CERCETĂRI PRIVIND SECURITATEA CIBERNETICĂ PENTRU SISTEMELE DE CONTROL INDUSTRIAL ȘI IOT

CYBER SECURITY RESEARCH FOR INDUSTRIAL CONTROL SYSTEMS AND IOT

DIONISIE Ștefania
Facultatea de Inginerie Industrială și Robotică, Specializarea: Logistică Industrială, Anul de studii: Master I, e-mail: stefi_dio@yahoo.com

Conducător ştiinţific: Ș.l. Dr. Ing. Adrian Popescu

SUMMARY: Computer network security is currently an integral part of the field of computer networks and it involves protocols, technologies, systems, tools and techniques to secure and stop cyber attacks. Cyber attacks and cyber security are one of the big issues for the digital age. They are no longer locked only in a cyberspace but interact with our real world through sensors and actuators. Such systems are known as CPS (Cyber Physical Systems), IoT / E (Internet of Things / Everything), Industry 4.0, industrial internet, M2M (Machine to machine), etc. Whatever they are called, the operation of any of these systems can have a serious impact on our real lives and appropriate risk mitigation measures must be taken. In this paper, cybersecurity in ICS (Industrial control system) is reviewed as an example of cyber physical security for critical infrastructures. Then, as a future aspect of it, the security of IoT (Internet of Things) is explained.

KEY WORDS: Cyber security, IoT, control systems, industry, SCADA.

1. Introducere

Societatea viitoare va depinde foarte mult de computere și rețele sub orice aspect. Acest lucru a fost deja sau devine adevărat în majoritatea infrastructurilor sociale bazate pe ICS (Sisteme industriale de control), care includ producția critică, industria chimică (tratarea materialelor periculoase), sistemele inteligente pentru rețeaua electrică, rețelele energetice, servicii medicale, auto, etc. În sens larg, ele sunt cunoscute și sub denumirea de CPS (Cyber Physical Systems), IoT / E (Internet of Things / Everything), Industry 4.0, Internet industrial, M2M și așa mai departe și au o caracteristică comună, care constau în senzori și actuatori și au interfețe și interacțiuni cu lumea noastră fizică. Consecințele ciberatacurilor asupra unor astfel de sisteme nu se vor limita într-un spațiu cibernetic, ci se vor răsfrânge și în viața noastră reală.

Ținând cont de această situație, această lucrare examinează cibersecuritatea în ICS ca un exemplu de frunte al unei asemenea securități fizice cibernetice. [1]

2. Configurație ICS

Chiar dacă în practică, configurațiile ICS sunt bogate în varietate, un exemplu este prezentat în Fig. 1 pentru a surprinde o imagine ICS.

În această figură, actuatorii și senzorii sunt conectați la rețelele de câmp / senzori (sau canale de transmitere a datelor), care sunt de obicei proprietăți și specifice industriei. Senzorii și actuatorii sunt controlați și gestionați de controlere, cum ar fi PLC (Programable Logic Controller) și DCS (Distributed Control System). Aceste controlere sunt, de asemenea, conectate la o rețea de sisteme de control, care este utilizată pentru a gestiona senzorii, actuatorii și controlerele lor, de ex. pentru a schimba punctul de referință prin HMI (Human Machine Interface), pentru a-și actualiza logica sau programele prin EWS (Engineering Work Station), pentru a colecta jurnalele și pentru a le supraveghea de SCADA (Control de

Supraveghere și Achiziție de Date). Rețelele sistemului de control constau de obicei din Ethernet industrial, care este compatibil cu protocoalele Ethernet standard, dar hardware-ul lor este proiectat pentru procesarea în timp real și medii dure. Pentru a gestiona producția sau operațiile din producție, unele informații sunt de obicei schimbate între rețelele corporative și rețelele de sisteme de control, iar unele dintre întrețineri ar putea fi efectuate de la distanță, care se numesc întreținere la distanță. [1]

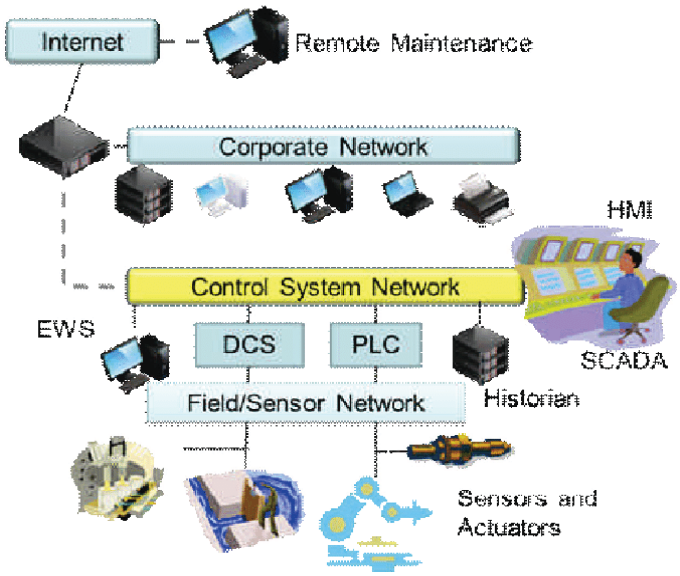


Fig. 1. Un exemplu de configurație ICS [1]

Caracteristici ale ICS în materie de Securitate:

Una dintre cele mai semnificative caracteristici ale ICS este că acestea au interfețe cu lumea reală și, datorită acestui fapt, acestea ar putea cauza o problemă serioasă vieții noastre reale, după exploatarea de către hackers. Alte caracteristici includ:

1) Disponibilitatea este de obicei o prioritate mai mare decât confidențialitatea și integritatea;
2) Ciclul de viață este mai lung decât la TIC (Informații și Tehnologii de comunicare);
3) Izolat de Internet;
4) Sunt utilizate protocoale proprii și / sau scopuri specifice și sisteme de operare.

Datorită punctelor 1) și 2), măsurile convenționale TIC nu sunt neapărat aplicabile așa cum sunt. De exemplu, patch-ul rapid și frecvent la bug-uri nu este potrivit pentru unele ICS-uri sensibile, deoarece patching-ul poate deteriora compatibilitatea cu driverele de dispozitiv minore sau performanțele pe care sistemul trebuie să le satisfacă, deși patching-ul este o necesitate și o contramăsură fundamentală în TIC.

Datorită 3) și 4), ICS nu a fost o țintă majoră a atacurilor cibernetice. Situația s-a schimbat însă. Protocoalele și sistemele de operare proprii și / sau cu scopuri specifice sunt înlocuite treptat cu cele cu scop general. Mediile izolate se conectează treptat la alte rețele. Așa cum se arată în Fig. 2, principalul sistem de operare în ICS a fost Windows urmat de Unix, Linux și RTOS (sistem de operare în timp real), apoi mai mult de o treime dintre ele au fost conectate la o rețea din 2008. Această tendință va fi urmată de la producția inteligentă, Industria 4.0, internetul industrial, etc. unde sunt introduse mai multe tehnologii TIC. [1]

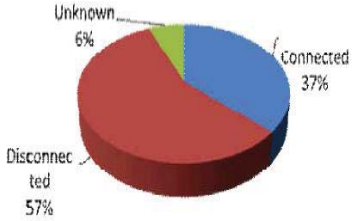


Fig. 2. Conectivitatea ICS-ului [1]

Numărul de incidente și vulnerabilități raportate la ICS-CERT este în creștere, așa cum se arată în Fig. 3, după incidentul de la Stuxnet, care a vizat software-ul specific industriei și rețeaua închisă și apoi centrifugele pentru nucleare, în Iran în anul 2010.

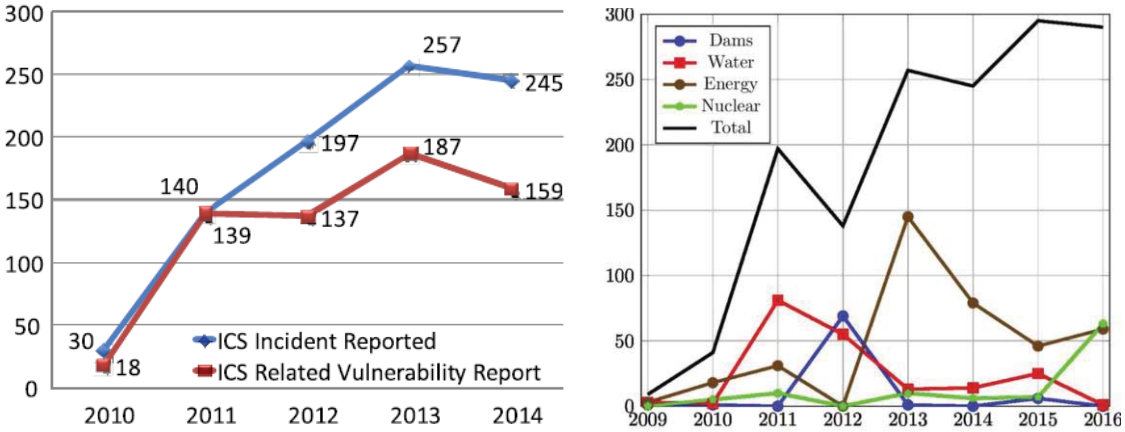


Fig. 3. Numărul de incidente ICS și vulnerabilitățile raportate [1]

3. Conceptul IoT

Conceptul Industriei 4.0 este denumit a patra revoluție industrială și este tendința actuală în automatizare, monitorizare și procesarea de date din procesele de fabricație. Principalele tehnologii pentru realizarea acestor sarcini sunt:

- IoT;
- CPS (sisteme cyber-fizice);
- CP (platforme cloud);
- CC (calcul cognitiv);
- dispozitive AR / VR (realitate augmentată / realitate virtuală);
- alte discipline conexe. [2]

În general, sistemele de fabricație, procesele de producție sunt în prezent adecvate pentru digitalizarea completă. Prima sarcină în digitalizarea proceselor este specificarea tehnologiilor adecvate. Pot fi definite două grupuri de dispozitive, primul pentru instalarea permanentă a produsului, care trebuie să fie cu costuri reduse și cel de-al doilea grup pentru monitorizarea mașinilor și a procesului de producție.

Tehnologiile pentru digitalizarea și colectarea datelor de la mașini, procese și produse sunt:

- Tag-uri RFID (identificare cu frecvență radio) pentru identificarea wireless a pieselor și emițător-receptor RFID pentru monitorizarea aparatelor în procesul de producție;
- Senzori MEMS integrați în produs pentru măsurarea datelor fără contact și, de asemenea, integrați în procesul de producție;
- Dispozitive IoT cu comunicație wireless independentă pentru încărcarea datelor pe platformele cloud pentru procesarea următoare;
- Platforme cloud cu extragere de date pentru extragerea cunoștințelor și reprezentare a datelor în planificări și alarme. [2]

O abordare modernă de identificare a produsului utilizează tehnologia RFID UHF (frecvență ultra înaltă), deoarece atinge distanțe mai mari precum tehnologia LF și HF (frecvență joasă și înaltă).

Senzorii MEMS au un consum minim de energie și pot fi alimentați de la baterie în timpul vieții unui produs. Acestea pot fi utilizate, de exemplu, pentru monitorizarea supraîncălzirii produsului și a vibrațiilor în timpul funcționării de către clienți și sunt utilizate în general pentru monitorizarea continuă a mediului produsului.

Sistemele moderne IoT se bazează pe tehnologii de comunicare specializate pentru izolarea datelor din rețelele Wi-Fi standard (Wireless-Fidelity) sau Bluetooth. Principalul standard de comunicare

IoT este LPWAN (rețea de mare putere) și include soluții precum LoRa / LoRaWAN și Sigfox. Alte tehnologii utilizează modificări ale rețelelor GSM (Sistemul Global pentru Comunicare Mobilă) pentru transfer redus de date.

Extragerea datelor și analiza acestora sunt sarcinile principale ale unui sistem cloud. Platformele Cloud pot furniza date într-o formă ușoară pentru utilizator, după termene, zi / săptămâni sau rapoarte automate lunare. De asemenea, poate fi integrat un sistem de alarmă pentru starea critică a producției, de obicei ca mesaj prin e-mail sau SMS.

Aplicarea unui model virtual pentru monitorizarea de la distanță este o nouă tendință a conceptului industriei 4.0 și poate reprezenta sistemul de fabricație real, procesul de producție sau produsul. Astfel de modele virtuale reproduc digital toate aspectele dispozitivelor reale și sunt numite gemeni digitali, care învață și se actualizează continuu din mai multe surse de date. [2]

4. Conceptul de sistem experimental de asamblare a fabricației inteligente

Conceptul sistemului de asamblare a fabricației inteligente experimentale este prezentat în figura 4 și realizarea fizică parțială în scopuri de cercetare și educație este prezentată în figura 5. Acest concept include toate tehnologiile necesare pentru achiziția de date digitale: tehnologia RFID, sisteme de viziune și dispozitive IoT. Toate datele din aceste tehnologii trebuie transformate în format industrial standardizat. PLC-ul este principalul colector de date pentru procesarea și transferul de date în sistemul cloud. Standardizarea datelor este atinsă de serverul de comunicații cu platformă deschisă (OPC), care asigură, de asemenea, distribuția datelor către gemenul digital bazat pe Siemens Tecnomatix-mulator și pe platforma cloud MindSphere.

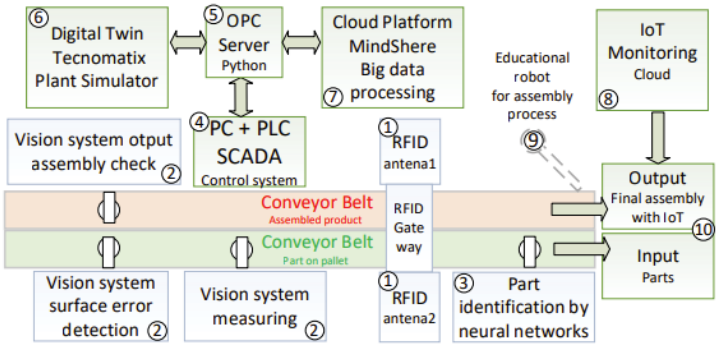
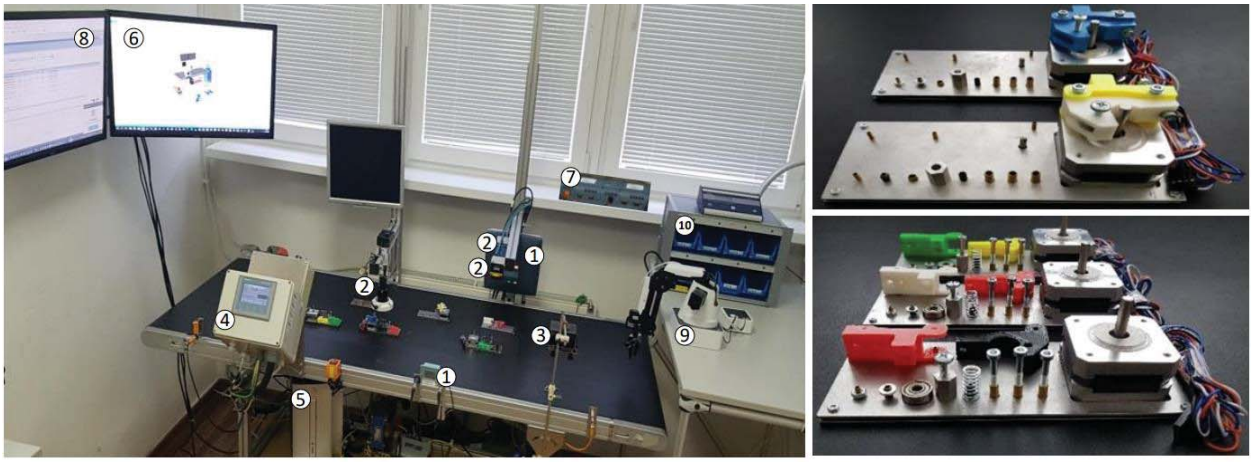


Fig. 4. Conceptul de sistem experimental de fabricație inteligentă de asamblare cu transfer de date către cloud [2]



(a) (b)

Fig. 5. (a) Sistemul experimental de asamblare; (b) dispozivitivul cu piese și ansamblul finalizat [2]

5. Dispozitive IoT pentru monitorizarea produsului pe termen lung de către senzorii MEMS

Au fost selectate trei tehnologii de comunicare IoT (tehnologie GSM, Sigfox și LoRaWAN) care pot asigura un transfer de date izolat pentru monitorizarea produsului pe termen lung. Sistemul experimental combină aceste tehnologii IoT la un singur modul cu colectarea datelor la un sistem open source, așa cum se arată în figura 6.

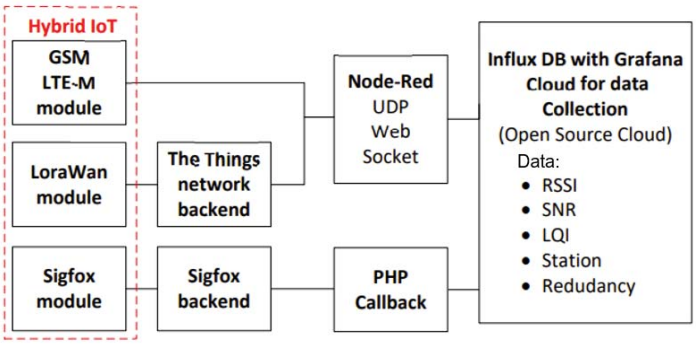


Fig. 6. Schema principală a dispozitivului IoT combinat experimental [2]

Programul a fost programat în Visual Studio și transferat la un modul FiPy. Comunicarea IoT multiplă a fost operată de modulul FiPy, care a fost conectat la un senzor MEMS pentru a colecta informații despre vibrații. Aceste dispozitive au fost utilizate pentru măsurători experimentale ale calității semnalului, iar pentru implementarea reală, acestea trebuie reduse ca dimensiune pentru integrare în produsul de asamblare final. Un exemplu de date digitale colectate de pe dispozitivul IoT hibrid de interfața de utilizator a rețelei LoRaWAN „Rețeaua lucrurilor" (TTN) este prezentat în figura 7.

Fig. 7. Date digitale de la: (a) rețea LoRaWAN TTN; (b) rețeaua Sigfox [2]

6. Arhitectura și securitatea sistemelor SCADA

Modernizarea sistemului SCADA, standardizarea protocoalelor de comunicare și creșterea interconectivității au crescut drastic atacurile cibernetice asupra sistemului SCADA de-a lungul anilor. Acest tip de atacuri devin mai sofisticate pentru a comite spionajul cibernetic și sabotajul într-un mod discret.

Arhitectura SCADA este clasificată în patru generații, adică a patra generație monolitică, distribuită, în rețea și bazată pe IoT. O analiză a atacurilor asupra sistemului SCADA este necesară pentru dezvoltarea tehnologiei de gestionare a atacurilor noi. Am analizat atacurile bazate pe țara (industria) atacului, componenta țintă, impactul atacului și tipul atacului. Am clasificat atacurile în cinci categorii, adică malware, atac non-cyber, acces la distanță neautorizat și întreruperea serviciilor. Sistemele de detectare a intruziunilor (IDS) sunt utilizate pentru detectarea și prevenirea acestor atacuri și recunoașterea vulnerabilităților din sisteme. [3]

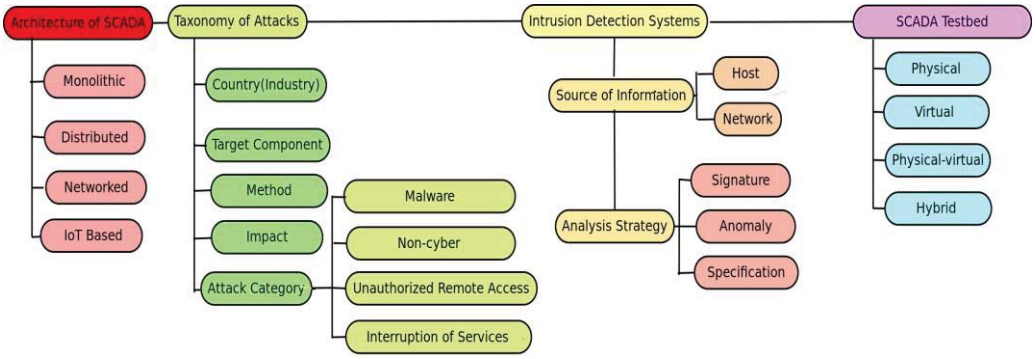


Fig. 8. Clasificarea arhitecturii SCADA [3]

Legătura de comunicare a componentelor sistemului MTU, RTU, HMI, Istoric și SCADA este reprezentată în Fig. 9. RTU este responsabil pentru colectarea de date și informații în timp real de la senzori care sunt conectați la mediul fizic folosind link-ul LAN / WAN. RTU transmite informații către MTU. Acestea sunt în plus responsabile de transmiterea datelor de stare actuale ale dispozitivelor fizice asociate cu sistemul.

MTU este stația centrală de monitorizare. Acesta este responsabil de controlul și comanda mașinii RTU prin legăturile de comunicare. De asemenea, răspunde la mesajele de la RTU, le procesează și le stochează pentru o comunicare reușită. HMI oferă o interfață de comunicare între componentele hardware și software SCADA. Este responsabil pentru controlul informațiilor operaționale SCADA, de exemplu, controlul, observarea și comunicarea între mai multe RTU și MTU sub formă de text, statistici sau alt conținut inteligibil.

Historian este utilizat pentru acumularea de date de comunicare, evenimente și alarme bidirecționale între centrul de control SCADA. Poate fi descris ca o bază de date centralizată sau un server situat într-o locație îndepărtată. [3]

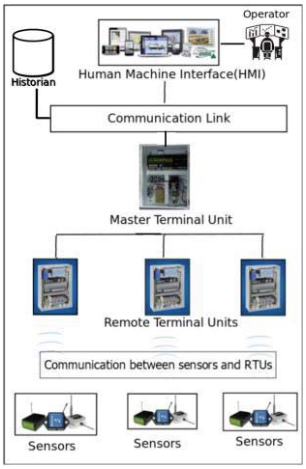


Fig. 9. Corelația componentelor sistemului SCADA [3]

Rețeaua oferă servicii de comunicare între diverse componente din cadrul rețelei SCADA. Mediul utilizat poate fi wireless sau cablu. În prezent, suportul wireless este utilizat în general, deoarece interfațează zonele circulate geologic și zonele mai puțin disponibile pentru a comunica fără efort. Progresul paradigmei comunicării este izolat în patru vârste primare, de exemplu, Prima epocă: Monolitic, A doua epocă: Distribuit, A treia era: Rețea, A patra era: Internetul lucrurilor tehnologie.

Deoarece alegerea celor mai bune protocoale se asigură că, dacă este nevoie, sistemul dezvoltat va avea un potențial bun de scalabilitate, sistemele ar trebui să aibă flexibilitatea de a încorpora securitatea în protocoalele de comunicare.

În afară de protocoale cunoscute de comunicare Modbus, DNP3 (Distributed Network Protocol), Fieldbus, Profibus, în a 4-a generație SCADA bazată pe IoT avem alte protocoale ca de ex. Zigbee, Bluetooth Low Energy (BLE), Long Range (LoRA) etc. [3]

7. Augmentarea unui firewall bazat pe SCADA

Un firewall industrial este un sistem utilizat pentru supravegherea și reglarea traficului către și dintr-o rețea în scopul securizării aparatelor pe o rețea. Analizează datele care îi trec la criterii sau protocoale deja definite, eliminând date care nu corespund cerințelor protocolului. De fapt, este un filtru care previne traficul nedorit de rețea și limitează selectiv tipul de transmisie care se produce între o linie de transmisie securizată. Un Firewall bazat pe SCADA este implementat pentru protecția transmiterii datelor către un PLC, împotriva dispozitivelor de hacking externe. Acest firewall este practic expus mai multor hackeri externi și gradul de vulnerabilitate este studiat cu atenție, pentru a dezvolta un Firewall ideal. [4]

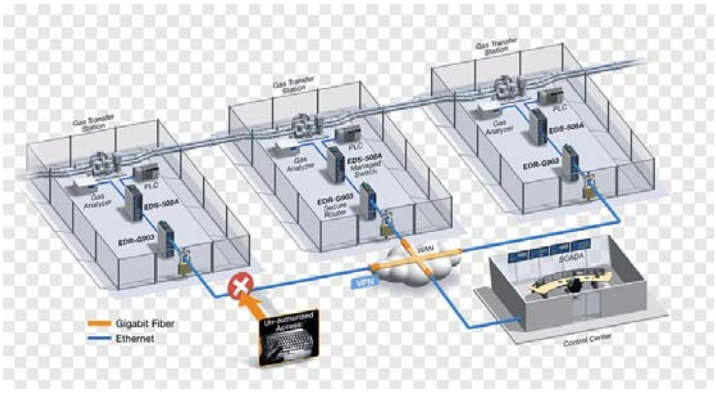


Fig. 10. Firewall bazat pe SCADA [5]

O gamă largă de firewall persistă pe piața de astăzi, cu atribute unice asociate cu fiecare dintre ele. Cele două mari categorii de distincții sunt firewall-urile gazdă și firewall-urile în rețea. Firewall-urile gazdă sunt instalate pe calculatoare personale sau în mai multe sisteme de operare, care sunt bazate în principal pe software. [4]

Tipul de firewall ulterior se numește firewall în rețea și după cum sugerează și numele, este tipul de firewall care face parte dintr-un sistem în rețea, spre deosebire de firewall-ul bazat pe gazdă. Figura 11 este o reprezentare a unui astfel de tip de firewall-uri în rețea industrială. Aceste tipuri de rețele pot fi întâlnite, de obicei, în industrii de scară largă, care stochează date pe un server centralizat, care pot fi accesate cu ușurință de mai mulți profesioniști autorizați pe baza codurilor de acces. Aceste firewall-uri distincte sunt utilizate în diferite site-uri dintr-un sistem în rețea pentru a oferi diferite tipuri de securitate ca parte a unei strategii. Acestea ajută la protejarea legăturii dintre rețeaua companiei și rețeaua industrială, asigurându-le împotriva hackerilor. De asemenea, mai multe tipuri de firewall sunt concepute cu un set de reguli specifice, pentru a limita un tip specific de comunicare. [4]

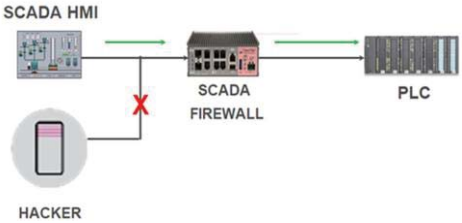


Fig. 11. Schema de lucru generală a firewall-ului industrial [4]

Diferența la un firewall industrial

Prima și cea mai importantă diferență este în ceea ce privește prioritatea securității. În cazul Sistemului de control industrial (ICS), accentul este orientat către disponibilitatea, vizibilitatea în diferite

procese și operațiunile implicate, integritatea și, în sfârșit, aspectul confidențialității. Utilizarea acestor dispozitive pentru protejarea rețelelor SCADA ajută la apărarea straturilor în cazul în care perimetrul rețelei externe este încălcat. De asemenea, vă ajută să vă protejați împotriva insiderilor nocivi și a programelor malware care au infectat sistemul.

În ceea ce privește latența, ICS se bazează întotdeauna pe cerințele în timp real, el fiind functional 24h/7. Pentru ICS, protocoalele tind să eșueze numai atunci când sunt contestate.

O diferență cheie este durata de viață tehnică și economică. Perioadele utilizate în mod tipic pentru ICS de „ștergere" sunt foarte lungi.

Siguranța instalațiilor este o parte crucială a exploatării instalației și ICS. Prin urmare, ICS include adesea sisteme integrate de siguranță (SIS), dar distincte. SIS este responsabil pentru asigurarea și menținerea operațiunilor sigure ale procesului prin plasarea procesului într-o stare sigură atunci când sunt detectate condiții de proces care amenință siguranța. [4]

8. Concluzii

Industria 4.0 este continuarea inevitabilă a unei curbe de dezvoltare naturală. Importanța securității cibernetice este că aceasta va fi supusă unor consecințe devastatoare dacă nu se iau măsuri împotriva hackerilor. Prin urmare, organizațiile mari încearcă să reducă la minimum sau chiar să elimine amenințările și strategiile și tehnicile de securitate pe care le-au dezvoltat. Conceptele precum evoluția digitală a industriei sau a 4-a revoluție industrială ne îndeamnă să ne gândim la viitor și să ne concentrăm pe „mâine". Drept urmare, va fi o cerință excelentă să asigure siguranța sistemelor critice de a doua generație și a liniilor de producție împotriva amenințărilor cibernetice, care vor crește semnificativ odată cu protocoalele de conectare și interacțiune care vin cu IoT. Industria 4.0 și securitatea cibernetică sunt foarte importante pentru producători.

Sistemele SCADA au evoluat spre sisteme complexe bazate pe sisteme avansate de tehnologie conectate la Internet, acest mediu conducând sistemul SCADA la o vulnerabilitate crescută.

ICS-ul este un exemplu al securității fizice cibernetice, în special pentru infrastructuri, unde identificarea seturilor optime de contramăsuri este semnificativă, luând în considerare restricțiile și constrângerile acestora. Necesitatea securității fizice cibernetice în viitor se va extinde nu numai la diverse infrastructuri, ci și la zona de consum cu IoT, unde păstrarea vieții private și protecția fizică a dispozitivelor vor juca roluri mai importante mai ales atunci când adversarii pot avea acces fizic la ele.

9. Bibligrafie

[1]. Kazukuni KOBARA 2016 , "Cyber Physical Security for Industrial Control Systems and IoT",
[2]. Milan Adámek 2020,"Digital Twin of Experimental Smart Manufacturing Assembly System for Industry 4.0 Concept",
[3]. Geeta Yadav, Kolin Paul, 2020, "Architecture and security of scada systems";
[4]. Abhishek Mungekar, 2019, "Augmentation of a SCADA based firewall against foreign hacking devices"
[5]. https://w0.pngwave.com/png/261/842/virtual-private-network-scada-industrial-control-system-computer-security-firewall-high-grade-building-png-clip-art.png