PLC kodetze praktika seguruak: Top 20 zerrenda

1.0 bertsioa (2021eko ekainaren 15a)

PLC Security TOP 20 LIST

1. PLC kodea modularizatu

PLC kodea moduluetan zatitu, funtzio-bloke desberdinak erabiliz (azpi-errutinak). Probatu moduluak modu independentean.

2. Jarraitu funtzionamendu moduak

Mantendu PLCa RUN moduan. PLCak RUN moduan ez badaude, alarma bat egon beharko luke operadoreentzat.

3. Utzi logika operatiboa PLCan bideragarria den guztietan

Utzi logika operatibo gehiena, adibidez, totalizazioa edo integrazioa, zuzenean PLCan. HMI-k ez du behar adina eguneratze jasotzen hau ondo egiteko.

4. Erabili PLC banderak osotasun egiaztapen gisa

Jarri kontagailuak PLC errore-marketan matematika-arazoak atzemateko.

5. Erabili kriptografikoak eta/edo checksum-en osotasunaren egiaztapenak PLC kodearako

Erabili hash kriptografikoak edo checksumak hash kriptografikoak erabilgarri ez badaude, PLC kodearen osotasuna egiaztatzeko eta alarma bat pizteko aldatzen direnean.

6. Tenporizadoreak eta kontagailuak balioztatu

Tenporizadoreak eta kontagailuen balioak PLC programan idazten badira, PLCak balioztatu beharko ditu arrazoizkotasunagatik eta zero azpitik atzerako zenbaketak egiaztatu beharko ditu.

7. Parekatutako sarrera/irteeretarako baliozkotu eta alerta

Seinaleak parekatuta badituzu, ziurtatu bi seinaleak ez direla batera aldarrikatzen. Alarmatu operadorea fisikoki bideragarriak ez diren sarrera/irteera egoerak gertatzen direnean. Kontuan izan parekatutako seinaleak independenteak izatea edo atzerapen-tenporizadoreak gehitzea irteerak txandakatzea eragingailuentzat kaltegarria izan daitekeenean.

8. HMI sarrerako aldagaiak balioztatu PLC mailan, ez bakarrik HMIn

HMI PLC aldagaietarako sarbidea HMI-n balio operatiboko balio-tarte batera mugatu daiteke (eta beharko litzateke), baina PLCan gurutze-egiaztapen gehiago gehitu behar dira programatutako tarte onargarrietatik kanpo dauden balioak saihesteko edo ohartarazteko. HMIa.

9. Zeharkak balioztatzea

Baliozkotu zeharkaketak array-muturrak pozoinduz hesi-zutoin akatsak harrapatzeko.

10. Esleitu izendatutako erregistro-blokeak funtzioaren arabera (irakurtzea/idatzi/balioztatzea)

Esleitu izendatutako erregistro-blokeak funtzio zehatzetarako datuak balioztatzeko, buffer gainezkatzea saihesteko eta baimenik gabeko kanpoko idazketak blokeatzeko kontroladorearen datuak babesteko.

11. Sinesgarritasuna egiaztatzeko tresna

Prozesua sinesgarritasuna egiaztatzeak ahalbidetzen duen moduan instrumentatzea, neurketa desberdinak gurutzatuta.

12. Sarrerak baliozkotzea sinesgarritasun fisikoan oinarrituta

Ziurtatu operadoreek prozesuan praktikoa edo fisikoki bideragarria dena soilik sar dezaketela. Ezarri ebakuntza baten tenporizadorea fisikoki hartu beharko lukeen iraupenarekin. Kontuan izan desbideraketak daudenean abisatzea.
Era berean, ohartarazi ustekabeko jarduerarik ez dagoenean.

PLC kodetze praktika seguruak: Top 20 zerrenda

1.0 bertsioa (2021eko ekainaren 15a)

PLC Security TOP 20 LIST

13. Desgaitu behar ez diren / erabiltzen ez diren komunikazio atakak eta protokoloak

PLC kontrolagailuek eta sareko interfaze-moduluek, oro har, lehenespenez gaituta dauden hainbat komunikazio-protokolo onartzen dituzte. Desgaitu aplikaziorako beharrezkoak ez diren atakak eta protokoloak.

14. Mugatu hirugarrenen datuen interfazeak

Mugatu konexio motak eta eskuragarri dauden datuak hirugarrenen interfazeetarako. Konexioak edo/eta datu-interfazeak ondo definitu eta mugatuta egon behar dira, beharrezkoa den datu-transferentziarako irakurtzeko/idazteko gaitasunak soilik baimentzeko.

15. Definitu prozesu-egoera seguru bat PLC berrabiarazten bada

Definitu prozesurako egoera seguruak PLC berrabiarazten direnean (adibidez, kontaktuak dinamizatu, desenergizatu, aurreko egoera mantendu).

16. Laburtu PLC ziklo-denborak eta joera horiek HMIn

Laburtu PLC zikloaren denbora 2-3 segundoz behin eta jakinarazi HMI-ri grafiko batean bistaratzeko.

17. Erregistratu PLCaren funtzionamendu-denbora eta joera HMIn

Erregistratu PLC-ren funtzionamendua noiz berrabiarazi den jakiteko. Joera eta erregistro-denbora HMIan diagnostikoetarako.

18. Erregistratu PLC geldialdi gogorrak eta joera horiek HMIan

Gorde PLC akatsen edo itzaltzeen gertaerak HMI alarma-sistemek berreskuratzeko, PLCa berrabiarazi aurretik kontsultatzeko. Denbora sinkronizatu datu zehatzagoak lortzeko.

19. Monitoreatu PLC memoriaren erabilera eta joera HMIn

Neurtu eta eman memoria-erabileraren oinarria produkzio-ingurunean inplementatutako kontrolagailu bakoitzeko eta joera HMI-n.

20. Harrapatu negatibo faltsuak eta positibo faltsuak alerta kritikoetarako

Identifikatu alerta kritikoak eta programatu alerta horientzako tranpa bat. Ezarri tranpa edozein desbiderapenen abiarazte-baldintzak eta alerta-egoera kontrolatzeko.

Secure PLC Programazio proiektuari buruz

PLC kodetze praktika seguruak: xehetasunak

1.0 bertsioa (2021eko ekainaren 15a)

1. PLC kodea modularizatu

PLC kodea moduluetan zatitu, funtzio-bloke desberdinak erabiliz (azpi-errutinak). Probatu moduluak modu independentean.

Segurtasun Helburua	Helburu-taldea
PLC logikaren osotasuna	Produktu hornitzailea

Orientazioa

Ez programatu PLC logika osoa leku batean, adibidez, Antolakuntza bloke nagusian edo errutina nagusian. Horren ordez, zatitu funtzio-bloke desberdinetan (azpi-errutina) eta kontrolatu haien exekuzio-denbora eta haien tamaina Kb-tan.

Sortu segmentu bereiziak modu independentean funtzionatzen duen logikarako. Horrek sarrera balioztatzen, sarbide-kontrolaren kudeaketan, osotasuna egiaztatzen eta abar laguntzen du.

Kode modularizatuak ere errazten du kode-moduluen osotasuna probatzea eta jarraipena egitea. Moduluaren barruko kodea zehatz-mehatz probatu bada, modulu hauetan egindako aldaketak jatorrizko kodearen hasharekin egiaztatu daitezke, adibidez, modulu horietako bakoitzaren hash bat gordez (PLC-n aukera bat denean). Horrela, moduluak balioztatu daitezke FAT/SAT-ean edo kodearen osotasuna zalantzan jartzen bada gorabehera baten ondoren.

Adibidea

Gas-turbinaren logika "abiarazpena", "sarrerako gida-labeen kontrola", "ohiko balbularen kontrola" eta abarretan bereizten da, logika estandarra sistematikoki aplikatu ahal izateko. Horrek arazoak azkar konpontzen laguntzen du segurtasun-intzidentziaren bat gertatuko balitz.

Zorrotz probatzen diren funtzio-bloke pertsonalizatuak aldaketarik gabe berrerabili daitezke (eta aldaketa saiakerak egiten badira abisatu) eta tratu txarren edo erabilera okerren aurka blokeatu pasahitz edo sinadura digital batekin.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	Gaiztoak izan daitezkeen kode-zati berriak detektatzeko errazten du. Logikaren estandarizazioan, koherentzian eta baimendu gabeko aldaketen aurka blokeatzen laguntzen du.
Fidagarritasuna	Programaren fluxu-sekuentzia kontrolatzen eta begiztak saihesten laguntzen du, logikak behar bezala ez erreakzionatzea edo huts egitea eragin dezakeena.
Mantentzea	Kode modularra arazketa errazagoa ez ezik (moduluak modu independentean probatu daitezke), mantentzea eta eguneratzea ere errazagoa da. Gainera, moduluak PLC gehigarrietarako erabil daitezke, horrela kode arrunta PLC bereizietan erabili eta identifikatu ahal izateko. Honek mantentze-langileei lagun diezaieke ohiko moduluak azkar ezagutzen arazoak konpontzerakoan.

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICSrako	**Taktika:** TA002 - Exekuzioa **Teknika:** T0844 - Programa Antolatzeko Unitateak
ISA 62443-3-3	**SR 3.4:** Softwarea eta informazioaren osotasuna
ISA 62443-4-2	**CR 3.4:** Softwarearen eta informazioaren osotasuna
ISA 62443-4-1	**SI-2:** Kodeketa estandarrak seguruak
MITRE CWE	**CWE-1120:** Gehiegizko kodearen konplexutasuna **CWE-653:** Konpartimentazio nahikoa

2. Jarraitu funtzionamendu moduak

Mantendu PLCa RUN moduan. PLCak RUN moduan ez badaude, alarma bat egon beharko luke operadoreentzat.

Segurtasun Helburua	Helburu-taldea
PLC logikaren osotasuna	Integrazio / Mantentze Zerbitzu Hornitzailea Aktiboen jabea

Orientazioa

PLCak RUN moduan ez badaude (adibidez, PROGRAM moduan), haien kodea alda daiteke RUN moduan jarraitzeko. PLC batzuek checksum bat dute kode-aldaketen berri emateko, baina hala egiten ez badute, arazo potentzial baten zeharkako adierazle bat dago gutxienez funtzionamendu moduen jarraipena egiten duen bitartean:

- PLCak RUN moduan ez badaude, alarma bat egon beharko luke operadoreentzat. Kontrol-sistema horretan norbait lanean ari dela jakitun bada, alarma onartu eta aurrera egin dezakete.

- HMIa konfiguratu behar da operadoreari txanda amaitzean alarmaren presentziaz berriro abisatzeko. Helburua prozesuan eragina izan dezaketen lan egiten duten lantegiko langile edo kontratistaren jarraipena izan behar da.

Salbuespen kasua: planta proba edo garapen fasean badago, kontuan hartu alarma hau desgaitzea, baina lantegia sareko maila altuagoetatik isolatu behar da.

Adibidea

PLCak ez badu hardware etengailurik funtzionamendu moduak aldatzeko, gutxienez PLC kodea aldatzea muga dezaketen software mekanismoak erabiltzea gomendatzen da, adibidez, PLC kodea irakurtzeko eta idazteko ingeniaritza softwarean pasahitz babesa.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	Funtzionamendu moduak (exekutatu / editatu / idatzi; Allen Bradley PLCentzat: RUN / PROGram / Remote) PLCa manipulatu daitekeen zehazten du. Tekla-etengailua Urrutiko egoeran badago, teknikoki posible da PLC programan aldaketak egitea komunikazio-interfazeen bidez PLCa martxan egon arren.
Fidagarritasuna	/
Mantentzea	/

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICSrako	**Taktika:** TA009 - Inhibit Erantzun Funtzioa **Teknika:** T0858 - Erabili/Aldatu Eragiketa Modua
ISA/IEC 62443-4-1	**SI-1 :** Segurtasunaren ezarpenaren berrikuspena

3. Utzi logika operatiboa PLCan bideragarria den guztietan

Utzi logika operatibo gehiena, adibidez, totalizazioa edo integrazioa, zuzenean PLCan. HMI-k ez du behar adina eguneratze jasotzen hau ondo egiteko.

Segurtasun Helburua	Helburu-taldea
PLC logikaren osotasuna	Produktu hornitzailea Integrazio / Mantentze Zerbitzu Hornitzailea Aktiboen jabea

Orientazioa

HMIek kodetze-gaitasunen bat eskaintzen dute, hasiera batean operadoreei bistaratzea eta alarma hobetzen laguntzeko xedea dutenak, programatzaile batzuek PLCan egon beharko luketen kodea sortzeko erabili dutena, osoa eta ikuskagarria izaten jarraitzeko.

Balioak eremutik ahalik eta hurbilen kalkulatzeak kalkulu hauek zehatzagoak egiten ditu. HMIak ez du behar adina eguneratze lortzen totalizazioa/integrazioa ondo egiteko. Gainera, beti dago latentzia HMI eta PLC artean. Gainera, kodea PLCan dagoenean eta HMI bat berrabiarazten denean, PLC batetik totalizatzaileak/zenbaketak jaso ditzake beti.

Bereziki, saihestu beharreko HMI kodea segurtasun- edo segurtasun-funtzioekin erlazionatutako edozein gauza da, hala nola interblokeoak, tenporizadoreak, atxikipenak edo permisiboak.

Prozesu-datuen balioak denboran zehar aztertzeko, prozesu-datuen historialaria HMIa baino aukera hobea da. Erabili kontsultak prozesuen historialarien datu-base batean guztirako balioak (aldi batean, lote batean, prozesu-ziklo batean) PLC logikan lokalean agregatutako guztizkoekin alderatzeko. Hori baino handiagoa den bariantza bati buruzko abisua datuen zehaztasun-desberdintasunek azal dezakete.

Adibidea

- ÿ Botoiak gaitzeko/desgaitzeko baldintzak ezartzeko kodea: Gaitu/desgaitu ekintzak PLC geruzan kontrolatu behar dira, bestela, HMIn (edo sarearen bidez) PLCan egin daitezke ekintzak, nahiz eta (aurreikusten diren) baldintzak betetzen ez diren.
- ÿ Operadoreari ekintzak ahalbidetzeko tenporizadoreak (motorra jarraian abiarazterako atzerapen-tenporizadorea, balbulak itxita/ireki edo motorra geldituta kontuan hartzeko tenporizadorea) ez dira jarri behar HMI geruzan, motor/balbula hori gobernatzen duen PLCan baizik.
- ÿ Alarmen atalaseek PLC kodeen parte izan behar dute, nahiz eta HMIetan bistaratu.
- ÿ Bolumen aldakorra duen ur depositua: Deposituaren eta irteteko emaria kontrolatzen duen PLCa bolumena erraz batu (eta guztizkoak gurutzatu). HMIk hau ere egin lezake, baina lehenik PLCtik balioak lortu beharko lituzke. Balio hauek denbora-zigilu zehatzak beharko lituzkete guztizko zuzenak lortzeko latentziaren kasuan, eta baliteke balioak galtzea HMI berrabiaraziz gero.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	**1.** Kode aldaketak egiaztatzeko koherentzia ahalbidetzen du. HMI kodetzeak PLCaz gain bere aldaketa kontrola du, oro har ez zorroztasun berdinarekin (batez ere eraikuntza eta martxan jartzeko faseetan), sistemaren jabeei ikuspegi osoa ez izatea eta gogoeta garrantzitsuak galdu ere. HMI-ek ez dituzte "seinale behartuak" edo aldatutako balioen zerrendak PLC edo SCADA gisa sartzen, beraz HMI maila aldatzen da

Onuragarria...?	Zergatik?
	detektatzeko zailagoak dira, ia ezinezkoa baimen-aldaketak kudeatzeko plan baten parte izatea. **2.** Erasotzaile batentzat, zailagoa da PLC askotan banatutako guztirakoak manipulatzea HMIan kalkulatutako guztirakoak manipulatzea baino. **3.** Gaitu/desgaitu funtzioen zati bat PLCan ez badago, baliteke erasotzaileek PLCa eta I/O manipulatu ahal izatea HMI zatia landu beharrik gabe, informazio egokia dagoeneko operadorearen pantailan lausotuta baitago.
Fidagarritasuna	**1.** Kalkuluak eraginkorragoak eta zehatzagoak dira eremutik gertuago baldin badira. Gainera, guztirakoak eta zenbaketak oraindik erabilgarri egongo dira HMI berrabiarazten bada (PLCak ez dira maiz berrabiarazten eta normalean balio horiek memoria ez lurrunkor batean gordetzen dituzte). **2.** Sarrera eta interblokeo iturri desberdinek ezetz esan dezakete espero diren porrotak. Planta batean HMIentzako teknologia desberdinak egon daitezke (SCADA geruza, baina baita eremuko kontroladoreen panelak ere) eta horietako batean egindako aldaketak ez dira gainontzeko geruzen bidez hedatuko, bistaratzeko inkoherentziak eta funtzionamenduan izan daitezkeen akatsak eraginez.
Mantentzea	Kodetzea erraza da ulertzeko eta PLCtik PLCra transferitzeko, ez hainbeste HMIetatik HMIetara.

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICSrako	**Taktika:** TA010 - Prozesuaren Kontrola kaltetu **Teknika:** T0836 - Parametroa aldatu
ISA 62443-3-3	**SR 3.6 :** Irteera deterministikoa
ISA 62443-4-2	**CR 3.6 :** Irteera deterministikoa

4. Erabili PLC banderak osotasun egiaztapen gisa

Jarri kontagailuak PLC errore-marketan matematika-arazoak atzemateko.

Segurtasun Helburua	Helburu-taldea
PLC logikaren osotasuna	Produktu hornitzailea Integrazio / Mantentze Zerbitzu Hornitzailea

Orientazioa

PLC kodea ondo funtzionatzen ari bazen baina bat-batean zeroz zatitzen badu, ikertu. Zerbait beste PLC batetik berdin-berdin komunikatzen ari bada eta funtzio/logikak zeroz zatitzen badu espero ez zenean, ikertu.

Programatzaile gehienek arazoa baztertuko dute matematikako errore gisa edo okerragoa dena, baliteke haien kodea perfektua dela suposatzea eta PLCari akats gogor batean sartzen utziko diote. Kodearen garapenean, ingeniariek beren kode-moduluak (zatiak edo errutinak) probatu eta balioztatu behar dituzte, espero diren mugetatik kanpo datuak sartuz. Hau Unitate-mailako proba dei daiteke.

Esleitu blokeatutako memoria-segmentu desberdinak firmware, logika eta protokolo pilarako. Probatu protokolo-pila tratu txar kasuetarako. Abusu kasuak paketeen goiburuko bandera-baldintza bereziak izan daitezke.

Adibidea

Mugetatik kanpoko datuek eragindako PLC akatsak oso ohikoak dira. Hau gertatzen da, adibidez, sarrerako balio batek array-indizeak mugetatik kanpo edo aurrezarpen negatiboak dituzten tenporizadoreak edo zero salbuespenekin zatitzen duenean.

Interesezko bandera tipikoak dira

- ÿ zeroz zatitu
- ÿ gainezkatze kontrakoa
- ÿ kontagailu negatiboa edo tenporizadorearen aurrez ezarri
- ÿ I/O eskaneatzea gainditzea

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	PLCen aurkako erasoek logika aldatzea, programa berri bat aktibatzea, kode berria probatzea, prozesu-errezeta berri bat kargatzea, mezuak bidaltzeko logika osagarria txertatzea edo funtzioren bat aktibatzea izan daitezke. PLC gehienek osotasun kriptografikoaren egiaztapenik ematen ez dutenez, banderak adierazle onak izan daitezke goiko logika aldaketaren bat gertatzen bada.
Fidagarritasuna	Serioski hartutako banderak PLCa programazio edo I/O akatsekin exekutatzen saihes dezake. Gainera, akatsen bat gertatzen bada, hutsegitearen iturria nabariagoa da.
Mantentzea	/

Erreferentziak

Estandarra/esparrua Mapping Tactic :	
MITRE ATT & CK ICSrako	TA010 - Prozesuaren Kontrola kaltetu **Teknika:** T0836 - Parametroa aldatu **SR 3.5:**
ISA 62443-3-3	Sarreraren baliozkotzea **SR 3.6:** Irteera deterministikoa **CR 3.5:** Sarreraren
ISA 62443-4-2	baliozkotzea **CR 3.6:** Irteera deterministikoa **SI-2:** Kodetze estandar seguruak **SVV-1:**
ISA 62443-4-1	Segurtasun-eskakizunen probak **CWE-128:** CWE **-190 biribilgarria:** Integer Overflow
MITRE CWE	**CWE-369 :** Zatitu Zero **CWE-754:** Ezohiko edo Salbuespenezko Baldintza desegokia egiaztatzea

5. Erabili kriptografikoak eta/edo checksum-en osotasunaren egiaztapenak PLCrako kodea

Erabili hash kriptografikoak edo checksumak hash kriptografikoak erabilgarri ez badaude, PLC kodearen osotasuna egiaztatzeko eta alarma bat pizteko aldatzen direnean.

Segurtasun Helburu Taldea	
PLC logikaren osotasuna	Produktu hornitzailea Integrazio / Mantentze Zerbitzu Hornitzailea Aktiboen jabea

Orientazioa

A) Checksumak

Hash (kriptografikoak) bideragarriak ez direnean, checksumak aukera bat izan daiteke. PLC batzuek Checksum bakarra sortzen dute kodea PLC Hardwarera deskargatzen denean. Checksum-a fabrikatzaileak/integratzaileak dokumentatu behar du SAT ondoren eta berme/zerbitzu-baldintzen parte izan.

Checksumaren funtzioa ez badago jatorrizko kontrolagailuan eskuragarri, hau EWS/HMI-n ere sor daiteke eta probatu, adibidez, egunean behin PLCko jatorrizko kodearen hasharekin alderatzeko, bat datozela egiaztatzeko. Honek denbora errealeko alertak emango ez dituen arren, nahikoa da inor PLC kodean aldaketak egiten saiatzen ari den jarraitzeko.

Kontrol-balioa PLC erregistro batera eraman daiteke eta alarma baterako konfiguratu daiteke aldatzen denean, balioa historialariei eta abar bidal daiteke.

B) Hashak

PLC CPUek, oro har, ez dute prozesatzeko gaitasunik exekutatzen ari diren bitartean hashak sortzeko edo egiaztatzeko. Hash bat saiatzeak PLCa huts egitea eragin dezake. Baina PLCren ingeniaritza softwareak PLC kodearen hashak kalkulatu eta PLCan edo beste nonbait gorde ditzake.

kontrol-sistema.

Adibidea

Checksum ezaugarriak dituzten PLC saltzaileak:

- ÿ Siemens (ikusi adibidea)
- ÿ Rockwell

Gainera, kanpoko softwarea erabil daiteke checksumak sortzeko:

- ÿ Bertsio txakurra
- ÿ Aktiboen zaintzailea
- ÿ EZ

Siemens inplementazio adibidea

Siemens S7-1500 PLC-n egiaztapen batuak sortzeko adibidea:

GetChecksum-Function Block benetako checksum irakurtzen du eta script arin batekin "SAT Checksum" erreferentzia gisa gorde daiteke. Erreferentzia-Checksum-aren desbideratze bat gorde daiteke

Datalog-Funtzioa.

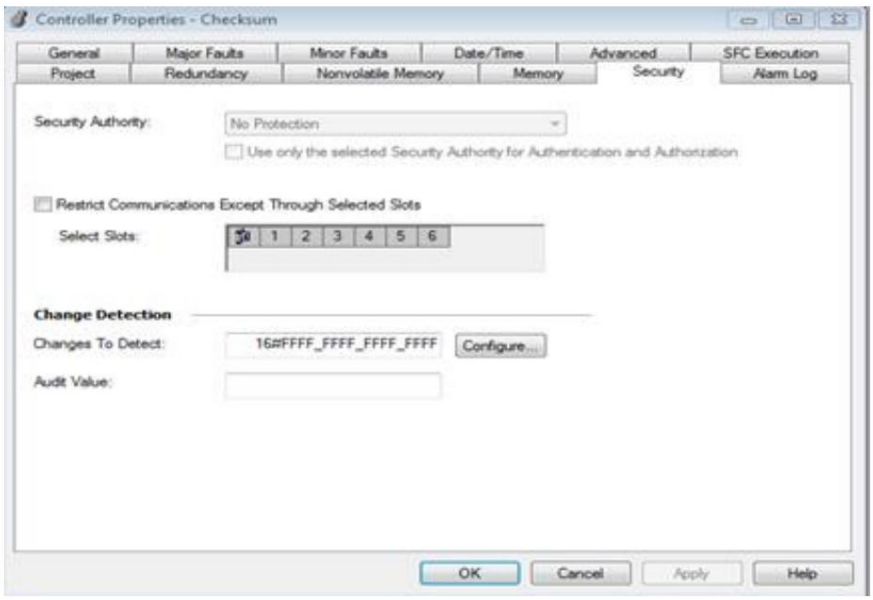
	Date	UTC Time	Referenz	Aktuell
1	11/21/2019	9:55:11	84 2A 76 DF 5B 31 F4 16	FF 2C EA 71 44 D7 81 04
2	11/21/2019	9:57:33	FF 2C EA 71 44 D7 81 04	FF 2C EA 71 44 D7 81 04
3	11/21/2019	9:58:17	FF 2C EA 71 44 D7 81 04	5B 7C 57 7E E2 3E EF C3
4	11/21/2019	9:58:36	FF 2C EA 71 44 D7 81 04	5B 7C 57 7E E2 3E EF C3
5	11/21/2019	9:58:44	5B 7C 57 7E E2 3E EF C3	5B 7C 57 7E E2 3E EF C3

Rockwell-en ezarpenaren adibidea:

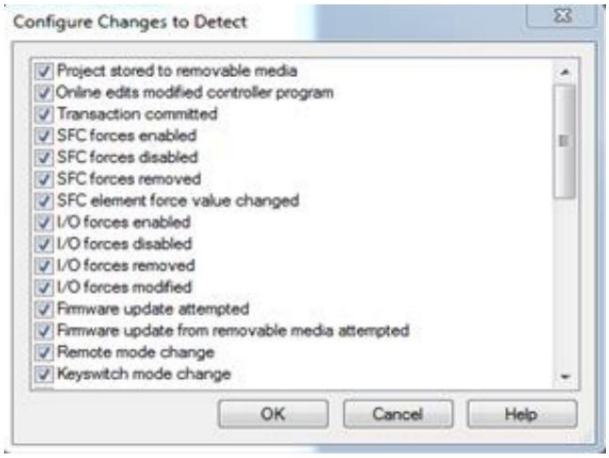
Hau da, erakunde batek PLC programaren aldaketak detektatzeko gaitasun maila bat garatzeko moduaren adibide partziala da bere ICS ingurunean. Adibide hau Rockwell Automation ControlLogix PLC baterako da bereziki eta ez dago osatua; hala ere, PLC prozesadorearen egoera PLCren erregistro batean nola berreskuratu erakusten du. Behin PLCko erregistro batean, erakundeak erabil dezake konfigurazio-aldaketaren alarma bat sortzeko HMI batean bistaratzeko, egoera gordinaren informazioa HMI bati helarazteko joerak eta jarraipena egiteko, edo Historialari bati epe luzera harrapatzeko.

Praktika honek aukera bat eskaintzen du, dauden tresnak eta gaitasunak erabiliz, ziber-aktibo kritikoak noiz aldatzen diren jakiteko egoeraren kontzientzia lortzeko. Erakundeari dagokio adibide honen erabilera bere ingurunean ondoen funtzionatzen duen metodo batean osatzea.

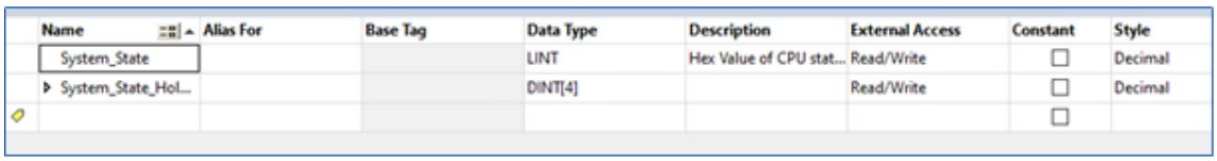
1. Kontrolagailuaren propietateen elkarrizketa-koadroan, hautatu "Aldatu detektatzeko" konfiguratzeko botoia.



2. Hautaketa leihoaren barruan, aukeratu kontrolatu beharreko elementu guztiak

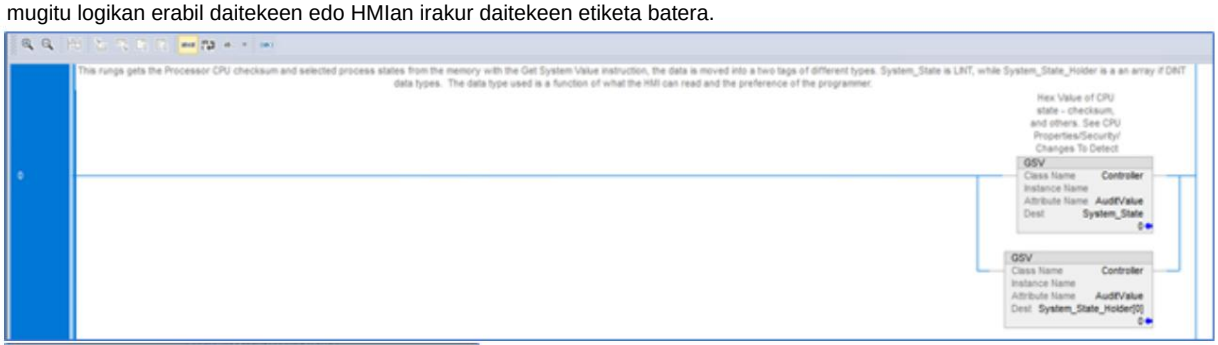


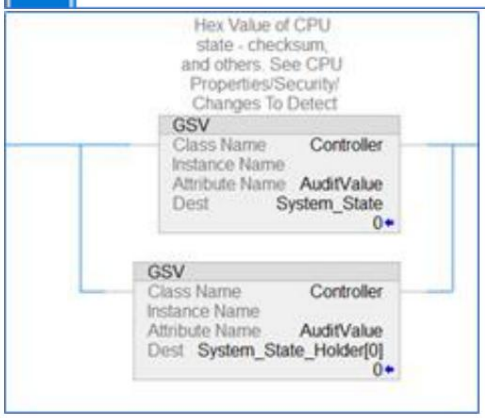
3. Sortu Etiketa bat prozesadorearen egoerari buruzko informazioa jasotzeko. Etiketa hau "LINT" motakoa edo "DINT" motako 2 hitz-matrizea izan daiteke



Name	Alias For	Base Tag	Data Type	Description	External Access	Constant	Style
System_State			LINT	Hex Value of CPU stat...	Read/Write	☐	Decimal
System_State_Hol...			DINT[4]		Read/Write	☐	Decimal
						☐	

4. Erabili Get System Values (GSV) instrukzioa memoriatik prozesadorearen egoeraren informazioa lortzeko eta mugitu logikan erabil daitekeen edo HMIan irakur daitekeen etiketa batera.





Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	PLC kodea manipulatu ote den jakitea ezinbestekoa da bai konpromiso bat antzemateko bai egiaztatzeko PLC bat segurua den konpromezu baten ondoren funtzionatzeko.
Fidagarritasuna	Hashes edo checksum-ak PLC integratzaileak / fabrikatzaileak onartutako kodea (oraindik) martxan dagoen egiaztatzeko bitarteko bat ere izan daiteke.
Mantentzea	/

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICSrako	**Taktika:** TA002 - Exekuzioa, TA010 - Prozesuaren Kontrola kaltetzea **Teknika:** T0873 - Project File Infection, T0833 - Kontrol-logika aldatu
ISA 62443-3-3	**SR 3.4 :** Softwarearen eta informazioaren osotasuna
ISA 62443-4-2	**CR 3.4 :** Softwarearen eta informazioaren osotasuna **EDR 3.12 :** Produktu hornitzaileen konfiantzazko sustraiak hornitzea
ISA 62443-4-1	**SI-1 :** Segurtasunaren ezarpenaren berrikuspena **SVV-1** Segurtasun-eskakizunen azterketa
MITRE CWE	**CWE-345:** Datuen egiazkotasunaren egiaztapen eskasa • **(seme-alaba) CWE-353:** Osotasuna egiaztatzeko euskarria falta da • **(seme-alaba) CWE-354:** Osotasun egiaztatzeko balioaren baliozkotze desegokia

6. Tenporizadoreak eta kontagailuak balioztatu

Tenporizadoreak eta kontagailuen balioak PLC programan idazten badira, PLCak balioztatu beharko ditu arrazoizkotasunagatik eta zero azpitik atzerako zenbaketak egiaztatu beharko ditu.

Segurtasun Helburua	Helburu-taldea
PLC aldagaien osotasuna	Integrazio / Mantentze Zerbitzu Hornitzailea Aktiboen jabea

Orientazioa

Tenporizadoreak eta kontagailuak teknikoki edozein baliotara ezarri daitezke. Hori dela eta, tenporizadore edo kontagailu bat aurrez ezartzeko balio duen tartea mugatu behar da funtzionamendu-baldintzak betetzeko.

Urruneko gailuek, hala nola HMI bat, tenporizadorea edo kontagailuaren balioak idazten badituzte programa batean:

- ÿ ez utzi HMI-ri tenporizadoreari edo kontagailuari zuzenean idazten, baizik eta baliozkotze-logika batetik pasatzen
- ÿ PLCan aurrezarpenak eta denbora-muga balioak balioztatu

Tenporizadorearen eta kontagailuen sarreren baliozkotzea erraza da PLCan zuzenean egitea (Deep Packet Inspection egiteko gai den sareko gailuren beharrik gabe), PLCak prozesuaren egoera edo testuingurua zein den "dakielako". "Zer" lortzen duen eta "noiz" lortzen dituen komandoak edo ezarpenak baliozta ditzake.

Adibidea

PLC abiaraztean, tenporizadoreak eta kontagailuak balio jakin batzuetarako aurrez ezarri ohi dira.

Alarmak 1,3 segundora pizten dituen tenporizadore bat badago, baina tenporizadore hori 5 minutura asmo txarrez ezarrita badago, baliteke alarma ez piztuko duena.

10.000ra iristen denean prozesu bat geldiaraztea eragiten duen kontagailu bat badago baina hasieratik 11.000ra ezartzen badu, baliteke prozesua ez gelditzea.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	I/O, tenporizadoreak edo aurrezarpenak zuzenean I/O-n idazten badira, PLCak balioztatu ez badu, PLCaren baliozkotze-geruza saihestu egiten da eta HMI-ri (edo sareko beste gailu batzuei) bermerik gabeko konfiantza-maila bat esleitzen zaie.
Fidagarritasuna	PLCak operadore batek ustekabean tenporizadorearen edo kontagailuaren balio txarrak aurrez ezartzen dituenean ere balioztatu dezake.
Mantentzea	Tenporizadoreetarako eta kontagailuetarako baliozko tarteak dokumentatuta eta automatikoki balioztatuta edukitzea lagungarria izan daiteke logika eguneratzean.

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICSrako	**Taktika :** TA010 - Prozesuaren Kontrola kaltetzea **Teknika:** T0836 - Parametroa aldatu
ISA 62443-3-3	**SR 3.5 :** Sarreraren baliozkotzea
ISA 62443-4-2	**CR 3.5 :** Sarreraren baliozkotzea
ISA 62443-4-1	**SI-2 :** Kodeketa estandarrak seguruak **SVV-1 :** Segurtasun-eskakizunen probak

7. Parekatutako sarrera/irteeretarako baliozkotu eta alerta

Seinaleak parekatuta badituzu, ziurtatu bi seinaleak ez direla batera aldarrikatzen. Alarmatu operadorea fisikoki bideragarriak ez diren sarrera/irteera egoerak gertatzen direnean. Kontuan izan parekatutako seinaleak independenteak izatea edo atzerapen-tenporizadoreak gehitzea irteerak txandakatzea eragingailuentzat kaltegarria izan daitekeenean.

Segurtasun Helburua	Helburu-taldea
PLC aldagaien osotasuna Erresilientzia	Produktu hornitzailea Integrazio / Mantentze Zerbitzu Hornitzailea

Orientazioa

Parekatutako sarrerak edo irteerak fisikoki aldi berean gertatu ezin direnak dira; elkarren esklusiboak dira. Parekatutako seinaleak aldi berean baieztatu ezin diren arren, hutsegite edo jarduera gaiztorik egon ezean, PLC programatzaileek askotan ez dute baieztapen hori gertatzea eragozten.

Balioztatzea PLCan zuzenean egiteko errazena da, PLCak prozesuaren egoera edo testuingurua ezagutzen duelako. Parekatutako seinaleak errazago ezagutzen eta jarraipena egiten dute helbide sekuentzialak badituzte (adibidez, 1. sarrera eta 2. sarrera).

Parekatutako sarrerak edo irteerak arazoak sor ditzaketen beste eszenatoki bat da aldi berean baieztatzen ez direnean, baina azkar txandakatzen direnean eragingailuak kaltetzen dituztenean.

Adibidea

Seinale parekatuen adibideak:

- ÿ HASI eta GELDITU
  - o Irteera eta geldialdi independenteak: konfiguratu irteera eta geldialdia irteera diskretu gisa, aktibatu/desaktibatu daitekeen irteera bakarra izan beharrean. Diseinuaren arabera, honek ez du aldibereko abiarazterik onartzen. Erasotzaile batentzat, askoz konplikatuagoa da bi irteera desberdin ezarri behar badira azkar aktibatzea / desaktibatzea.
  - o Berrabiarazteko tenporizadorea: ere kontuan hartu tenporizadorea gehitzea berriro abiarazteko, geldialdia igorri ondoren. saihestu abiarazte/gelditzeko seinaleak desaktibatzea.
- ÿ AURRERA eta ATZERA
- ÿ IREKI eta ITXI

Kaltegarriak izan daitezkeen parean dauden seinaleak aldatzeko adibideak:

PLC / MCC-k sarrera diskretu bat onartzen badu, erasotzaile batek eragingailuetan kalte fisikoak eragiteko aukera erraza eskaintzen du. Irteerak aldatzeko kalteak egiteko eszenatoki ezaguna MCC bat izango litzateke, baina praktika hau txandakatzeak kalteak eragin ditzaketen eszenatoki guztietan aplikatzen da. Idahoko Laborategi Nazionalak 2007an Aurora Generator Testa izan zen, non azkar aldatzeko irteerak benetako kalteak eragin ditzakeen kontzeptuaren froga, non irteeren txandakatzeak sinkronizatzeak etengailuaren kalteak eragin zituen.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	1. PLC programek zer gertatuko den kontuan hartzen ez badute parekatuta dauden bi sarrera-seinaleak aldi berean aldarrikatzen dira, hau eraso-bektore ona da. 2. Bi sarrera-seinale parekatuak baieztatzen diren funtzionamendu-errore bat, programazio-errore bat edo zerbait gaizto gertatzen ari den abisua da. 3. Horrek kalte fisikoa izan daitekeen eraso-eszenatoki bat saihesten du eragingailuei eragindakoa.
Fidagarritasuna	1. Parekatutako sarrera-seinaleek sentsore bat hautsi edo gaizki dagoela adierazi dezakete kableatuta edo trabatuta dagoen etengailu bat bezalako arazo mekaniko bat dagoela. 2. Abiadura eta geldialdia bizkor aldatzea ere akatsez egin liteke, beraz, nahi gabe egin daitezkeen kalteak ere saihesten ditu.
Mantentzea	/

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICSrako	**Taktika:** TA010 - Prozesuaren Kontrola kaltetu **Teknika:** T0836 - Aldatu parametroa, T0806 - Brute Force I/O **SR 3.5:** Sarreraren
ISA 62443-3-3	baliozkotzea **SR 3.6:** Irteera deterministikoa
ISA 62443-4-2	**CR 3.5:** Sarreraren baliozkotzea **CR 3.6:** Irteera deterministikoa
ISA 62443-4-1	**SI-2:** Kodeketa estandarrak seguruak **SVV-1:** Segurtasun-eskakizunen azterketa
MITRE CWE	**CWE-754:** Ezohiko edo Salbuespenezko Baldintzen egiaztapen desegokia

8. HMI sarrerako aldagaiak balioztatu PLC mailan, ez bakarrik HMIn

HMI PLC aldagaietarako sarbidea HMI-n balio operatiboko balio-tarte batera mugatu daiteke (eta beharko litzateke), baina PLCan gurutze-egiaztapen gehiago gehitu behar dira programatutako tarte onargarrietatik kanpo dauden balioak saihesteko edo ohartarazteko. HMIa.

Segurtasun Helburua	Helburu-taldea
PLC aldagaien osotasuna	Produktu hornitzailea Integrazio / Mantentze Zerbitzu Hornitzailea

Orientazioa

Sarrerako baliozkotzeak balio operatiboen balioak eta baliozko balioak mugaz kanpoko egiaztapenak izan ditzake, baita prozesuari dagozkion datu-moten arabera ere.

PLC aldagai batek mugaz kanpo dagoen balio bat jasotzen badu, eman PLC logika biei

- ÿ Prozesuari kalterik eragiten ez dion aldagai horri **lehenetsitako balio** bat sartu, eta egin dezake abisuetarako bandera gisa erabili, edo
- ÿ Sartu balio horri **azken balio zuzena** eta erregistratu gertaera gehiago aztertzeko.

Adibidea

1. adibidea

Eragiketa batek erabiltzaileak balbula-presioaren balio bat sartu behar du HMI batean. Eragiketa honetarako baliozko tarteak 0-100 dira, eta erabiltzailearen sarrera HMIko erabiltzailearen sarrera funtziotik PLCko V1 aldagaira pasatzen da. Kasu honetan,

1. V1 aldagaiaren HMI sarrerak 0-100 (dec.) tarte mugatua du HMIan programatuta.
2. PLCak egiaztapen gurutzatuaren logika bat du, hau dioena:

V1 < 0 BADIN EDO V1 > 100, SET V1 = 0.

Honek balio segurua den erantzun positiboa ematen dio aldagai horren sarrera baliogabe bati.

2. adibidea

Eragiketa batek erabiltzaileak sartzea eskatzen du neurtzeko atalaseak INT2 datu-barruti baten barruan egon behar duen aldagai batean. Erabiltzailearen sarrera HMItik V2 aldagaira pasatzen da PLCan, hau da, 16 biteko datu-erregistro batera.

1. V2 aldagaiaren HMI sarrerak -32768 eta 32767 bitarteko tarte mugatua du (dec.) programatuta. HMIa.
2. PLCak gainezkatze-aldagaia (V3) kontrolatzen duen datu-motako gurutzatze-logika du. PLCaren memoria-egituran V2 ondoren existitzen da:

V2 = -32768 EDO V2 = 32767 ETA V3 != 0,

SET V2 = 0 ETA SET V3 = 0 ETA EZAR DataTypeOverflowAlarm = EGIA.

3. adibidea

Eskalatu PV (Prozesuaren Balioa), SP (Set Point) eta CV (Kontrol Aldagaia) PID (Proportzionala, Integrala, Deribatua kontrolatzailea) unitate koherenteetara edo gordinetara, kontrol-arazoak eragiten dituzten eskalatze-akatsak ezabatzeko. Eskalatze okerrak nahigabeko tratu txar kasuak sor ditzake.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	**1.** HMIek normalean sarreraren baliozkotze moduko bat ematen badute ere, aktore gaizto batek aldatutako paketeak landu edo errepika ditzake PLCko aldagaiei balio arbitrarioak bidaltzeko, zeinak kanpoko eraginetarako irekita dauden (HMI batetik pasatako balioetarako irekita, adibidez). **2.** PLC protokoloak normalean protokolo "ireki" gisa merkaturatzen dira eta publiko orokorrarentzat argitaratua, beraz, protokolo-informazioa "irekia" erabiltzen duen malwarea sortzea hutsala izan daiteke garatzea. PLC aldagaien mapaketa normalean trafikoaren analisiaren bidez gerta daiteke eraso baten ezagutza-faseetan, eta horrela intrusoari beharrezko informazioa ematen dio trafiko gaiztoa helburura bideratzeko eta, ondorioz, prozesu bat baimendu gabeko tresnekin manipulatzeko. Datu horiek prozesuan inplementatu aurretik PLCra pasatzen diren balio gurutzatuak egiaztatzen ditu baliozko datu-barrutiak eta memoria-kokapen horietan baliorik gabeko balio bat arintzen du, PLCan zehar balio bat mugaz kanpo dagoela detektatzen denean barruti seguruak indarrez ezarriz. eskaneatu.
Fidagarritasuna	/
Mantentzea	/

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICSrako	**Taktika:** TA010 - Prozesuaren Kontrola kaltetu **Teknika:** T0836 - Parametroa aldatu
ISA 62443-3-3	**SR 3.5:** Sarreraren baliozkotzea **SR 3.6:** Irteera deterministikoa
ISA 62443-4-2	**CR 3.5:** Sarreraren baliozkotzea **CR 3.6:** Irteera deterministikoa
ISA 62443-4-1	**SI-2:** Kodeketa estandarrak seguruak **SVV-1:** Segurtasun-eskakizunen azterketa
MITRE CWE	**CWE-1320:** Mugetatik kanpo seinale-mailaren abisuetarako babes desegokia

9. Zeharkak balioztatzea

Baliozkotu zeharkaketak array-muturrak pozoinduz hesi-zutoin akatsak harrapatzeko.

Segurtasun-helburua Helburu-taldea Produktu-hornitzailea Integrazioa /	
PLC aldagaien osotasuna	Mantentze-zerbitzu-hornitzailea

Orientazioa

Zeharka erregistro baten balioa beste erregistro batean erabiltzea da. Zeharkakotasunak erabiltzeko arrazoi asko daude.

Beharrezko bidegurutzeen adibideak hauek dira:

- ÿ Maiztasun aldakorreko unitateak (VFD), maiztasun desberdinetarako ekintza desberdinak abiarazten dituztenak bilaketa-taulak.
- ÿ Zein ponpa martxan jarri behar den lehen unean uneko iraupen-denboretan oinarrituta erabakitzea

PLCek normalean ez dute "matrize baten amaiera" banderarik, beraz, ideia ona da softwarean sortzea; helburua ezohiko/planifikatu gabeko PLC eragiketak saihestea da.

Adibide

Instrukzio Zerrenda (IL) Programazioa

Planteamendua funtzio-bloke gutxitan bihur daiteke eta, agian, beste aplikazio batzuetarako berrerabili daiteke.

1. Sortu array maskara

Egiaztatu matrizea tamaina bitarra den. Tamaina bitarra ez bada, sortu hurrengo tamainarako maskara eskala bitar batean. adibidez, 5 erregistro behar badituzu (ez bitar-tamaina):

[21 31 41 51 61]

definitu 8ko array bat:

[xx 21 31 41 51 61 x]

Ondoren, hartu indizearen balioa zeharkakoa jasotzeko - adibide honetan, 3 da.

Oharra: indizea 0-n hasten da!

[21 31 41 **51** 61]
_____^

Aurkibidea: 3

gehitu offset bat amaiera pozoitua osatzeko. Desplazamendua 1 edo handiagoa izan daiteke, kasu honetan 2 da:

[xx 21 31 41 **51** 61 x] _____^

Desplazamendua barne indizea: 3 + 2 = 5

eta gero ETA indizea desplazamendua barne matrizearen tamaina berdina duen maskara batekin.
Adibide honetan matrizearen tamaina 8 da, beraz, indizea 7, beraz, maskara 0x07 izango litzateke. Maskarak ziurtatzen du lor dezakezun indize maximoa 7 dela, adibidez:

6 ETA 0x07k 6 itzuliko luke.
7 ETA 0x07k 7 itzuliko luke 8 ETA 0x07k
0 itzuliko luke.
9 ETA 0x07k 1 itzuliko luke.

Horrek ziurtatzen du beti matrizeko balio bat zuzentzen duzula.

2. Txertatu pozoitutako muturrak

Pozoitzeko muturrak hautazkoa da. Pozoitzerik gabe manipulatutako zeharka detektatzeko gai izango zenituzke, baina pozoitzeak hesi-zuten akatsak harrapatzen laguntzen du, zentzurik ez duen balio bat berreskuratzen duzulako.

Kontua da matrizeko 0 indizean baliogabea den balio bat egon beharko litzatekeela, hala nola -1 edo 65535.
Hau da "amaiera pozoitua". Era berean, arrayaren azken elementuetan gauza bera egiten duzu:

Beraz, goiko arrayrako, pozoitutako bertsioa honelakoa izan daiteke:

[-1 -1 21 31 41 51 61 -1]

3. Erregistratu zeharkako helbidearen balioa maskararik gabe

Ondoren, erregistratu zeharkako helbidearen balioa ETA maskararik eta desplazamendurik gabe:
Adibide honetan, 3. indizerako 51 grabatuko zenuke.

[21 31 41 **51** 61] _____^

_____3. aurkibidea

4. Exekutatu AND maskara eta alderatu balioak (=norabidearen baliozkotzea)

Konparatu zure grabatutako balioa desplazamendua eta ETA maskara egin ondoren balioarekin.

4a. A kasua: norabide zuzena

Lehenik eta behin, desplazamendua:

Indizea + Desplazamendua = 3 + 2 = 5

Bigarrena, maskara:
5 ETA 0x07 = 5

Hirugarrena, zeharkako
egiaztapena: [-1 -1 21 31 41 **51** 61 -1]
_____^ Indizea desplazamendua
barne: 5 Balioa = 51 grabatutako balioaren
berdina da, beraz, dena ondo dago.

4b. B kasua: norabide manipulatua

Orain zeharkako manipulatua bazenuen, demagun 7, ikus dezagun zer gertatzen den:

Lehenik eta behin, desplazamendua:

Indizea + Desplazamendua = 7 + 2 = 9

Bigarrena, maskara:

9 ETA 0x07 = 1

Hirugarren, zeharkako egiaztapena:

[-1 **-1** 21 31 41 51 61 -1]

_____^

Desplazamendua barne indizea: **1**

Balioa = **-1** ez da erregistratutako balioaren berdina eta zure amaiera pozoitua ere adierazten du, beraz, zure zeharkakotasuna manipulatuta dagoela jakingo zenuke.

5. Exekutatu matxura / programatzailearen alerta

Balidatutako balio hau zure grabatutakoaren desberdina bada, badakizu zerbait gaizki dagoela. Piztu softwarearen kalitatearen alarma.

Ondoren, egiaztatu zeharkako balioa. Pozoitutako balio bat bada, beste softwarearen kalitatearen alarma piztu beharko zenuke. Hau hesi-zutoinaren akats baten seinale da.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	PLC gehienek ez dute matrizeetarako mugaz kanpoko indizeak kudeatzeko ezaugarririk. Zeharkako akatsetatik **sor daitezkeen bi eszenatoki arriskutsu** daude : **Lehenik eta behin,** zeharkatze batek erregistro okerretik irakurtzera eramaten badu, programa balio okerrak erabiliz exekutatzen da. **Bigarrenik,** zeharkatze oker batek erregistro okerrean idaztera eramaten badu, programak gorde nahi dituzun kodea edo balioak gainidazten ditu. Bi kasuetan, zeharkako akatsak antzematen zailak izan daitezke eta eragin larriak izan ditzakete. Giza akatsak eragin ditzakete baina maltzurrez txerta daitezke.
Fidagarritasuna	Programazioan giza akats ez-maltzurrak identifikatzen ditu.
Mantentzea	/

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICSrako	**Taktika:** TA010 - Prozesuaren Kontrola kaltetu **Teknika:** T0836 - Parametroa aldatu
ISA 62443-3-3	**SR 3.5:** Sarreraren baliozkotzea **SR 3.6:** Irteera deterministikoa
ISA 62443-4-2	**CR 3.5:** Sarreraren baliozkotzea **CR 3.6:** Irteera deterministikoa
ISA 62443-4-1	**SI-2:** Kodeketa estandarrak seguruak **SVV-1:** Segurtasun-eskakizunen azterketa
MITRE CWE	**CWE-129:** Array-indizearen baliozkotze okerra

10. Izendatutako erregistro-blokeak funtzioen arabera esleitu (irakurtu/idatzi/balioztatu)

Esleitu izendatutako erregistro-blokeak funtzio zehatzetarako datuak balioztatzeko, buffer gainezkatzea saihesteko eta baimenik gabeko kanpoko idazketak blokeatzeko kontroladorearen datuak babesteko.

Segurtasun Helburua	Helburu-taldea
PLC aldagaien osotasuna	Produktu hornitzailea Integrazio / Mantentze Zerbitzu Hornitzailea

Orientazioa

Aldi baterako memoria, scratch pad memoria bezala ere ezagutzen dena, erraz ustiatzen den memoria-eremua da praktika hori betetzen ez bada. adibidez, mugaz kanpo dagoen "Modbus" erregistroan idazteak aldi baterako kalkuluetarako erabiltzen diren memoria-erregistroak gainidaztea ekar dezake.

Orokorrean, erregistro-memoria PLC sareko beste gailu batzuek sar dezakete irakurtzeko eta idazteko eragiketak egiteko. Erregistro batzuk HMI batek irakur ditzake, eta beste batzuk SCADA sistema batek idatz ditzake eta abar. Aplikazio jakin baterako erregistro-matrize espezifikoak izateak ere errazten du (kontrolagailuan edo kanpoko suebaki bat erabiltzen da) beste batetik Irakurtzeko soilik sarbidea konfiguratzea. gailua/HMI.

Izendatutako erregistro-blokeek zentzua duten funtzioen adibideak hauek dira:

- irakurketa
- idazketa (HMI/Kontroladoretik/kanpoko beste gailu batetik)
- idazketak baliozkotzea
- kalkuluak

Onartutako erregistroetan kanpoko idazketak ziurtatzeak memoria nagusia berrezartzeko akatsak saihesten laguntzen du, mugaz kanpoko exekuzio edo saiakera maltzurengatik. Izendatutako erregistro-bloke hauek I/O, tenporizadore eta kontagailuen idazketarako buffer gisa erabil daitezke, buffera guztiz idatzita dagoela egiaztatuz (ez duela datu zaharraren zati bat, berriaren zati bat) eta buffereko datu guztiak balioztatuz.

Aurrekariak:

Memoria nagusia eta erregistro memoria ezberdin erabiltzen dira. Memoria nagusia unean exekutatzen ari den programaren logika gordetzeko erabiltzen da, eta erregistro-memoria aldi baterako memoria gisa erabiltzen du une honetan exekutatzen ari den logikak. Erregistro-memoria aldi baterakoa den arren, exekutatzen ari den logikak erabiltzen ari denez, logika nagusiari eragingo dioten aldagai garrantzitsu batzuk eduki behar ditu.

Adibidea

Praktika hau ezartzen ez bada gerta daitekeenaren adibideak:
(Erreferentzia: GPH Sandaruwan, PS Ranaweera, Vladimir A. Oleshchuk, PLC segurtasuna eta azpiegitura kritikoen babesa):

- Siemens-ek normalean scratchpad memoria erabiltzen du banderaren eremuan 200.0 banderatik 255.7 banderara. Eremu horretan bit bat aldatzen bada, PLCaren matxura larria izateko probabilitatea dago bit edo byte horren garrantziaren arabera.
- Demagun erasotzaile batek PLC sareko makinetako batean sar dezakeela eta makina hori erregistroan balio arbitrarioak idazteko gai den harra batekin kutsatu

memoria. Erregistro-memoriaren balioak arbitrarioki aldatu direnez, presioaren balioa alda dezake.

- Logika exekutatzeak balio berri bat ezarriko du aldaketaren arabera, eta horrek sistemaren segurtasun-marjinak gainditzea eragin dezake eta agian hutsegite batera eraman dezake.

Praktika hau ezartzeko adibideak:

- Segurtasun-eremu bat dagoen agertoki batean (baina DCSk irakur dezake), suebakiak edozein "idazketa" saiakera erregistra ditzake erregistro hauek segurtasun-eremuan BAKARRIK IRAKURTZEKO arau batekin.
- Beste agertoki batean, idazteko gai diren erregistro batzuk egon litezke, eta beste batzuk irakurtzeko soilik dira, baina IRAKURTZEKO BAKARRIK erregistro guztiak array bakarrean edukitzeak erraztu egiten du kontrolagailuan (edo suebaki batean) konfiguratzea.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	Errazagoa da kontroladorearen datuak funtzioaren arabera babestea (irakurtzea/idatzi/balioztatzea). Protokolo sentikorrak diren suebakiek beren lana errazten dute: arauak erraztu egiten dira, oso argi baitago zein erregistro-bloke dauden HMIk sartzeko baimenduta. Errazago kudeatzen ditu arauak (sinpleagoak). suebakia. Barne memoria aldi baterako baimenik gabeko aldaketak egitea erraza da ahultasun ustiagarria (By-pass Logiko Erasoa). PLC errutinen sarrerak eta irteerak behar bezala balioztatzen direnean, edozein aldaketa (aktore gaizto baten edo akatsen bidez) erraz atzeman daiteke sekuentzia logikoan egon beharrean, akatsak botatzeko / geroago exekuzioan arazoak sortu beharrean.
Fidagarritasuna	Irakurketak eta idazketak azkarrago egiten ditu transakzio kopurua delako murriztua. Baimendutako aldaketek eta programazio-akatsek matxura bat sor dezakete aldi baterako memoria babestuta ez badago. Mezu luzeetan sare- eta komunikazio-erroreek nahi gabeko akatsak sor ditzakete prozesatu aurretik datuen baliozkotasuna egiaztatzen ez bada.
Mantentzea	Programazio akatsak aldi baterako memorian idaztea eragiten duen akatsak aurkitzea zaila izan daiteke, beraz, arazoa saihestu daiteke idazketetarako erregistro espezifikoak esleituta.

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICSrako	**Taktika :** TA009 - Erantzun-funtzioa inhibitzea, TA010 - Prozesuaren Kontrola kaltetzea **Teknika:** T0835 - I/O irudia manipulatu , T0836 - Aldatu parametroa
ISA 62443-3-3	**SR 3.4 :** Softwarearen eta informazioaren osotasuna **SR 3.5 :** Sarreraren baliozkotzea **SR 3.6 :** Irteera determinista
ISA 62443-4-1	**SD-4:** Diseinu seguruaren praktika onenak **SI-1:** Segurtasunaren ezarpenaren berrikuspena **SI-2 :** Kodeketa estandarrak seguruak **SVV-1 :** Segurtasun-eskakizunen probak
ISA 62443-4-2	**CR 3.4 :** Softwarearen eta informazioaren osotasuna **CR 3.5 :** Sarreraren baliozkotzea **CR 3.6 :** Irteera deterministikoa
MITRE CWE	**CWE-787:** Mugetatik kanpo Idatzi **CWE-653:** Konpartimentazio nahikoa

11. Sinesgarritasuna egiaztatzeko tresna

Prozesua sinesgarritasuna egiaztatzeak ahalbidetzen duen moduan instrumentatzea, neurketa desberdinak gurutzatuta.

Segurtasun Helburua	Helburu-taldea
I/O balioen osotasuna	Produktu hornitzailea Integrazio / Mantentze Zerbitzu Hornitzailea

Orientazioa

Neurketak balioztatzeko sinesgarritasun fisikoa erabiltzeko modu desberdinak daude:

a) Neurketa integratuak eta denboraren arabera independenteak alderatu ditu

Sinesgarritasun-egiaztapenak denboraren araberako balioak integratuz edo bereiziz egin daitezke denbora-tarte batean eta denboraren araberako neurketarekin alderatuz.

b) Konparatu neurketa iturri desberdinak

Gainera, fenomeno bera modu ezberdinetan neurtzea sinesgarritasun egiaztapen ona izan daiteke.

Neurketa-iturri ezberdinek ez dute zertan sentsore fisiko desberdinak izan behar, baina komunikazio-bide alternatiboak erabiltzea ere esan nahi du (ikus adibideak).

Adibidea

a) Neurketa integratuak eta denboraren arabera independenteak alderatu ditu

- ÿ Neurtutako ponpa eta deposituaren maila-neurgailua: aldaketa bolumetrikoak emari integratua berdindu behar du.
- ÿ Erregailua galdara batean: gehitutako bero kalorikoa tenperatura igoera berdina izan beharko luke.

b) Konparatu neurketa iturri desberdinak

- ÿ Airearen abiadura, horizonte artifiziala, abiadura bertikala eta altitudea hegazkinean neurtzeko igoera/jaisten den hegazkinaren fenomenoa.
- ÿ Prozesuaren parametroen balioak datu-erregistratzaile independenteetatik (4-20 mA-ko begiztetan edo errele-kontaktuetan lotuta eta komunikazio-kanal independenteen bidez transmititzen dira) SCADA sistemaren datuekin (modu "normalean" datozen PLC eta HMI bidez) eta desbideratzeen eta nabarmen desaktibatzeari buruzko abisua ematea. -zehaztutako balioak.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	Balio manipulatuen jarraipena errazten du (sentsore guztiak aldi berean manipulatzen ez direla suposatuz).
Fidagarritasuna	Sarrera gisa hondatutako / okerreko neurketak onartzea eragozten du edo identifikatzen ditu (etorkizuneko ekintzak egiteko).
Mantentzea	Arinago baztertzen ditu hutsegiteen arrazoi fisiko posibleak.

Erreferentziak

Estandarra/esparrua Mapping Tactic:	
MITRE ATT & CK ICSrako	TA010 - Prozesuaren Kontrola kaltetu **Teknika:** T0806 - Brute Force I/O **SR 3.5:**
ISA 62443-3-3	Sarreraren baliozkotzea **SR 3.6:** Irteera deterministikoa **CR 3.5:** Sarreraren
ISA 62443-4-2	baliozkotzea **CR 3.6:** Irteera deterministikoa **CWE-754:** Ezohiko edo salbuespenezko
MITRE CWE	baldintzen egiaztapen desegokia

12. Sarrerak baliozkotzea sinesgarritasun fisikoan oinarrituta

Ziurtatu operadoreek prozesuan praktikoa edo fisikoki bideragarria dena soilik sar dezaketela.

Ezarri ebakuntza baten tenporizadorea fisikoki hartu beharko lukeen iraupenarekin. Kontuan izan desbideraketak daudenean abisatzea. Era berean, ohartarazi ustekabeko jarduerarik ez dagoenean.

Segurtasun Helburua	Helburu-taldea
I/O balioen osotasuna	Integrazio / Mantentze Zerbitzu Hornitzailea

Orientazioa

a) Aurreikusitako iraupen fisikoak kontrolatzea

Eragiketak uste baino denbora gehiago behar badu mutur batetik bestera joateko, horrek alarma bat merezi du. Bestela, azkarregi egiten badu, horrek ere alarma bat merezi du.

Irtenbide sinple bat urrats-denbora-abisua izan liteke. Hau erabilgarria izango litzateke sekuentzia/urratsez kontrolatutako zereginetarako.

Adibidez, "mugitu objektua A-tik B-ra" urratsak 5 segundo behar ditu urratsa hasten denetik trantsizio-baldintza (sentsorea: objektua B-ra iritsi den) betetzen den arte.

Baldintza nabarmen goizegi edo beranduegi betetzen bada, urrats-denbora-muga alerta abiarazten da.

b) Aurreikusitako jarduera fisiko errepikakorra kontrolatzea

Sinesgarritasun fisikoaren egiaztapenak fisikoki sinesgaitza den inaktibitaterako alerta ere esan dezake: gertakarien ziklo erregular eta errepikakorraren itxaropena badago (adibidez, loteak, eguneko ereduak), jarduerarik gabeko tenporizadore batek abisatu egingo du aldaketaren bat espero den zerbait (diskretua edo analogikoa). balioa) estatiko geratzen da denbora gehiegiz.

Adibidea

a) Aurreikusitako iraupen fisikoak kontrolatzea

- ÿ Presa bateko ateek denbora jakin bat behar izaten dute guztiz itxitatik guztiz irekitzera pasatzeko
  - ÿ Hondakin-uren zerbitzu batean, putzu heze batek denbora jakin bat behar du betetzeko

b) Aurreikusitako jarduera fisiko errepikakorra kontrolatzea

- ÿ Fabrikazio-prozesuak edo kanalizazio-bateak aldizka kontrol-barrutien artean zikloa egin behar du edo funtzionamendu moduak.
- ÿ Udal hondakin-uren araztegiek normalean eguneko jarduera-zikloa/eredua izaten dute eragin-emari-abiadurak.

c) Mugatu operadorearen sarrera ezarri puntuetarako praktiko/fisikoki posible dena.

- ÿ Adibidez, Oldsmar Florida kasuak operadorearen sarrera onartzen zuen, a) normalean behar zena baino milaka aldiz gehiago b) fisikoki ezinezkoa dena. Saiatu funtzionamendu-mugak PLC kodean konfiguratzen ahal den guztietan HMI script-ak erabili beharrean.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	**1.** Desbideratzeek eragingailu bat bidaia-egoera baten erdian zegoela edo norbait I/O-a faltsutzen saiatzen ari dela adieraz dezakete, adibidez, errepikapen-eraso bat eginez. **2.** Aktibitaterik gabeko alertak izoztutako edo behartutakoen jarraipena errazten dute sistema edo gailu manipulazioaren ondorio izan daitezkeen balio konstanteak.
Fidagarritasuna	**1.** Desbideratzeek alerta goiztiarra ematen dizute apurtutako ekipoengatik akats elektriko edo mekanikoak. **2.** Aktibitaterik gabeko abisuek neurketak edo sistemaren kontrol-begiztak markatzen laguntzen dute, gailu fisikoaren akatsengatik edo kontrol-algoritmo logikoarekin edo operadorearen sarrera huts/desegokiengatik huts egin dezaketen (beraz, estatikoak).
Mantentzea	

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICSrako	**Taktika:** TA010 - Prozesuaren Kontrola kaltetu **Teknika:** T0806 - Brute Force I/O **SR 3.5:**
ISA 62443-3-3	Sarreraren baliozkotzea **SR 3.6:** Irteera deterministikoa
ISA 62443-4-2	**CR 3.5:** Sarreraren baliozkotzea **CR 3.6:** Irteera deterministikoa
MITRE CWE	**CWE-754:** Ezohiko edo Salbuespenezko Baldintzen egiaztapen desegokia

13. Desgaitu behar ez diren / erabiltzen ez diren komunikazio atakak eta protokoloak

PLC kontrolagailuek eta sareko interfaze-moduluek, oro har, lehenespenez gaituta dauden hainbat komunikazio-protokolo onartzen dituzte. Desgaitu aplikaziorako beharrezkoak ez diren atakak eta protokoloak.

Segurtasun Helburua	Helburu-taldea
Gogortzea	Integrazio / Mantentze Zerbitzu Hornitzailea

Orientazioa

Lehenespenez gaitu ohi diren protokolo arruntak, adibidez, HTTP, HTTPS, SNMP, Telnet, FTP, MODBUS, PROFIBUS, EtherNet/IP, ICMP, etab.

Praktika onena PLCaren eta sistemako beste osagaien artean beharrezkoak diren komunikazioak irudikatzen dituen datu-fluxuaren diagrama bat garatzea da.

Datu-fluxuaren diagramak PLCko ataka fisikoak zein sare logikoetara konektatuta dauden erakutsi behar ditu. Portu fisiko bakoitzeko, beharrezkoak diren sare-protokoloen zerrenda identifikatu behar da eta gainerako guztiak desgaitu.

Adibidea

Adibidez, PLC askok web zerbitzari bat barne hartzen dute mantentze eta arazoak konpontzeko. Ezaugarri hau erabiliko ez bada, ahal bada, desgaitu egin beharko litzateke, eraso-bektore bat izan baitaiteke.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	Gaitutako ataka eta protokolo bakoitzak PLCaren balizko eraso-azalera gehitzen ditu. Erasotzaile batek baimenik gabeko komunikaziorako erabili ezin dituela ziurtatzeko modurik errazena horiek guztiz desgaitzea da.
Fidagarritasuna	PLC batek ezin badu ataka edo protokolo jakin baten bidez komunikatu, horrek (okerreko) trafiko-kopurua ere murrizten du, gaiztoa izan ala ez, eta horrek PLCa huts egiteko aukerak murrizten ditu nahi gabeko / gaizki osaturiko komunikazio-paketeengatik.
Mantentzea	Erabiltzen ez diren atakak eta protokoloak desgaitzeak mantentze-lanak ere errazten ditu, PLCaren konplexutasun orokorra murrizten duelako. Hor ez dagoena ez da administratu edo eguneratu beharrik.

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICSrako	**Taktika:** TA005 - Aurkikuntza **Teknika:** T0808 - Kontrol-gailuen identifikazio -zerbitzuaren , T0841 - Sarea eskaneatzea, T0854 - Serieko konexioen zenbaketa
ISA 62443-3-3	**SR 7.6:** Sarearen eta segurtasunaren konfigurazio-ezarpenak **SR 7.7:** Funtzionalitate txikiena
ISA 62443-4-2	**EDR 2.13 :** Diagnostiko eta probako interfaze fisikoen erabilera
ISA 62443-4-1	**SD-4:** Diseinu seguruaren praktika onenak **SI-1:** Segurtasunaren ezarpenaren berrikuspena **SVV-1:** Segurtasun-eskakizunen azterketa

14. Mugatu hirugarrenen datuen interfazeak

Mugatu konexio motak eta eskuragarri dauden datuak hirugarrenen interfazeetarako. Konexioak edo/eta datu-interfazeak ondo definitu eta mugatuta egon behar dira, beharrezkoa den datu-transferentziarako irakurtzeko/idazteko gaitasunak soilik baimentzeko.

Segurtasun Helburua	Helburu-taldea
Gogortzea	Integrazio / Mantentze Zerbitzu Hornitzailea

Orientazioa

Zenbait kasutan, kable luzeak edo datu-truke handia direla eta, interfazea duten datu-konexioek negozio-kasu hobea aurkezten dute bi alderdi ezberdinen arteko kable gogorreko datu-trukea baino.

Hirugarrenen datu-trukearen interfazea diseinatzean eta inplementatzen denean, jarraibide hauek kontuan hartu eta jarraitu behar dira praktikoa denean:

- ÿ Erabili komunikazio-modulu dedikatu bat, zuzenean 3. PLCra edo datuak trukatzeko ekipoetara zuzenean konektatuta, edo erabili sare-ekipo espezifiko bat alderdi bakoitzaren oinarrizko saretik fisikoki bereizita.

- ÿ Konektatutako gailuen MAC helbidea normalean sistema-aldagaietan eskuragarri dago ICS Ethernet-a gaitutako edozein gailurentzat, eta gailuaren identitatea faktore anitzeko ikuspegi batekin egiaztatzea ahalbidetzen du (IP helbidea + MAC egilearen kodea = gailu fidagarria). Praktika hau, zalantzarik gabe, ez da engainagarria, MAC eta IP helbideak faltsutu daitezkeelako, baina ICS sistema eta gailu fidagarrien arteko komunikazioei dagokienez muga igotzeko balio du.
- ÿ Hirugarrenen interfazeetarako protokolo bat hautatzerakoan, aukeratu protokoloa minimizatzen duen hirugarrenak jabearen sisteman datuak idazteko duen gaitasuna.
- ÿ Aukeratu hirugarrena izatea eragozten duen konexio-metodo bat eta konexio-ataka jabearen PLCa edo datuak trukatzeko ekipoak konfiguratzeko gai da.
- ÿ Hirugarrenak ezin izango luke irakurri edo idatzi esplizituki izan ez den daturik zehaztu eta eskuragarri jarri.
- ÿ Erabili watchdog tenporizadore bat komunikazioa kontrolatzeko, komandoak a-ra bidali ez daitezen PLC matxura moduan.
- ÿ Serie-konexioa: Erabili komunikazio-modulu dedikatu bat hirugarrenen interfaze bakoitzeko datu-sorta mugatu batekin. Ziurtatu konexioaren jabearen aldea abiarazlea dela eta hirugarrena erantzuntzailea dela.

- ÿ Ethernet/IP: PLC batzuek komunikazio-moduluek suebaki gisa funtzionatzea ahalbidetzen dute eta Deep Packet Inspection (DPI) egin dezakete, edo komunikazio-moduluen interfazeak mugatu ditzakete datu-trukea aurrez definitutako azpimultzo batera mugatzeko. Ezaugarri hauek erabilgarri badaude eta Ethernet/IP protokolo bat erabiltzen bada, ziurtatu funtzioak gaituta eta konfiguratuta daudela.
- ÿ Eragiketa- edo kontratu-baldintzek jabeari eragozten diotenean aurreko elementuak, kontuan hartu "datuen kontzentratzaile" (proxy/DMZ) PLC bereizi bat erabiltzea datuak gordetzeko eta jabea hirugarrenen nahi ez diren idazketa/programazioetatik babesteko. Ziurtatu PLC honen atzeko planoa ezin dela hirugarrenen saretik zeharkatu.

Adibidea

ÿ Transferentzia eta kontagailuak dituzten Pipeline edo Lease Automatic Custody Transfer (LACT) unitateak hidrokarburoak edo ura ekoizten duten edo kanalizazio-enpresa baten eta sare edo serie-interfazedun konexioak dituzten kanalizazio-enpresa baten eta enpresen artean neurketa, egoera eta baimen-informazioa partekatzen duten korronte erdiko enpresa baten artean.

ÿ Eskualdeko ur edangarriaren hornitzaileak (inportatzaileak) hornitzen ari den ur-emaria partekatzen du tokiko udal baten ur plantara.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	1. Mugatu esposizioa hirugarrenen sare eta ekipoetarako. 2. Autentifikatu kanpoko gailuak faltsutzea ekiditeko.
Fidagarritasuna	Nahita edo nahi gabe aldaketak egiteko edo hirugarrenen kokapen edo ekipoetatik atzitzeko gaitasuna mugatzen du.
Mantentzea	

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICS	**Taktika:** TA010 - Prozesuaren Kontrola kaltetu **Teknika:** T0836 - Parametroa aldatu
ISA 62443-3-3	**SR 7.6:** Sarearen eta segurtasunaren konfigurazio-ezarpenak **SR 7.7:** Funtzionalitate txikiena
ISA 62443-4-2	**CR 7.6:** Sarearen eta segurtasunaren konfigurazio-ezarpenak **CR 7.7:** funtzionalitate txikiena
ISA 62443-4-1	**SD-4:** Diseinu seguruaren praktika onenak **SI-1:** Segurtasunaren ezarpenaren berrikuspena **SVV-1:** Segurtasun-eskakizunen azterketa

15. Definitu prozesu-egoera seguru bat PLC berrabiarazten bada

Definitu prozesurako egoera seguruak PLC berrabiarazten direnean (adibidez, kontaktuak dinamizatzea, desaktibatu, aurreko egoera mantendu).

Segurtasun Helburua	Helburu-taldea
Erresilientzia	Produktu hornitzailea Integrazio / Mantentze Zerbitzu Hornitzailea

Orientazioa

Zerbaitek PLC bat lan-prozesu baten erdian berrabiarazteko agintzen badu, programak ondo hastea espero beharko genuke prozesuari etenaldi minimo batekin. Ziurtatu kontrolatzen duen prozesua berrabiarazteko segurua dela.

PLCa seguru berrabiarazteko konfiguratzea ez bada praktikoa, ziurtatu gertakari horren berri ematen dizula eta ez duela komando berririk igortzen. Era berean, kasu horretarako, ziurtatu Eragiketa Prozedura Estandarrak (SOP) eskuzko kontrolak ezartzeko argibide oso argiak dituela, PLCak prozesua behar bezala abiarazi dezan.

Era berean, dokumentatu abiarazteko, itzaltzeko, egoera egonkorreko kontrol eta hegan kontrolatzeko sistema berrabiarazteko prozedura guztiak.

Adibidea

/

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	**Ustekabeko jokabide potentzialak kentzen ditu:** PLC baten eraso-bektorerik oinarrizkoena kraskatzea eta/edo berrabiaraztea behartzea da. PLC askorentzat ez da hain zaila egitea, PLC askok ezin baitute ondo aurre egin ustekabeko sarrera edo trafiko gehiegiri. Exekutatzen ari den bitartean kontrolagailuen ekintzei buruzko hainbat diagnostiko dauden arren, abian abian den prozesu batekin abiarazteari nola kudeatzen duen ez dago argi. Hau ezohikoa izan daiteke, baina oinarrizko eraso-bektorea da erasotzaile baten portaera gaiztoa kontuan hartzen badugu.
Fidagarritasuna	**Saihestu ustekabeko atzerapenak:** PLCa piztu ondoren, egoera-makina prozesua hasten uzten ez duten baldintza batzuekin hasieratzen bada eta operadoreak sistema normalizatu ezin badu, teknikari batek PLC programan sartu beharko luke baldintzak behartzeko. nahi den egoerara funtzionatzen hasi ahal izateko. Horrek atzerapenak eta ekoizpen-galerak eragin ditzake.
Mantentzea	/

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICS	**Taktika:** TA009 - Inhibit Erantzun Funtzioa **Teknika:** T0816 - Gailua Berrabiarazi/Itzaltzea
ISA 62443-3-3	**SR 3.6:** Irteera deterministikoa
ISA 62443-4-2	**CR 3.6:** Irteera deterministikoa
ISA 62443-4-1	**SVV-1:** Segurtasun-eskakizunen azterketa

16. Laburtu PLC ziklo-denborak eta joera horiek HMIn

Laburtu PLC zikloaren denbora 2-3 segundoz behin eta jakinarazi HMI-ri grafiko batean bistaratzeko.

Segurtasun Helburuen	Helburu-taldea
Jarraipena	Integrazio / Mantentze Zerbitzu Hornitzailea

Orientazioa

Ziklo-denborak PLC bateko sistema-aldagaiak izan ohi dira eta PLC kodean laburtzeko erabil daitezke.
Laburpena egin behar da batez bestekoa, gailurra eta gutxieneko ziklo-denborak kalkulatzeko. HMI-k balio horien joerak eta aldaketa nabarmenak egonez gero abisatu beharko luke.

Ziklo-denbora PLCaren logikaren iterazio bakoitza kalkulatzeko behar den denbora da. Iterazioak Ladder Diagrams (LD), Function Block Diagrams (FBD), Instruction List (IL) eta Structured Text (ST) konbinazioak dira. Osagai logiko hauek Funtzio Sekuentzial Diagramak (SFC) batera daitezke.

Ziklo-denborak konstanteak izan behar dira PLC batean, adibidez, aldaketarik egon ezean

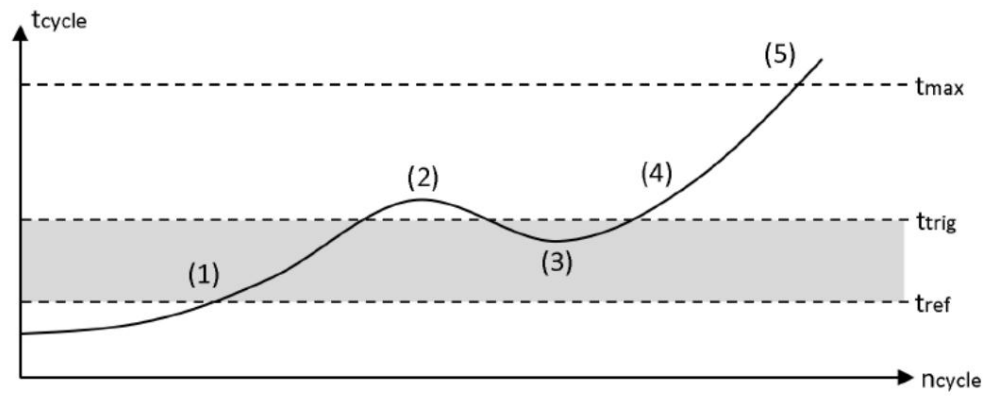
- sare-ingurunea
- PLC logika
- prozesua

Hori dela eta, ezohiko ziklo-denbora aldaketak PLCren logika aldatu izanaren adierazle izan daitezke eta, beraz, informazio baliotsua eskaintzen dute osotasuna egiaztatzeko.

Grafiko bat erabiliz denboran zehar balioak bistaratzeak modu intuitiboa eskaintzen du balio absolutuak soilik izateagatik antzematea zailago litzatekeen anomaliei arreta erakartzeko.

Adibidea

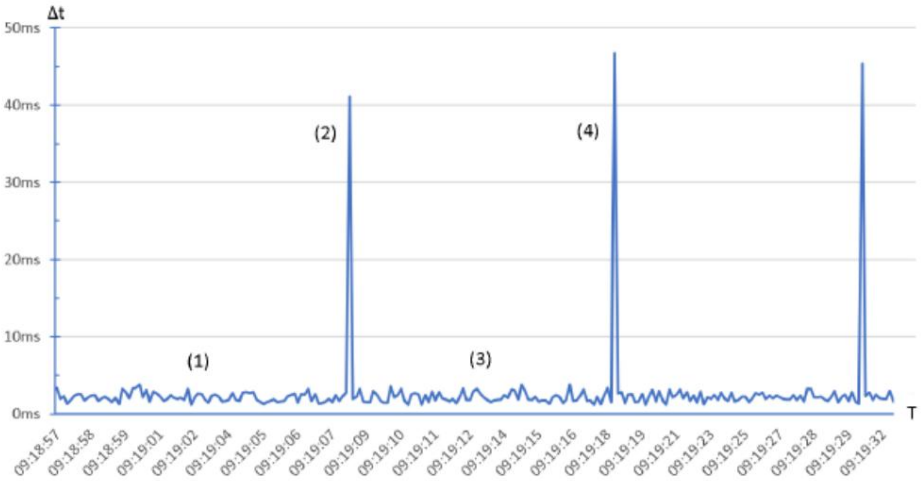
PLC askok "ziklo-denbora maximoa" monitorizatzen dute hardware mailan. Ziklo-denborak gehienezko balioa gainditzen badu, hardwareak CPU STOP (5) ezartzen du.
Jakina, erasotzaileak horretaz jakitun dira eta balizko eraso-kode bat ahalik eta leunena mantenduko dute, ziklo-denbora orokorrean eragina gutxitzeko. Softwarearen ziklo-denbora monitorizatzeko programa gehigarri batean, erreferentzia-ziklo-denbora tref oinarrizko ziklo-denbora gisa definitzen da. Gorabehera txikiak naturalak direnez, atalase onargarri bat definitu behar da (1,3) Zikloaren jarraipena abiarazten da, atalasea gainditzen bada (2,4).



Erreferentzia-denboratik edozein desbideratzea honelako erregistro-fitxategi batean gorde daiteke:

SeqNo	Date	UTC Time	Abweichung
1	2019-11-22	09:05:50.021	40,821ms
2	2019-11-22	09:06:00.069	44,391ms
3	2019-11-22	09:06:10.120	44,994ms
4	2019-11-22	09:06:20.166	40,561ms
5	2019-11-22	09:06:30.211	40,725ms

Ziklo-denborak HMI-ra jotzen badira, PUZaren karga astunak ikus daitezke begirada batean. Ondorengo adibide-diagramak PLC-Programa bat erakusten du aldian-aldian exekutatzen den kode gaiztoa duena. (1,3) ziklo-denboraren gorabehera onargarriak ("zarata") erakusten ditu funtzionamendu arruntean, eraso-kodea (2,4) exekutatzen da eta horrek ziklo-denbora handitzen du.



Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	PLCen aurkako erasoen artean, logika aldatzea, programa berri bat aktibatzea, kode berria probatzea, prozesu-errezeta berri bat kargatzea, logika osagarria sartzea mezuak bidaltzeko edo funtzioren bat aktibatzeko. PLC gehienentzat, osotasun kriptografikoen egiaztapen tradizionalak ez dira bideragarriak. Hala ere, komeni da goiko logikaren aldaketaren bat gertatzen bada abisatzea. Ziklo-denborak nahiko konstanteak direnez egoera normalean, ziklo-denbora aldaketak goiko osagai logikoetako batean logika aldatu izanaren adierazle ona dira.
Fidagarritasuna	Ikusi segurtasuna, baina kausa ez-maltzurengatik.
Mantentzea	/

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICS	**Taktika:** TA002 - Exekuzioa **Teknika:** T0873 - Project File Infection **SR 3.4:**
ISA 62443-3-3	Softwarea eta informazioaren osotasuna
ISA 62443-4-2	**EDR 3.2:** Kode maltzurren aurkako babesa
MITRE CWE	**CWE-754:** Ezohiko edo Salbuespenezko Baldintzen egiaztapen desegokia

17. Erregistratu PLCaren funtzionamendu-denbora eta joera HMIn

Erregistratu PLC-ren funtzionamendua noiz berrabiarazi den jakiteko. Joera eta erregistro-denbora HMIan diagnostikoetarako.

Segurtasun Helburuen	Helburu-taldea
Jarraipena	Integrazio / Mantentze Zerbitzu Hornitzailea

Orientazioa

Egin jarraipena PLC-ren denboraren jarraipena

- PLCan bertan (funtzio-denbora PLCan sistema aldagai bat bada)
- PLCan bertan MIB-2 / SNMP inplementazioren bat badu

ÿ kanpotik, adibidez, SNMP bidez

PLCak MIB-2-rekin SNMP badu, oso ohikoa dena, funtzionamendurako OID "sysUpTimeInstance(0)" 1.3.6.1.2.1.1.3 da. Eguneko denbora berrezartzeak PLC berrabiarazteko adierazle garrantzitsuak dira. Ziurtatu HMIak edozein PLC berrabiarazteko abisatzen duela.

Errore-kodeekin erlazionatutako funtzionamendu-denbora diagnostiko onak dira.

Adibidea

/

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	PLC baten eraso-bektorerik oinarrizkoena kraskatzea eta/edo berrabiaraztea behartzea da. PLC askorentzat ez da hain zaila egitea, PLC askok ezin baitute ondo aurre egin ustekabeko sarrera edo trafiko gehiegiri. Horrela, ustekabeko berrabiarazteak PLCak ezohiko ekintzak topatzen dituen adierazle izan daitezke.
Fidagarritasuna	PLC berrabiarazteko ere onak dira hutsegiteen kasuan diagnostikatzeko eta zein PLCtan lan egiten den zein ordutan kontrolatzeko.
Mantentzea	/

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICS	**Taktika:** TA009 - Inhibit Erantzun Funtzioa **Teknika:** T0816 - Gailua Berrabiarazi/Itzaltzea
ISA 62443-3-3	**SR 7.6:** Sarearen eta segurtasunaren konfigurazio-ezarpenak
ISA 62443-4-2	**CR 7.6:** Sarearen eta segurtasunaren konfigurazio-ezarpenak
MITRE CWE	**CWE-778:** Erregistro eskasa

18. Erregistratu PLC geldialdi gogorrak eta joera horiek HMIan

Gorde PLC akatsen edo itzaltzeen gertaerak HMI alarma-sistemek berreskuratzeko, PLCa berrabiarazi aurretik kontsultatzeko. Denbora sinkronizatu datu zehatzagoak lortzeko.

Segurtasun	Helburu-taldea
Jarraipena	Integrazio / Mantentze Zerbitzu Hornitzailea

Orientazioa

Matxura-gertaerek PLC bat zergatik itzali den adierazten dute, arazoa berrabiarazi aurretik konpondu ahal izateko.

PLC batzuek errore-kodeak izan ditzakete PLCak akatsa izan duen edo gaizki itzali den azken kasuko.
Grabatu akats horiek eta gero garbitu. Ideia ona izan daiteke akats horiek HMI-ri informazio-datu gisa edo agian syslog zerbitzari bati jakinaraztea, ezaugarri horiek eta azpiegitura hori existitzen badira.

PLC gehienek ere gertaerak sortzen dituzten lehen eskaneatu eginbideren bat dute. PLC ekipamendu ia guztiek moduren batean duten portaera da. Funtsean, bandera bat edo gehiago da, edo "esnatu ondoren" PLC baten lehen eskanean exekutatzen den errutina izendatua. Lehen eskaneatu hau erregistratu eta jarraitu behar da.

Adibidea

/

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	Erregistroek arazoak konpontzea ahalbidetzen dute gorabeheraren bat izanez gero. PLC bat martxan jarri aurretik, batez ere arazoak izan ondoren, garrantzitsua da fidagarria dela ziurtatzea.
Fidagarritasuna	Erregistroak ere iturri onak dira arazketarako, gertaera maltzurrez sortu ez bada.
Mantentzea	/

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICS	**Taktika:** TA009 - Inhibit Erantzun Funtzioa **Teknika:** T0816 - Gailua berrabiarazi/Itzali 1
ISA 62443-3-3	**SR 7.6:** Sarearen eta segurtasunaren konfigurazio-ezarpenak
ISA 62443-4-2	**CR 7.6:** Sarearen eta segurtasunaren konfigurazio-ezarpenak
MITRE CWE	**CWE-778:** Erregistro eskasa

19. Monitoreatu PLC memoriaren erabilera eta joera HMIn

Neurtu eta eman memoria-erabileraren oinarria produkzio-ingurunean inplementatutako kontrolagailu bakoitzeko eta joera HMI-n.

Segurtasun Helburua	Helburu-taldea
Jarraipena	Integrazio / Mantentze Zerbitzu Hornitzailea Aktiboen jabea

Orientazioa

Kode-lerroak logikan handitzeak exekuzioan memoria-kontsumoa areagotzea ekar dezakeenez, PLC programatzaileei gomendatzen zaie oinarrizko lerrotik edozein desbideraketa jarraitzea eta gertaera honi alarma-klase bat eskaintzea.

Adibidea

Rockwell Allen Bradley PLC-etan, oinarrizko lerro bat ezar daiteke kontrolagailu batean eta memoriaren erabileraren jarraipena egin daiteke RSLogix 5000 Task Monitor Tool erabiliz. Memoria nagusia ez ezik, I/O memoria eta Ladder/Tag memoria ere jarrai daitezke joerak erabiliz.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	Memoria-erabilera handitzea aldatutako kodea exekutatzen ari den PLCaren adierazle izan daiteke.
Fidagarritasuna	Exekutatzen diren programen memoria-erabileraren jarraipena erabilgarria izan daiteke PLC kontrolagailuaren memoria-kontsumo osoa eta akats-egoera saihesteko.
Mantentzea	Memoriaren erabileraren jarraipena kontrolatutako kontrolagailuaren eskaneaketa denbora onena sintonizatzeko eta aurkitzeko erabil liteke, baina baita egoera akastunekin lotutako arazoak eta arazoak konpontzeko ere.

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICS	**Taktika:** TA002 - Exekuzioa **Teknika:** T0873 - Project File Infection **SR 3.4:**
ISA 62443-3-3	Softwarea eta informazioaren osotasuna
ISA 62443-4-2	**EDR 3.2:** Kode maltzurren aurkako babesa

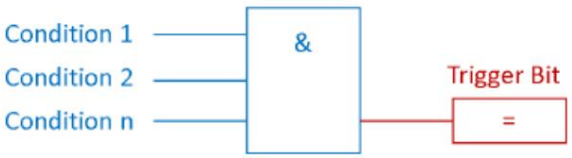
20. Harrapatu negatibo faltsuak eta positibo faltsuak alerta kritikoetarako

Identifikatu alerta kritikoak eta programatu alerta horientzako tranpa bat. Ezarri tranpa edozein desbiderapenen abiarazte-baldintzak eta alerta-egoera kontrolatzeko.

Segurtasun	Helburu-taldea
Jarraipena	Integrazio / Mantentze Zerbitzu Hornitzailea

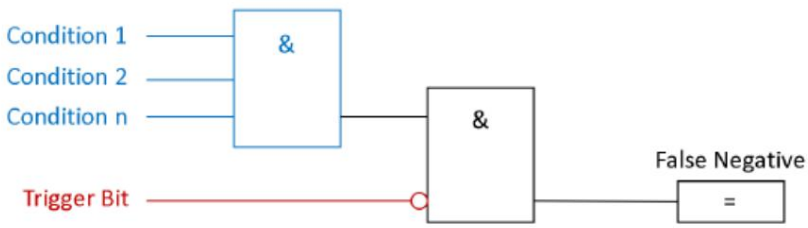
Orientazioa

Kasu gehienetan, alerta-egoerak boolearrak dira (Egia, Gezurra) eta behean bistaratzen diren baldintza jakin batzuek abiarazten dituzte. Esaterako, alertaren 'gainpresioa'ren abiarazle-bita EGIA bihurtzen da, 1. Baldintza 'Presio-etengailua 1', 2. Baldintza 'Presio-sentsorearen atalase kritikoaren gaineko balioa', n. bidez, EGIA bada.



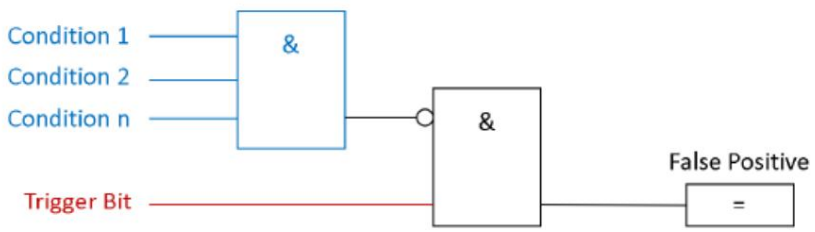
Eraso bat ezkutatzeko, etsai batek alerta-abiarazlearen bit-a kendu eta negatibo faltsu bat eragin dezake.

Negatibo faltsuentzako tranpa batek abiarazte-bitaren eta abiarazle-bitaren beraren baldintzak kontrolatzen ditu. Konfigurazio sinple honekin, negatibo faltsu bat detektatzen da. Ikusi hurrengo irudia:



Beste kasu batzuetan, aurkari batek positibo faltsuak eragin ditzake nahita, prozesuko operadorearen arreta gutxitzeko.

Negatibo faltsuko tranparen era berean, positibo faltsuak ere detekta daitezke alerta-abiarazle-bitaren jarraipena eginez eta abiarazte-baldintzak betetzen badira. Baldintzak EZ badira betetzen, baina abiarazte-bita aktibo badago, positibo faltsu bat detektatzen da: Ikusi argazki hau:



Adibidea

1. adibidea: Siemens-ek bere Siemens S7-1200/1500 produktuetan funtzio ugari dituen Web zerbitzari bat eskaintzen du, adibidez PLC-egoera, ziklo-denbora edo esparru-erregistroak bistaratzea. Datu-taulak eta aldagaiak ikusteko eta aldatzeko aukera ere badu. Webzerbitzarirako sarbide-eskubideak PLC-Hardware ezarpenetan alda daitezke. Gaizki konfiguratutako sarbide-eskubideen kasuan, aurkari batek PLC aldagai eta datu-blokeetarako sarbidea lor dezake. Positibo faltsu bat sortzeko, aurkariak alerta-abiarazle-bit bat hautatzen du eta egoera aldatzen du.

2. adibidea: Triton/Trisys/HatMan erasoan, kode maltzurrak alerta-egoerak kendu zituen.

3. adibidea: autobus-injekzioaren eraso batek alerta positibo faltsu bat bidal diezaioke maila altuko SCADA bezero bati.

Zergatik?

Onuragarria...?	Zergatik?
Segurtasuna	Aurkari batek erasoa nahastu izanak eragindako alerta-mezuen negatibo faltsuak edo positibo faltsuak arintzen ditu (adibidez, kode maltzurra, autobus-injekzioa, seguru gabeko web-zerbitzarietan PLC eskuragarri dauden egoera-taulak manipulatzea).
Fidagarritasuna	/
Mantentzea	/

Erreferentziak

Kartografia estandarra/esparrua	
MITRE ATT & CK ICS	**Taktika :** TA009 - Inhibit Erantzun Funtzioa **Teknika:** T0878 - Alarma kentzea **SR 3.5 :**
ISA 62443-3-3	Sarreraren baliozkotzea
ISA 62443-4-2	**CR 3.5 :** Sarreraren baliozkotzea
ISA 62443-4-1	**SI-1 :** Segurtasunaren ezarpenaren berrikuspena
MITRE CWE	**CWE-754:** Ezohiko edo Salbuespenezko Baldintzen egiaztapen desegokia

Secure PLC Programazio proiektuari buruz

Urte askotan, Kontrolatzaile Logiko Programagarriak (PLC) ez dira seguruak izan diseinuagatik. Hainbat urtetan ITtik praktika onak pertsonalizatzen eta aplikatzean, protokolo seguruak, komunikazio enkriptatuak, sarearen segmentazioa eta abar sortu ziren. Hala ere, orain arte, ez da arreta jarri PLC-en (edo SCADA/DCS) ezaugarriak segurtasunerako erabiltzean. edo nola programatu PLCak segurtasuna kontuan hartuta. Proiektu honek, lehendik dauden ITrako Kodetze Praktika Seguruetan inspiratua, hutsune hori betetzen du.

Nork irakurri eta ezarri beharko lituzke Secure PLC Kodetze Praktika?

Praktika hauek ingeniarientzat idatzi dira. Proiektu honen helburua softwarea sortzen ari diren ingeniariei jarraibideak ematea da (eskailera-logika, funtzio-diagramak, etab.) Industria Kontrol Sistemen segurtasun-jarrera hobetzen laguntzeko. Praktika hauek PLC/DCS-n natiboki eskuragarri dauden funtzionalitateak baliatzen dituzte. Praktika hauek ezartzeko software-tresna edo hardware gehigarri gutxi behar dira.
Guztiak PLC programazio eta funtzionamendu-fluxu arruntean sartu daitezke. Praktika horiek ezartzeko segurtasun-esperientzia baino gehiago, babestu beharreko PLCen, haien logika eta azpiko prozesuaren ezagutza ona behar da.

Zein da zerrenda hau bada / nola definitzen duzu PLC Kodeketa?

20 Secure PLC Kodetze praktiken zerrendaren esparrura egokitzeko, praktikek PLC batean zuzenean egindako aldaketak izan behar dituzte. Dokumentu honetan ikusten duzuna PLC kodetze-jardunbide seguruen kopuru handiagoaren Top 20 aukeraketa bat da. Arkitektura orokorrari, HMIei edo dokumentazioari buruzko zirriborro-praktika osagarriak ere badaude. Horiek ez dute PLC kodetze seguruaren esparrura egokitzen, baina etorkizuneko zerrenda batean egon litezke PLC ingurune seguruan.

Zeintzuk dira PLC Kodetze Praktika Seguruak aplikatzearen onurak?

Praktika hauek erabiltzeak segurtasun-onurak ditu, batez ere eraso-azalera murriztea edo segurtasun-intzidentziaren bat gertatuko balitz arazoak azkarrago konpontzea ahalbidetzea. Hala ere, praktika askok segurtasunaz harago abantaila gehigarriak dituzte. Batzuek PLC kodea ere fidagarriagoa egiten dute, arazketa errazagoa eta mantendu, komunikatzeko errazagoa eta, agian, leunagoa ere. Gainera, PLC kodetze praktika seguruek erabiltzaileei erasotzaile gaizto bat izanez gero laguntzeaz gain, PLC kodea sendoagoa egiten dute ustekabeko konfigurazio okerrak edo giza akatsak jasateko.

Nor dago proiektu honen atzean?

Jake Brodsky-ren S4x20 hitzaldiarekin hasi zen dena “Secure Coding Practices for PLCs”.

Konferentziaren ostean , Dale Petersonek Top 20 proiektuari hasiera eman zion. Jake Brodskyk eta Sarah Fluchsek hainbat ordu eman zituzten telefonoz Jake-k proposatutako PLC kodetze praktika seguruak paperera eramateko. Ondoren, Dale, Jake eta Sarah plataforma bat sortu zuten top20.isa.org webgunean, ISA GCA-k lagunduta, ICS segurtasunaren eta ingeniarien komunitateen ekarpen gehigarriak egituratzeko eta biltzeko.

Praktikako testuen eztabaidak eta finkatzeak eta Top 20 praktika garrantzitsuenen zerrenda osatzeak urtebete inguru behar izan zuen; prozesua bizkortu zuen Vivek Ponnadak eta horrek ekarpena egiteaz gain eta edukia berrikusiz, ohiko deiak ere antolatu zituen praktikei buruzko iruzkin guztiak konpondu arte, Mohamed Abdelmoez Sakesli-k estandar-erreferentzia guztiak gehitu zituen ahalegin handi batean, MITRE CWE taldeak azken momentuan CWE erreferentziak eman zituena, Sarahk zuk dokumentua bildu zuena. irakurtzen ari dira orain, eta Jake, Dale, John Cusimano, Dirk Rotermund, Josh Ruff, Thomas Rabenstein, Gus Serino, Walter Speth, Agustin Valencia Gil-Ortega, Marcel Rick-Cen eta Al Ratheesh R, ohiko deialdietan ekarpenak eman zituztenak. .

Laguntzaileen zerrenda

Secure PLC Kodetze Proiektua komunitatearen benetako ahalegina da eta izaten jarraitzen du, eta ezinezkoa izango zen ekarpen ugarik eskuzabaltasunez beren denbora eta PLC/segurtasun ezagutzak partekatu gabe. Guztira 943 Erabiltzaile erregistratu dira plataforman eztabaidatzeko eta ekarpenak egiteko. Hona hemen izendatzea espresuki onartu zuten guztien zerrenda alfabetikoa. Eskerrik asko proiektu hau laguntzeko denbora hartu duzuen guztioi!

Aagam Shah

Adam Paturej

Agustin Valencia Gil-Ortega

Aitor Garcia Alminana

Alec Summers

Al Ratheesh. R

Andreas Falk

Anton Shipulin

Arkaitz Gamino

carlos olave

Chris van den Hooven

Chris Sistrunk

Christos Alexopoulos

Cris DeWitt

Dale Peterson

Dene Yandle

Dennis Verschoor

Dirk Rotermund

Edorta Echave García

Gananand Kini

George Alex Holburn

Gus Serino

Josie Houghton

Jozef Sulwinski

Juan Pablo Angel Ispilua

Khalid Ansari |

Marc Weber

Marcel Rick-Cen

Martin Huddleston

Massimiliano Zonta

Matthew Loong

Matthew Mueller

Michael Thompson

Michal Stepien

Miguel Angel Frias

Mohamed Abdelmoez Sakesli

Ilargia Eluvangal Chandran

Nahuel Iglesias

Nalini Kanth

Narasimha S. Himakuntala

Omar Morando

Oscar J. Delgado-Melo

Päivi Brunou

Peter Donnelly

Hakija Agic

Hector Medrano

Heiko Rudolph

Isiah Jones

Jacob Brodsky

Javier Perez Quezada

JD Bamford

Joe Weiss

John Cusimano

John Hoyt

John Powell

John Kingsley

Joseph J. Januszewski

Josh Ruff

Peter Jackson

Ravindra Deshakulakarni

Rick Booij

Robert Albach

Rushi Purohit

Sarah Fluchs

Sergei Biberdorf

Stephan Beirer

Steve Christey Coley

Thomas Rabenstein

Tim Gale

Vivek Ponnada

Vytautas Butrimas

Walter Speth

Esker bereziak proiektu-taldeari erabiltzeko azpiegitura eskuzabal eskaini dieten erakunde hauei, hala nola domeinuak, hostinga eta web diseinua eta diseinu grafikoa: