Suport curricular

Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 – Ianuarie 2025

Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Modulul 5 – Securitatea rețelelor și sistemelor de conducere industriale (UTM-I40-005)

Grigore Stamatescu

grigore.stamatescu@astiautomation.com

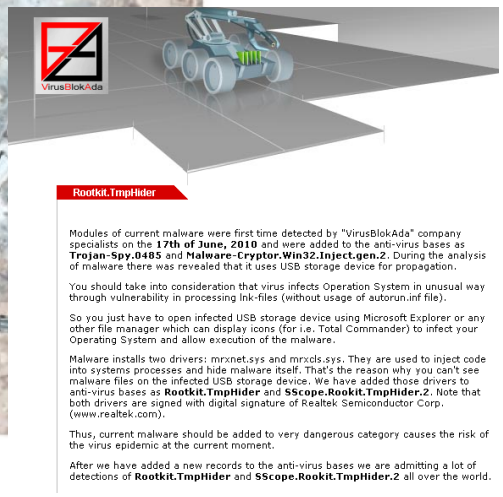
Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Agenda – Modulul 5

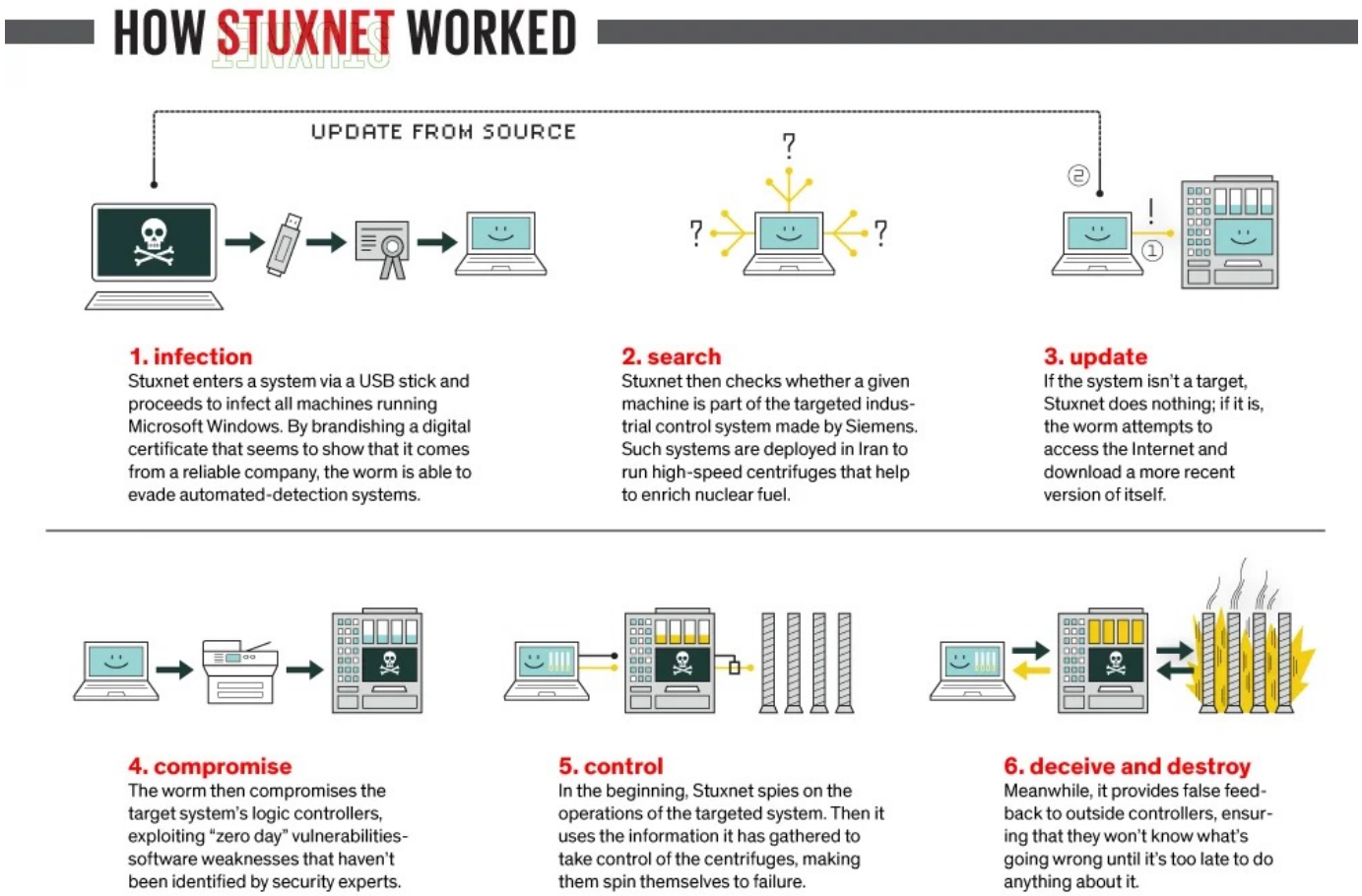
- Concepte generale de securitate cibernetică pentru sistemele de conducere industriale (ICS); principii de asigurare a confidențialității, integrității și disponibilității în cadrul ICS și analiza comparativă IT/OT
- Modelul Purdue pentru securitatea ICS și ghidul NIST SP 800-82r3 pentru securitatea tehnologiei operaționale (OT)
- Aspecte de standardizare: familiile de standarde ISO27001 – Sistem de management pentru securitatea informațiilor și ISA/IEC 62443 – Securitate cibernetică industrial
- Cadrul European actual de reglementare și certificare pentru securitatea cibernetică pentru operatori esențiali și de infrastructuri critice (elemente cheie ale directivelor NIS2, CSA, CRA și schema Europeană de certificare EUCC pentru produse, sisteme și servicii informatice)
- **Studiu de caz**: Proiectul ELECTRON. **Demo**: Configurarea și testarea echipamentelor dedicate pentru securitate cibernetică în mediul industrial. Exemplificare Siemens SCALANCE XC208/S615 cu PLC din seria S7-1500.

Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Atacuri cibernetice – Stuxnet (2010)



Atacuri cibernetice – Stuxnet



Atacuri cibernetice – Black Energy (2015)

Ukraine power grid hack

From Wikipedia, the free encyclopedia

On December 23, 2015, the power grid of Ukraine was hacked, which resulted in power outages for roughly 230,000 consumers in Ukraine for 1-6 hours.

Black Out In Ukraine: BlackEnergy In Power Grid Cyberattack

Home / Articles / Black Out in Ukraine: BlackEnergy...

KIM ZETTER SECURITY MAR 3, 2016 7:00 AM

BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry

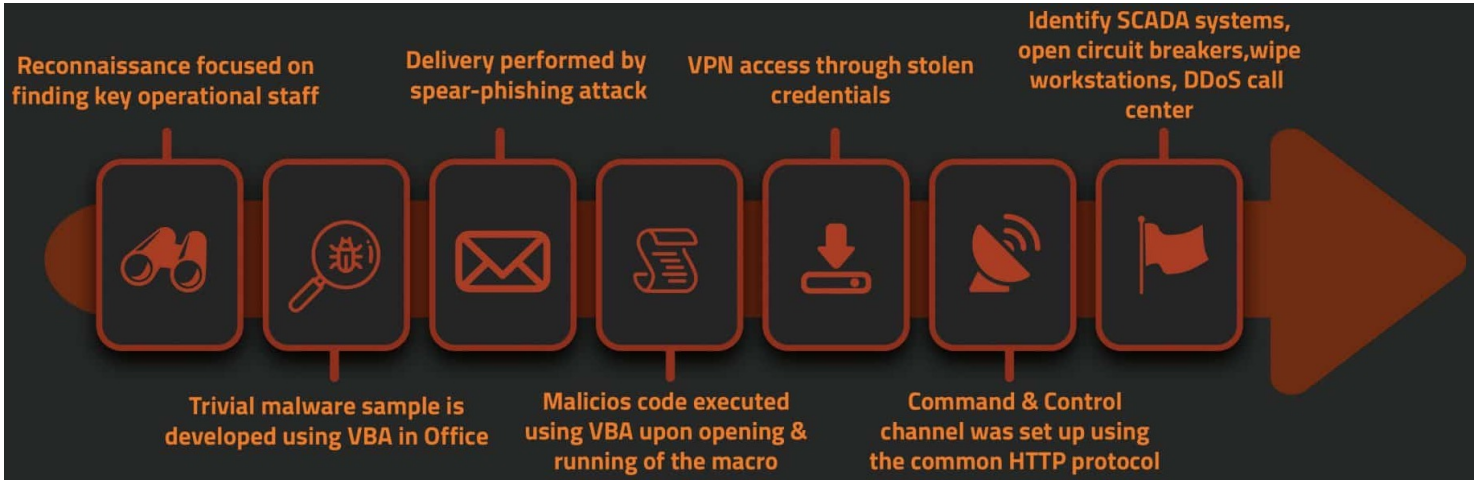
Posted on January 5, 2016 by ESET Ireland

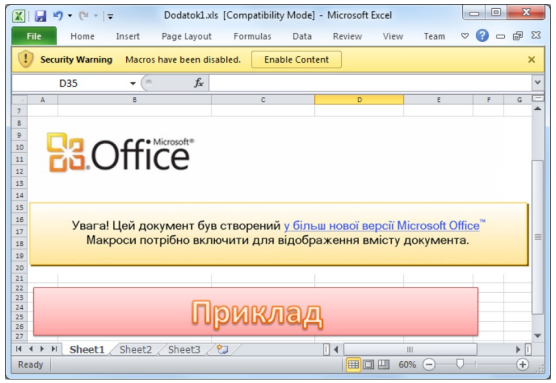
Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

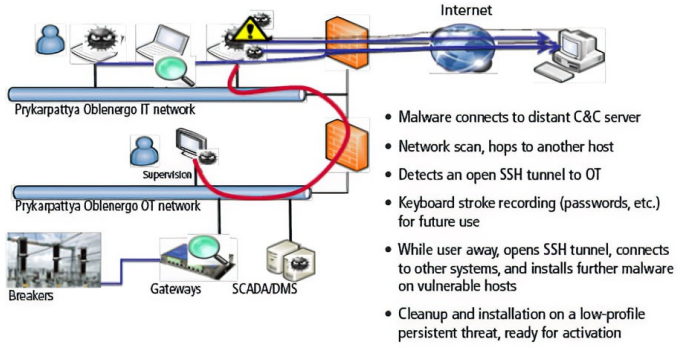
The hack on Ukraine's power grid was a first-of-its-kind attack that sets an ominous precedent for the security of power grids everywhere.

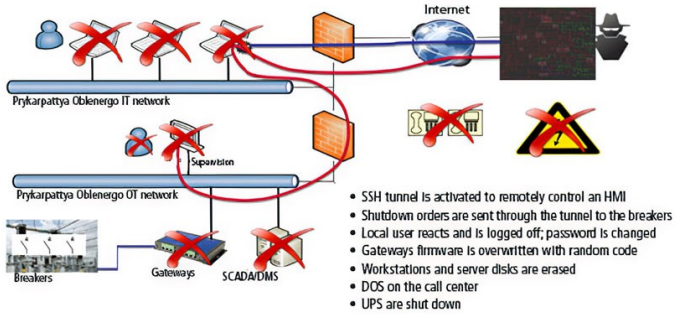
Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Atacuri cibernetice – Black Energy









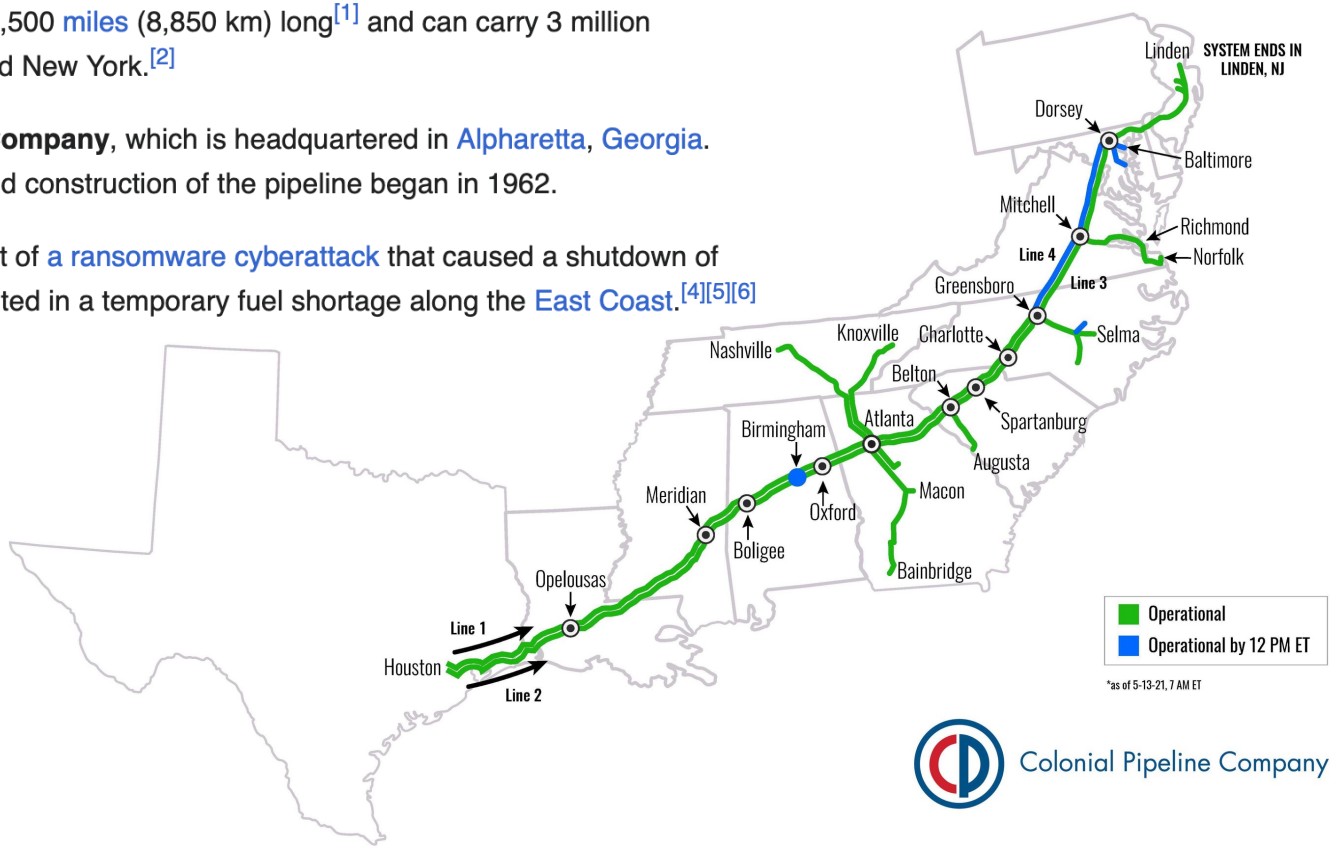
Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Atacuri cibernetice – Colonial (2021)

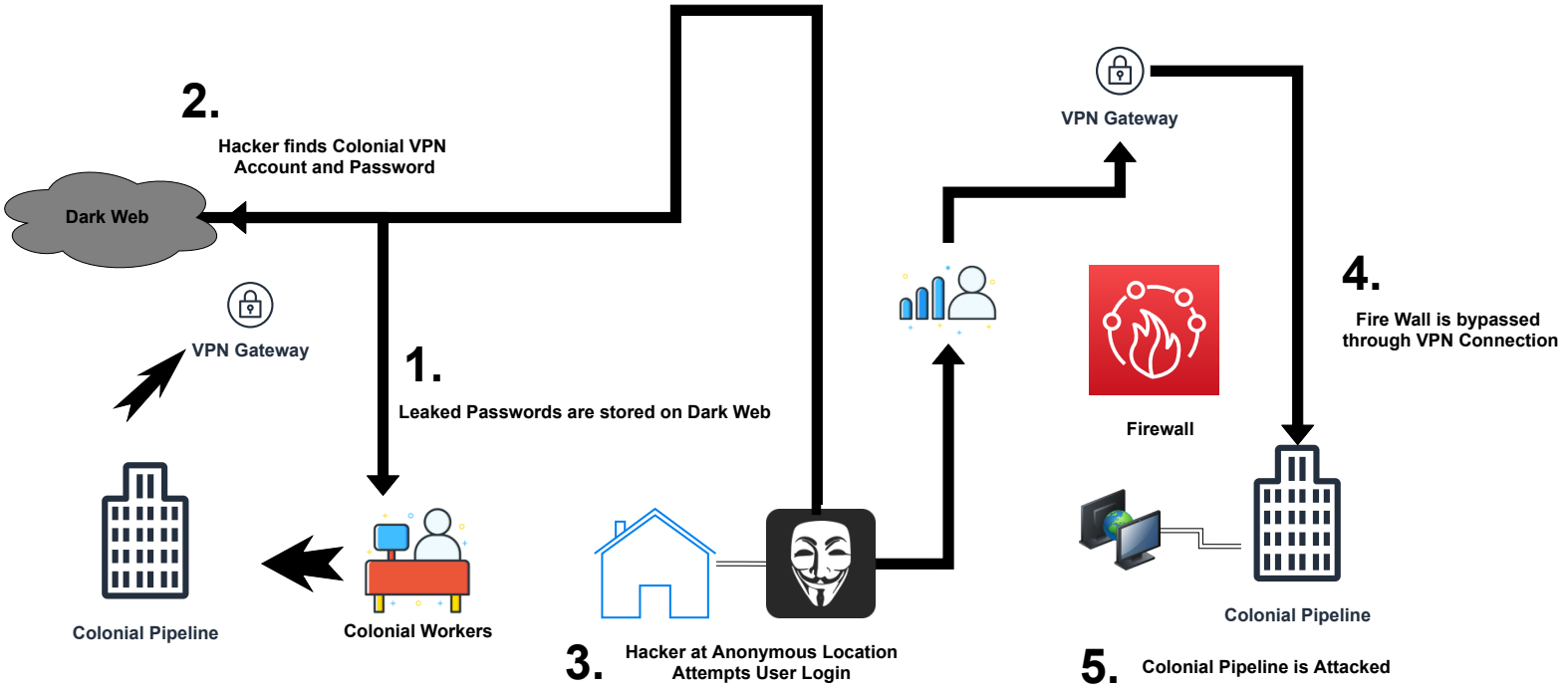
The **Colonial Pipeline** is the largest pipeline system for refined oil products in the U.S.[1] The pipeline – consisting of three tubes – is 5,500 miles (8,850 km) long[1] and can carry 3 million barrels of fuel per day between Texas and New York.[2]

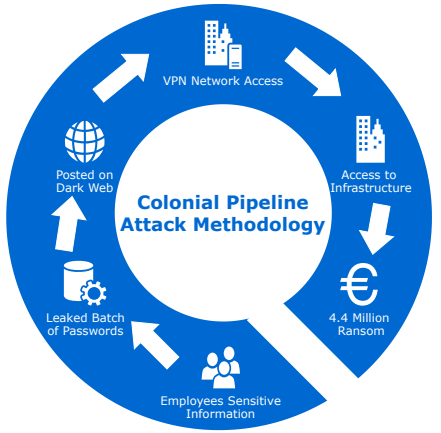
It is operated by the **Colonial Pipeline Company**, which is headquartered in Alpharetta, Georgia.[3] The company was founded in 1961 and construction of the pipeline began in 1962.

In May 2021, the pipeline was the subject of a ransomware cyberattack that caused a shutdown of their operations for five days, which resulted in a temporary fuel shortage along the East Coast.[4][5][6]



Atacuri cibernetice – Colonial





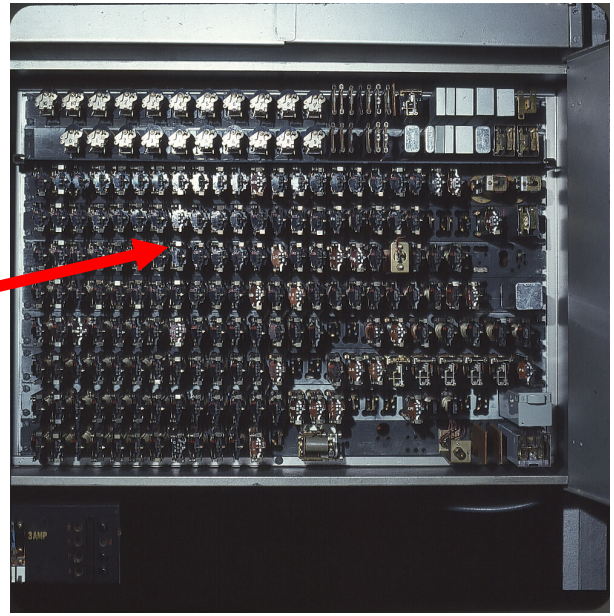
J. Beerman, D. Berent, Z. Falter and S. Bhunia, "A Review of Colonial Pipeline Ransomware Attack," *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, Bangalore, India, 2023

Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Sisteme de conducere industriale

- *Industrial Control Systems (ICS)* sau *Industrial Automation and Control Systems (IACS)*
- Automatizarea echipamentelor pe liniile de asamblare înainte de sistemele de conducere bazate pe calculatoare era realizată cu scheme logice bazate pe relee.
- Acestea erau asamblate manual, fiind costisitoare și orice modificare în logica de comandă implica recablarea (anevoioasă!)

Releu individual cu rol de comutator logic automat



Panou cu relee

Automate programabile

- În anul 1968, General Motors a dorit înlocuirea sistemelor de automatizare costisitoare cu relee
- Propunerea câștigătoare a provenit de la Bedford Associates - MOdular Digital CON (MODICON) sub forma primului PLC
- A permis modificări ieftine și rapide în minute în loc de zile

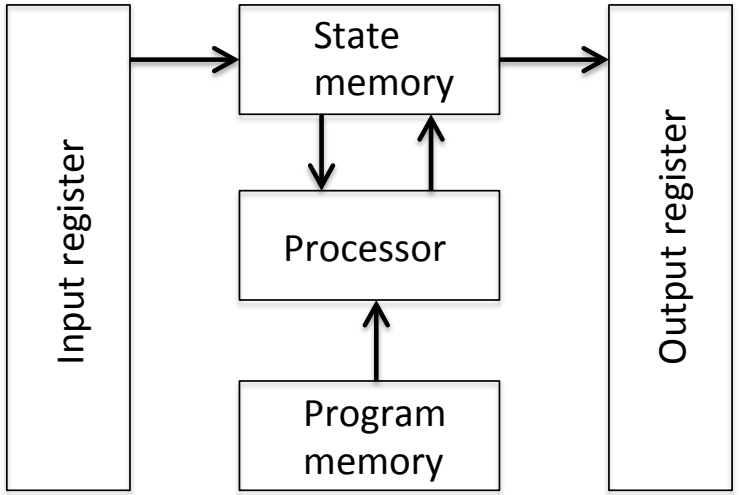
PLC din Seria Siemens S7-300 cu CPU și module I/O

Sisteme ierarhizate

- Un **PLC (*Programmable Logic Controller*)** controlează de regulă procese relativ mici e.g. o stație dintr-un proces de asamblare cu până la câteva sute de semnale de I/O
- Sistemele **SCADA (*Supervisory Control and Data Acquisition*)** include PLC-uri conectate pentru controlul mai multor procese de mici dimensiuni, inclusiv aflate în zone izolate
- Un sistem **DCS (*Distributed Control System*)** este utilizat pentru procese de mari dimensiuni e.g. centrale electrice sau rafinării, folosind unități DPU (Distribute Processing Units) și o rețea - fiecare DPU gestionează mii de puncte de I/O

Sisteme de conducere industriale

- Sistemele PLC, DPU, SCADA și DCS sunt cuprinse în categoria ICS
- Arhitectura unui PLC este teoretic similară cu cea a unui DPU, astfel încât considerăm un PLC ca fiind reprezentativ pentru categoria ICS
- Arhitectura PLC:
  - Memoria de program conține logica de comandă
  - Memoria de stare conține variabilele de proces
  - Registrul de intrare conține intrările de la senzorii de câmp sau de la elementele de control manual ale procesului
  - Registrul de ieșire conține ieșirile către elemente de acționare cum sunt lămpile indicatoare, motoare și valve care operează asupra echipamentelor de proces



Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

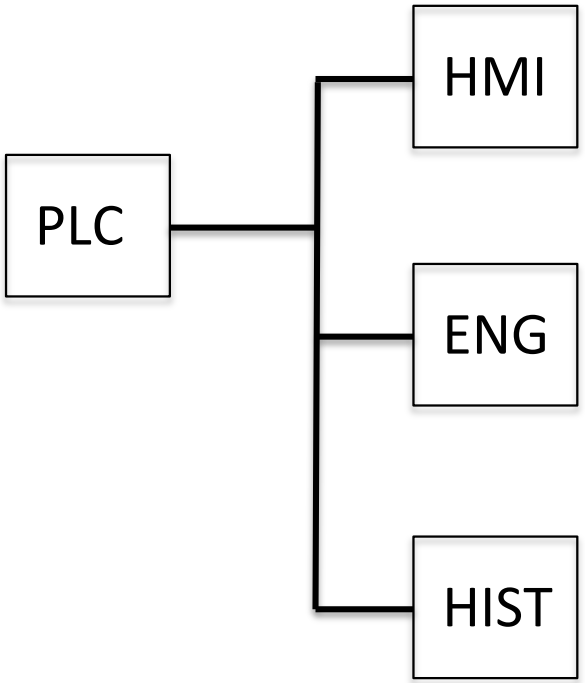
Sisteme de conducere industriale

- PLC-ul colectează datele de proces, execută logica de comandă și transmite comenzi către echipamentele de câmp
- Componente suplimentare într-un ICS
  - Interfața om-mașină (HMI – Human Machine Interface)

  Permite operatorului uman să verifice starea procesului și să acționeze local direct asupra procesului
  - Stația de inginerie (ENG – Engineering workstation)

  Permite modificări și actualizări ale sistemului ICS
  - Arhiva datelor de proces (HIST - Historian)

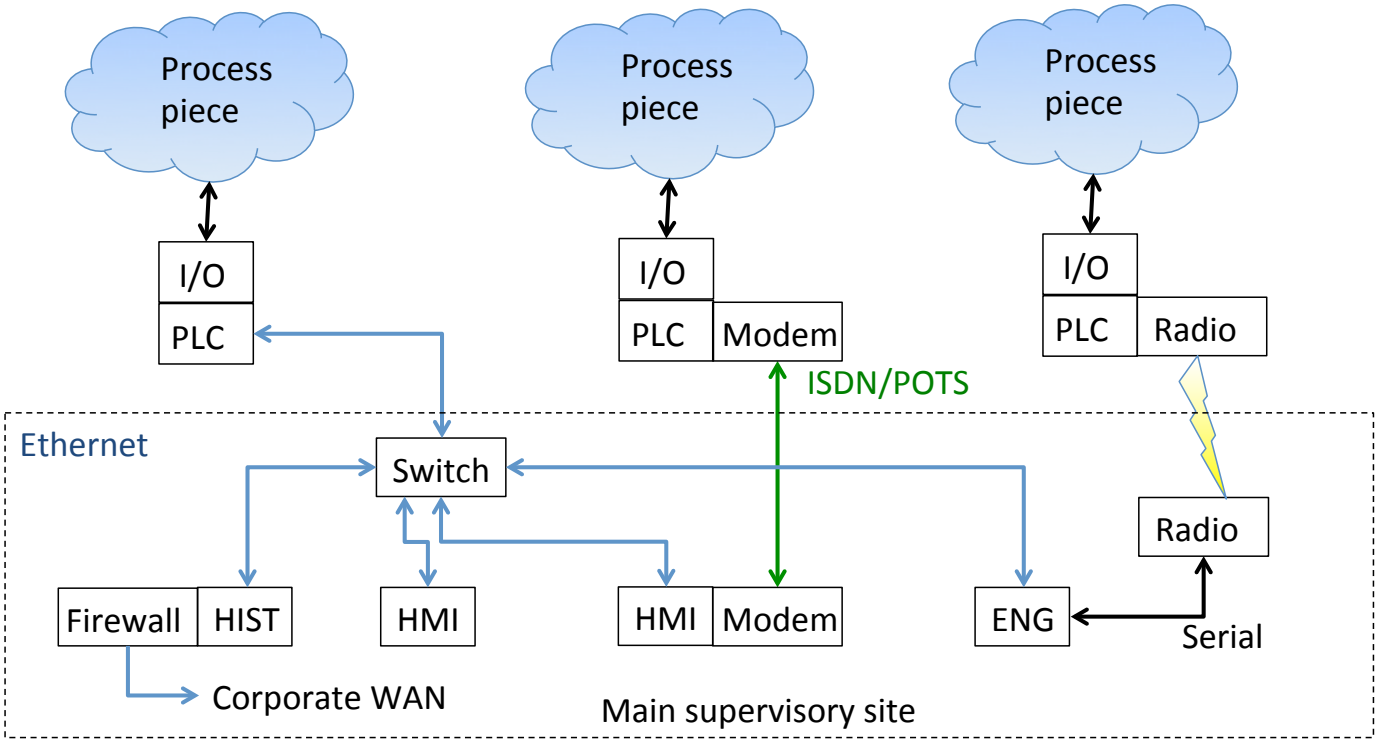
  Colectează datele de proces într-o bază de date pentru analiza ulterioară și depanare



Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

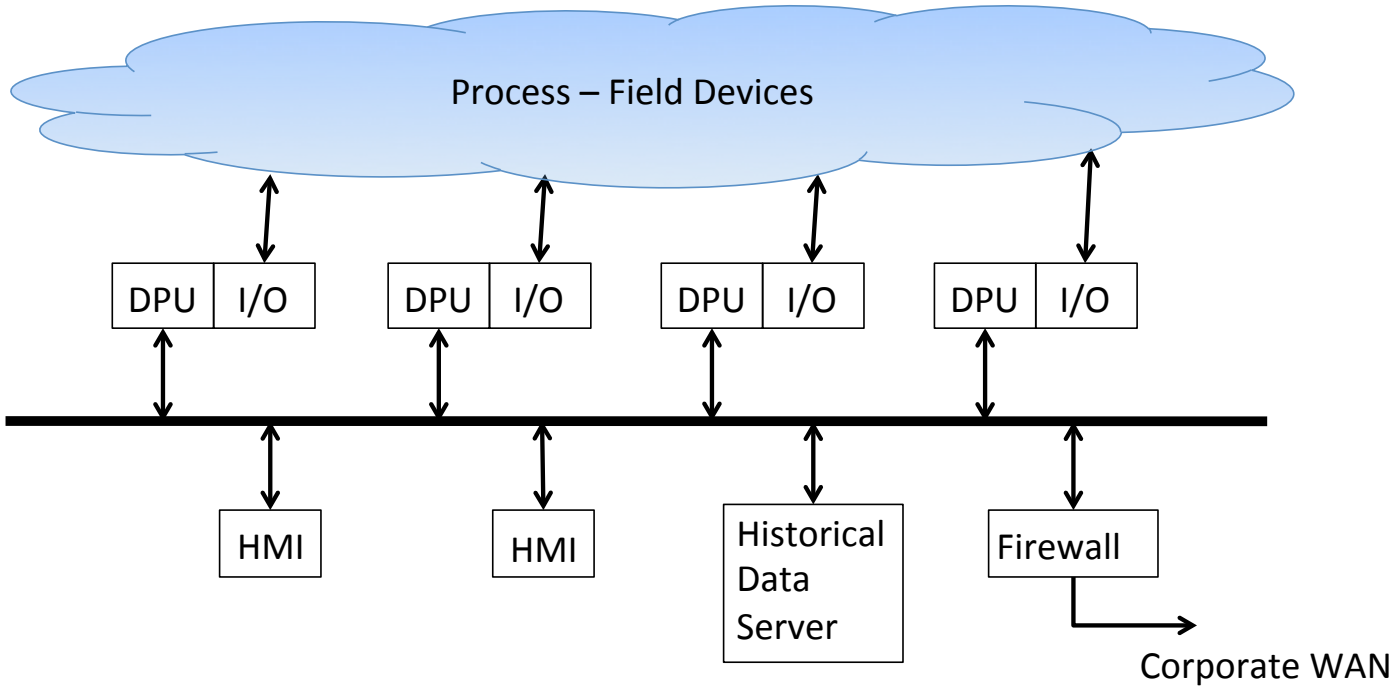
Configurații ICS tipice

- Pentru procese distribuite geografic în locații izolate, e.g. SCADA



Configurații ICS tipice

- Pentru procese mari, centralizare e.g. DCS



Provocări de securitate cibernetică

- Aspectele de securitate cibernetică specifice ICS
- Mediul de operare ICS
  - Conectarea directă la procesul fizic și conducerea în timp real
  - Motivațiile și considerațiile utilizatorilor și ale organizațiilor
- Configurații de rețea unice și protocoale de comunicații industriale

Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Terminologie

- **Amenințare**: Un potențial de încălcare a securității, care există atunci când există o circumstanță, o capacitate, o acțiune sau un eveniment care ar putea încălca securitatea și poate cauza prejudicii.
- **Vulnerabilitate**: O slăbiciune într-un sistem IT (ICS) care poate fi exploatată cu succes de către un atacator

- **Riscul**: Produsul dintre nivelul amenințării și nivelul vulnerabilității, care stabilește probabilitatea unui atac de succes
- **Evaluarea riscurilor**: Procesul prin care riscurile sunt identificate și impactul acelor riscuri este determinat

Mediul de operare ICS

- Aplicațiile ICS controlează un proces fizic și operează într-un mediu de timp real
  - Datele pot deveni inutile într-o perioadă foarte scurtă de timp (secunde) și pot conduce la scăderea eficienței procesului, daune sau oprire
  - Fiabilitatea ICS este critică și este necesară operarea continuă și în cazul unui atac cibernetic
- Mediile de operare ICS sunt dificile, zgomotoase, murdare, cu variații extreme de temperaturi, etc.
- Ineficiențele și opririle de proces sunt adesea foarte costisitoare în special pentru procesele foarte mari (Mio. USD)
- În infrastructurile critice, pierderea unui sistem ICS poate avea efecte negative asupra sănătății publice, siguranței și protecției mediului

Utilizatorii ICS și securitatea cibernetică

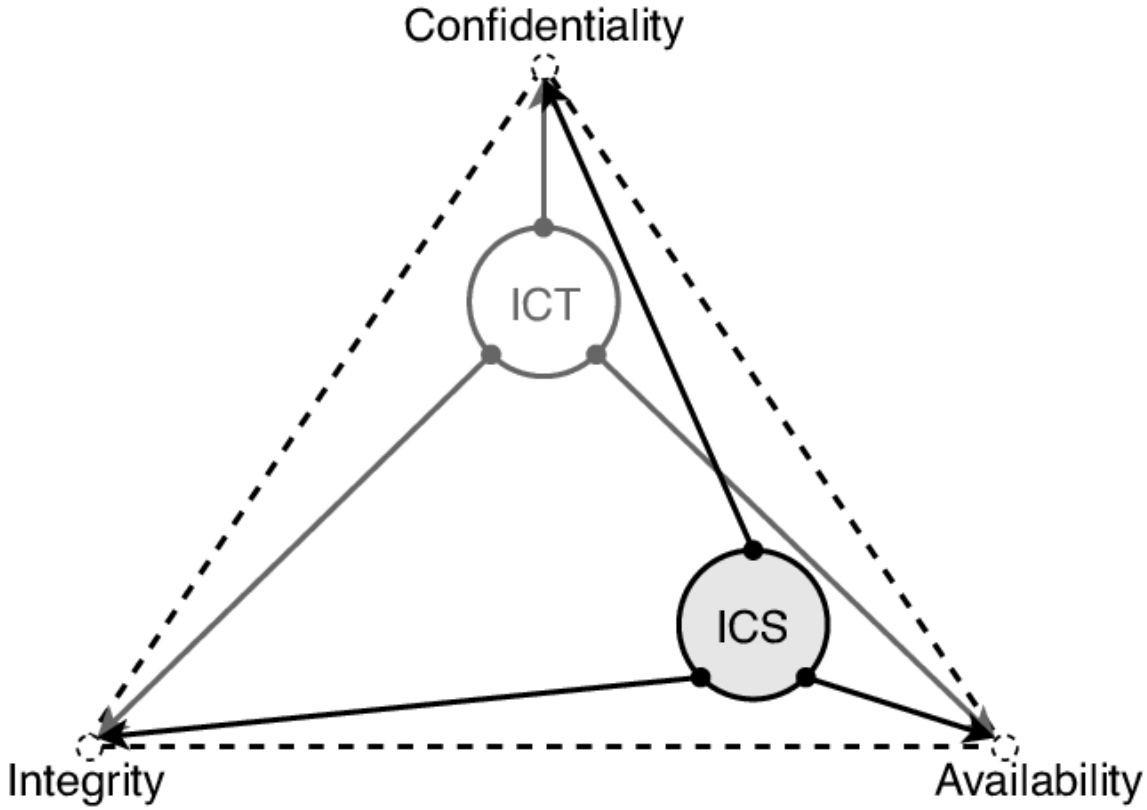
- Tradițional sistemele ICS au fost izolate fizic de lumea exterioară (securitatea = control acces personal)
- În prezent sistemele sunt interconectate cu rețelele WAN ale companiilor și către Internet pentru monitorizarea și mentenanța la distanță
- Inginerii automatiști, tehnicienii și operatorii nu au cunoștințe de securitate cibernetică
  - Din perspectiva opusă, specialiștii IT nu au cunștințe de proces și automatizare
  - Rezultă roluri și obiective diferite și uneori opuse în structura companiei
- Justificarea investițiilor în securitatea cibernetică este dificilă

Securitatea cibernetică în ICS

- Obiectivul este menținerea funcționării procesului
- Măsurile de securitate cibernetică pot crea puncte de defectare, afecta performanța procesului și îngreunează mentenanța
- În sistemele IT, informația este obiectivul în timp ce în ICS informația este cuplată cu și relevantă doar în contextul procesului fizic
  - Datele de proces sunt valori de temperatură, presiune, comenzi, etc. și sunt rareori confidențiale*
  - Validarea informației și autentificarea sunt însă foarte importante
- ICS utilizează hardware și software proprietar
  - Reacții incompatibile sau necunoscute la actualizările de securitate cibernetică – ICS operează adesea cu software ne-actualizat
  - Soluțiile bazate pe IT e.g. *firewalls* nu sunt adaptate pentru protocoalele de comunicații industriale

Securitatea cibernetică în ICS

- Confidențialitate: Protejarea infomațiilor la accesul neautorizat
- Integritate: Datele sunt de încredere, complete și nu au fost modificate, accidental sau de către un utilizator neautorizat
- **Disponibilitate: Datele sunt accesibile atunci când sunt necesare**



Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

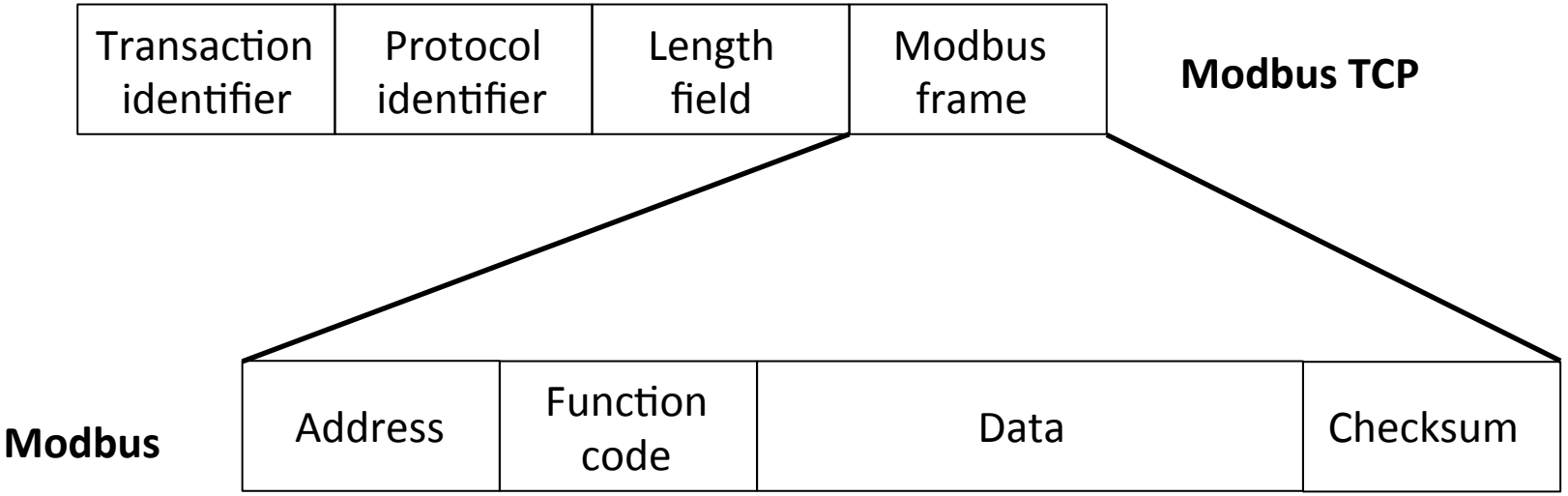
Interfețe de rețea în ICS

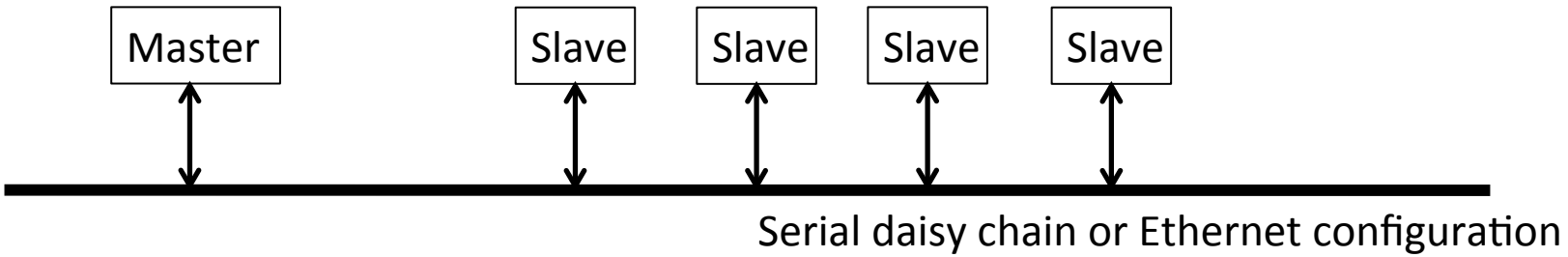
- Sistemele moderne sunt bazate pe Ethernet, 10M – 1G baud
  - Suficient de rapide pentru a evita probleme de latență, fără a opera în timp real sau cu acces garantat
  - Disponibilitatea largă a Ethernet reduce costul sistemelor noi de automatizare
- Conexiuni seriale, 9600 – 57k baud
  - Acces punct la punct și legături directe RS232 / RS485
  - Protocolul Modbus serial, timp real, acces garantat
  - Utilizate în continuare pentru conexiuni simple la instrumentație și sisteme legacy
- Interfețe proprietare, bucle sau daisy chain, 1– 4M baud
  - Tipic token ring cu multiplexare în timp real și acces garantat, în curs de înlocuire

Protocoale de rețea în ICS

- Ethernet TCP/IP
  - Utilizat pentru beneficiile componentelor COTS și suficient de rapid pentru emularea accesului în timp real
- Modbus și Modbus TCP
  - Protocol comun utilizat în comunicații seriale încă de la MODICON
  - Rețea master-slave în care nodul master trimite comenzi/cereri de date de la noduri slave și primește un răspuns. Nodul slave nu inițiază comunicații.
  - Accesul este pe bază de adrese. Fără autentificare, criptare sau alte măsuri de securitate încorporate în standard
  - Modbus TCP – o versiune Modbus actualizată peste Ethernet, fără securitate. Comunicația Modbus este încapsulată în pachete Ethernet.

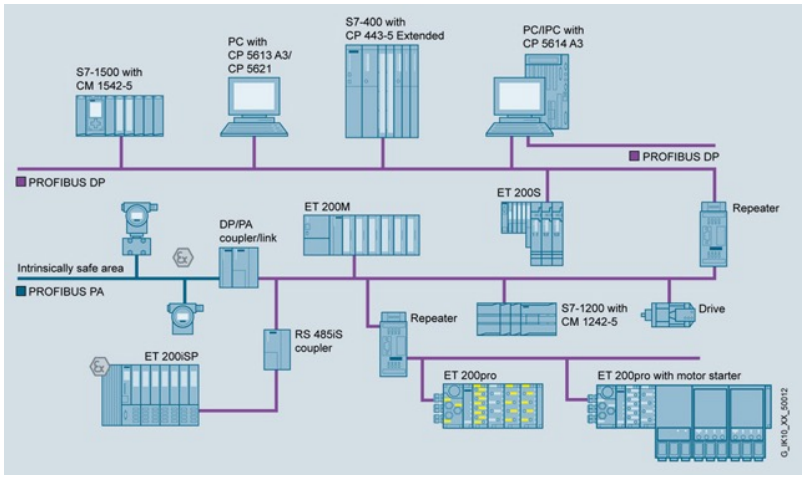
Protocoale de rețea – Modbus



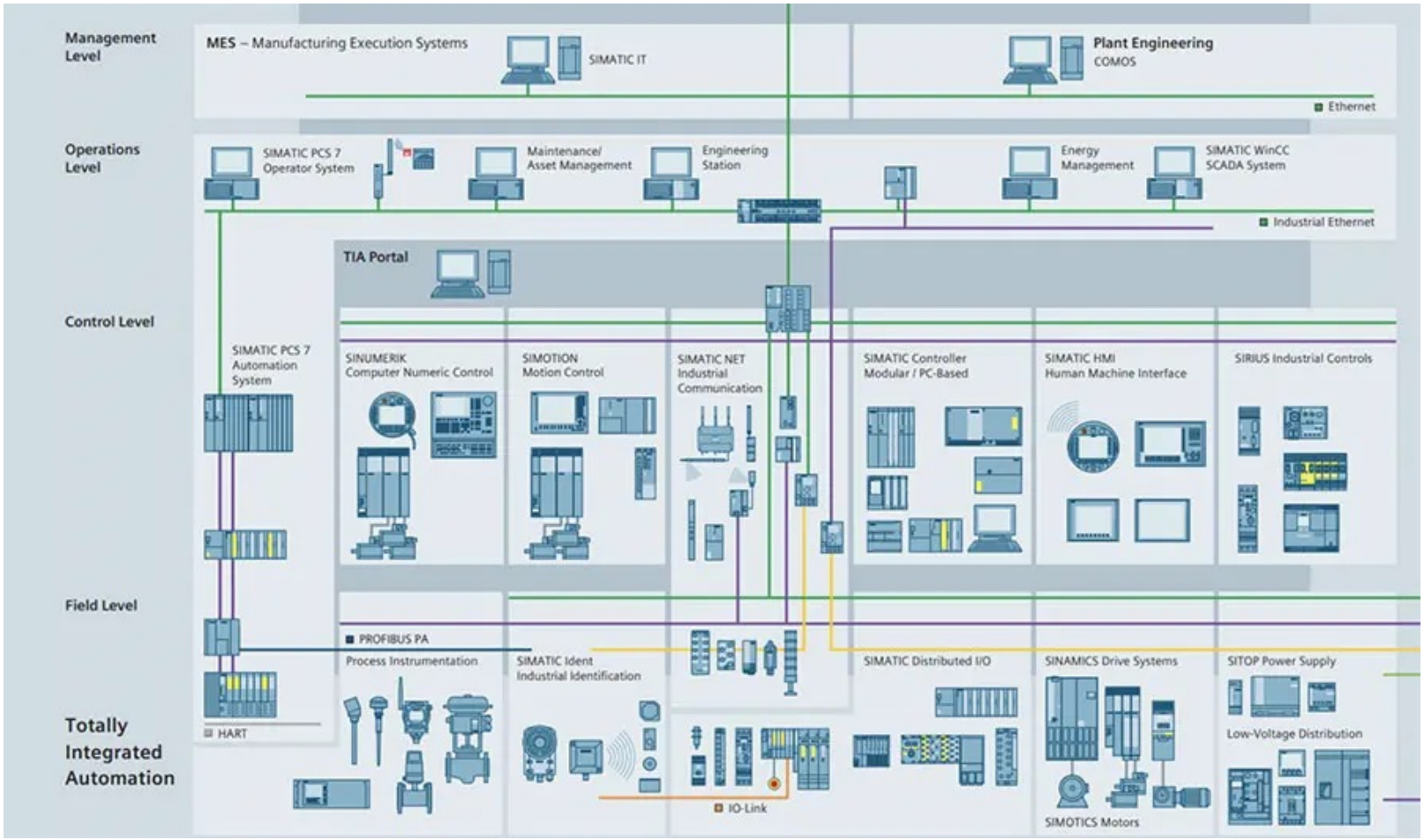


Alte protocoale utilizate în ICS

- Rețelele cu pasare de jetoane (token ring)
  - E.g. Siemens PROFIBUS, utilizează un tip de rețea deterministă prin partajarea și pasarea unui jeton virtual care determină nodul cu prioritate în rețea
  - Posesorul jetonului poate iniția comunicația. La expirarea timpului de deținere a jetonului, se trece la următorul nod dintr-o listă.
  - Sunt înlocuite treptat cu protocoale bazate pe Ethernet e.g. Siemens SIMATIC NET, Allen Bradley Ethernet/IP

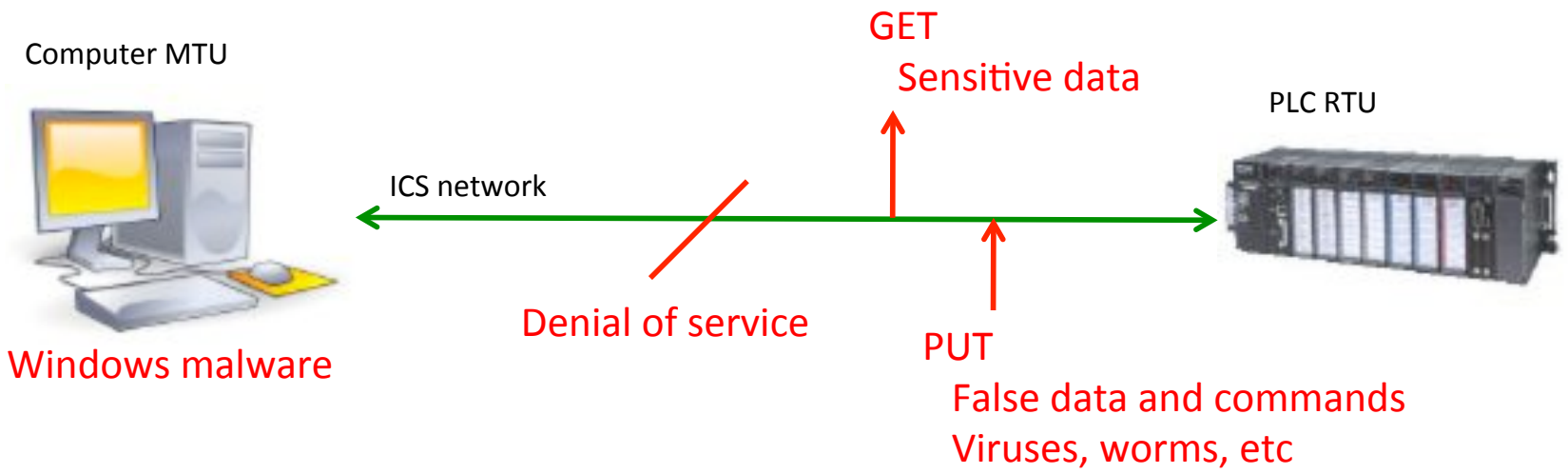


Arhitectura Siemens PCS7



Amenințări cibernetice ICS

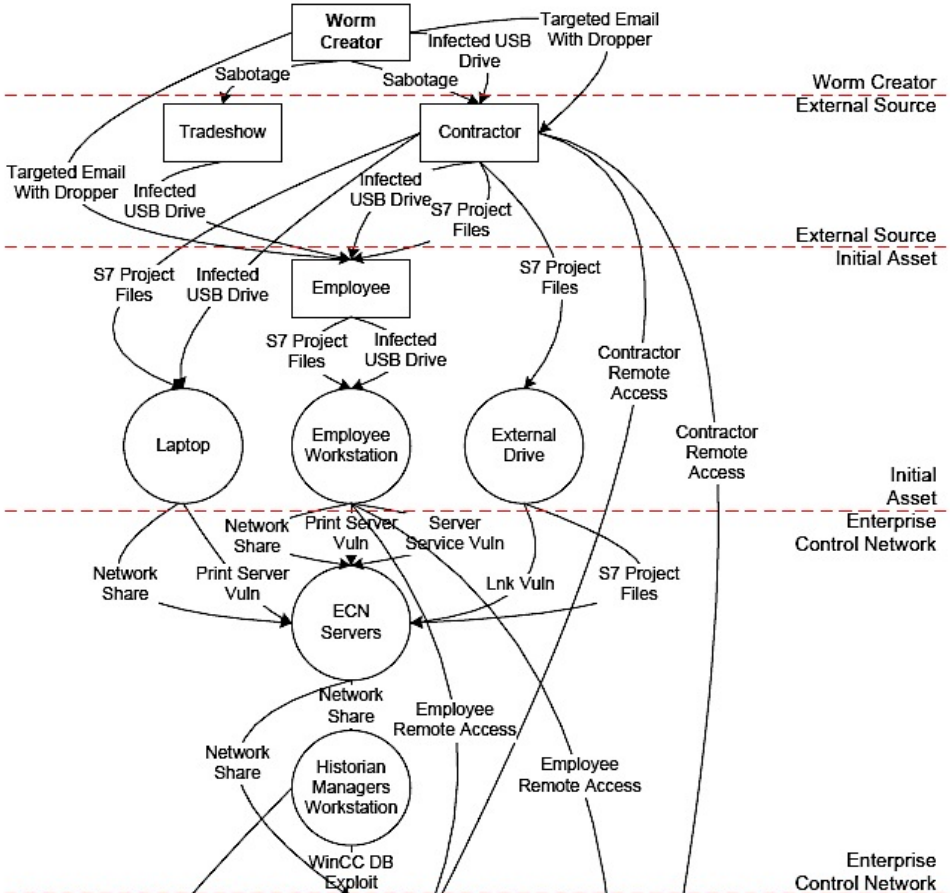
- Numărul în creștere de atacuri stimulate de utilizarea în creștere a Windows și a altor soluții COTS (*Commercial-off-the-Shelf*)
- Atacurile pot împiedica accesul sau serviciul furnizat, pot extrage date sensibile sau insera informații și comenzi false și cod malițios în rețea



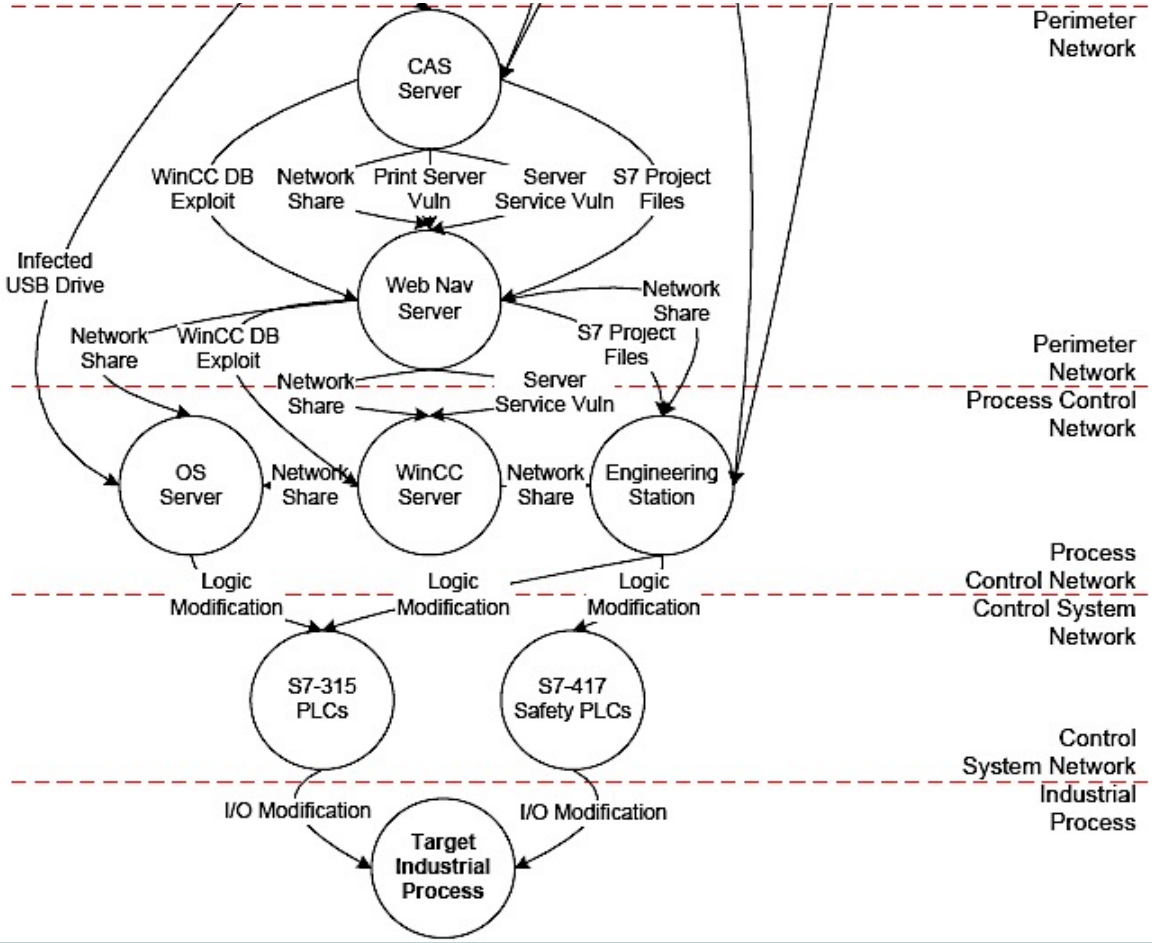
Viermele Stuxnet

- Atac direct asupra ICS. Moment de referință din care infrastructura critică a devenit un obiect de referință pentru teroriști.
- Foarte sofisticat și adresat specific, proiectarea acestuia indică resurse vaste implicate la nivel național
- Nu afectează calculatoarele generice, se activează doar atunci când este utilizat într-o rețea ICS cu anumite PLC-uri Siemens
- Realizează anumite acțiuni pentru a induce în eroare operatorii asupra stării procesului (afectează reprezentarea datelor și logicii de proces
- PC-urile pot fi actualizate dar nu și PLC-urile – ICS rămâne vulnerabil și după ce atacul este cunoscut

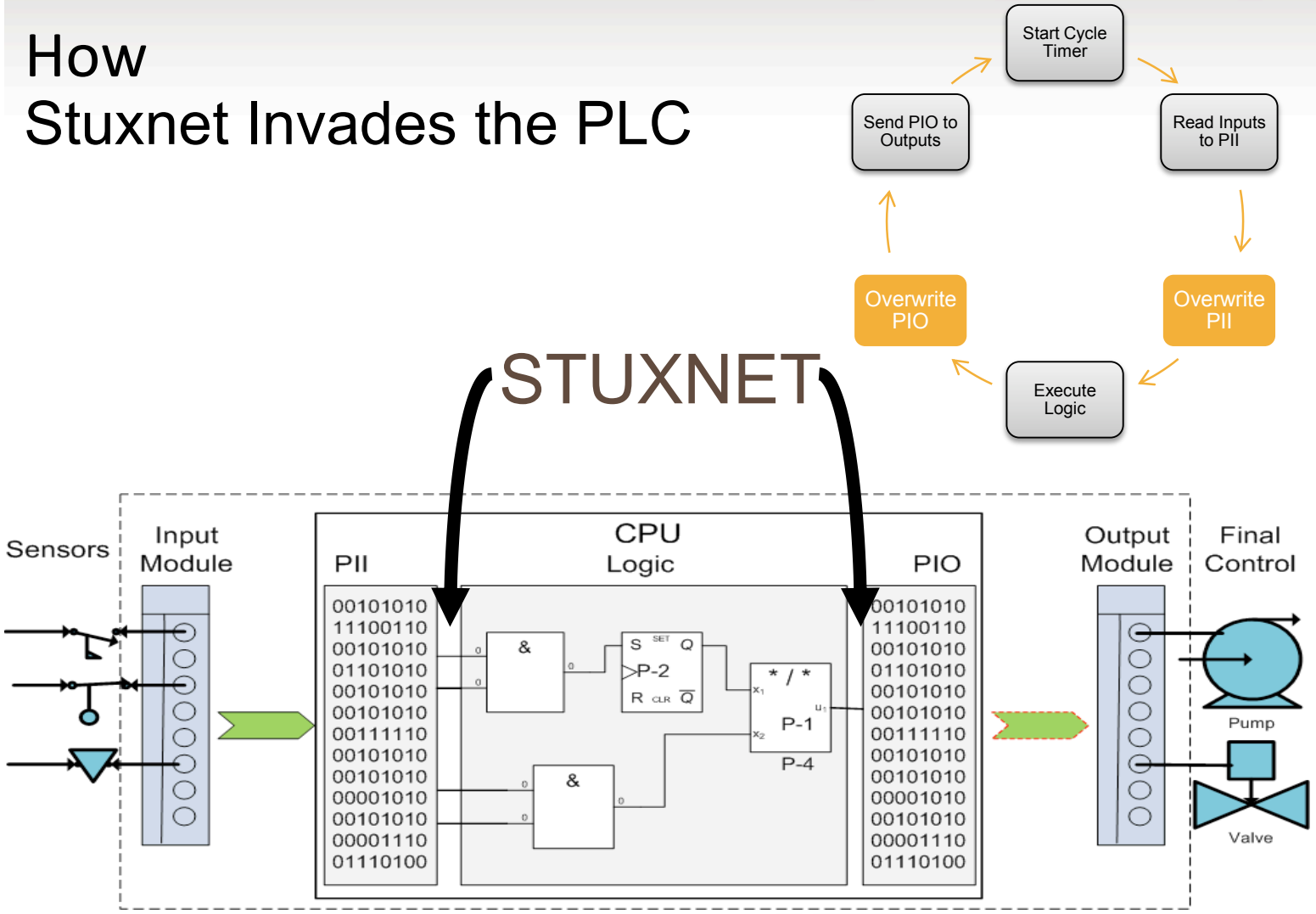
Infectarea cu viermele Stuxnet



Infectarea cu viermele Stuxnet



How
Stuxnet Invades the PLC



Mod de acțiune Stuxnet

1. Identifică și infectează stațiile de programare Siemens STEP 7
2. Înlocuiește rutinele DLL STEP 7 pe stații (împiedică vizualizarea ulterioară a modificărilor efectuate asupra PLC-urilor)
3. Caută modele specifice de PLC-uri Siemens (6ES7-315-2 și 6ES7-417)
4. Identifică PLC-ul victimă prin căutarea unor configurări specifice
5. Injectează una dintre cele trei componente de cod STEP 7 în PLC pentru a modifica operarea procesului

Modificări PLC Stuxnet

- Înlocuirea driverului PROFIBUS al PLC-ului
- Principalul bloc de program al PLC-ului (OB1) și principalul bloc watchdog (OB35) sunt modificate semnificativ
- Sunt injectate între 17 și 32 de blocuri de funcții suplimentare în PLC
- Componentele de cod ‘A’ și ’B’ modifică frecvențele de operare ale convertizoarelor de frecvență și astfel viteza motoarelor
- Componenta de cod ‘C’ este proiectată pentru a controla un sistem master – posibil un sistem safety

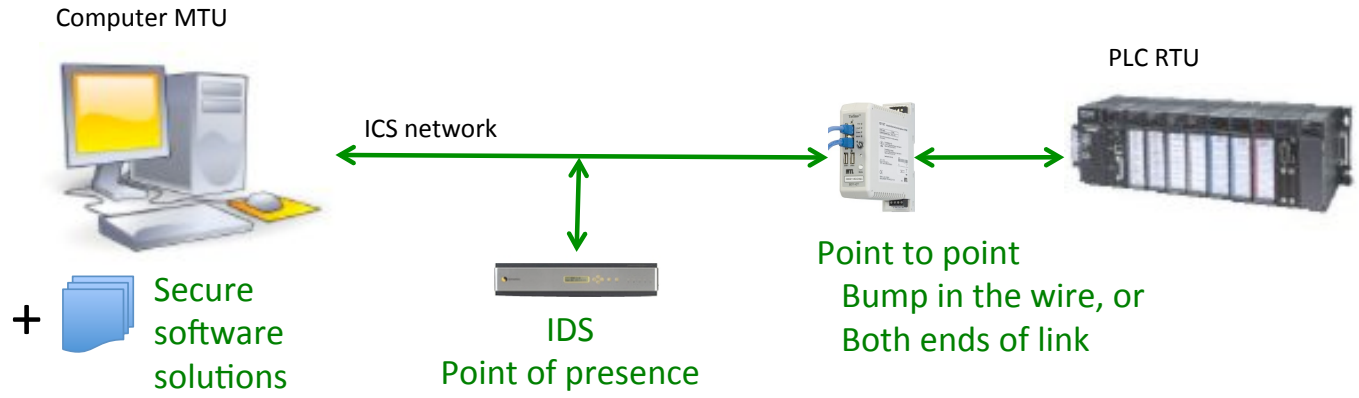
Stuxnet – Lecții învățate

- Un exemplu de virus care poate prelua controlul asupra unui PLC
- Nu sunt disponibile actualizări de securitate pentru logica PLC

- Atacurile sunt concentrate și particularizate profesionist pe sisteme și locații specifice
  - Nu mai sunt vizate sistemele cele mai uzuale
  - Atacurile precedente reprezintă tipare (modificate!) pentru atacuri viitoare
  - Prevalența ICS în infrastructuri critice conduce la daune societale majore
  - Motivația financiară și de reputație pentru atacuri este înlocuită treptat de națiuni ostile și acte de terorism

Măsuri de reducere a riscurilor

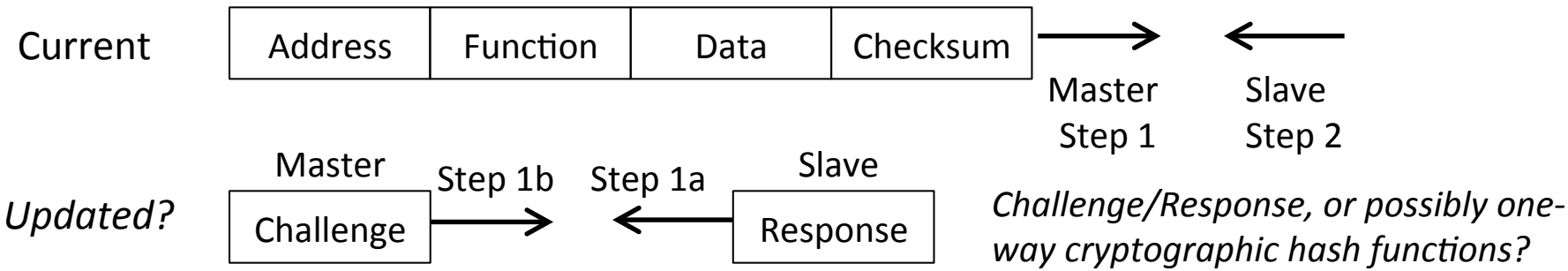
- Noi metode de autentificare și protocoale
- Noi politici și reglementări și abordări hardware și software
- Formare profesională și validarea sistemelor de automatizare
- ICS includ elemente specifice de securitate cibernetică cum ar fi sistemele de detecție ale intruziunilor (IDS), pe echipamente sau la nivelul interfețelor de rețea



Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Autentificarea în ICS

- Problema autentificării în protocoalele existente e.g. Modbus

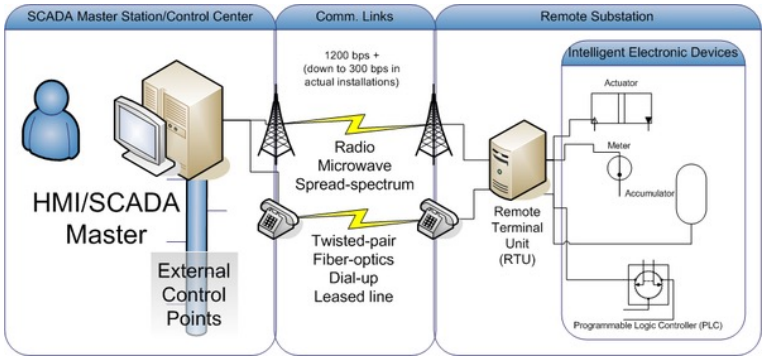


- Securizarea Modbus poate conduce la incompatibilitate cu standardul și cu echipamentele existente
- Durata de viață a sistemelor de automatizare de 15-20 ani impune interoperabilitatea peste diferitele generații ICS

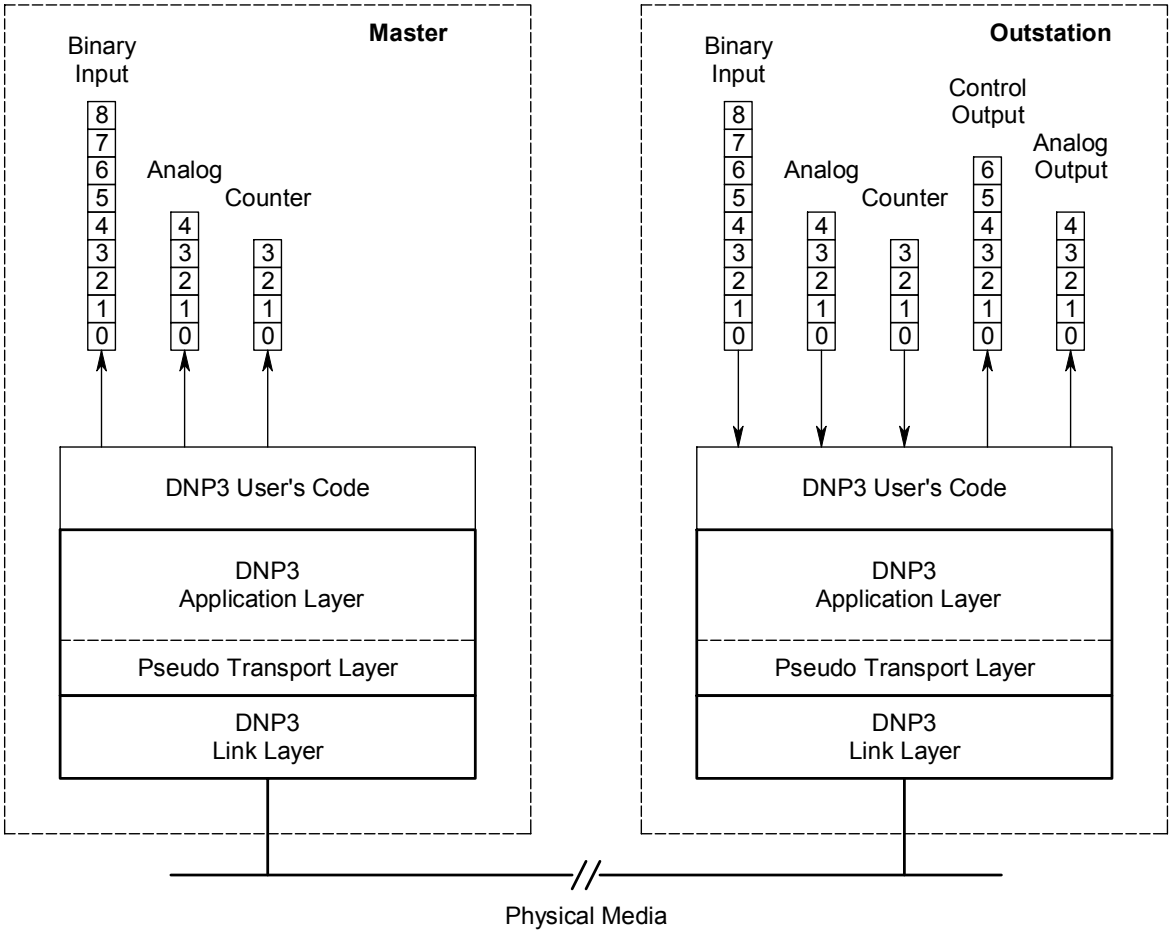
Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Protocoale ICS noi

- DNP3 - https://www.dnp.org
  - Efort amplu de a implementa interoperabilitatea deschisă, bazată pe standard, între echipamentele de proces: PLC, RTU (Remote Terminal Unit), IED (Intelligent Electronic Devices) și calculatoarele din camera de comandă: HMI, ENG, servere
  - Proiectat pentru a fi mai robust, eficient și compatibil față de vechile protocoale cum este Modbus, cu un cost de complexitate mai mare
  - Include îmbunătățiri de securitate



DNP3


Master
Binary Input
8
7
6
5
4
3
2
1
0
Analog
4
3
2
1
0
Counter
3
2
1
0
DNP3 User's Code
DNP3 Application Layer
Pseudo Transport Layer
DNP3 Link Layer
Outstation
Binary Input
8
7
6
5
4
3
2
1
0
Analog
4
3
2
1
0
Counter
3
2
1
0
Control Output
6
5
4
3
2
1
0
Analog Output
4
3
2
1
0
DNP3 User's Code
DNP3 Application Layer
Pseudo Transport Layer
DNP3 Link Layer
Physical Media

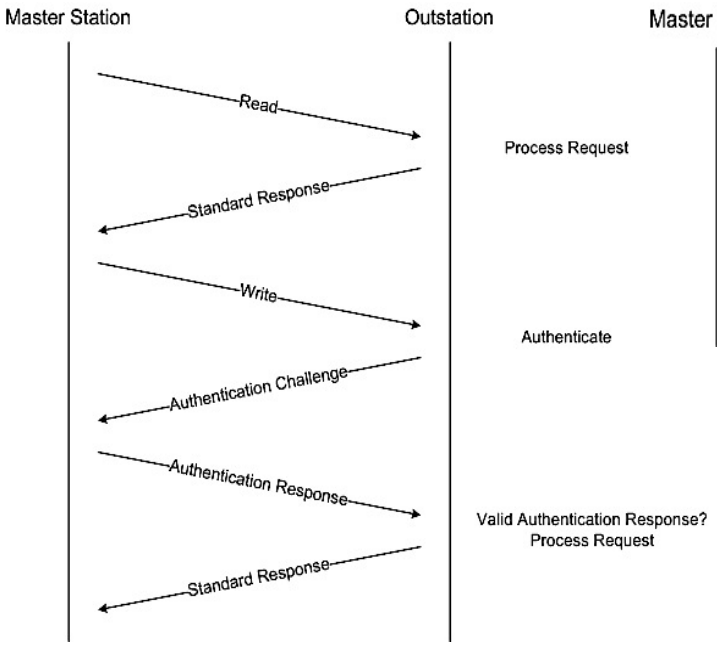
Autentificarea în DNP3

1. Inițializare: Atunci când o stație master inițiază o sesiune DNP3 cu o stație la distanță, Secure DNP3 va autentifica atât stația master cât și clientul. Este generată o cheie de sesiune unică și aceasta este partajată în timpul inițializării folosind chei partajate anterior.
2. Periodică: Stația master și clientul realizează reverificări periodice pentru a evita deturnarea comunicației (hijacking) și alte atacuri. Este generată și schimbată o nouă cheie de sesiune în timpul acestei actualizări periodice.
3. Cereri de funcții critice: Cererile critice sunt definite prin protocol și de către aplicație.
4. Specifice implementării: Furnizorii și utilizatorii finali pot implementa cerințe speciale de autentificari pentru funcții suplimentare.

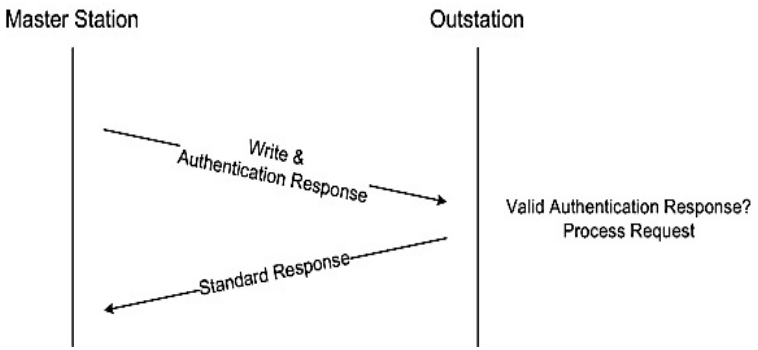
DNP3

- În prezent DNP3 include autentificare sigură, managementul cheilor și îmbunătățiri criptografice

Challenge/response

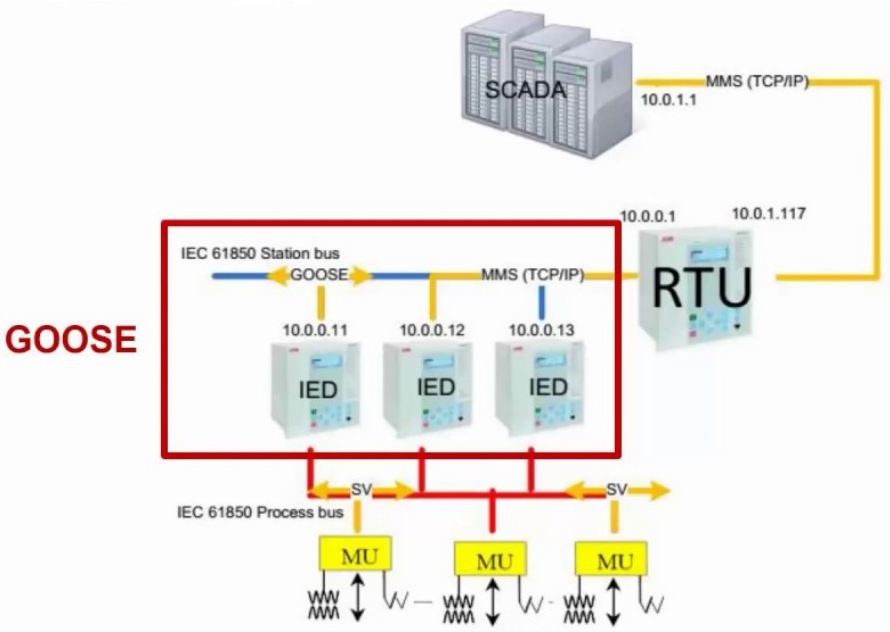


Aggressive mode



IEC 61850

- Standard internațional care definește protocoale de comunicație pentru IED în stațiile electrice
- Modele de date abstracte și asocieri cu protocoale: MMS, GOOSE, SV, SMV
- Extensii de securitate cibernetică prin IEC 62351 – Managementul sistemelor energetice și schimbul de informații asociat – Securitatea datelor și a comunicațiilor

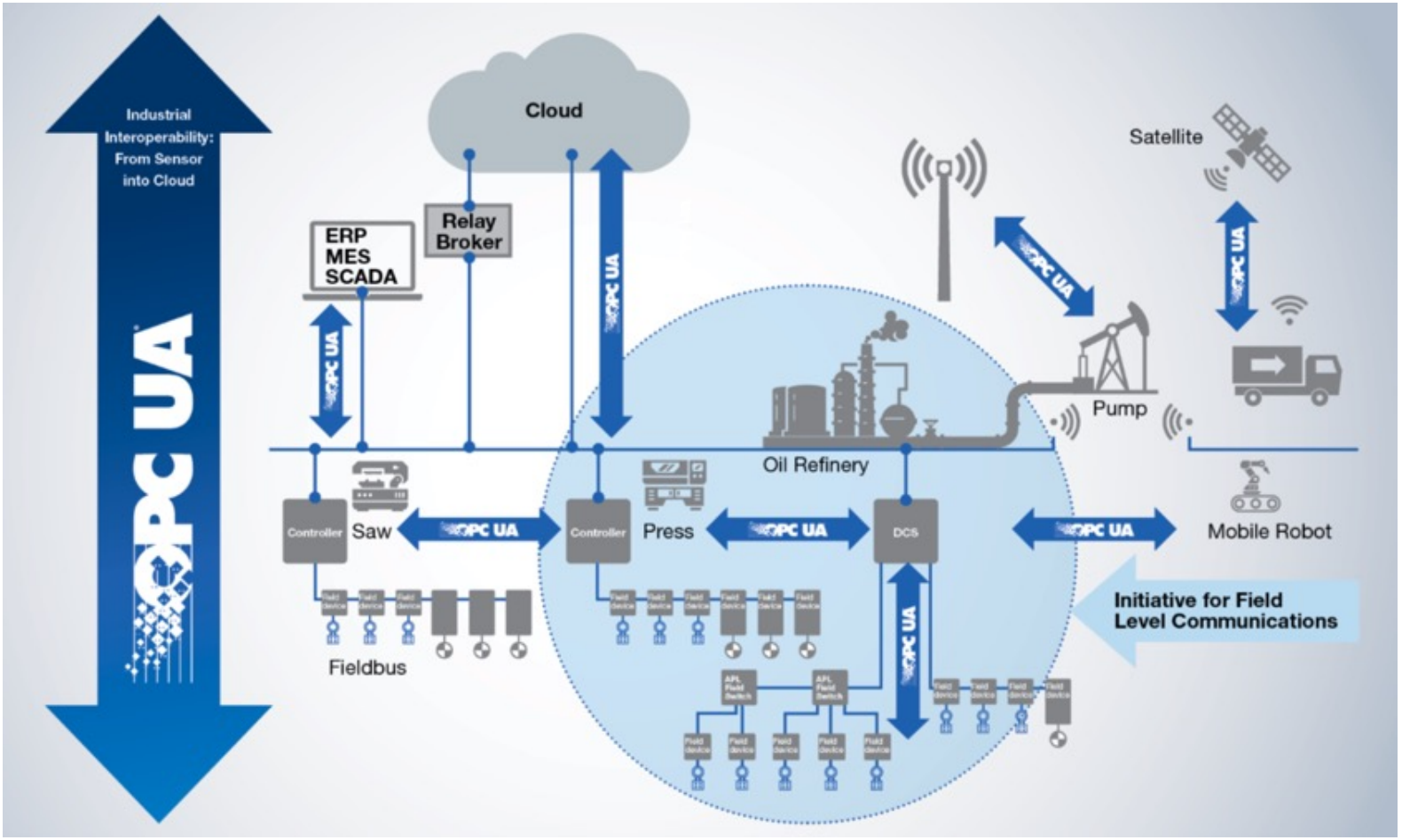


Protocoale ICS noi - OPC

- OPC – original OLE for Process Control, folosind componentele Microsoft OLE COM/DCOM
  - Necesită de regulă a configurație DCOM total deschisă, foarte permisivă. Probleme cu depășiri de buffer ș.a. exclusiv Windows.
  - Noua specificație, **Unified Architecture (OPC UA)** este bazată pe servicii web pentru utilizarea și include îmbunătățiri de securitate și stabilitate
  - Model client-server implementat prin Ethernet

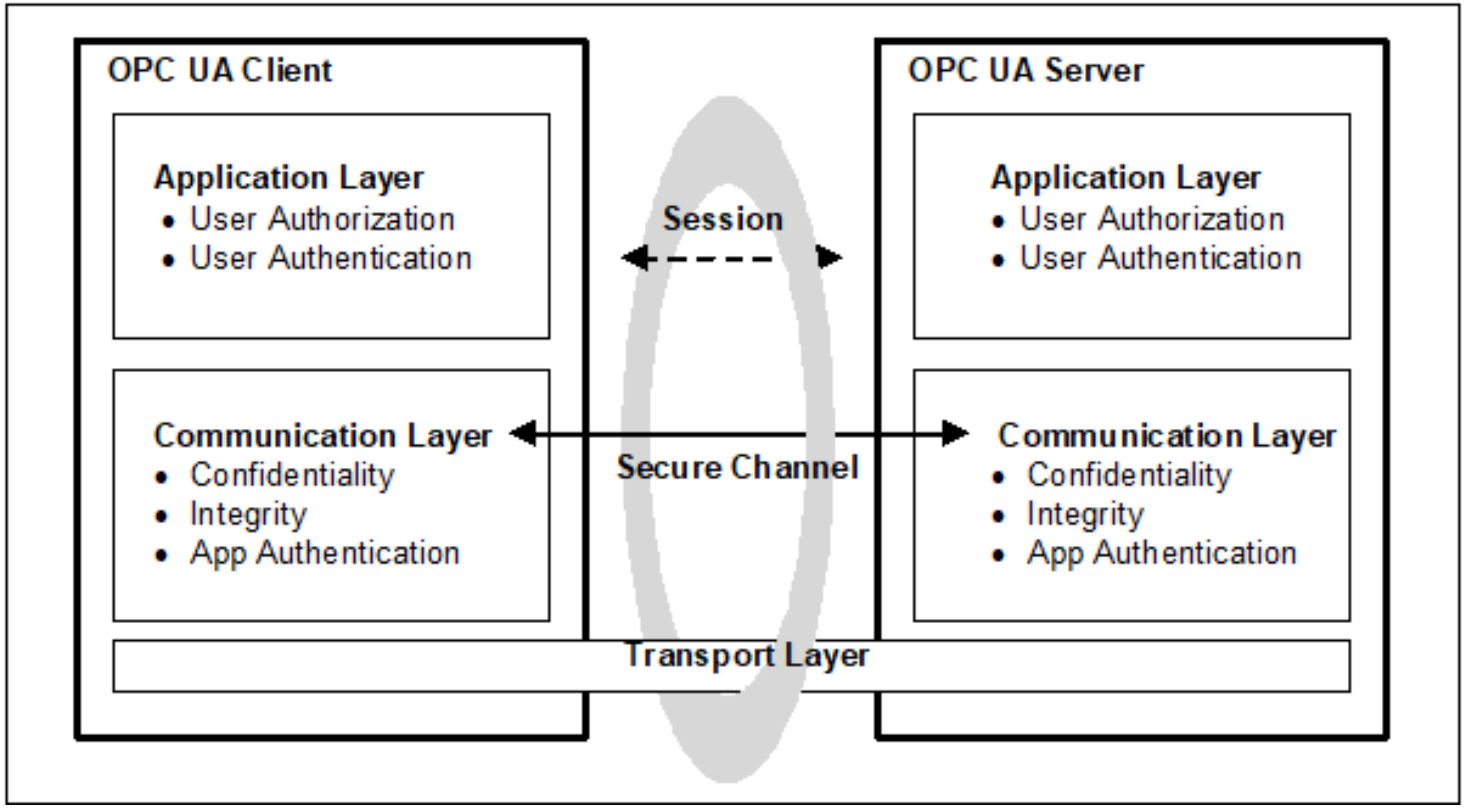
- Folosit în prezent pe scară largă în ICS
- Proiectat ca un standard deschis - https://opcfoundation.org

OPC UA


Industrial Interoperability: From Sensor into Cloud
OPC UA
Cloud
ERP MES SCADA
Relay Broker
OPC UA
Satellite
OPC UA
OPC UA
Pump
Oil Refinery
Controller
Saw
OPC UA
Controller
Press
OPC UA
DCS
OPC UA
Mobile Robot
Initiative for Field Level Communications
Fieldbus
OPC UA

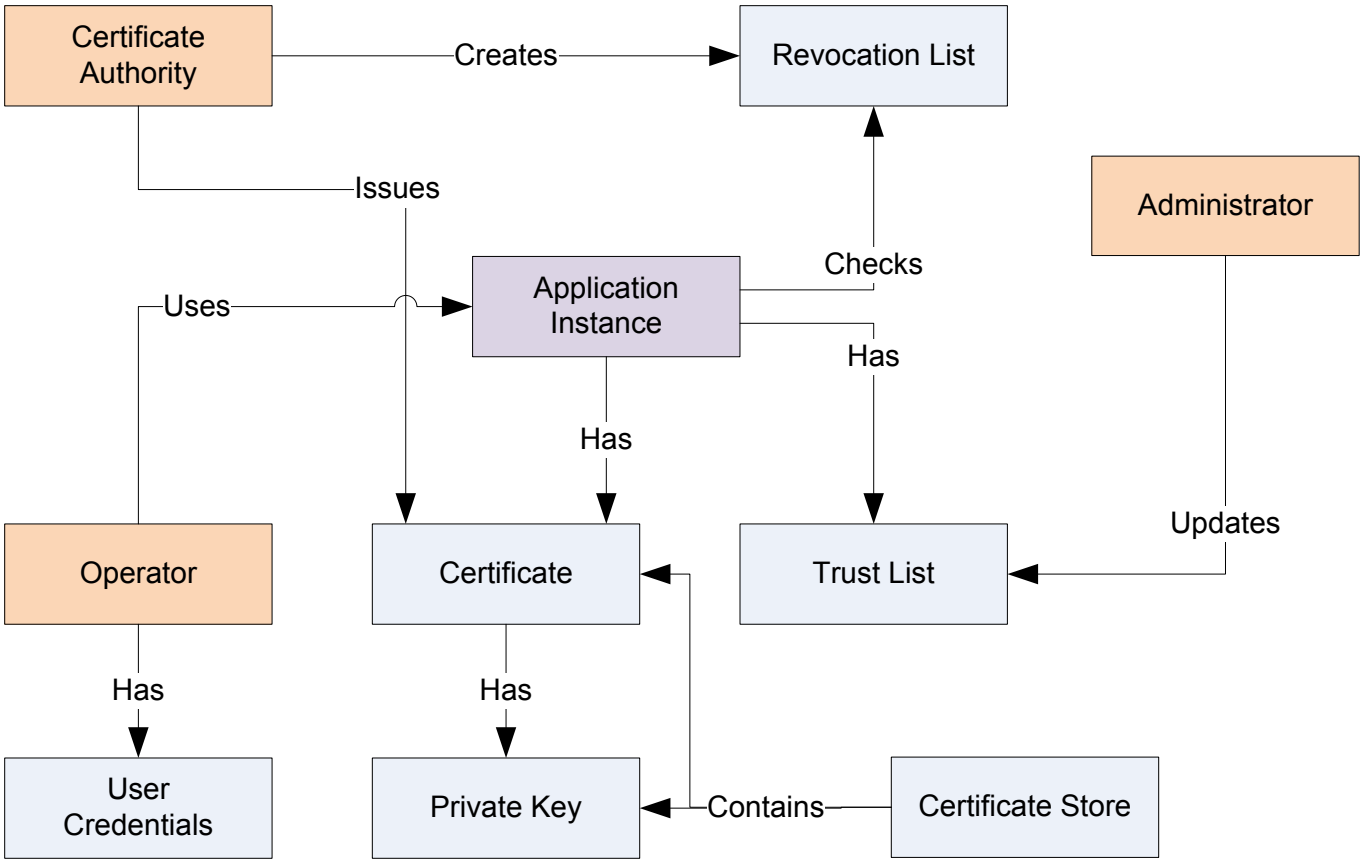
OPC-UA

- OPC-UA include măsuri de securitate cibernetică și de autentificare



Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Autentificarea în OPC-UA



Comparație IT/OT

- În sistemele IT, informația este obiectivul principal
- În ICS, informația este cuplată cu procesul industrial extern, care este obiectivul principal
  - Datele colectate în timp real de la echipamentele din procesul fizic
  - Siguranța fizică a personalului și a instalațiilor este critică
- Hardware și software proprietar
  - Reacții incompatibile sau necunoscute la actualizări de securitate cibernetică. Adesea sistemele nu sunt actualizate perioade lungi de timp.
  - Protocoale de comunicații specifice, necunoscute soluțiilor COTS de securitate
- Mod *fail open* – sistemul trebuie să rămână disponibil în timpul atacurilor cibernetice

Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Comparație IT/OT

- Un număr foarte redus de utilizatori
  - De regulă un singur operator la un moment dat cu toți operatorii partajând un cont comun. Operare 24/7.
  - Tehnicienii și inginerii au acces
  - Utilizatorii din companie accesează baza de date în mod read only
- Fluxuri de date constante de mici dimenisiuni
  - Nu sunt transferate fișiere mari în rețeaua ICS – transferuri de date mici și continue între toate nodurile rețelei
  - Actualizări la fiecare secundă și importanța ordinii de actualizare pentru fiecare echipament fizic
- Autentificarea și fiabilitatea sunt critice
- Confidențialitatea este mai puțin importantă (spre deosebire de informațiile financiar-bancare de exemplu)

Comparație IT/OT

- Securitatea cibernetică în ICS este cu atât mai importată decât în sistemele IT generice deoarece poate afecta siguranța personală și funcții critice ale societății
- Depindem de ICS pentru operarea majorității infrastructurilor critice (energie, utilități, telecomunicații, sănătate, transporturi/logistică ș.a.)

- Dezvoltarea soluțiilor de securitate ICS mai lentă dar în creștere
- Grupurile responsabile de securitate cibernetică IT și ICS provin din zone diferite și au obiective diferite dar trebuie să colaboreze

Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Rezumat IT/OT

CATEGORIE	TEHNOLOGIA INFORMAȚIEI (IT)	TEHNOLOGIA OPERAȚIONALĂ (OT)
Cerințe de performanță	Fără cerințe de timp real Răspunsul consistente. Rată mare de transfer. Latența și jitter ridicate pot fi acceptabile. Controlul stric al accesului poate fi implementat conform cerințelor de securitate.	Operate în timp real. Timp de răspuns critic. Rata redusă de transfer acceptabilă Latență mare / jitter inacceptabile Răspunsul la interacțiuni umane sau de urgență este critic. Accesul la OT controlat strict, fără a împiedica interacțiunea om mașină.
Cerințe disponibilitate (fiabilitate)	Răspunsuri precum resetarea sunt acceptabile Deficiențe de disponibilitate pot fi uneori acceptate	Resetarea sistemelor poate să nu fie acceptabilă datorită cerințelor de disponibilitate Se poate impune redundața sistemelor
Managementul riscurilor	Gestiunea datelor și asigurarea confidențialității și integrității Întârzierea operațiilor de afaceri	Control asupra lumii fizice Siguranța umană urmată de protejarea procesului Toleranță la defecte

Rezumat IT/OT

CATEGORIE	TEHNOLOGIA INFORMAȚIEI (IT)	TEHNOLOGIA OPERAȚIONALĂ (OT)
Operarea sistemelor	Utilizează sisteme de operare comune, de uz general Actualizările se fac direct prin instrumente automate	Utilizează sisteme diferite, proprietare, fără funcții de securitate integrate Schimbările software se fac controlat, de către furnizori, considerând impactul asupra algoritmilor de control, hw/sw
Constrângeri de resurse	Sistemele sunt proiectate cu suficiente resurse pentru a suporta adăugarea unor aplicații terțe e.g. soluții de securitate	Sistemele sunt proiectate pentru procesul industrial și pot avea limitări de calcul și/sau memorie pentru funcții noi
Comunicații	Sunt folosite protocoale de comunicație IT standard Rețele cu fir și rețele wireless locale Bune practici de administrate a rețelelor IT	Protocoale de comunicație multiple, eterogene, proprietare și/sau standardizate* Mix de medii de comunicație prin legături cu fir și la distanță Rețele complexe care necesită expertiza inginerilor automatiști

Rezumat IT/OT

CATEGORIE	TEHNOLOGIA INFORMAȚIEI (IT)	TEHNOLOGIA OPERAȚIONALĂ (OT)
Managementul schimbărilor	Modificări software aplicate la timp, alături de politici și proceduri clare de securitate (automate de multe ori)	Modificările software trebuie testate riguros și implementate gradual pentru a asigura integritatea sistemului OT Deconectarea OT trebuie planificată cu zile/luni în avans. OT poate folosi software care nu mai este suportat și multe aplicații particularizate
Gestionare suport tehnic	Modalități diversificate de asigurare a suportului	Suportul tehnic oferit de regulă printr-un singur furnizor
Durata de viață a componentelor	De 3-5 ani	De 10-15-20 de ani
Localizarea componentelor	Locale și ușor de accesat	Pot fi izolate, la distanță și impun effort fizic semnificativ pentru a fi accesate

Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Soluții de securitate cibernetică

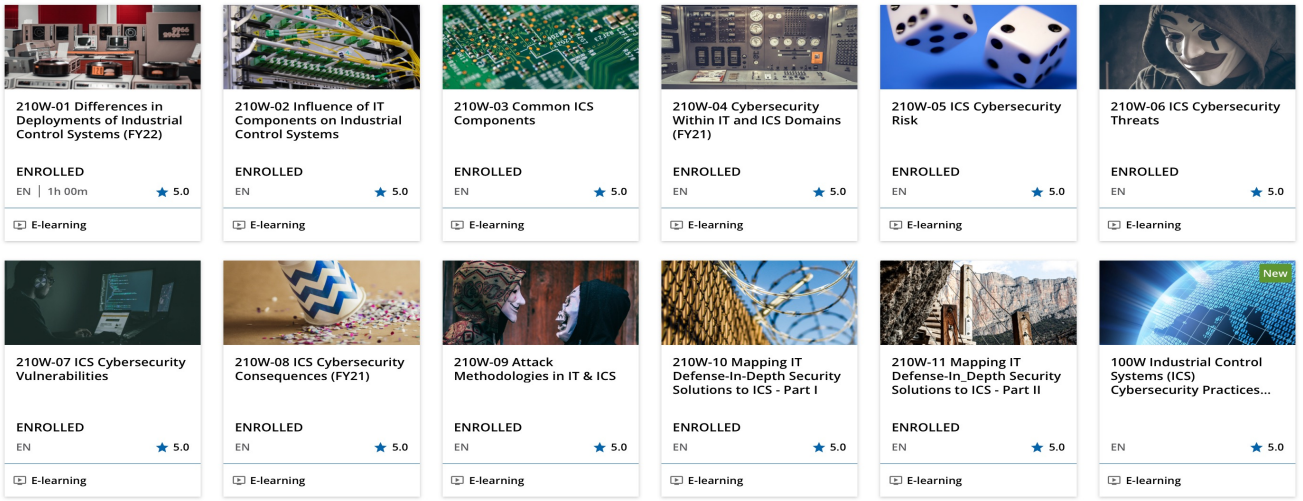
- Există o serie de produse pentru infrastructuri IT și care pot fi aplicate în ICS dar foarte puține specifice pentru ICS (e.g. “diode de date” Waterfall)
- Limitări hardware și software care nu permit implementarea unor algoritmi sau metode complexe
  - Sisteme legacy cu resurse de calcul și de memorie limitate, sisteme de operare obscure
  - Necesită adesea un server exter – externalizarea securității de pe echipamente
- Multe protocoale de comunicații nu includ funcții de securitate
- Formarea personalului este esențială

CISA

- *Cybersecurity and Infrastructure Security Agency – S.U.A.*
- Obiective:
  - Apărarea mediilor ICS împotriva amenințărilor urgente
  - Identificarea și neutralizarea adversarilor înainte de a putea provoca daune
  - Echiparea proprietarilor și operatorilor de infrastructuri (critice) cu tehnologii și instrumente eficiente
  - Susținerea rezilienței operaționale
- Portal de învățare (VLP):

Igienă cibernetică +

Conștientizare



Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

CISA VLP

Certificate of Training

Completion

Presented by the

U.S. Department of Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA)

Awarded To

Grigore Stamatescu

For completion of the

Virtual Industrial Control Systems Cybersecurity (301V) Training

On

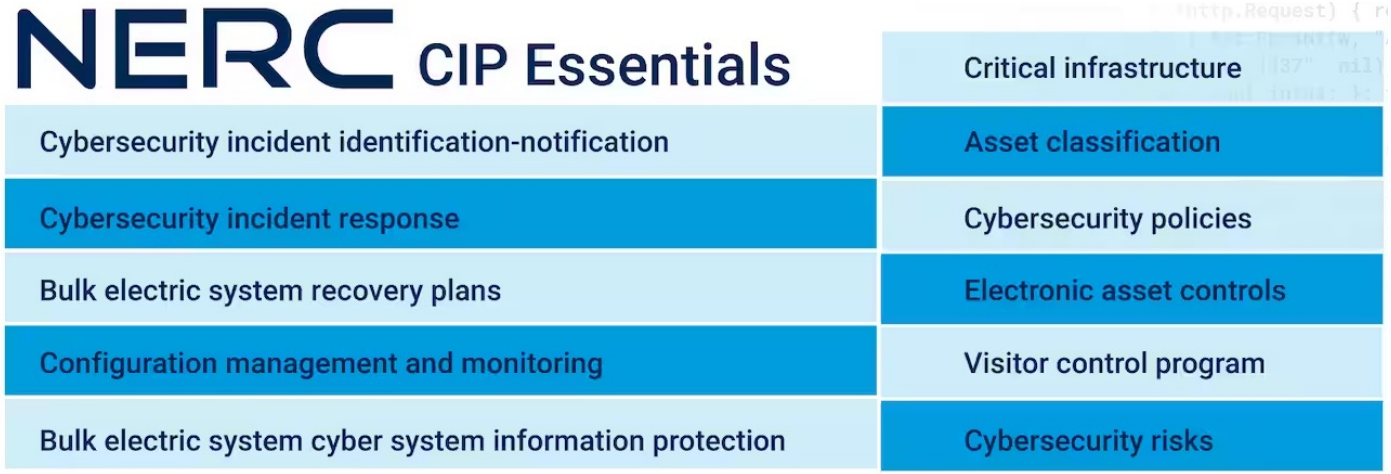
7/28/2022

CEUs Awarded: 1.4

Contact Hours: 14

NERC CIP

- North American Electric Reliability Corporation Critical Infrastructure Protection
- Set de standarde pentru reglementarea, respectarea, monitorizarea și gestionarea aspectelor de Securitate cibernetică în sistemele energetice: https://www.industrialdefender.com/blog/what-is-nerc-cip



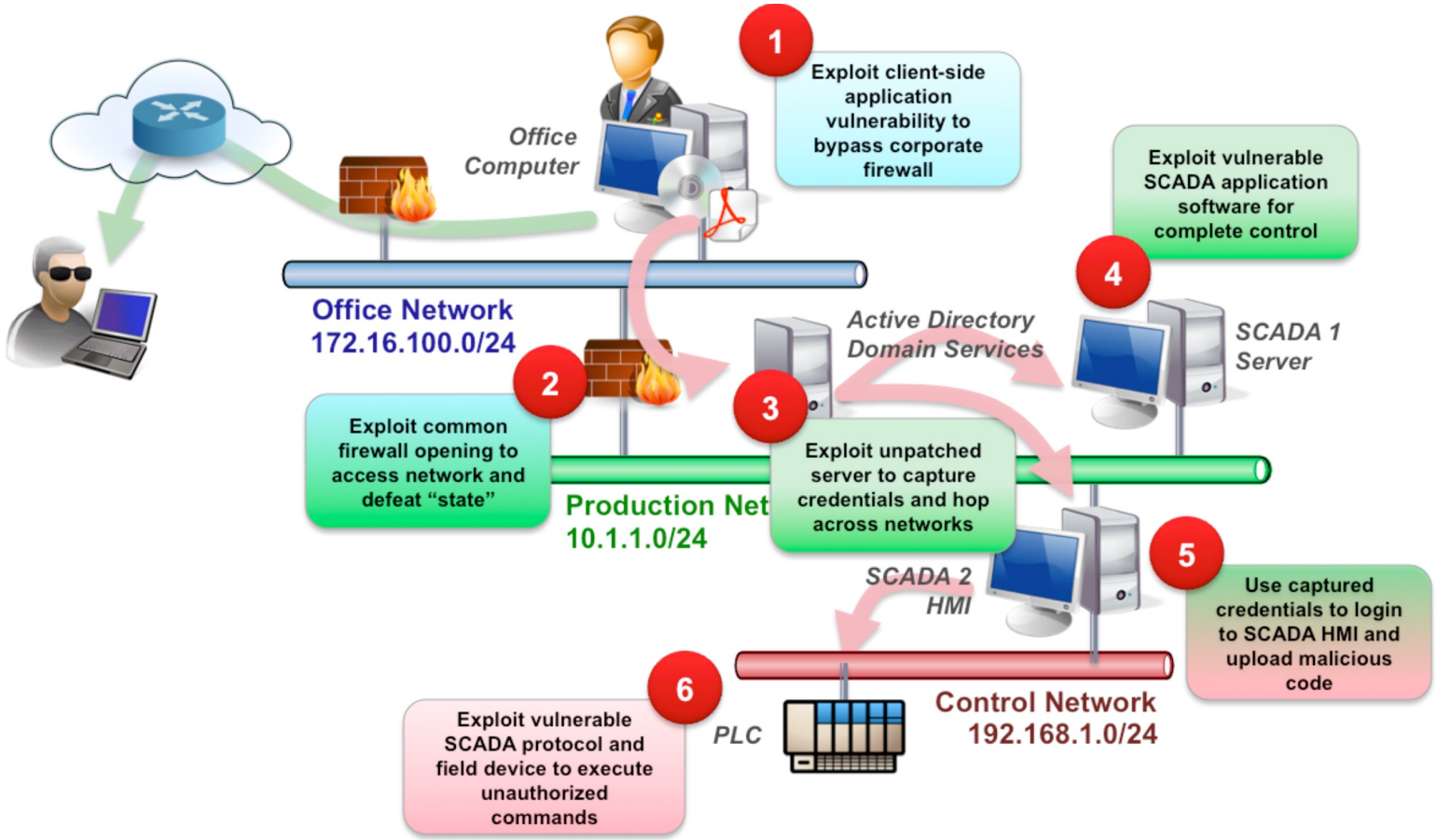
Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

National SCADA Test Bed - DoE

- Facilități de testare într-un mediu controlat pentru validarea securității cibernetice și a rezilienței ICS
- Concentrat pe securitatea sistemelor de automatizare în energie
- Permite partenerilor industriali să își testeze soluțiile
- Partenerii de cercetare pot organiza experimente și sesiune de formare

- Fact sheet: https://www.energy.gov/ceser/articles/national-scada-test-bed-enhancing-control-systems-security-energy-sector-september

Etape atac cibernetic



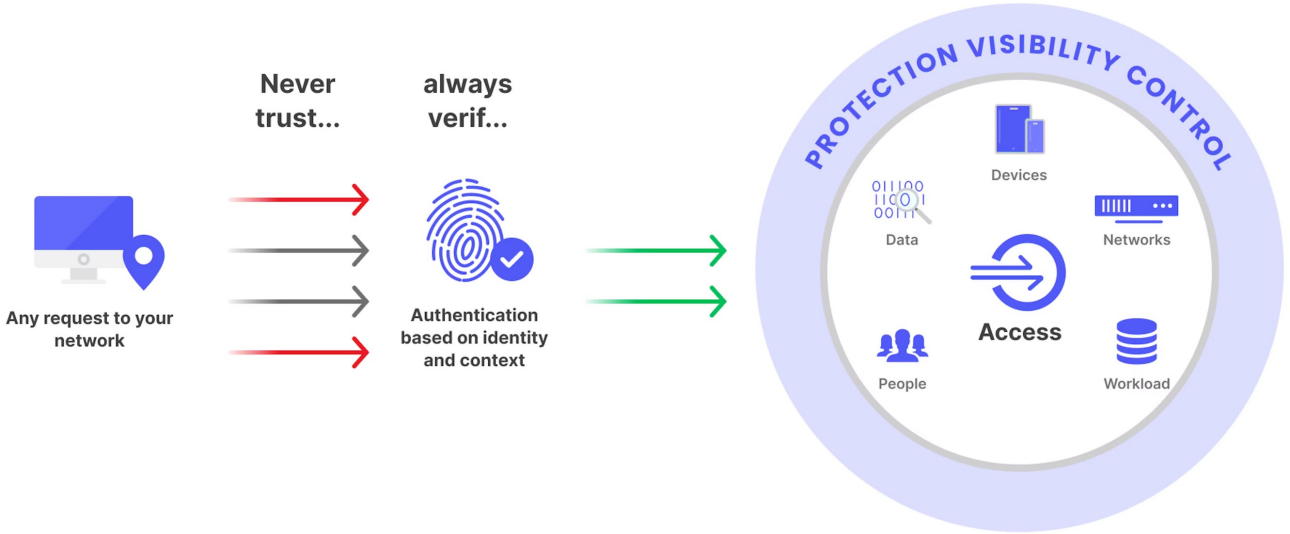
NIST Cybersecurity Framework 2.0

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Cybersecurity Supply Chain Risk Management	GV.SC
	Roles, Responsibilities, and Authorities	GV.RR
	Policies, Processes, and Procedures	GV.PO
	Oversight	GV.OV
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Zero Trust

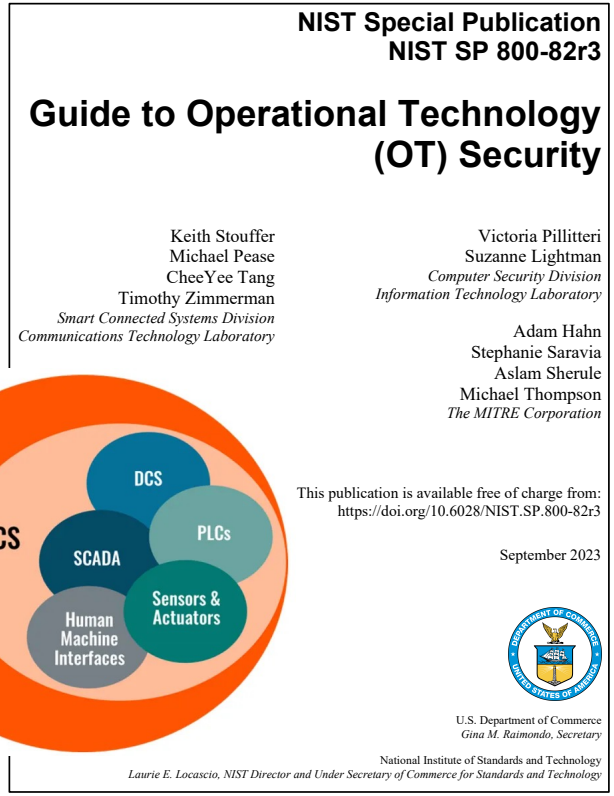
- **Zero Trust** este un cadru de securitate care necesită ca toți utilizatorii, fie din interiorul sau din afara rețelei organizației, să fie autentificați, autorizați și validați continuu pentru configurarea și poziția de securitate înainte de a li se acorda sau de a păstra accesul la aplicații și date



Ghidul NIST 800-82r3

- NIST Guide to Operational Technology (OT) Security
  Disponibil on-line: https://csrc.nist.gov/pubs/sp/800/82/r3/final

- Acoperă următoarele tematici:
  - Bune practici pentru securizarea OT considerând caracteristicile specifice de performanță, fiabilitate și siguranță în operare
  - Prezentarea topologiilor tipice de sisteme OT
  - Identificarea amenințărilor și vulnerabilităților
  - Contra-măsuri de securitate pentru reducerea riscurilor
- ICS este un subset al OT


NIST Special Publication
NIST SP 800-82r3

Guide to Operational Technology (OT) Security

Keith Stouffer
Michael Pease
CheeYee Tang
Timothy Zimmerman
Smart Connected Systems Division
Communications Technology Laboratory

Victoria Pillitteri
Suzanne Lightman
Computer Security Division
Information Technology Laboratory

Adam Hahn
Stephanie Saravia
Aslam Sherule
Michael Thompson
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-82r3

September 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Tipuri de incidente OT

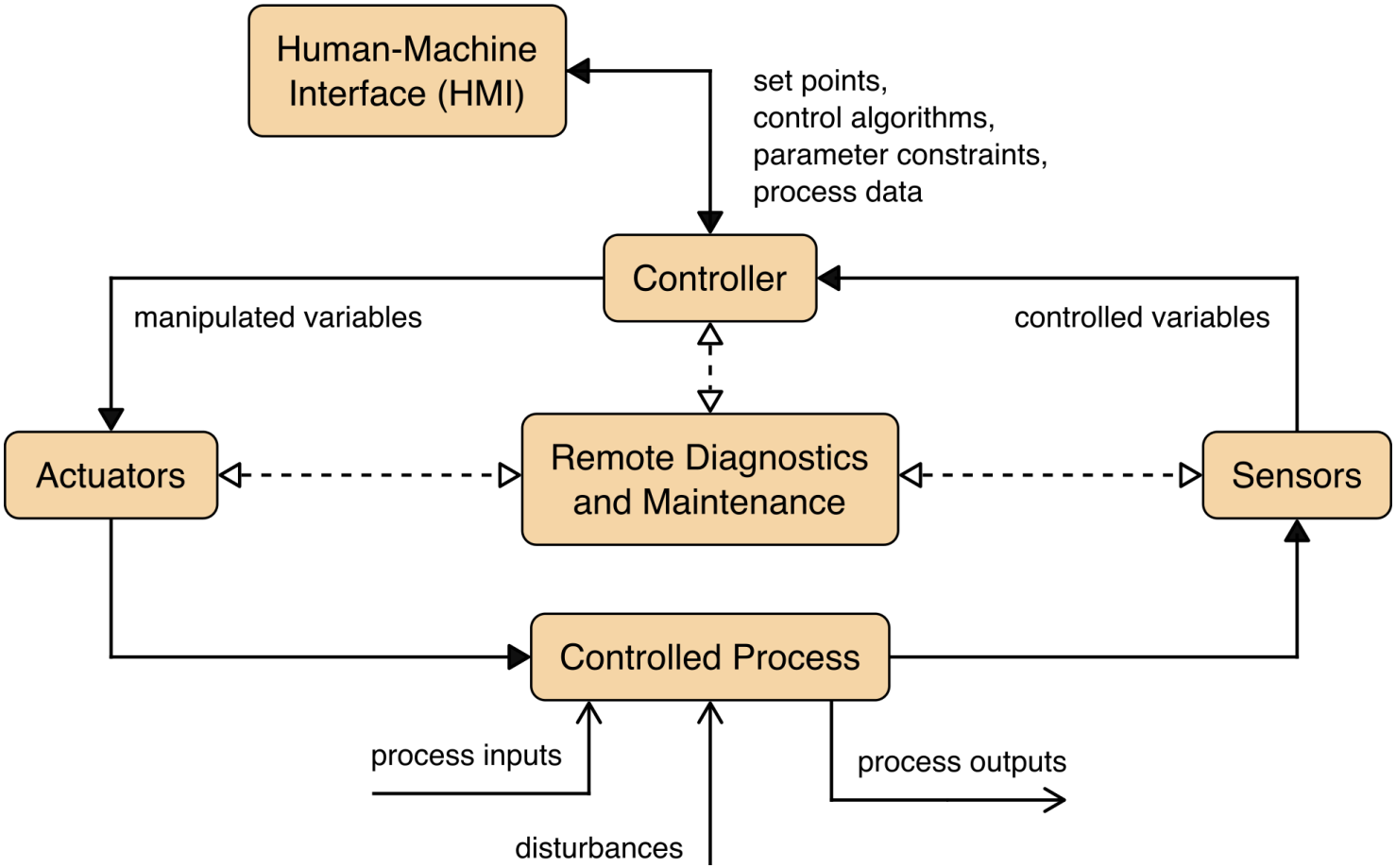
- Fluxul de infomații prin rețelele OT este blocat sau întârziat cu posibil impact asupra operării: pierderea vizbilității și pierderea controlului
- Modificări neautorizate ale instrucțiunilor, comenzilor sau pragurilor de alarmă care pot distruge, dezactiva sau opri echipamentele, punând în pericol viața umană și mediul înconjurător
- Informații incorecte transmise operatorilor, fie pentru a obfusca modificările neautorizare, fie pentru a provoca acțiuni nepotrivite cu efecte negative
- Modificarea software-ului sau a setărilor de configurare sau infectarea cu malware OT
- Interferența cu buna funcționare a sistemelor de protecție a echipamentelor care cauzează daune semnificative
- Interferența cu sistemele safety care poate pune în pericol viața umană

Obiectivele securității OT

- Restricționarea accesului logic la rețeaua OT, la activitatea de rețea și la sistemele OT
- Restricționarea accesului fizic la echipamentele și rețeaua OT
- Protejarea la exploatare a componentelor OT individuale
- Restricționarea modificării neautorizate a datelor
- Detectarea evenimentelor și incidentelor de securitate cibernetică
- Menținerea funcționalităților în condiții adverse
- Restaurarea și recuperarea sistemului după un incident

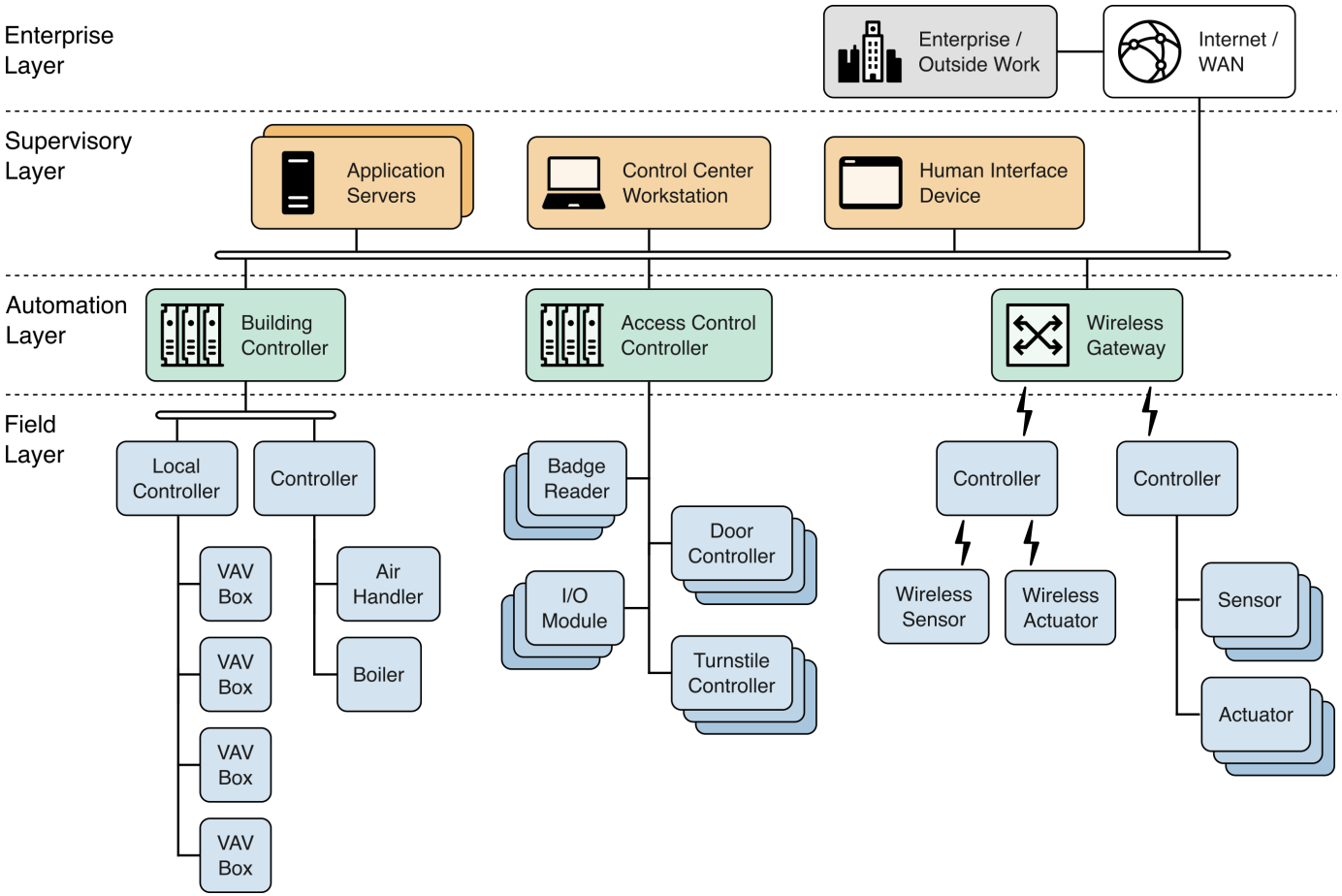
Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Structura unui sistem OT



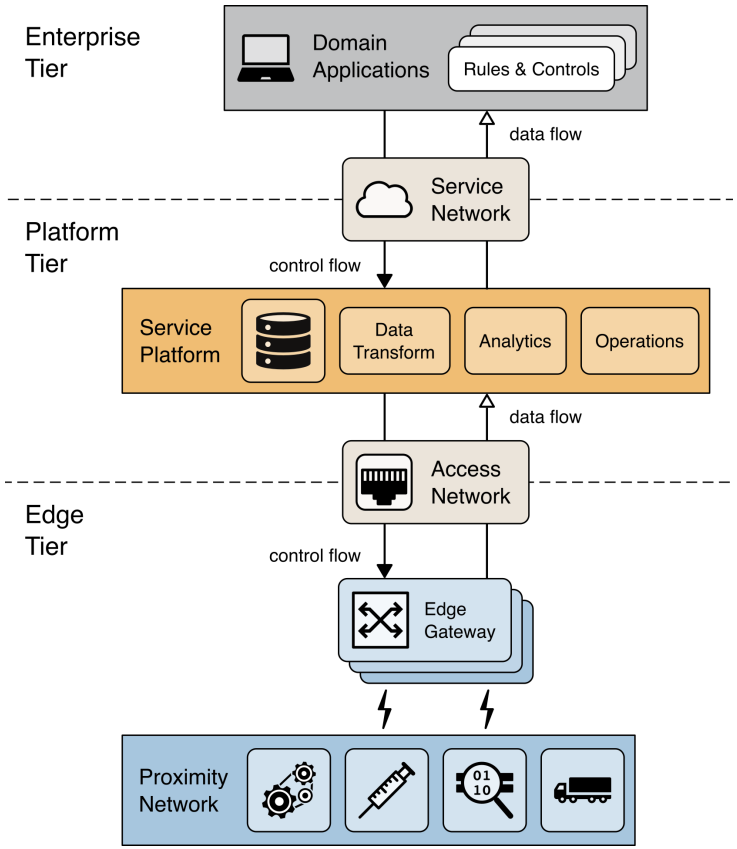
Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Exemplificare – BAS/BMS



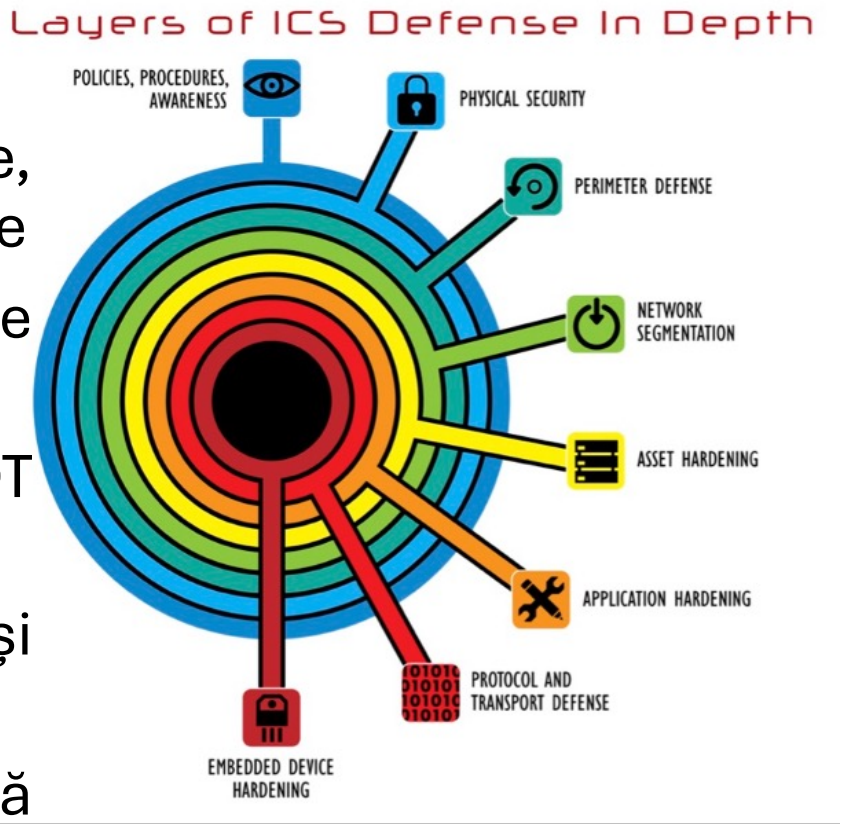
Exemplificare – IIoT

- Industrial Internet of Things (IIoT) compus din senzori, instrumentație, echipamente și alte componente interconectate care folosesc conectivitatea la Internet pentru îmbunătățirea proceselor și aplicațiilor industriale și de fabricație
- Model pe trei niveluri definit de Industry IoT Consortium
- Arhitectură distribuită de sistem și moduri de colaborare și interoperabilitate diferite
- Exploatarea resurselor locale de calcul și comunicație prin *edge computing*



Strategia de apărare în profunzime

- **Defense-in-depth (DiD)**
- Dezvoltarea de politici de securitate, proceduri, formare, materiale educaționale
- Abordarea securității pe întregul ciclu de viață al sistemelor OT
- Implementarea unei topologii de rețea OT cu straturi multiple
- Separarea logică între rețelele companiei și rețelele OT
- Identificarea zonelor unde este necesară separarea fizică



Strategia de apărare în profunzime

- Utilizarea unei arhitecturi de rețea DMZ pentru prevenirea traficului direct între rețeaua companiei și cea OT
- Utilizarea autentificării multi-factor pentru accesul la distanță la sistemele OT
- Asigurarea redundanței pentru componentele critice, în rețele redundante
- Proiectarea pentru degradare grațioasă (toleranță la defecte) pentru prevenirea evenimentelor catastrofice în cascadă
- Dezactivarea porturilor și serviciilor nefolosite pe echipamentele OT după testarea că acestea nu vor influența operarea
- Limitarea privilegiilor utilizatorilor OT la cele minime RBAC

Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Strategia de apărare în profunzime

- Utilizarea de mecanisme de autentificare și credențiale separate pentru utilizatorii rețelei OT și a celei a companiei (e.g. conturile din rețeaua OT nu sunt aceleași cu cele din rețeaua companiei)
- Implementarea controalelor de securitate e.g. sisteme de detecție și prevenire a intruziunilor, software antivirus, verificare integritate pentru a preveni, descuraja, detecta și remedia acțiunile software-ului malițios
- Aplicarea unor tehnici de securitate, cum este criptarea la comunicațiile și stocarea datelor OT, acolo unde este posibil
- Aplicarea de actualizări software după testarea acestora pe un sistem dedicat în condiții realiste

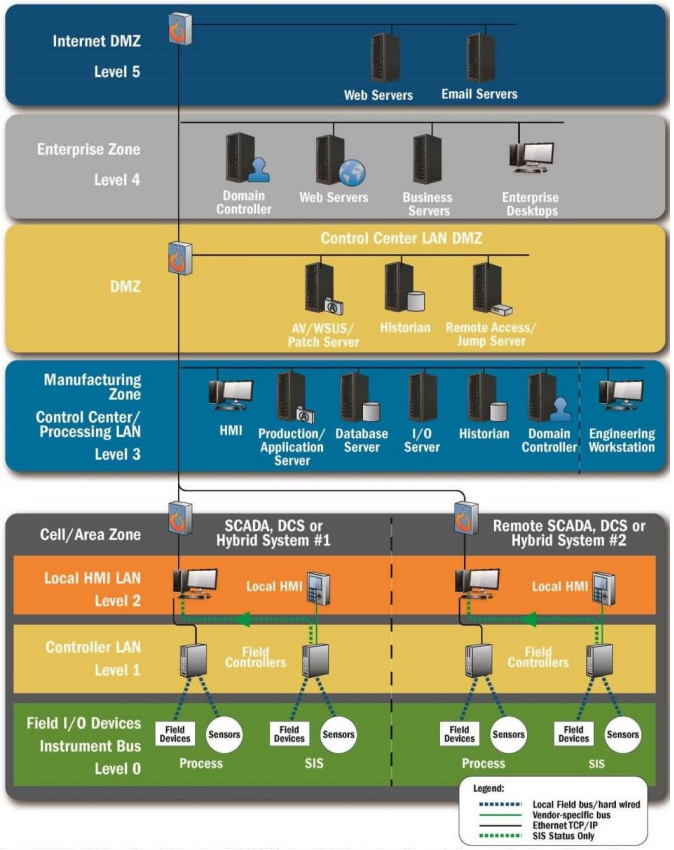
Arhitectura Defense-in-Depth

- Inițiativele de transformare digitală din industrie implementează noi arhitecturi informaționale care asigură de regulă:
  - Mentenanța echipamentelor, telemetrie, sisteme de conducere integrate
  - Colectarea pe scară largă a datelor și diseminarea acestora
  - Accesul la distanță
- Integrarea IT-OT necesită niveluri multiple de securitate cibernetică
- Straturile unei arhitecturi DiD sunt următoarele:
  - Nivelul 1 – Managementul securității
  - Nivelul 2 – Securitatea fizică
  - Nivelul 3 – Securitatea rețelelor
  - Nivelul 4 – Securitate hardware
  - Nivelul 5 – Securitate software

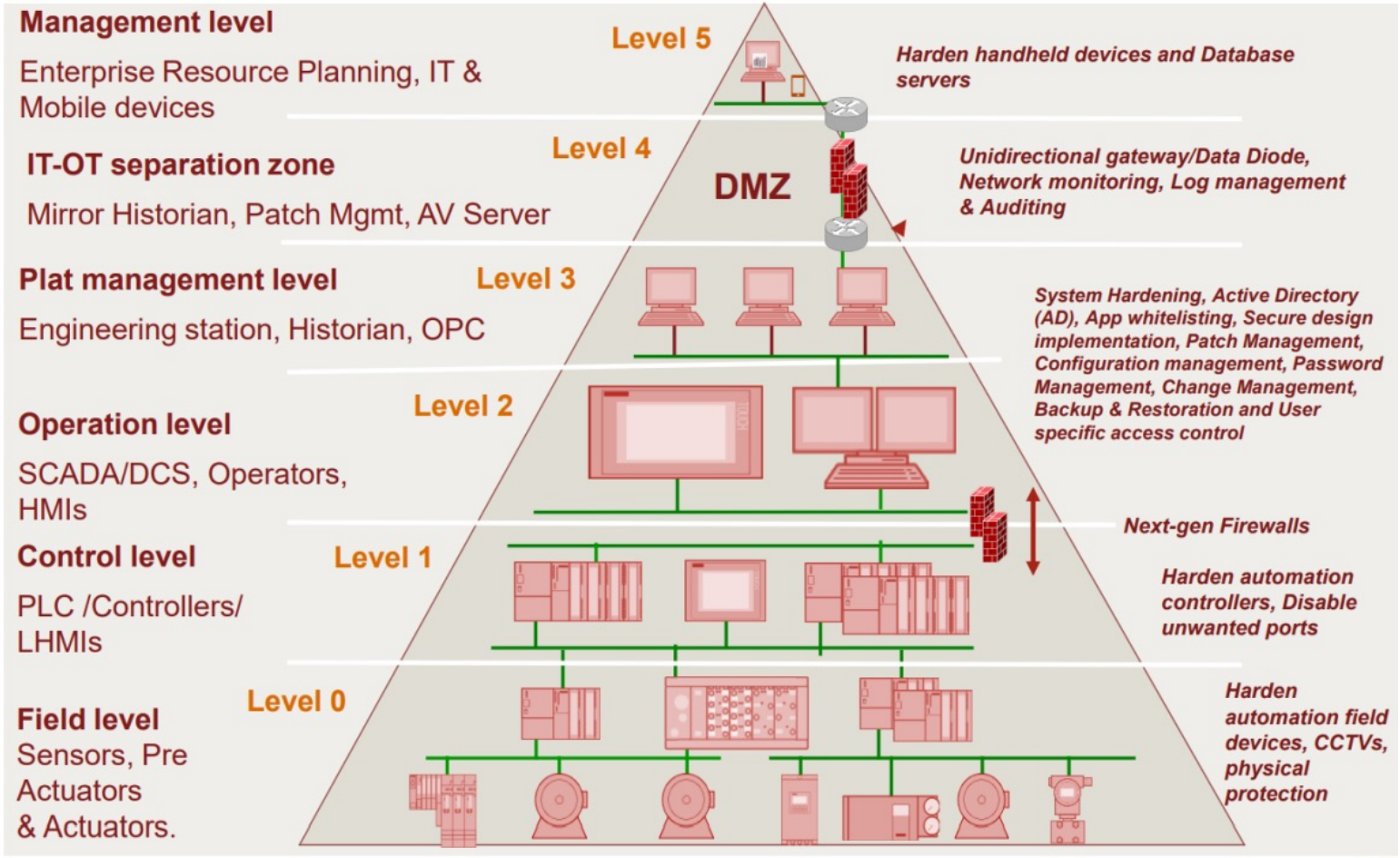
Modelul Purdue

- Williams, Theodore J. "The Purdue enterprise reference architecture." Computers in industry 24.2-3 (1994): 141-158.
- Modelul Purdue a fost conceput ca model de referință pentru fluxurile de date în fabricația integrată în computer (CIM).
- Ulterior, acest model a ajuns să definească standardul pentru construirea unei arhitecturi de rețea ICS care acceptă securitatea OT prin separarea straturilor rețelei.
- Comitetul ISA99

https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99

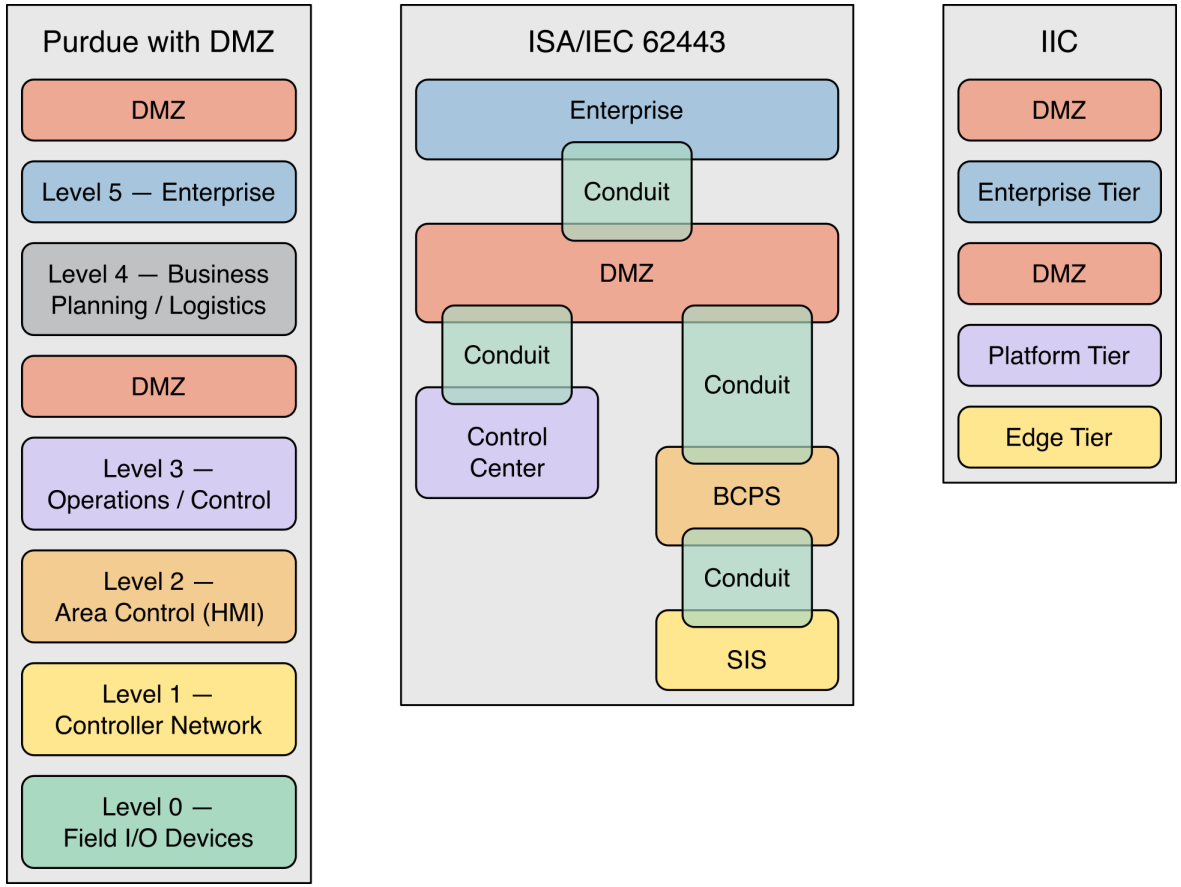


Modelul Purdue



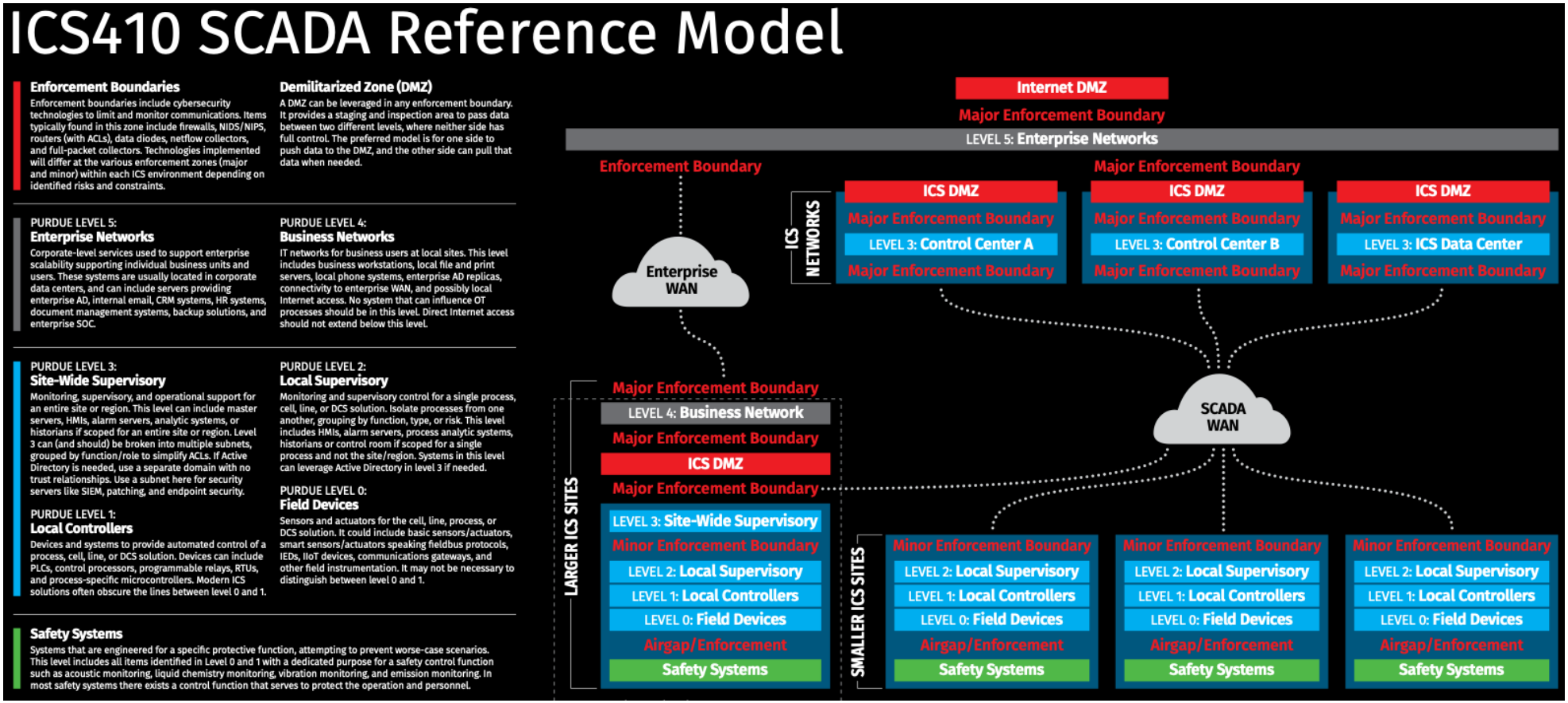
Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Comparație Purdue – ISA/IEC62443

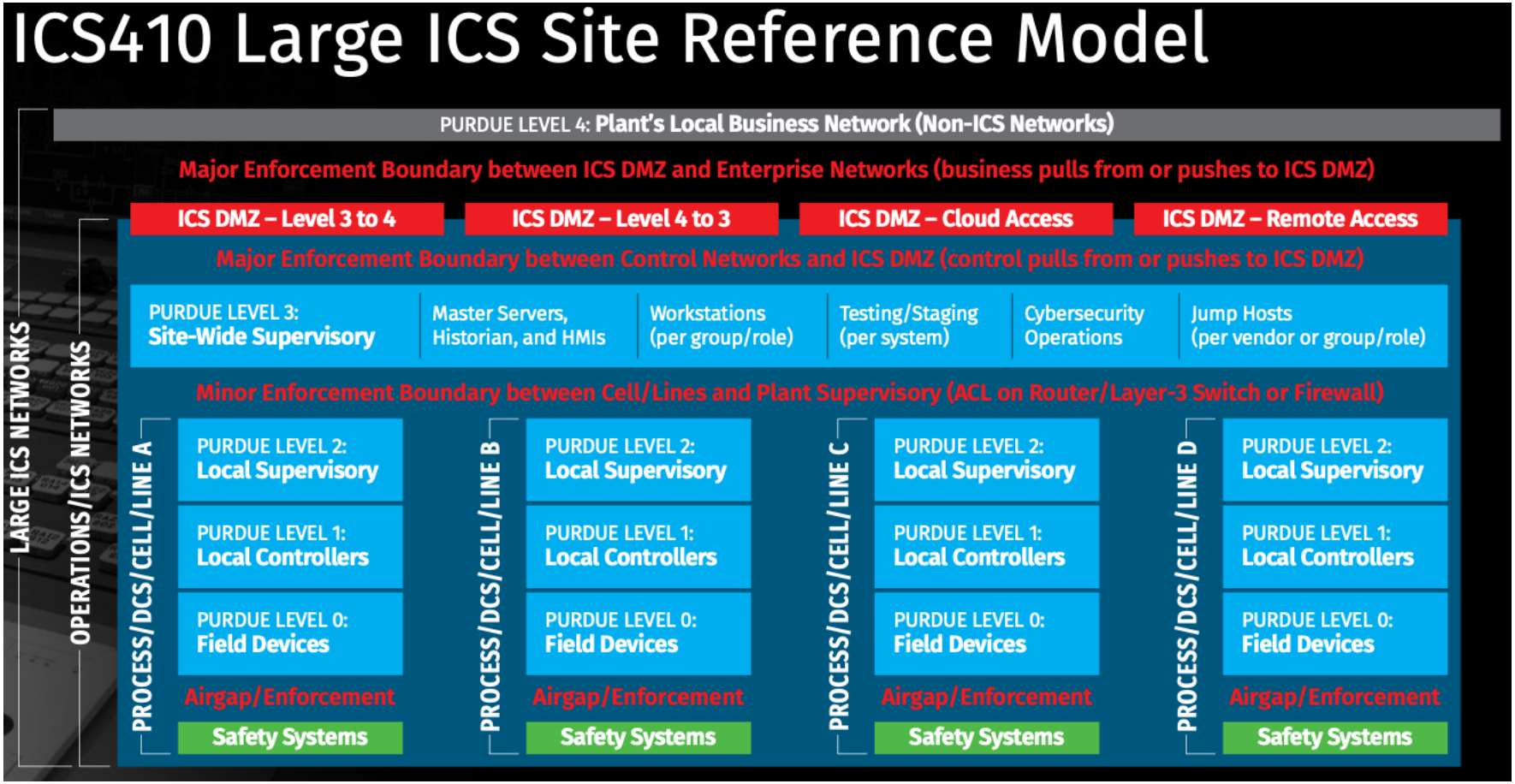


Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Modelul SANS SCADA



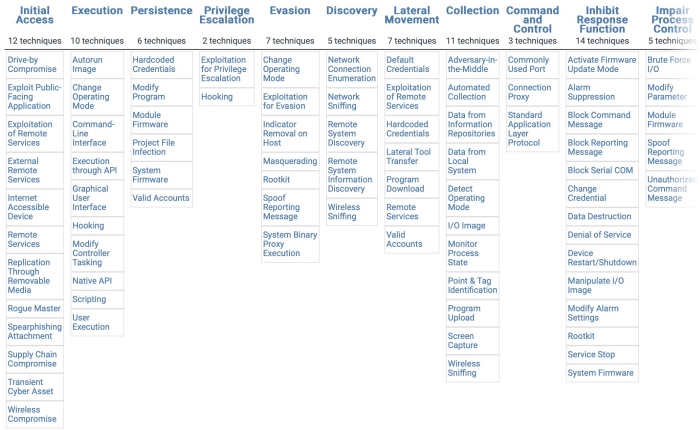
Modelul SANS SCADA - Detaliere



Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

MITRE ATT&CK

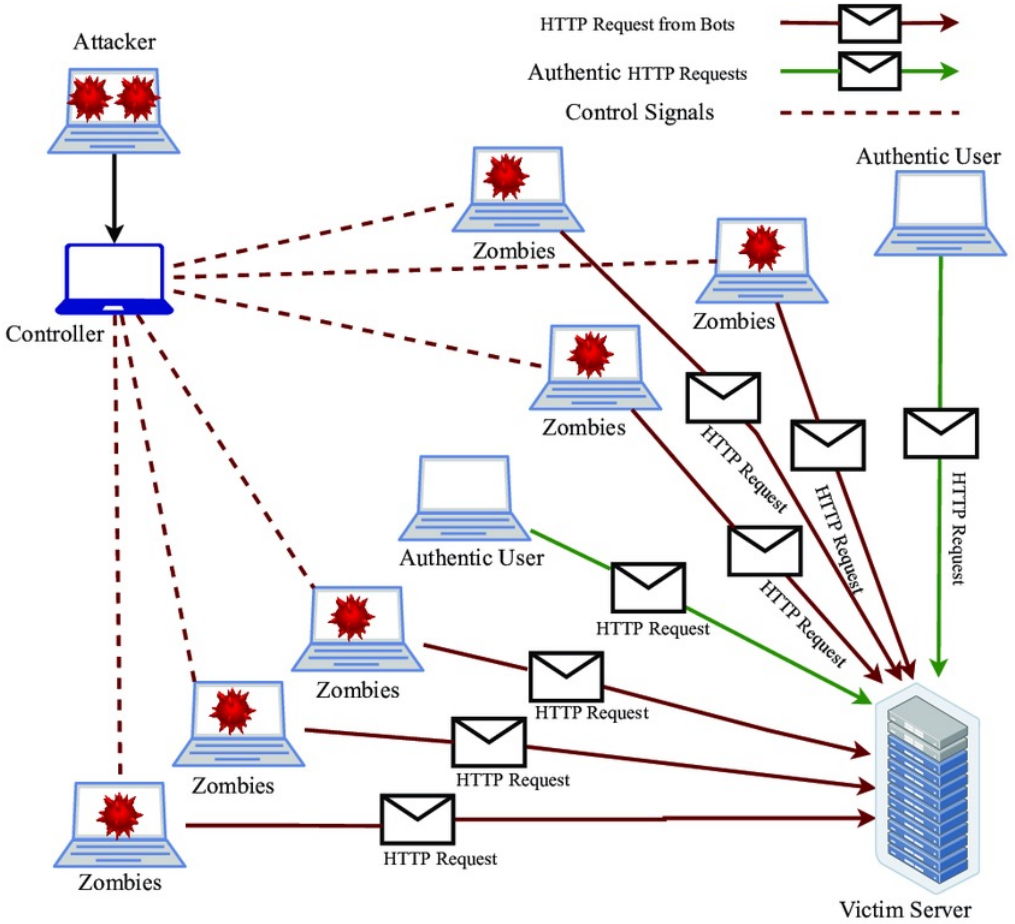
- *Adversarial Tactics, Techniques & Common Knowledge*
- Cadru, bază de cunoștințe și instrumente de evaluare pentru securitatea cibernetică a organizațiilor
- Aplicabilitate și instrumente specifice pentru domeniul ICS
- https://attack.mitre.org/matrices/ics/



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control
12 techniques	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential	
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction	
Rogue Master	Native API						Point & Tag Identification		Denial of Service	
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown	
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image	
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings	
Wireless Compromise									Rootkit	
									Service Stop	
									System Firmware	

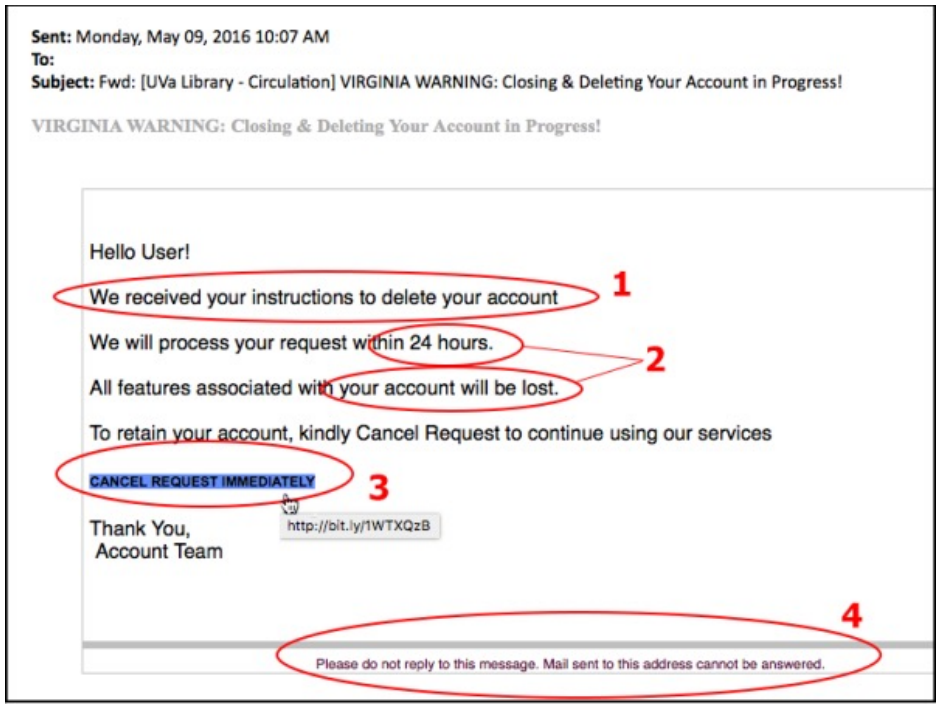
Tipuri de atacuri - DDoS

- (Distributed) Denial of Service (DDoS)
- Atacatorii identifică sisteme, servere sau rețele pe care le indundă cu solicitări pentru a le epuiza resursele și lățimea de bandă
- Serverele nu pot gestiona valul de cereri și se blochează
- În versiunea distribuită, atacatorii folosesc multe sisteme compromise



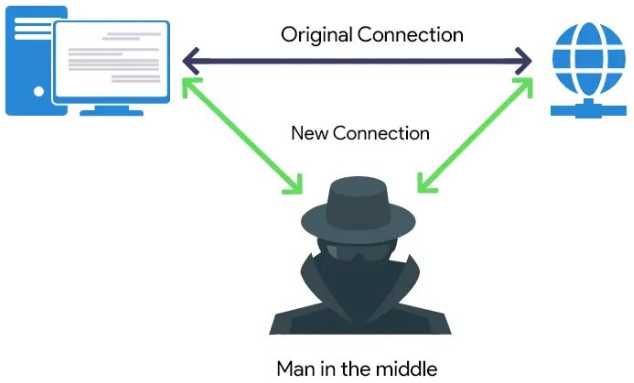
Tipuri de atacuri - Phishing

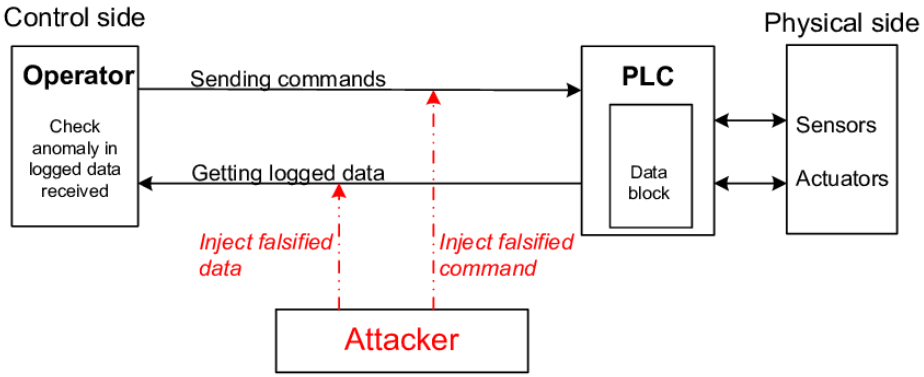
- Cele mai răspândite atacuri
- Atac de tip inginerie socială unde atactorul impersonează un contact legitim și transmite mesaje e-mail false victimei
- Victima accesează link-uri compromise/atașamente și permite astfel accesul la informații confidențiale sau instalarea de malware
- Variante: spear-phishing, whale phishing



Tipuri de atacuri – Man-in-the-Middle

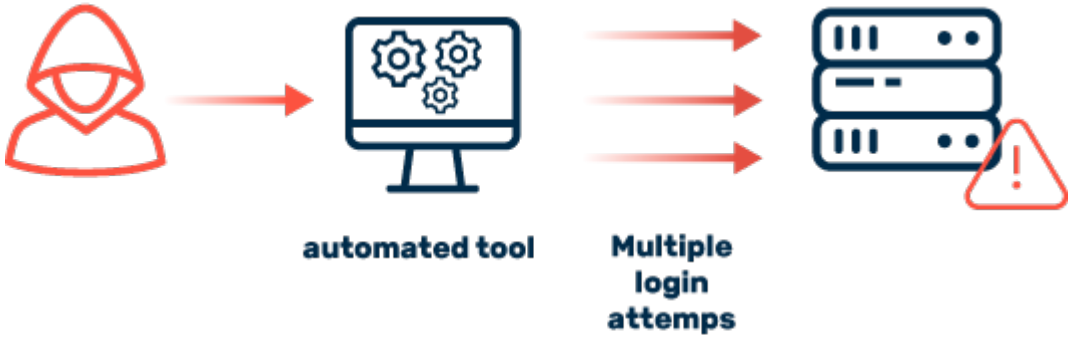
- MITM cunoscut și drept atac de ascultare
- Atacatorul se interpune între două terminale care comunică e.g. între client și gazdă/master
- Poate asculta pasiv pentru a colecta informații sau intervine activ pentru a modifica și manipula datele și comenzile





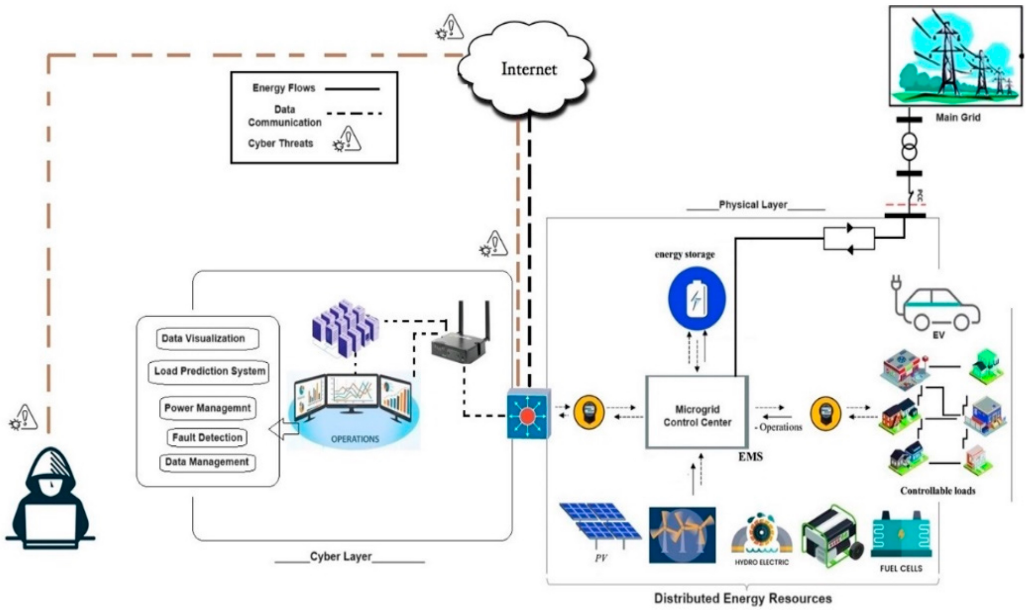
Tipuri de atacuri – Acces neautorizat

- O persoană care nu are permisiune să se conecteze la sau să utilizeze un sistem, în accesează, de o manieră nedorită de către proprietarul sistemului (“hacking”)
- Exploatarea unor greșeli software prin rutine automate
- Utilizarea malware sau a atacurilor de tip ”phishing”



Tipuri de atacuri – False Data Injection

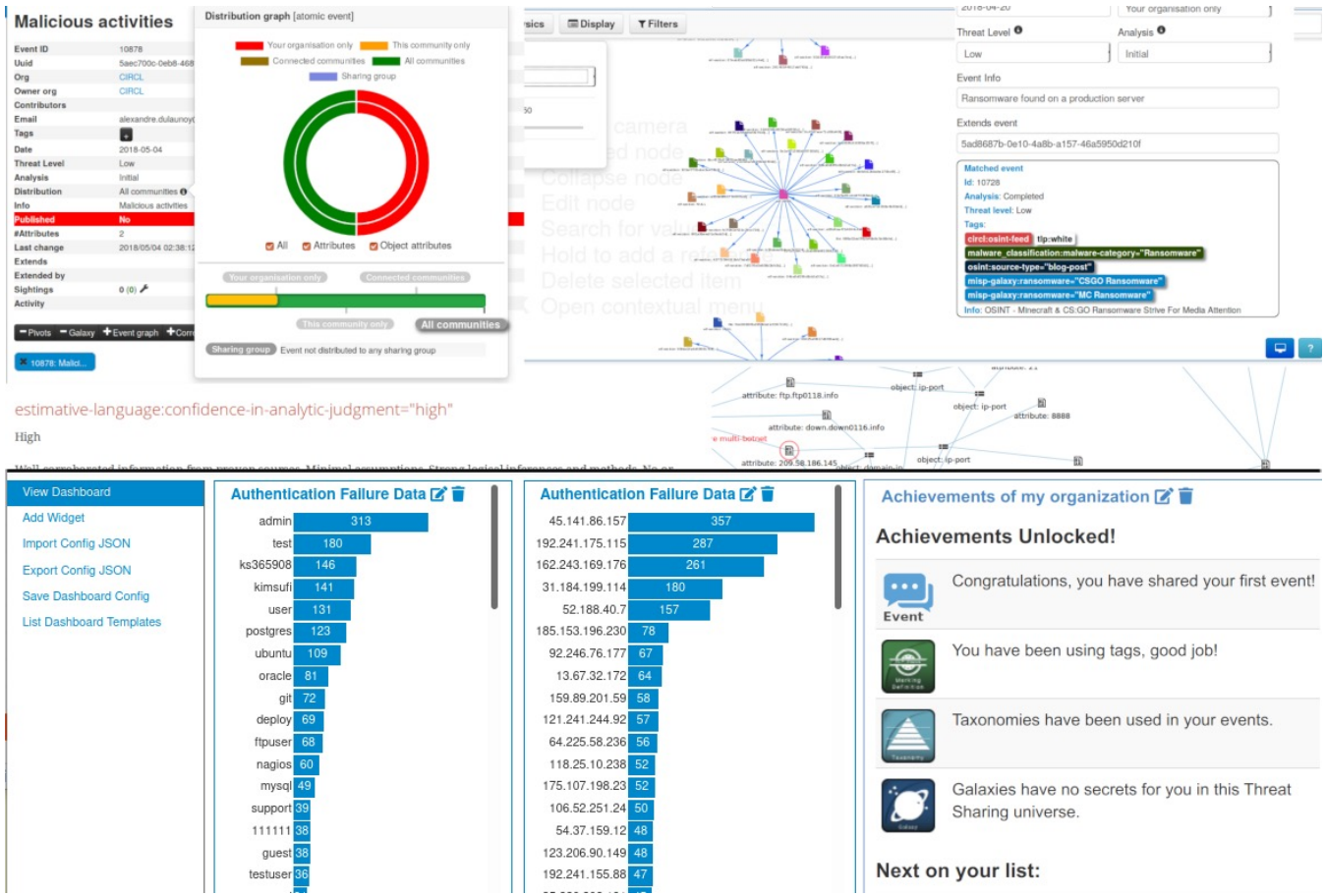
- FDI este un tip de atac cibernetic prin care sunt injectate date false într-un sistem de către o entitate malițioasă
- Exemplu: modificarea estimărilor de stare într-o rețea electrică inteligentă
- Se pot preveni prin mecanisme a validare a datelor/comenzilor e.g. consens distribuit



MISP

- *Malware Information Sharing Platform*
- Inițiat de CIRCL Luxemburg în 2012
- Un instrument software open-source pentru colectarea de informații de la parteneri, analiști și fluxuri de date de securitate cibernetică
- Normalizează, corelează și îmbogățește datele
- Permite colaboarea prin echipe și comunități
- Alimentează instrumente de securitate cibernetică (e.g. SIEM)
- https://github.com/MISP/MISP

Interfața MISP



Common Vulnerability Exposure

- Misiunea Programului CVE este de a identifica, defini și cataloga vulnerabilitățile de securitate cibernetică dezvăluite public
- Există o înregistrare CVE pentru fiecare vulnerabilitate din catalog
- Vulnerabilitățile sunt descoperite, apoi atribuite și publicate de organizații din întreaga lume care au colaborat cu Programul CVE
- Partenerii publică înregistrări CVE pentru a comunica descrieri consecvente ale vulnerabilităților
- Profesioniștii în tehnologia informației și securitatea cibernetică folosesc înregistrările CVE pentru a se asigura că discută aceeași problemă și pentru a-și coordona eforturile de a prioritiza și aborda vulnerabilitățile

Exemplu: CVE-2014-2259

CNA: MITRE Corporation

Published: 2014-03-16 **Updated:** 2020-02-10

Description

Siemens SIMATIC S7-1500 CPU PLC devices with firmware before 1.5.0 allow remote attackers to cause a denial of service (defect-mode transition) via crafted HTTPS packets.

Product Status

Learn more

Information not provided

References 3 Total

- http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens_security_advisory_ssa-456423.pdf
- http://ics-cert.us-cert.gov/advisories/ICSA-14-073-01
- https://cert-portal.siemens.com/productcert/pdf/ssa-456423.pdf

CVE Program

Updated: 2024-08-06

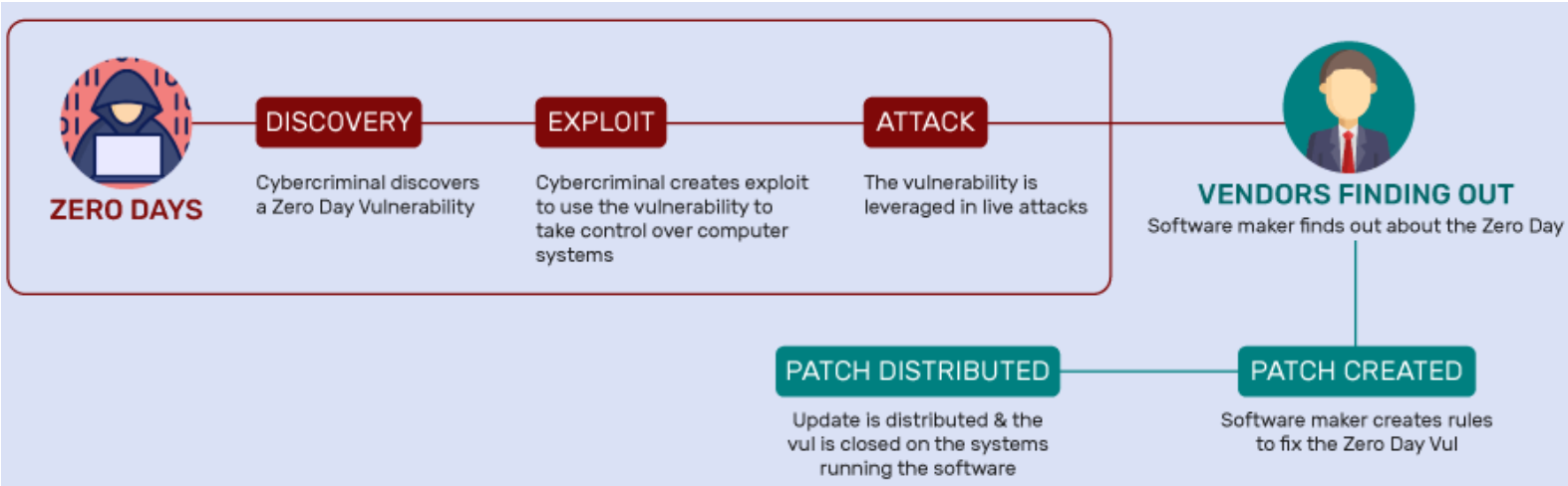
This container includes required additional information provided by the CVE Program for this vulnerability.

References 3 Total

- http://www.siemens.com/innovation/pool/de/forschungsfelder/siemens_security_advisory_ssa-456423.pdf x_transferred
- http://ics-cert.us-cert.gov/advisories/ICSA-14-073-01 x_transferred
- https://cert-portal.siemens.com/productcert/pdf/ssa-456423.pdf x_transferred

Zero Day

- **Zero Day** este o vulnerabilitate în software sau hardware care este de obicei necunoscută furnizorului și pentru care nu este disponibil niciun patch sau altă remediere
- Vânzătorul are astfel zero zile pentru a pregăti un patch, deoarece vulnerabilitatea a fost deja descrisă sau exploatată



CVSS

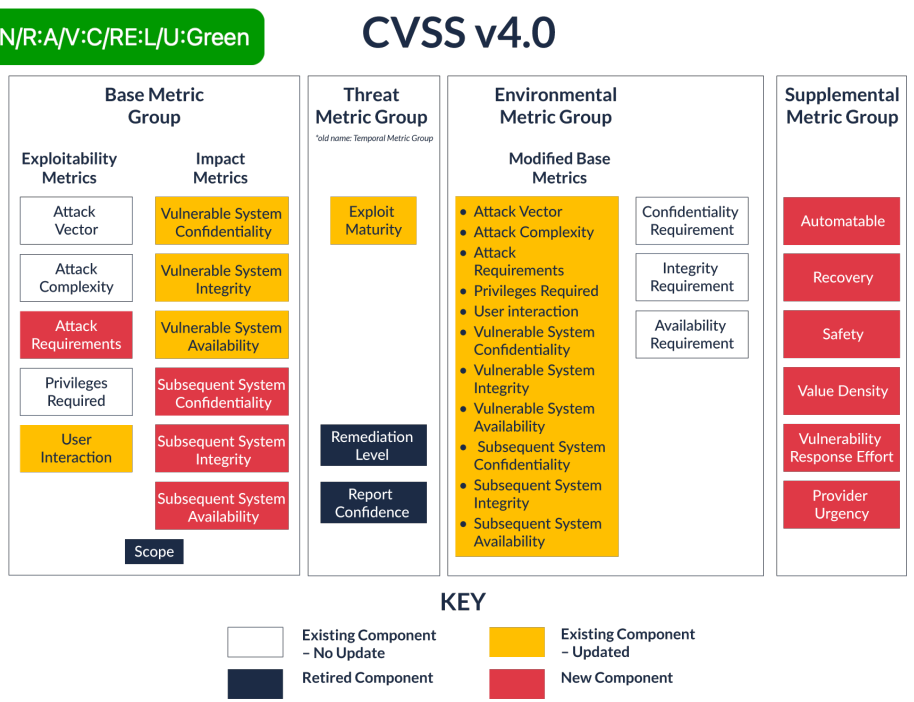
- Common Vulnerability Scoring System
- Metodă pentru generarea unei măsuri calitative a severității

CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:H/VI:L/VA:H/SC:H/SI:L/SA:H/E:A/MAV:N/MAT:P/MPR:N/MVC:H/S:N/R:A/V:C/RE:L/U:Green

CVSS v4.0 Score: **9.2 / Critical**

CVSS v3.1 Severity and Metrics:
Base Score: 9.0 CRITICAL
Vector: AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
Impact Score: 6.0
Exploitability Score: 2.2

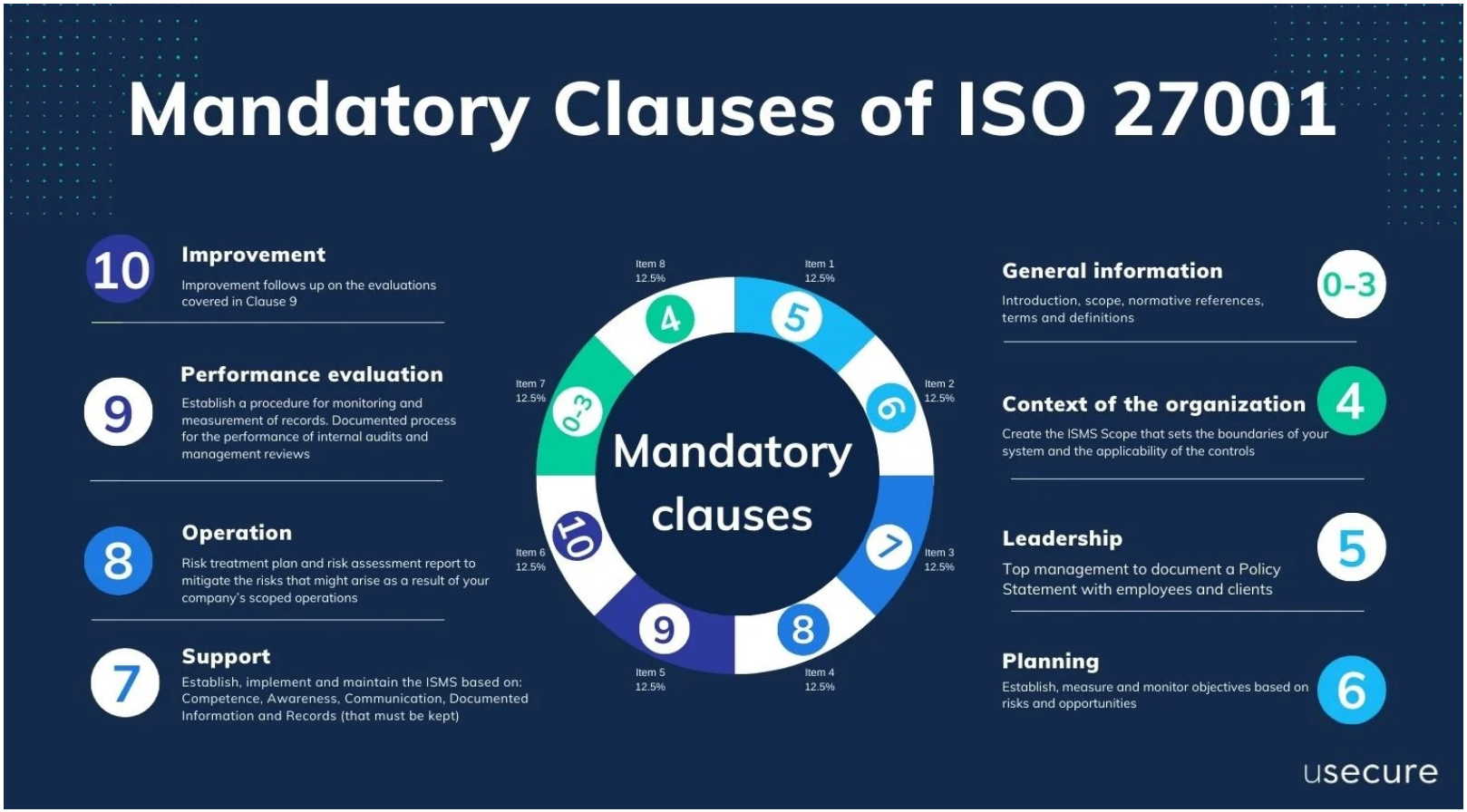
Attack Vector (AV): Network
Attack Complexity (AC): High
Privileges Required (PR): None
User Interaction (UI): None
Scope (S): Changed
Confidentiality (C): High
Integrity (I): High
Availability (A): High



Standarde – ISO27001

- Stabilește cerințe pentru Sisteme de Management al Securității Informațiilor (ISMS – Information Security Management Systems)
- Asigurarea confidențialității, integrității și disponibilității prin managementul riscurilor și oferirea de încredere către părțile interesate că informațiile cu gestionate adecvat
- Cerințe generice, aplicabile oricărei organizații
- Rolurile managementului, politici, planificare, conștientizare, evaluare și revizii periodice
- Anexa A precizează controale de securitate a informațiilor, grupate pe 14 domenii: **politici, organizație, resurse umane, active, control acces, criptografie, securitare fizică, securitatea operațiunilor, comunicații, sisteme, furnizori, managementul incidentelor, compliance**

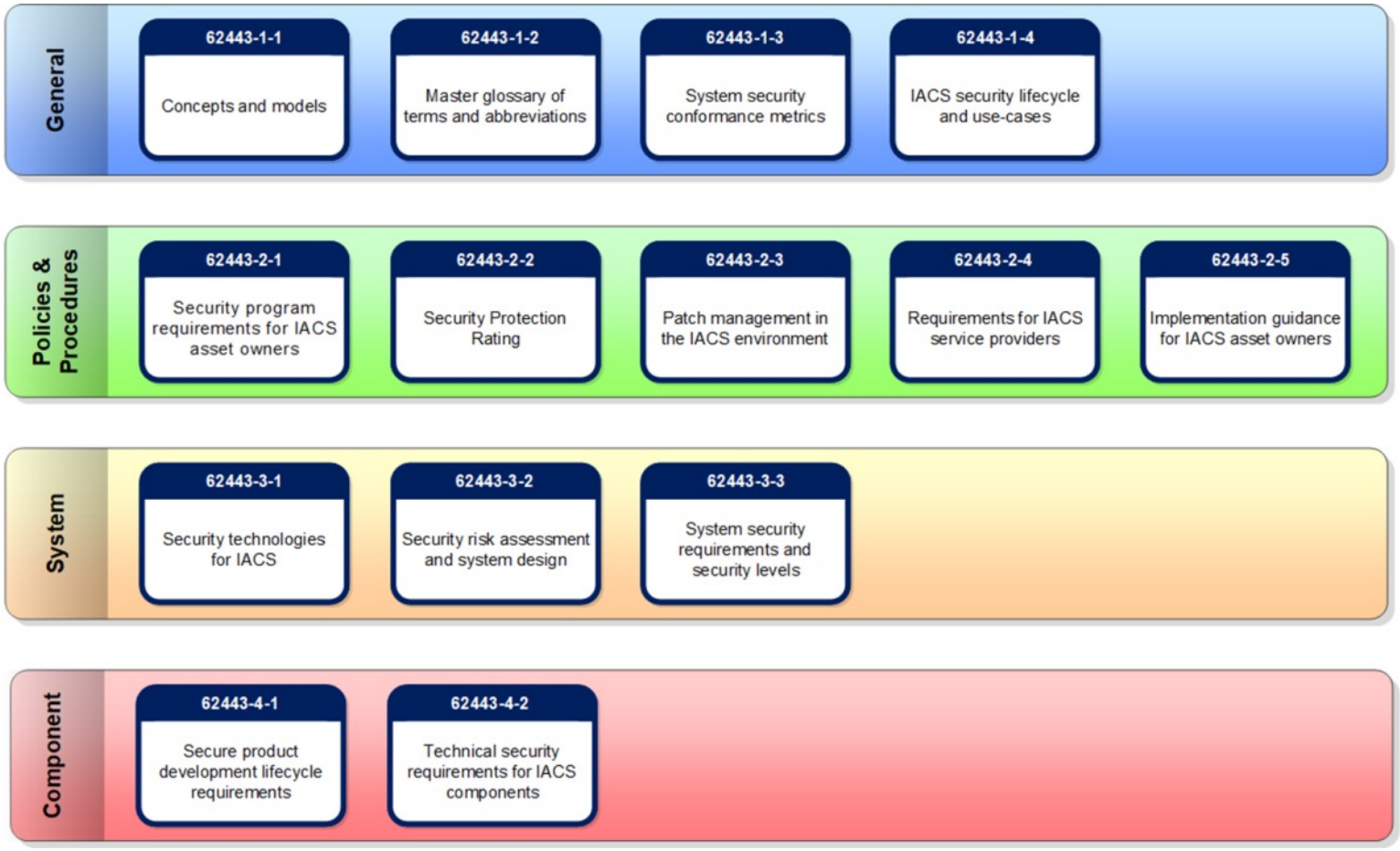
Standarde – ISO27001



Standarde – ISA/IEC62443

- Seria de standarde ISA/IEC 62443 definește cerințele și procesele pentru implementarea și menținerea sistemelor de automatizare și control industrial (IACS) securizate electronic
- Aceste standarde stabilesc cele mai bune practici pentru securitate și oferă o modalitate de a evalua nivelul de performanță de securitate
- Abordarea lor față de provocarea securității cibernetice este una holistică, reducând decalajul dintre operațiuni și tehnologia informației, precum și între siguranța proceselor și securitatea cibernetică

Standarde – ISA/IEC 62443



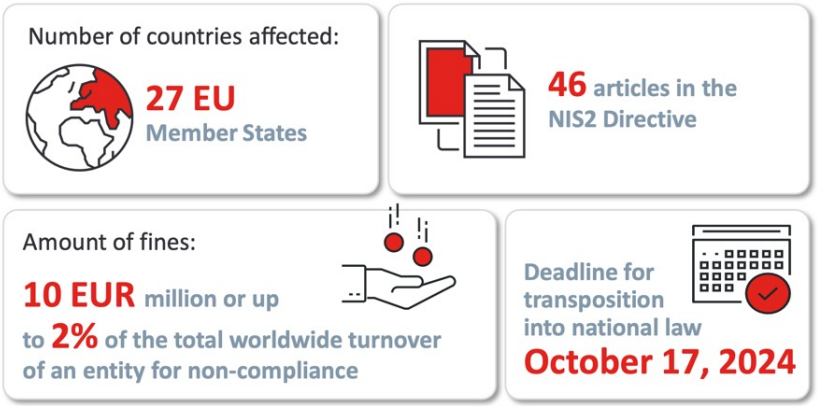
Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Reglementări Europene

- "Regulation (eu) 2019/881 of the european parliament and of the council of 17 april 2019 on and on information and communications technology cybersecurity certification (**cybersecurity act**)," Official Journal of the European Union, 2019. Available on-line: https://eur-lex.europa.eu/eli/reg/2019/881/oj
- "Directive (eu) 2022/2555 of the european parliament and of the council of 14 december 2022 on measures for a high common level of cybersecurity across the union (**nis 2 directive**)," Official Journal of the European Union, 2022. Available on-line: https://eur-lex.europa.eu/eli/dir/2022/2555
- Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the **resilience of critical entities** and repealing Council Directive 2008/114/EC (OJ L 333, 27.12.2022, pp. 164–198). Available on-line: https://eur-lex.europa.eu/eli/dir/2022/2557/oj
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. Available on-line: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454 – **Cyber Resilience Act**
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents. Available on-line: https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-cyber-solidarity-act - **Cyber Solidarity Act**

Reglementări – NIS2

- Impune și strategii naționale de Securitate cibernetică în UE
- Stabilește cerințe și capacități tehnice pentru CSIRT naționale, cooperare și schimbul de informații
- Stabilește obligații de management al riscurilor și de raportare pentru entități esențiale și importante
- Face referire la scheme de certificare Europene și standarde



Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Transpunerea NIS2 în România

- OUG 155/2024 definește sectoarele de activitate și entitățile (publice și private) pentru care normele de securitate cibernetică sunt obligatorii, inclusiv în:
  - **sectoare critice** (energie, transporturi, infrastructură digitală, sănătate, apă și apă uzată, administrație publică centrală, spațiu etc.)
  - **sectoare de importanță majoră** (servicii poștale și de curierat, gestionarea deșeurilor, producția și distribuția de substanțe chimice, producția alimentară, industria de fabricare, cercetare, furnizori digitali ș.a.)
- Sfera de aplicare este împărțită între:
  - **entitățile esențiale**: cele din administrația publică centrală, furnizorii de servicii DNS, prestatorii de servicii de încredere calificate și orice entitate clasificată drept „esențială” prin încadrările din anexe (energie, transporturi, sector bancar, infrastructuri de piață financiară, sănătate, alimentare cu apă, infrastructură digitală ș.a.)
  - **entitățile importante**: organizate după criteriul de mărime (întreprinderi mari și mijlocii) și care furnizează servicii considerate critice, dar care nu se încadrează la entități esențiale; exemple - operatori de gestiune a deșeurilor, servicii poștale și de curierat, producție alimentară, anumite fabrici etc.

Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

Transpunerea NIS2 în România

- Impune realizarea unei **analize de risc și implementarea măsurilor tehnice**, organizaționale și operaționale corespunzătoare pentru protecția rețelelor și sistemelor informatice
- Organizarea unui **sistem intern de management al securității cibernetice** revine entităților esențiale și entităților importante, astfel cum acestea sunt definite și încadrate în actul normativ (în funcție de domeniul de activitate, criteriile de mărime și importanță sau de impactul serviciilor furnizate), care include
  - numirea unei persoane responsabile de securitatea rețelelor și sistemelor informatice;
  - aprobarea și monitorizarea de către organele de conducere a politicilor de securitate;
  - instruirea periodică a personalului, inclusiv membri din conducere.
- Sunt prevăzute **obligații de audit și raportare a incidentelor**, mai exact, un audit de securitate cibernetică periodic (sau ad-hoc, la cererea DNSC) pentru entitățile identificate ca fiind esențiale sau importante, precum și obligația de a raporta imediat incidentele semnificative (în maximum 24-72 de ore, în funcție de natura evenimentului) prin Platforma națională pentru raportarea incidentelor de securitate cibernetică (PNRISC)

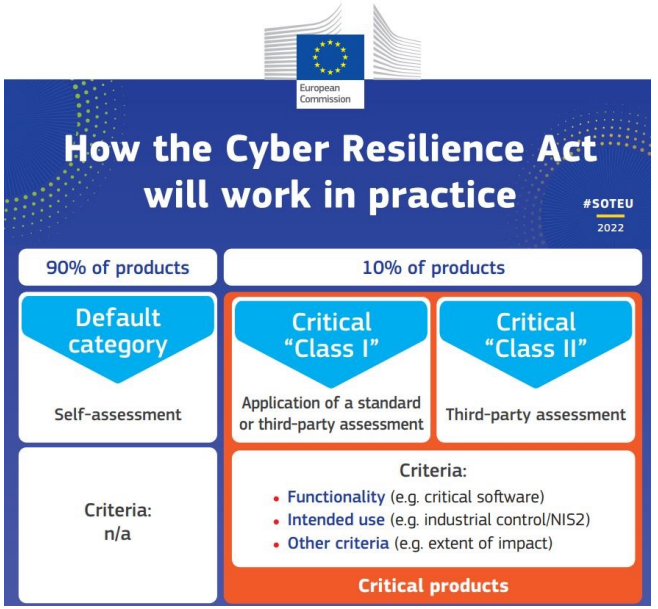
Proiectul "Instruirea și certificarea utilizatorilor în domeniul ingineriei fabricației pentru Industria 4.0 a fost finanțat printr-un grant al Băncii Mondiale (GEAR 4.0), contract nr. MD-TECHUNI-354549-CS-CQS

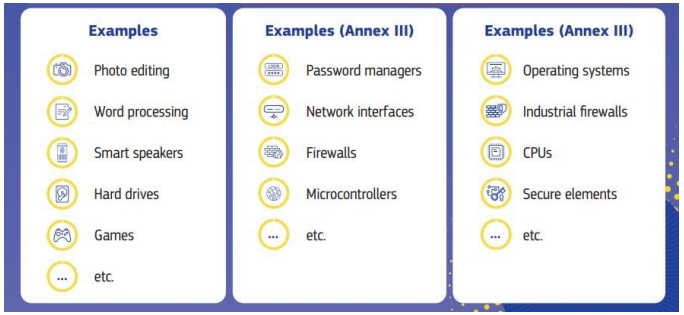
Entități esențiale NIS2 - Exemplu

1. Energie	a) Electricitate	— Întreprinderile din domeniul energiei electrice, astfel cum sunt definite ca „operatori economici” la art. 3 pct. 73 din Legea energiei electrice și a gazelor naturale nr. 123/2012 care îndeplinesc funcția de „furnizare de energie electrică”, astfel cum este definită la art. 3 pct. 46 din Legea energiei electrice și a gazelor naturale nr. 123/2012, cu modificările și completările ulterioare
		— Operatorii de distribuție, astfel cum sunt definiți la art. 3 pct. 70 din Legea nr. 123/2012
		— Operatorii de transport și de sistem, astfel cum sunt definiți la art. 3 pct. 71 din Legea nr. 123/2012
		— Producătorii, astfel cum sunt definiți ca „producători de energie electrică” la art. 3 pct. 92 din Legea nr. 123/2012
		— Operatorii desemnați ai pieței de energie electrică, astfel cum sunt definiți la art. 3 pct. 68 din Legea nr. 123/2012 — Participanții la piață, astfel cum sunt definiți la art. 3 pct. 79 din Legea nr. 123/2012, care furnizează serviciile de agregare, consum dispecerizabil sau stocare de energie, astfel cum sunt definite la art. 3 pct. 6, 29, și respectiv, 121 — Operatorii unui punct de reîncărcare, astfel cum este definit la art. 3 pct. 96 din Legea nr. 123/2012, care sunt responsabili cu gestionarea și exploatarea unui punct de reîncărcare care furnizează un serviciu de reîncărcare clienților finali, astfel cum sunt definiți la art. 3 pct. 20, inclusiv în numele și în contul unui furnizor de servicii de mobilitate, astfel cum aceștia sunt definiți la art. 2 pct. 36 din Regulamentul (UE) 2023/1.804 al Parlamentului European și al Consiliului din 13 septembrie 2023 privind instalarea infrastructurii pentru combustibili alternativi și de abrogare a Directivei 2014/94/UE — Operatori economici, concesionarii și dezvoltatorul centralei electrice eoliene offshore prevăzuți de Legea nr. 121/2024 privind energia eoliană offshore

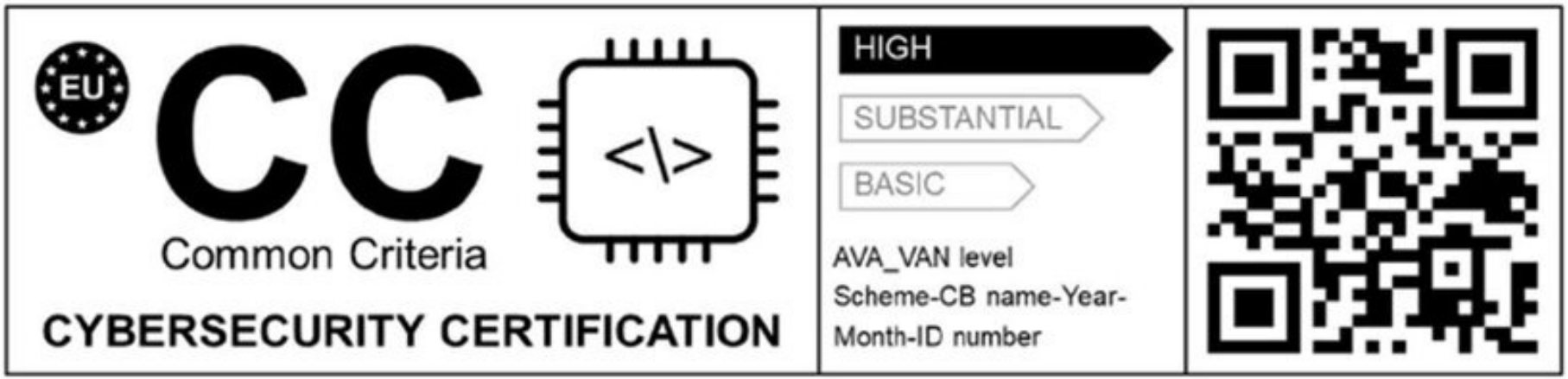
EU Cyber Resilience Act

- Obiective specifice:
  - să se asigure că producătorii îmbunătățesc securitatea produselor cu elemente digitale încă din faza de proiectare și dezvoltare și de-a lungul întregului ciclu de viață
  - să asigure un cadru coerent de securitate cibernetică, facilitând conformitatea pentru producătorii de hardware și software
  - îmbunătățirea transparenței proprietăților de securitate ale produselor cu elemente digitale
  - permite întreprinderilor și consumatorilor să utilizeze în siguranță produsele cu elemente digitale





EUCC


EU
CC
Common Criteria
CYBERSECURITY CERTIFICATION
HIGH
SUBSTANTIAL
BASIC
AVA_VAN level
Scheme-CB name-Year-
Month-ID number

STUDIU DE CAZ

Proiectul ELECTRON

https://electron-project.eu

DEMO

Monitorizare trafic rețele industriale cu Wireshark

Configurare rețea industrială SIEMENS S7-1500 cu XC208/S615

Network Security Training Panel

- AA054.400.01
- Include:
  - Siemens SCALANCE XC208
  - Siemens SCALANCE S615
- Router LAN **SCALANCE S615**; pentru protecția dispozitivelor/rețelelor în tehnologia de automatizare și pentru protecția comunicațiilor industriale prin VPN și firewall; Alte funcții: conversie adrese (NAT/NAPT), conexiune la SINEMA RC, comutator cu 5 porturi, 1x dig. intrare, 1x ieșire digitală.

Portalul de Training Siemens SCE

Laboratorul AISENSE - ASTI

- *Artificial Intelligence for Sensing, Low-power Networking and ICS Cybersecurity*
- Infrastructură de cercetare pentru securitate cibernetică OT
- Colaborare dintre Asti Automation și Institutul de Cercetări PRECIS al UPB

Vă mulțumim!