Poslijediplomski specijalistički studij „Informacijska sigurnost“

Laboratorij za informacijsku sigurnosti i privatnost

Udruga MIPRO – Savjetovanje Sigurnost informacijskih sustava

Sigurnost upravljačkih sustava

Doc. dr. sc. Stjepan Groš
Izv. prof. dr. sc. Mario Vašak

Sveučilište u Zagrebu

Fakultet elektrotehnike i računarstva

Sadržaj

- Ukratko o predavanju
- Razvoj upravljačkih sustava prema IT-ju
- Incidenti u upravljačkim sustavima
- Istraživanje ranjivosti upravljačkih sustava
- Primjer analize jednostavnog sustava
- Što dalje?

O predavanju (1)

- Svrha
  - Osvještavanje dionika koji su uključeni u dizajn, izgradnju, instalaciju, nadzor i održavanje upravljačkih sustava
  - Potaknuti raspravu o sigurnosti upravljačkih sustava u Hrvatskoj
- Za koga je predavanje?
  - Stručnjake koji se bave razvojem, implementacijom i održavanjem raznih upravljačkih sustava…
  - … **ali, nisu stručnjaci za informacijsku sigurnost**.

O predavanju (2)

- Na predavanju su radili:
  - Groš
    - Područja interesa računalne mreže, operacijski sustavi, sigurnost navedenih sustava i općenito sigurnost
  - Vašak
    - Područje interesa: upravljački sustavi za obnovljive izvore energije, zgrade i infrastrukturne sustave, te u industrijskim postrojenjima
  - Jelenković
    - Područje interesa ugrađeni sustavi (engl. embedded) i operacijski sustave

Kakvi su upravljački sustavi nekada bili…

- Izolirani
  - „Air-gap principle”
- Specifična tehnologija
  - Sklopovlje
  - Programska podrška
  - Komunikacija
- Izrađeni po narudžbi
- *Sigurnost temeljena na izolaciji i skrivanju (engl. obfuscation)*

… i kakvi su danas …

- Upotreba komercijalnih „off-the-shelf” komponenti
  - Windows/Linux operacijski sustavi, osobna računala, mrežni uređaji
- Upotreba standardiziranih tehnologija
  - Mrežni protokoli (TCP/IP/Ethernet)
- Spajanje na Internet i integracija s poslovnim sustavima
  - Radi lakšeg pristupa i održavanja
  - Upravljanje korištenjem informacija dostupnih preko mreže (npr. vremenske prognoze)
  - Dohvat podataka bitnih za upravljanje poslovanjem

… ipak neke stvari se nisu promijenile

- Kritični sustavi
  - Pogreške u radu mogu biti katastrofalne!
- Dugogodišnja upotreba
  - Sustavi se upotrebljavaju godinama, desetljećima
- Mogu biti na teško dostupnim ili nedostupnim područjima
  - Raspodijeljeni po velikoj geografskoj površini
- Mogu sadržavati velik broj primitivnih komponenata

Okolina i prijetnje

- U razvoju upravljačkih sustava vodi se briga o
  - Fizičkoj sigurnosti (engl. safety)
  - Pouzdanosti (engl. reliability)
  - Raspoloživosti
- Prijetnje koje se razmatraju **djeluju slučajno**
- Novost su **namjerne prijetnje**
  - Kriminalne skupine, nezadovoljni (bivši) zaposlenici, teroristi, nacionalne države, aktivisti
  - Ne ponašaju se u skladu sa statističkim modelima kojima se modeliraju slučajne prijetnje

Što je novog iz informacijske sigurnosti

- Općenito sigurnost čine (minimalno) tri svojstva
  - Tajnost (engl. Confidentiality), Integritet (engl. Integrity), Raspoloživost (engl. Availability)
- U poslovnoj okolini koriste se *informacijske tehnologije* (IT)
  - Najbitnija je *tajnost informacija*, a potom integritet i raspoloživost
- U upravljačkim sustavima koriste se *operacijske tehnologije* (OT) – najbitnija *raspoloživost*, a potom integritet i tajnost
- **IT i OT konvergiraju s obzirom na korištene tehnologije!**
  - **interes za sigurnost u upravljačkim sustavima (engl. cyberphysical security)**

Treba li brinuti o sigurnosti u upravljačkim sustavima?

- Što kažu proizvođači opreme i sustava (ako ih se uopće nešto pita!)
  - Naši sustavi/komponente su sigurne!
  - Mi brinemo o sigurnosti!
- Neka pitanja
  - Jesu li proizvođači u pravu? Kako im možemo vjerovati?
  - Je li to dovoljno kako bi krajnji proizvod bio siguran?
  - Je li to dovoljno kako bi sustav u upotrebi bio siguran?
- Sve to, a i više, je već puno puta viđeno u sigurnosti informacijske tehnologije

INCIDENTI

FER

Stuxnet

- Primjer narušavanja sigurnosti postrojenja za obogaćivanje urana
- Vrlo sofisticiran i ciljan napad!
- Vjerojatno najpoznatiji i najčešće spominjani slučaj
- Baš zato nećemo puno o tom primjeru!

Napad na Ukrajinski energetski sustav (1)

- U cijelom događaju još je dosta stvari nejasno, ali u ovom trenutku je vrlo izvjesno da se radi o kibernetičkom napadu
- Tri komponente napada
  - Zloćudni kod (engl. malware)
  - DoS na telefonske sustave korisničke podrške
  - Za sada nepoznat način postizanja fizičke štete
    - Zloćudni kod ili direktna interakcija napadača s upravljačkim sustavima
- Direktni utjecaj na transformatorske stanice zbog kojih je 80,000 korisnika ostalo bez električne energije
- Oporavak brzim prebacivanjem na ručno upravljanje

https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

Napad na Ukrajinski energetski sustav (2)

- Što je za sada poznato da se dogodilo
  - Napadači pokrenuli inicijalne napade na produkcijske SCADA sustave
  - Zarazili radne stanice i poslužitelje
  - Zaslijepili dispečere DoS napadima
  - Djelovali s ciljem oštećivanja SCADA sustava
    - Otežavanje oporavka
    - Otežavanje forenzičke istrage
  - Preplavili korisničku podršku kako bi spriječili prijavu problema
- Još je puno nepoznanica te je potrebno vrijeme da se utvrde sve činjenice

Napad na Njemačku čeličanu

- Kraj 2014. godine
- Za ulazak u sustav korišten je napredni društveni inženjering
  - „Spear phishing” napad na operatere industrijskih procesa
  - Elektronička pošta je sadržavala zlćudni kod u privitku
  - Nakon pokretanja zlćudni kod je uspostavljao komunikaciju s napadačima
- Nakon ulaska napadači su prešli na upravljačku mrežu te ugasili visoku peć i na taj način prouzročili značajnu fizičku štetu

http://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf

Ostali incidenti

- Pojedini incidenti ne dođu do upravljačke mreže
  - Ne zbog zaštite već zbog nedostatka motiva napadača
- Nisu svi incidenti poznati iz dva razloga
  - Incidenti prođu neopaženo
  - Kada se dese zataškavaju se iz raznih razloga ili se ne žele objaviti informacije
- Na Internetu postoji baza incidenata specifično vezanih uz upravljačke sustave
  - The Repository of Industrial Security Incidents

http://www.risidata.com/

ISTRAŽIVANJA RANJIVOSTI

FER

Sigurnost upravljačkih sustava vlakova

- Istraživanje djelomično objavljeno ove godine na 32C3 (*32nd Chaos Communication Congress*)
  - Istraživanje obavila grupa pod nazivom *SCADA StrangeLove*
  - Dijelovi istraživanja napravljeni su po narudžbi za pojedine željeznice te su pod NDA i nisu objavljeni
- Identificirali sigurnosne probleme u upravljačkim sustavima vlakova
  - Zaključak: Nije teško kompromitirati upravljačke sustave vlakova ali zahtjeva specifična znanja i okoline za testiranje.
- Napadači mogu biti prvenstveno nacionalne države.

http://www.securityweek.com/trains-vulnerable-hacker-attacks-researchers

Sigurnost upravljačkih sustava vozila

- Sve više informacijskih tehnologija prisutno u automobilima
  - Kupci traže a proizvođači se takmiče tko će staviti više elektroničkih sustava u automobile – računala, komunikacijske mreže
    - Pretvaranje automobila u *pametne telefone*
  - Ti elektronički sustavi povezani su s upravljačkim sustavom
- Demonstracija napada na Jeep Cherokee tijekom vožnje na autocesti
  - Ranjivost zabavnog sustava omogućila je bilo kome tko zna IP adresu pristup automobilu i upravljanje njime

http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Sigurnost PLC uređaja

- INTERNET-FACING PLCS - A NEW BACK ORIFICE
  Johannes Klick & Stephan Lau & Daniel Marzin & Jan-Ole Malchow & Volker Roth
  BlackHat US 2015.
- PoC pretvaranja PLC-a spojenog na Internet u *gateway* koji omogućuje pristup internoj mreži
  - Konkretno na primjeru Siemens PLC
  - Na PLC-u ne postoji ispravna autentifikacija zbog čega je omogućen jednostavan pristup
- Implementirani SNMP skener i SOCKS posrednički poslužitelj – instalacija bez prekida rada PLC-a!

https://www.blackhat.com/us-15/briefings.html#internet-facing-plcs-a-new-back-orifice

Još problema

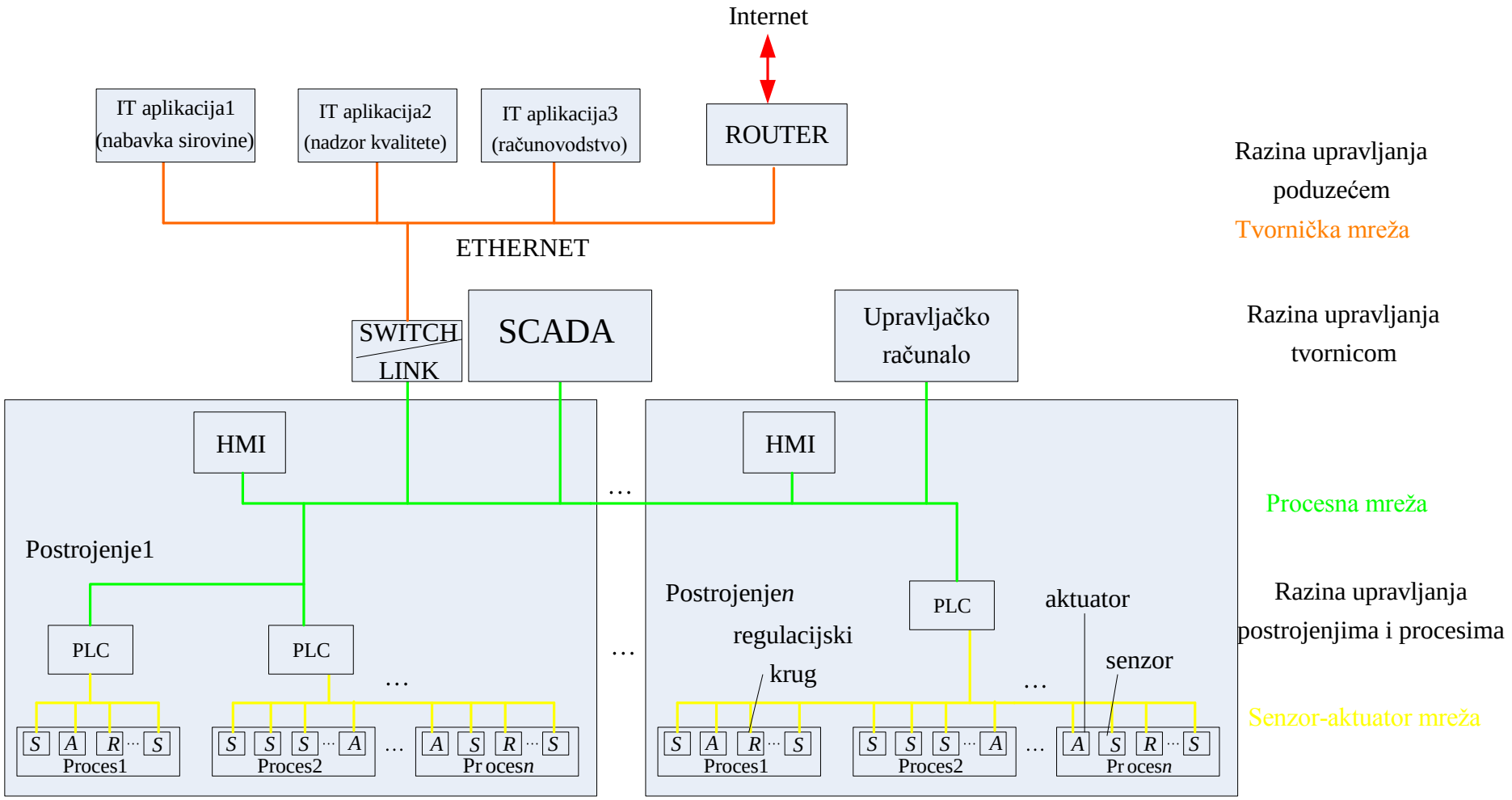
- Svi problemi koji se mogu naći u IT-ju zbog konvergecije mogu se pronaći i u OT-u
  - Zlćudni kod (engl. malware), ranjivosti u operacijskim sustavima i aplikacijama, društveni inženjering (engl. social engineering)
- Upravljačka oprema ima i svoje specifične probleme
  - ICS-CERT

Ostali upravljački sustavi

- Medicinska oprema i uređaji
  - Medicinska oprema također sve više koristi „off-the-shelf” komponente
  - Omogućuje priključak na računalnu mrežu radi dohvata podataka
  - Korištenje bežičnih mreža
- Internet stvari
  - Cilj je povezivanje svih mogućih uređaja na Internet
    - Frižideri, mašine za pranje rublja, televizori, …
  - Povezuju se uređaji kod kojih se ne vodi računa o sigurnosti
    - Niti oni koji ih povezuju vode računa o sigurnosti

PRIMJER ANALIZE TIPIČNOG SUSTAVA

Sigurnost upravljačkog sustava tvornice



Analiza mogućnosti ulaska napadača

- Analiza sigurnosti primjenom površine napada (engl. attack surface)
  - *Površina napada* su sva potencijalna mjesta ulaza napadača
- Površina napada upravljačkog sustava tvornice
  - Internet pristup preko kojeg napadači mogu pokušati ući u sustav
    - „Legalne” veze u mreži, ali i one nepoznate
  - Zaposlenici
    - Surfanje po zaraženim Web stranicama
    - Korištenje USB uređaja/CD-ROM diskova
    - Otkrivanje tajnih podataka (npr. lozinke, gubljenje računala)

Nakon ulaska

- Napadač prikriva tragove te se kreće po mreži prema upravljačkim dijelovima
- Potencijalne ranjivosti
  - Ethernet mreža nezaštićena
  - Skok između upravljačke i poslovne mreže nije zaštićen (u ovom slučaju)
  - Na upravljačkoj mreži koristi se opet Ethernet
  - Operacijski sustavi i aplikacije
  - Upravljačko računalo
  - Programabilni logički sklopovi (PLC)

Industrijski Ethernet

- Primjer preklopnika
  - Industrial Ethernet Switches SCALANCE X-300 / X-400
- Radi se o preklopniku s mogućnostima koje imaju „klasični” preklopnici
  - (R)STP, VLAN, SNMP, …
- Ethernet je mreža koju je teško zaštiti

Zaštita (1)

- Zaštita se mora provoditi u svakom koraku životnog ciklusa sustava
- *Dizajn i izgradnja sustava*
  - Analiza potencijalnih prijetnji
  - Upotreba tehnologija i proizvoda koje nemaju poznatih ranjivosti
  - Ako ima ranjivosti treba upotrijebiti dodatne zaštitne mehanizme
- *Implementaciju/Puštanje u pogon (comissioning)*
  - Tijekom implementacije mora se u potpunosti provesti zaštite predviđene tijekom dizajna sustava

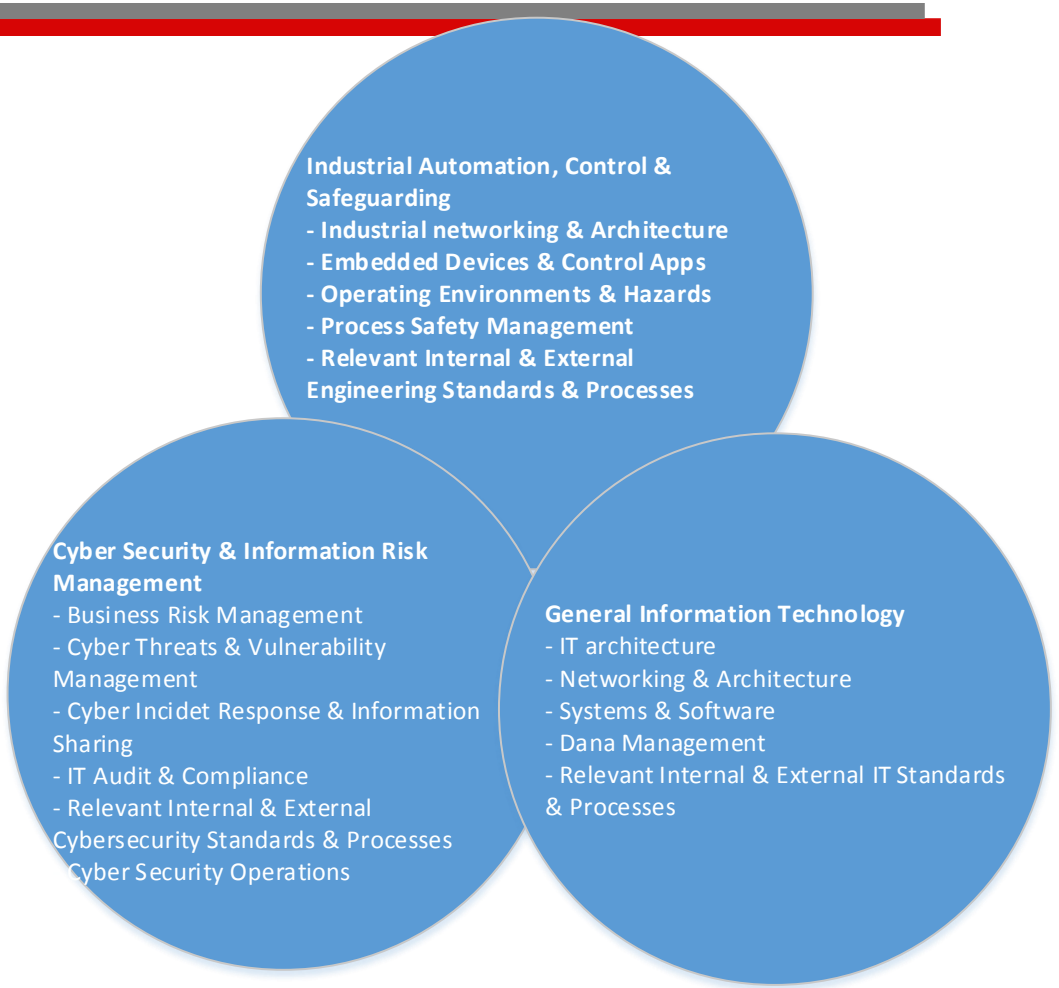
Zaštita (2)

- *Održavanje*
  - Procjena rizika – taktički alat
  - Edukacija
  - Stalno praćenje zbivanja
  - Redoviti nadzor sustava – revizije, penetracijska ispitivanja, ispitivanja ranjivosti
  - Primjena dobrih praksi

ŠTO DALJE?

Edukacija

- Razna certificiranja
  - SANS
  - FER InfoSig
- ENISA preporuka za certificiranje
  - Domene znanja koje je potrebno pokriti certificiranjem
- Praćenje raznih hakerskih i znanstvenih konferencija



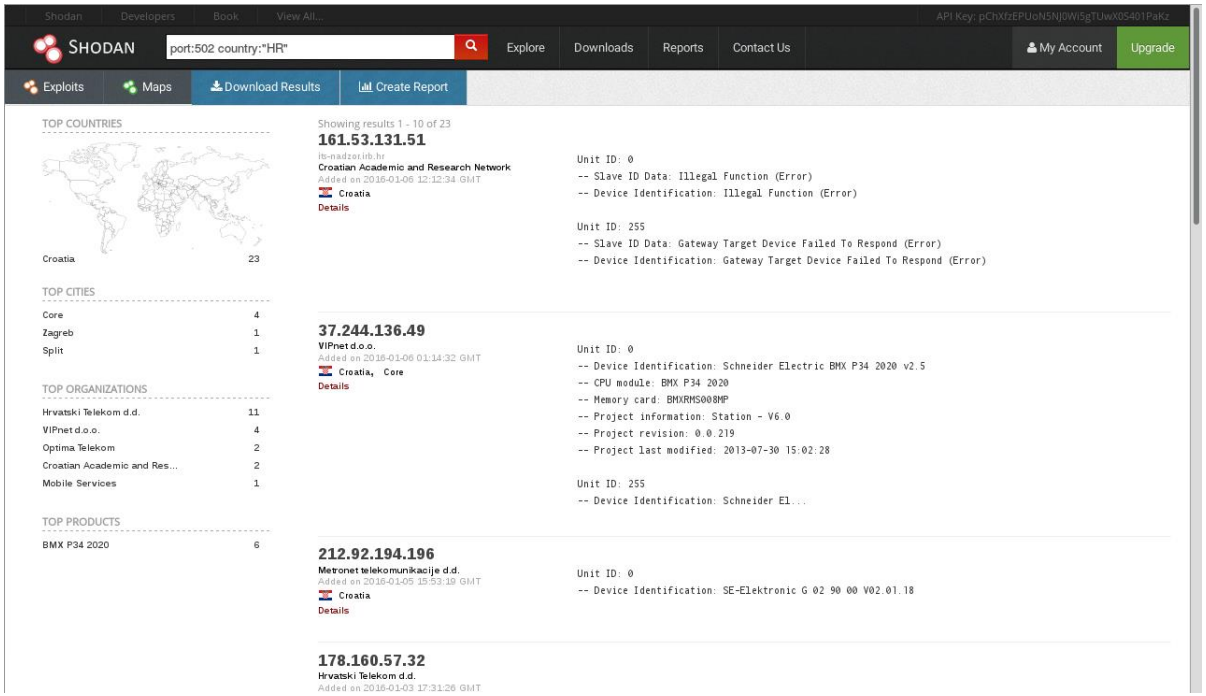
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals

Istraživanje i razvoj

- Sigurnost u IT sustavima je vrlo problematična
  - Nema „rješenja” koje će dati potpuno siguran sustav
  - Vrlo intenzivna istraživanja
- Upravljački sustavi unose svoja specifična svojstva
  - Specifična svojstva znači da rješenja za IT sustave često nisu direktno primjenjiva na OT sustave
    - Najčešća metoda zaštite u IT sustavima je „detect & patch”, neprimjenjiva u upravljačkim sustavima

Kako stoji Hrvatska po tom pitanju?

- **Zna li itko?**
- Shodan



Dodatna literatura i izvori na Internetu

Cheminod, Manuel, Luca Durante, and Adriano Valenzano. "Review of security issues in industrial networks." *Industrial Informatics, IEEE Transactions on* 9.1 (2013): 277-293.

SCADA / ICS | Information Security News, IT Security News & Expert Insights: http://www.securityweek.com/scada-ics

SANS ICS: Industrial Control Security, https://ics.sans.org/

SCADASEC-L Mailing List, http://www.infracritical.com/?page_id=53

BlackHat konferencija

Razne znanstvene konferencije