljinske kontrole i upravljanja fizičkim uređajima

- **Zašto je OT bezbednost važna?**

  Kako industrijski sistemi postaju sve više povezani, tako postaju i izloženiji napadima

ЕПС ДИСТРИБУЦИЈА

VRSTE PRETNJI U OT SISTEMIMA

- Malware i APT (Advanced Persistant Threat)
- Backdoor napadi preko mrežnog perimetra
- OPC/DCOM napadi (OLE for process control/ Distributed Componenet Object Model)
- Napadi na bazu podataka i data injection napadi
- Man-in-the-middle (MITM) napadi
- Supply Chain napadi
- BYOD napadi (Bring Your Own Device)

ЕПС ДИСТРИБУЦИЈА

ODNOS BEZBEDNOSTI IT I OT SISTEMA

Tema	Korporativna mreža	Industrijska mreža
Anti-virusni softver	Preporučeno, skoro neophodno	Retko implementirano, često nemoguće implementirati
Podrška za određenu tehnologiju	3-5 godina, EOS – EOL	Rešenja su dizajnirana da traju preko 20 godina
Outsourcing	Često se koristi	Retko se koristi
Instalacija zakrpa	Redovna, od mesečnog do reda veličine sekunde.	Ne radi se često, pre svega zbog pouzdanosti sistema
Kritičnost usluga	Odlaganje od par sati ili dana je moguće	Odlaganje je neprihvatljivo
Dostupnost	Nedostupnost je moguća	Nedostupnost je neprihvatljiva
Fizička sigurnost	Veoma osigurane prostorije data centara	Lokacije su udaljene i bez ljudskog prisustva

ЕПС ДИСТРИБУЦИЈА

BLACKOUT

- **14. avgust 2003. - najveći *blackout* u istoriji Severne Amerike**

  Palo nekoliko stabala u severnom Ohaju.

  Lančano zahvatio severozapad SAD i deo Kanade, 50 miliona ljudi, 11 ljudi stradalo, šteta: 6mlrd. USD.

- **2010. Stuxnet - Iran**

  Malware dizajniran za napad na SCADA sisteme.

  Ozbiljne štete na nuklearnom programu.

- **23. decembar 2015. - Ukrajina**

  30 trafostanica je isključeno, oko 230.000 isključeno u periodu od 1 do 6 sata.

  Neisporučena energija 73MWh.

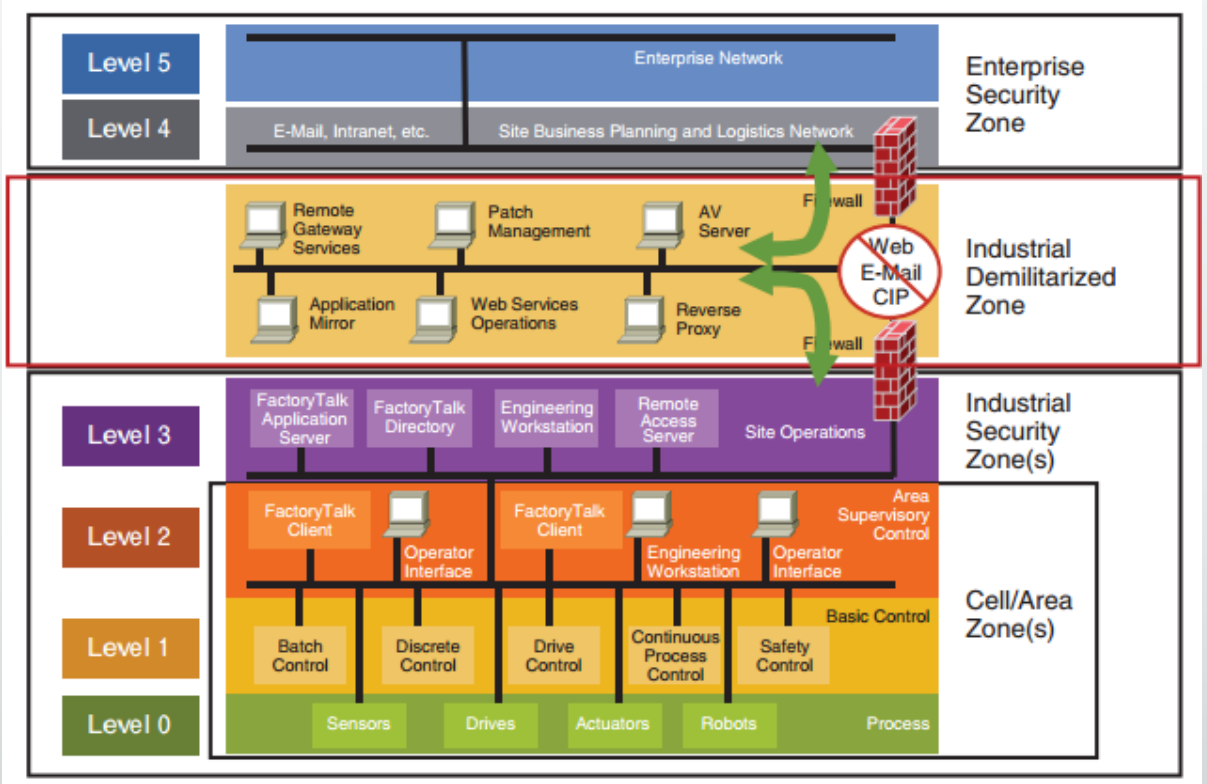
ZAŠTITA – PURDUE MODEL

- **Purdue Enterprise Reference Architecture (PERA)**

  Model za segmentaciju kontrolnih sistema

- **Tri zone i šest nivoa segmentacije**

  1. Poslovna zona
     - Nivo 5: Poslovna mreža
     - Nivo 4: Planiranje i logistika
  2. Industrijska demilitarizovana zona (IDMZ)
  3. Industrijska zona
     - Nivo 3: Lokalne operacije
     - Nivo 2: Nadgledanje
     - Nivo 1: Kontrolni novi
     - Nivo 0: Proizvodni procesi



OT LAN TIP 1 I OT LAN TIP 2

- **OT LAN Tip 1**

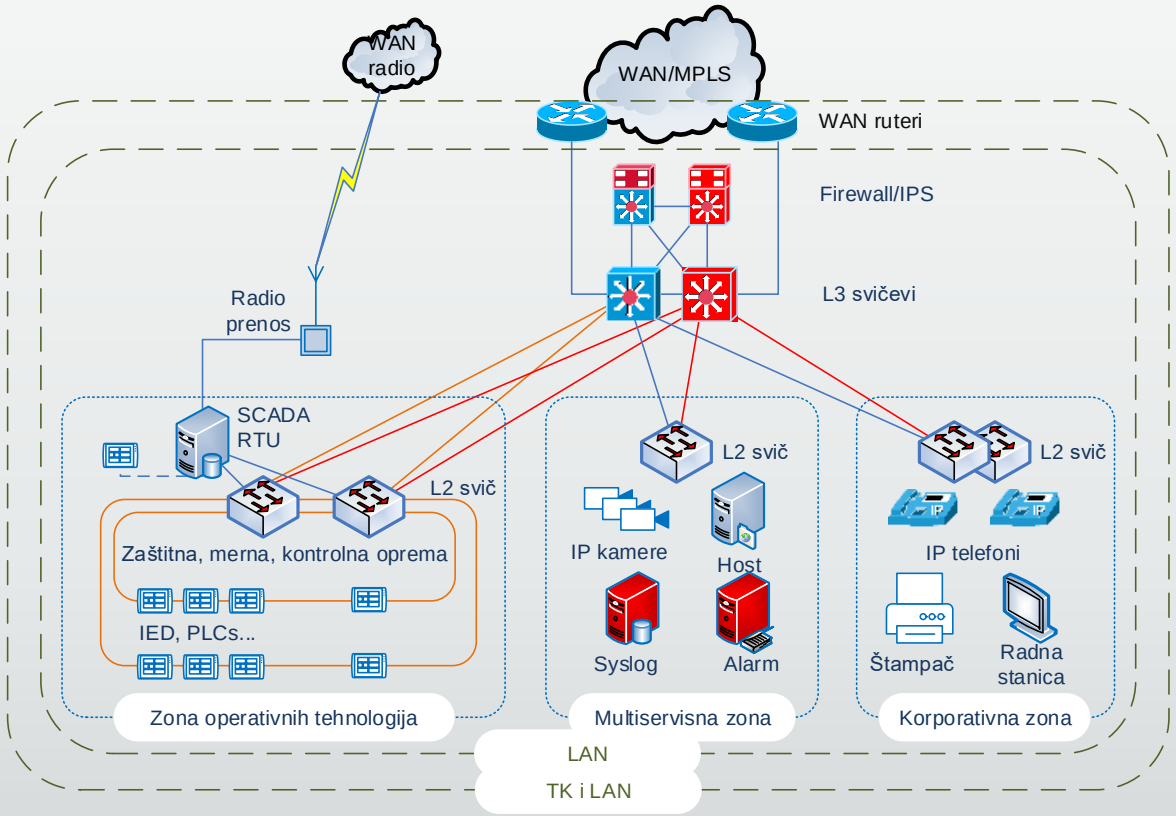
  Složeno industrijsko okruženje koje obuhvata i OT i IT mrežne segmente, sa visokim zahtevima po pitanju dostupnosti, raspoloživosti i drugih bezbednosnih aspekata.

  Redundatne veze prema centralnoj lokaciji i više desetina različitih uređaja u lokalnoj mreži.

- **OT LAN Tip 2**

  Segmentiran na isti način kao i Objekat Tip 1 samo pojedine komponente nisu realizovane u redundansi (bez crvenih elemenata na slici 3.).

  Razlozi za ovo mogu biti od nivoa značaja objekta, nekih tehničkih ograničenja, nasleđene opreme do finansijskih razloga.



OT LAN TIP 3 I OT LAN TIP 4

- **OT LAN Tip 3**

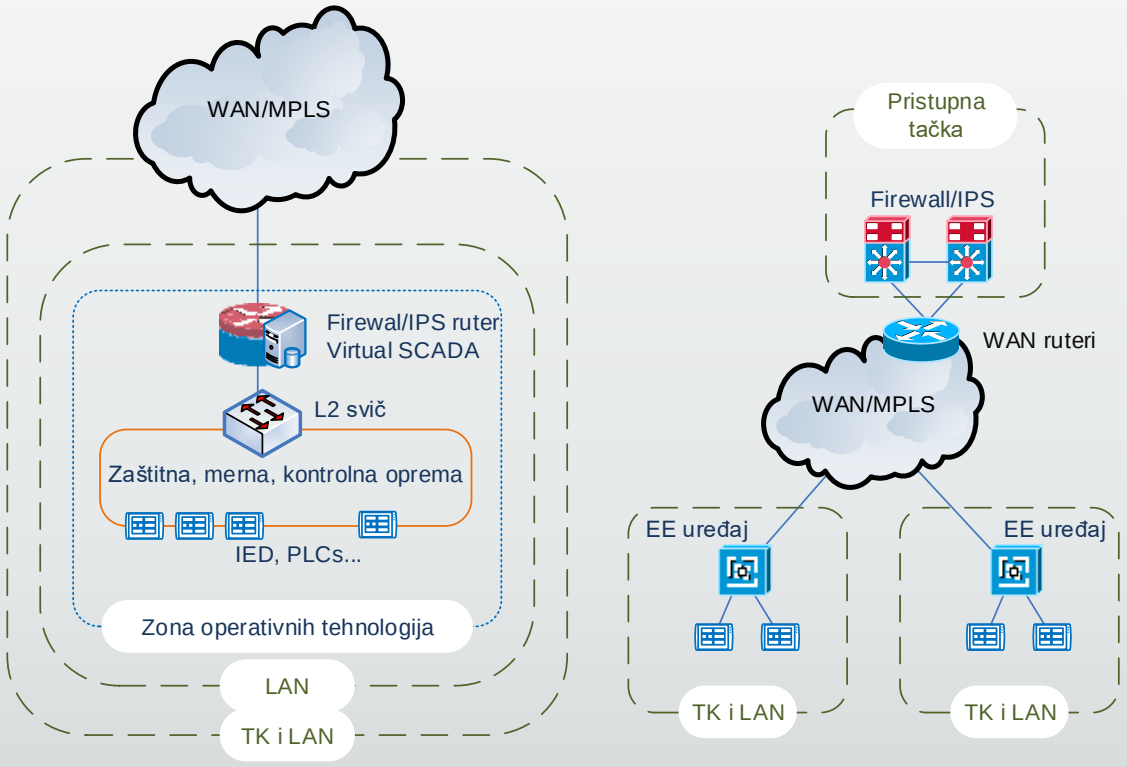
  Jednostavna lokalna mrežna infrastuktura.

  Veze prema centralnoj lokaciji i nekoliko uređaja u lokalnoj mreži.

- **OT LAN Tip 4– Objekti sa izmeštenom zaštitom**

  Vrlo jednostavna lokalna mrežna infrastuktura.

  Veze prema centralnoj lokaciji i nekoliko ili često samo jedan uređaj u lokalnoj mreži.



ЕПС ДИСТРИБУЦИЈА

ZAKLJUČAK

- **Umesto zaključka evo sedam preporuka koje bi trebalo primeniti da bi OT sistemi bili spremni za bezbednosne izazove:**
  1. Uložite u nadogradnju OT mreža.
  2. Postavite teška pitanja i definišite odgovornost.
  3. Priznajte svoje nedostatke.
  4. Proverite da li postoji segmentacija između vaših IT i OT mreža.
  5. Učinite OT mrežu vidljivom.
  6. Zaštita OT mreža nije jednokratna vežba.
  7. Edukujte rukovodioce o uticaju napada na OT mreže.

INTERNATIONAL FORUM FOR CLEAN ENERGY TECHNOLOGIES

ЕПС ДИСТРИБУЦИЈА

HVALA NA PAŽNJI

EPS Distribucija, Beograd