

PLC kodetze-praktika seguruuenak 20



PLC kodetze praktika seguruak - Top 20 zerrenda

ZENTROA
ZIBERSEGURTASUNA
INDUSTRIALA



EDIZIOA
GAZTELANIA

ZENTROA ZIBERSEGURTASUNA INDUSTRIALA



Zibersegurtasun Industrialerako **Zentroa** (CCI) irabazi-asmorik gabeko erakunde independente bat da, eta bere eginkizuna Zibersegurtasun Industriala sustatzea eta hobetzen laguntzea da, fabrikazioa edo energia bezalako sektoreetako erakundeek eraikuntzan zeregin garrantzitsua duten testuinguru batean. egungo gizartearena, ongizate estatuaren atrezzo gisa.

CCIk erronka horri aurre egiten dio ikerketa eta analisi jarduerak garatuz, iritziak sortuz, azterketak eta tresnak prestatu eta argitaratzen eta informazio eta ezagutza trukatzearen bidez, bi teknologien eraginari buruz, haien prozesu eta praktikak barne, eta baita ere. norbanakoak, Ziberespazioan industria-prozesuak eta azpiegiturak integratzearren ondoriozko arriskuei -eta horien kudeaketa- aldean.

CCI da, gaur egun, Zibersegurtasun Industrialarekin kaltetutako, kezkatuta edo lanpetuta dauden entitateen -pribatu zein publiko- eta profesionalen ekosistema eta topagunea; eta erdal erreferentea da, halaber, esperientziak trukatzeko eta arlo horretan diharduten sektoreak biziberritzeko.



Lan honen edozein erreprodukzio, banaketa, komunikazio publiko edo eraldaketa erabat debekatuta dago eta legeak ezarritako zigorrak ezarriko ditu. Egilea bakarrik (Industrial Cybersecurity Center, www.CCI-es.org), edozein zatiren fotokopia edo eskaneatzea baimen diezaiekezu bertan interesa duten pertsonei.

TOP 20 SEGURA PLC KODEA PRAKTIKAK



Ingeniariek ingeniarientzat idatzia.

Proiektu honen helburua softwarea sortzen ari diren ingeniariei (eskailera-logika, funtziografikoak, etab.) orientazioa ematea da, industria-kontrol-sistemen segurtasun-jarrera hobetzen laguntzeko.

Praktika hauek PLC/DCS-n natiboki eskuragarri dauden funtzionaltasunaz baliatzen dira. Praktika hauek ezartzeko hardware edo software-tresna gehigarri gutxi behar dira. Guztiak PLC programazio arruntean eta lan-fluxu operatiboan sartu daitezke. Segurtasun-esperientzia baino gehiago, babestu beharreko PLCak, haien logika eta azpiko prozesua ondo ezagutzea beharrezkoa da praktika horiek ezartzeko.

PLC seguruen kodetze-praktika onenen zerrendaren esparruan sartzeko, praktikek PLC batean zuzenean egindako aldaketak izan behar dituzte.

Horregatik guztiagatik, proiektu honek praktika hauek guztiei hizkuntza ezberdinetan eman diezaieketen beste entitate eta profesional batzuekin lankidetzan aritzeko beharra ikusten du eta kasu honetan, **Zibersegurtasun Industrialerako Zentroarekin** batera, hau emateko batu direnek. agiria gaztelaniaz .erdal komunitate osora heltzeko.

aurkibidea

1. PLC KODEA MODULARIZATU

7

PLC kodea modulueta banatu, funtziobloke desberdinak erabiliz (azpirutina). Probatu moduluak modu independentean.

2. JARRAITU ERAGIKETA MODUEI

10

Mantendu PLCA RUN moduan. PLCAk RUN moduan ez badaude, alarma bat egon beharko luke operadoreentzat.

3. Utzi LOGIKA ERAGILEA PLCAN Ahal den guztietan Logika operatibo gehiena, totalizazioa edo integrazioa adibidez, zuzenean PLCan. HMIak ez du behar adina eguneraketa jasotzen ondo egiteko

13

4. PLC ADIERAZLEAK ERABILI OSOTASUNA EGITEKO BEZALA

17

Jarri kontagailuak PLCareen errore-banderetan matematika-arazoak harrapatzeko.

5. EGIN KRIPTOGRAFIKO OSOTASUN EGITEKO EGITEKO EGITEKOA ETA/EDO PLC KODEAREN KONTROLAZIOA

20

Kriptografikoak, edo hash kriptografikoak erabilgarri ez badaude, PLC kodearen osotasuna egiazatzeko eta alarma bat pizteko aldatzen direnean.

6. TEMPORIZADOREAK ETA KONTATZAILEAK BALIOZTU

26

Temporizadoren eta kontagailuen balioak PLC programan idazten badira, PLCAk balioztatu beharko ditu arrazoizkoak direla egiazatzeko eta zero azpiko atzerako kontaketarik dagoen egiazatzeko.

AHOLKUA:

Oin-oinean edo orrialde-zenbakian klik eginez aurkibidera itzultzen zara
Alt+ezkerreko gezia hiperesteka batera joan ondoren aurreko ikuspegira itzultzeko.

**7. BALIOZTU ETA ALERTA PAREKATUTAKO SARRERA/IRTEERAK**

29

Parekatutako seinaleak badituzu, ziurtatu bi seinaleak batera ez daudela baiezatzen.

Eragileari alarma ematen dio fisikoki bideragarriak ez diren sarrera/irteera egoerak gertatzen direnean. Demagun parekatu seinaleak independenteak izatea edo atzerapen-temporizadoreak gehitza irteerak aldatzea eragingailuentzat kaltegarria izan daitekeenean.

8. SARRERA-ALDAGAIAK BALIOZTU

33

HMI PLC MAILAN, EZ HMIAN BAKARRIK

HMI PLC aldagaietarako sarbidea HMIn baliozko balio operatibo batzuetara mugatu daiteke (eta behar da), baina beste egiatzapen gurutzatu batzuk gehitu behar dira PLCan, tarte onargarrietatik kanpoko balioak saihesteko edo ohartarazteko. HMian programatuta daudenak.

9. ZUZENDARITZAK BALIOZTU

38

Baliozkotu zeharkaketak array-aren muturrak pozoituz hesi-zutoinetan akatsak hautemateko.

10. FUNTZIOAREN ARABERA IZENDUTAKO ERREGISTRO

44

BLOKEAK ESLEITU (IRAKURRI / IDATZI / BALIOA)

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

11. TRESNAK SINDEGARRITASUNA EGITEA

49

Prozesua neurketa desberdinak gurutzatuz egiatzatzea ahalbidetzen duen modu honetan.

12. SARRERAK BALIOZTU SINTETASUN FISIKOAN OINARRITUTAKO

52

Ziurtatu operadoreek praktikoa edo fisikoki bideragarria dena soilik sartu dezaketela prozesuan. Ezarri temporizadorea eragiketa baterako fisikoki izan behar duen iraupena duen. Kontuan izan desbideraketak daudenean abisatzea. Era berean, jakinarazi ustekabeko geldialdia dagoenean.

13. PORTU ETA PROTOKOLOAK DESGAITU

56

BEHARREZKOAK/ERABILTZEN EZ DUEN KOMUNIKAZIO-SISTEMAK

PLC kontrolagailuek eta sareko interfaze-moduluek, oro har, lehenespenez gaituta dauden hainbat komunikazio-protokolo onartzen dituzte. Desgaitu aplikazioak behar ez dituen ataka eta protokoloak.

14. MURRIZTU HIRUGARRENEN DATU INTERFAZEAK

59

Mugatu hirugarrenen interfazeetarako eskuragarri dauden konexio eta datu motak.

Konexioak eta/edo datu-interfazeak ondo definitu eta mugatuta egon behar dira, beharrezkoa den datu-transferentziarako irakurtzeko/idazteko gaitasuna soilik uzteko.

**15. DEFINITU PROZESU EGOERA SEGURUA**

63

PLC-A BERRIAK HASITZEKO KASU

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

16. PLC ZIKLO DENBORAK ETA JOERA HMI 66

Laburtu PLCareen ziklo-denbora 2-3 segundoz behin eta jakinarazi HMI-ri grafiko batean bistaratzezko.

17. GRABATU PLCareen EGOERA DENBORA ETA BERE JOERA HMI-AN 70

Grabatu PLCareen funtzionamendu-denbora noiz berrezarri zen jakiteko. Diagnostikorako HMI-n egonkortasunaren joera eta grabazioa.

**18. PLCareen GELDITU GOGORRAK GRABATU
ETA JOERA HMI HMI**

73

HMI alarma-sistemek PLCa berrabiarazi aurretik konsulta ditzaten akatsen edo itzaltzeen ondorioz PLC gogor gelditzeko gertaerak gordetzen ditu. Sinkronizazioa datu zehatzagoak lortzeko garaia.

**19. PLC-KO MEMORIA ERABILTZEKO JARRAIPENA
ETA HMI-REN JOERA**

76

Neurtu eta eman memoria-erabilera oinarrizko lerroa ekoizpen-ingurunean implementatutako kontrolagailu bakoitzarentzat eta HMI-n joera.

**20. PROGRAMAZIO NEGATIBO FALTSUA TXAPENA
ETA ALERTA KRITIKOEN POSITIBO GEZURRA**

79

Identifikatu alerta kritikoak eta ezarri trampa bat alerta horientzat. Konfiguratu trampa abiarazte-baldintzak kontrolatzeko eta edozein desbiderapenen alerta-egoera kontrolatzeko.

SURE PLC PROGRAMAZIO PROIEKTUARI BURUZ

83

1.

PLC kodea modularizatu

PLC kodea moduluetan banatu, funtzio-bloke desberdinak erabiliz (azpirutina). Probatu moduluak modu independentean.



segurtasun helburua

Talde objektiboa

PLC Osotasun Logikoa

kodea hornitzalea

ORIENTAZIO

Ez programatu PLC logika guztia leku batean, adibidez, antolaketa bloke nagusian edo errutina nagusian. Horren ordez, zatitu funtzio-bloke desberdinatan (azpirutina) eta kontrolatu haien exekuzio denbora eta tamaina Kb-tan.

Sortu segmentu bereiziak modu independentean funtzionatzen duen logikarako. Horrek sarrera balioztatzen, sarbide-kontrolaren kudeaketan, osotasuna egiaztatzen, etab.

Kode modularizatuak kode moduluen osotasuna probatzea eta jarraipena egitea errazten du. Moduluaren kodea ondo probatu bada, modulu horien aldaketak jatorrizko kodearen hasharekin egiaztu daitezke, adibidez, modulu horietako bakoitzaren hash bat gordez (PLCn aukera bat denean). Horrela, moduluak balioztatu daitezke FAT/SAT-ean edo kodearen osotasuna zalantzan jartzen bada gorabehera baten ondoren.

ADIBIDEA

Gas-turbinaren logika "abiaraztea", "sarrerako paleta kontrola", "purga-balbularen kontrola" eta abar bereizten da, logika estandarra koherentziaz aplikatu ahal izateko. Horrek ere laguntzen du segurtasun-intzidentziaren bat gertatzu gero arazoak azkar konpontzen.

Zorrotz probatutako funtzio-bloke pertsonalizatuak aldaketarik gabe berrerabili daitezke (eta aldaketak egiten saiatuz gero abisatu) eta tratu txarren / erabilera okerren aurka blokeatu pasahitz / sinadura digital batekin.



ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

Gaiztoak izan daitezkeen kode gehitu berriak hautematea errazten du. Logikaren, koherentziaren eta baimendu gabeko aldaketen aurkako blokeoaren estandarizazioa lagunten du.

fidagarritasuna

Programaren fluxu-sekuentzia kontrolatzen eta begiztak saihesten lagunten du, logikak behar bezala ez erreakzionatzea edo zintzilikatzea eragin dezakeena.

Mantentzea

Kode modularra arazketa errazagoa ez ezik (moduluak modu independentean probatu daitezke), mantentzea eta eguneratzea ere errazagoa da.

Gainera, moduluak beste PLC batzuetarako erabil daitezke, eta horri esker, kode komun bat erabili eta identifikatu daiteke PLC ezberdinetan. Honek mantentze-langileek modulu arruntak azkar ezagutzen lagun diezaike arazoak konpontzerakoan.

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICSrako

Taktika: TA002 - Exekuzio teknika

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

Talde objektiboa

PLC Osotasun Logikoa

Aktiboen jabea Mantentze/Integrazio
Zerbitzu Hornitzalea

ORIENTAZIO

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

ÿ PLCak RUN moduan ez badaude, operadoreentzako alarma bat egon behar da. Badakite norbait monitorizazio sistema horretan lanean aritu behar dela, alarmaren aurrean erreakzionatu eta aurrera egin dezake.

ÿ HMI-a konfiguratu behar da alarmaren presentziaren txanda amaitzean operadoreari berriro abisatzeko. Prozesuan eragina izan dezaketen lanak egiten dituzten lantegiko langile edo kontratista guztien jarraipena egitea izan behar da helburua.

Salbuespen kasua: panela proba edo garapen fasean badago, kontuan hartu alarma hau desgaitzea, baina panela sareko maila altuagoetatik isolatuta egon behar da.

ADIBIDEA

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



ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

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

fidagarritasuna

/

Mantentzea

/

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICSrako

Taktikoa: TA009 - Inhibit Erantzun Funtzioa

Teknika: T0858 - Erabili/aldatu funtzionamendu modua

ISA/IEC 62443-4-1

SI-1: Segurtasun Aplikazioaren Berrikuspena

3.

Utzi logika operatiboa PLCan ahal den guztietañ

Utzi logika operatibo gehiena, totalizazioa edo integrazioa adibidez, zuzenean PLCan. HMIak ez du behar adina eguneraketa jasotzen ondo egiteko.



segurtasun helburua

Talde objektiboa

PLC Osotasun Logikoa

kodea hornitzalea

Integrazio/mantentze-zerbitzuen hornitzalea

Aktiboen jabea

ORIENTAZIO

HMIek kodetze-gaitasunen bat eskaintzen dute, hasiera batean operadoreei bisualizazioa eta alarmak hobetzen laguntzeko pentsatuta, programaztale batzuek PLCan geratu beharko luketen kodea sortzeko erabili dutena, osoa eta ikuskagarria izaten jarraitzen.

Balioak eremutik ahalik eta hurbilen kalkulatzeak kalkulu hauek zehatzagoak egiten ditu. HMIak ez du guztizko eguneraketa/integrazioa ondo egiteko. Gainera, beti dago latentzia HMI eta PLCareن artean. Gainera, kodea PLCan dagoenean eta HMI bat berrezartzen denean, PLC batetik totalizatzaileak/zenbaketak beti jaso ditzake.

Bereziki, saihestu beharreko HMI kodea segurtasun- edo segurtasun-eginbideekin erlazionatutako edozer gauza da, hala nola interblokeoak, temporizadoreak, blokeoak edo baimenak.

Prozesuko datuen balioak denboran zehar aztertzeko, prozesuko datuen historialaria HMI baino aukera hobea da. Erabili kontsultak prozesuko historialarien datu-base baten aukako balio totalizatuak (aldi batean, lote batean, prozesu-ziklo batean) PLC logikan lokalean agregatutako guztizkoekin alderatzeko. Bariantza handiago bat buruzko abisua datuen granularitateen desberdintasunengatik azal daiteke.

ADIBIDEA

ÿ Kontrolak gaitzeko/desgaitzeko baldintzak ezartzeko kodea: gaitzeko/desgaitzeko ekintzak PLC geruzan kontrolatu behar dira, bestela HMIn (edo sarearen bidez) PLCan egin daitezke ekintzak PLCan, nahiz eta (espero) baldintzak ez dira betetzen.

ÿ Operadorearen ekintzak ahalbidetzeko temporizadoreak (motorra jarraian abiarazterako atzerapeneko temporizadorea, balbulak itxita/irekita edo motorra geldituta kontuan hartzeko temporizadorea) ez dira HMI geruzan jarri behar motor/balbula hori kudeatzen duen PLCan baizik.

ÿ Alarma-atalaseek PLC kodeen parte izan behar dute, nahiz eta erakutsi HMletan trebatu.



ŷ Bolumen aldakorra duen ur depositua: deposituan sartu eta irteteko emaria kontrolatzen duen PLCak bolumena erraz batu dezake (eta guztizkoak gurutzatu ditzake). HMIk ere egin lezake hori, baina lehenik PLCTik balioak lortu beharko lituzke. Balio hauek denboraz zehatzak beharko lituzkete guztizko zuzenak lortzeko latentziaren kasuan edo balioak galdu ditzakete HMI berrabiaraziz gero.

ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

1. Aldaketen egiazapenean koherentzia onartu kodearen. HMI kodetzeak PLCTik bereizita dauka aldaketa-kontrola, orokorrean ez da zorroztasun berdinarekin (batez ere eraikitze- eta martxan jartzeko faseetan), sistema-jabeek ikuspegi osoa izan dezaten eta gogoeta garrantzitsuak ere galdu gabe. HMItxek ez dituzte "seinalde behartuak" edo PLCAk edo SCADA bezalako aldatutako balioen zerrendak sartzen, beraz HMI mailan aldaketak zailagoak detektatzen dira, eta ia ezinezkoa da baimenen aldaketak kudeatzeko plan baten parte izatea. H
2. Erasotzaile batek manipulatzea zailagoa da totalak HMItxan kalkulatutako guztirakoak manipulatzen dituzten PLC askotan banatuta.
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 lausotuta baitago operadorearen pantailan.



Onuragarria...?

Zergatik?

fidagarritasuna

1. Kalkuluak eraginkorragoak eta zehatzagoak dira eremutik gertuago. Gainera, guztirakoak eta zenbaketak oraindik erabilgarri egongo dira HMI berrezartzen bada (PLCeK ez dituzte horren maiz berrezartzen eta normalean balio horiek memoria ez-hegazkorran gordetzen dituzte).
2. Sarrera eta interblokeo iturri ezberdinak ustekabeko hutsegiteak ekar ditzakete. Planta batean HMItarako teknologia desberdinak egon daitezke (SCADA geruza, baina baita eremuko kontrol-panelak ere) eta horietako batean aldaketak ez dira gainerako geruzetan zehar hedatuko, eta horrek bistaratzean inkoherentziak eragingo ditu eta gerta daitezkeen hutsegiteak eragingo ditu. eragiketa.

Mantentzea

Kodetzea erraza da ulertzeko eta PL Ctik PLCra transferitzeko, ez hainbeste HM Itik HM Ira.

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICSrako**Taktikoa:** TA010 - Prozesuaren kontrola hondatza**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 PLCareن errore-banderetan matematika-arazoak harrapatzeko.



segurtasun helburua

Talde objektiboa

PLC Osotasun Logikoa

kodea hornitzalea

Integrazio/mantentze-zerbitzuen hornitzalea

ORIENTAZIO

PLC kodea ondo funtzionatzen bazen, baina bat-batean zeroz zatitzen badu, hori ikertu behar da.

Zerbait peer to peer beste PLC batetik komunikatzen ari bada eta funtziologikak zeroz zatitzen badu espero ez denean, hori ikertu behar da.

Programatzaile gehienek arazoa alde batera utziko dute matematikako errore bat balitz bezala, edo okerragoa dena, baliteke beren kodea perfektua dela pentsatzea eta PLCAk akats gogor batean sartzen utziko dute. Kodearen garapenean, ingeniariek beren kode-moduluak (zatiak edo errutinak) probatu eta balioztatu behar dituzte, aurreikusitako mugetatik kanpo datuak sartuz. Honi unitate-probak dei diezaiokagu.

Esleitu blokeatutako memoria-segmentu desberdinak firmware, logika eta protokolo pilarako.

Probatu protokolo-pila tratu txar kasuetarako. Tratu txarren kasuak pakete baten goiburuko adierazleen baldintza bereziak izan daitezke.

ADIBIDEA

Mugetatik kanpo datuek eragindako PLC akatsak oso ohikoak dira. Hau gertatzen da, adibidez, sarrerako balio batek array-indizeak mugetatik kanpo edo aurrezarpen negatiboak dituzten temporizadoreak edo zeroz zatitutako salbuespenak eragiten dituenean.

Interes-adierazle tipikoak hauek dira:

ÿ zati zeroz

ÿ kontagailua gainezka egitea

ÿ Kontadore negatiboa edo aurrez ezarritako temporizadorea

ÿ I/O eskaneatzeko gainkarga



ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

PLCen aurkako erasoen artean, haien logika aldatzea, programa berri bat aktibatzea, kode berria probatzea, prozesu-formula berri bat kargatzea, mezuak bidaltzeko logika osagarria txertatzea edo edozein funtziak aktibatzea izan daitezke. PLC gehienek osotasun kriptografikoaren egiaztapenik ematen ez dutenez, banderak seinale ona izan daitezke goiko logika aldaketaren bat gertatzen bada.

fidagarritasuna

Serioski hartutako banderak PLCak programazio edo I/O akatsekin funtzionatzea eragotzi dezake. Gainera, akatsen bat gertatzen bada, hutsegitearen iturria nabariagoa da.

Mantentzea

/

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICSrako

Taktikoa: TA010 - Prozesuaren kontrola hondatzea

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-baldintzen proba

MITRE CWE

CWE-128: Gutunazala

CWE-190: Integer Overflow

CWE-369: Zeroz zatitu

CWE-754: Ezohiko baldintzen egiaztapen okerra edo apartekoak

5.

PLC kodearen osotasun kriptografikoa edo/eta checksum- egiaztapenak egin

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



segurtasun helburua

Talde objektiboa

PLC Osotasun Logikoa

kodea hornitzalea

Integrazio/mantentze-zerbitzuen hornitzalea

Aktiboen jabea

ORIENTAZIO

A) Checksumak

Hash (criptografikoak) bideragarriak ez direnean, checksumak aukera bat izan daitezke.

PLC batzuek checksum bakarra sortzen dute kodea PLC hardwarea deskargatzenean. Checksum-fabrikatzaila/integratzaileak dokumentatu behar du SAT-aren ondoren eta bermearen/zerbitzuaren baldintzen parte izan behar du.

Checksum funtzioa ez badago berez kontrolagailuan eskuragarri, EWS/HMI-n ere sor daiteke eta egiaztatu, adibidez, egunean behin PLCko jatorrizko kode hasharekin alderatzeko, bat-etortze hori egiaztatzeko. Honek denbora errealeko alertak emango ez dituen arren, nahikoa da norbait PLC kodean aldaketak egiten saiatzen ari den jarraitzeko.

Kontrol-balioa PLC erregistro batera ere eraman daiteke eta alarman ezarri daiteke aldatzen denean, balioa historialariei bidal diezaieke, etab.

B) Hashak

PLC CPUek normalean ez dute prozesatzeko ahalmenik hash-ak etengabe sortzeko edo egiaztatzeko. Izan ere, hash bat saiatzeak PLCa huts egin dezake. Baino PLC ingeniaritza softwareak PLC kodearen hashak kalkulatu eta PLCan edo kontrol sistemaren beste nonbait gorde ditzake.

ADIBIDEA

Checksum funtzioak dituztela ezagutzen duten PLC saltzaileek:

ÿ Siemens (ikus adibidea)

ÿ Rockwell



Gainera, kanpoko softwarea erabil daiteke checksumak sortzeko:

ÿ Bertsio txakurra

ÿ Asset Guardian

ÿ EZ

Siemens implementazio adibidea

Siemens S7-1500 PLC batean checksumak sortzeko adibidea:

GetChecksum-Function bloakeak benetako checksuma irakurtzen du eta script arin batekin "SAT-Checksum" gorde dezakezu erreferentzia gisa. Erreferentziako kontrol-sumaren desbideratze bat gorde daiteke datuak erregistratzeko funtziorekin.

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

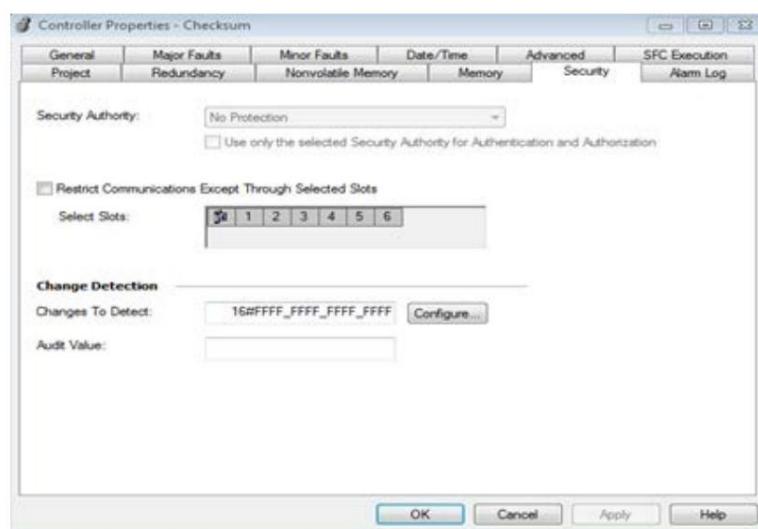
Rockwell ezarpenaren adibidea:

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

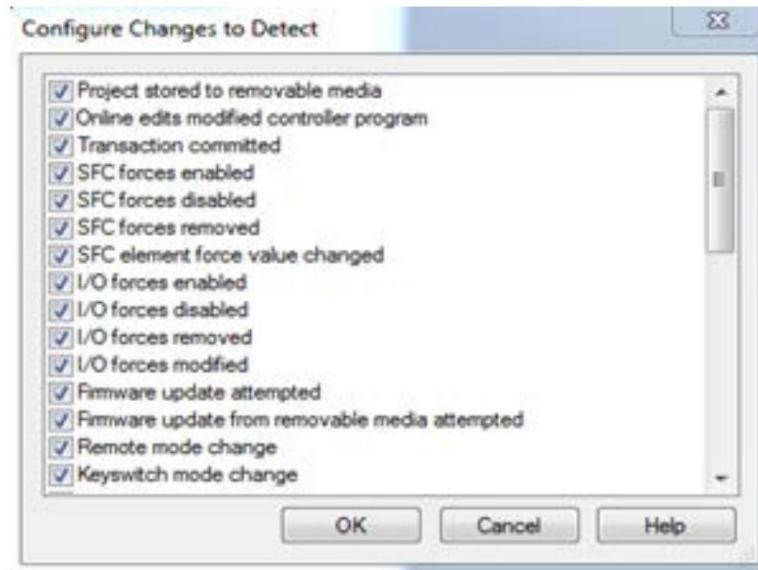
Praktika honek aukera bat eskaintzen du, dauden tresnak eta gaitasunak erabiliz, ziber-aktibo kritikoak aldatzen direnean egoeraren kontzientzia lortzeko. Erakundeari dagokio lagin honen erabilera bere ingurunean ondoen funtzionatzen duen metodo batean osatzea.



1. Kontrolagailuaren propietateen elkarriketa-koadroan, hautatu ezarpenen botoia "Cam detektatzeko biar"



2. Hautaketa leihoaaren barruan, aukeratu kontrolatu beharreko elementu guztiak

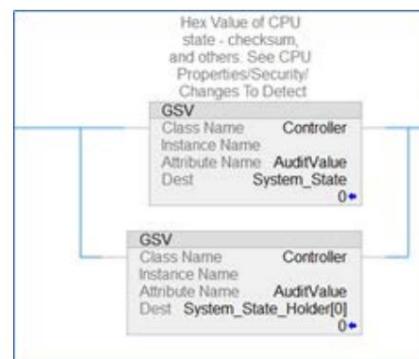


3. Sortu etiketa bat prozesadorearen egoerari buruzko informazioa jasotzeko. Etiketa hau izan daiteke idatzi "LINT" edo "DINT" motako 2 hitzez osatutako matrizea

Name	Alias For	Base Tag	Data Type	Description	External Access	Constant	Style
System_State			LINT	Hex Value of CPU stat...	Read/Write	<input type="checkbox"/>	Decimal
System_State_Hol...			DINT[4]		Read/Write	<input type="checkbox"/>	Decimal



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





ZERGATIK?

Onuragarria...?	Zergatik?
Segurtasuna	PLC kodea manipulatu ote den jakitea ezinbestekoa da bai konpromiso bat antzemaneko bai PLC bat balizko arrisku baten ondoren funtzionatzeko segurua den egiaztatzeko.
fidagarritasuna	Hashes edo checksum-ak PLCak integratzaileak/fabrikatzaleak onartutako kodea exekutatzen ari den (oraindik) egiaztatzeko baliabideak ere izan daitezke.
Mantentzea	/

ERREFERENTZIAK

estandarra / esparrua	mapaketa
MITRE ATT & CK ICSrako	Taktika: TA002 - Exekuzioa, TA010 - Kontrolaren hondatzea Prozesua
	Teknika: T0873 - Project File Infection, T0833 - Kontrol-logika aldatu
ISA 62443-3-3	SR 3.4: Softwarea eta Informazioaren Osotasuna
ISA 62443-4-2	CR 3.4 : Softwarearen eta informazioaren osotasuna EDR 3.12: Produktuen hornitzaileen konfiantzazko erroak hornitzea
ISA 62443-4-1	SI-1 : Segurtasun Aplikazioaren Berrikuspena SVV-1 Segurtasun Baldintzen proba
MITRE CWE	CWE-345: datuen benetakotasunaren egiaztapen nahikoa eza <ul style="list-style-type: none"> • (semea) CWE-353: egiaztatzeko euskarria falta da osotasuna • (seme-alaba) CWE-354: osotasuna egiaztatzeko balioaren baliozkotze okerra

6.

Baliozkotu temporizadoreak eta kontagailuak

Temporizadoreen eta kontagailuen balioak PLC programan idazten badira, PLCak balioztatu beharko ditu arrazoizkoak direla egiaztatzeko eta zero azpiko atzerako kontaketarik dagoen egiaztatzeko.



segurtasun helburua

Talde objektiboa

PLC aldagaien osotasuna

Integrazio/mantentze-zerbitzuen hornitzailea

Aktiboen jabea

ORIENTAZIO

Tenporizadoreak eta kontagailuak teknikoki edozein baliotara ezarri daitezke. Hori dela eta, temporizadorea edo kontagailua aurrez ezartzeko balio duen tarte mugatu behar da funtzionamendu-baldintzak betetzeko.

Urruneko gailuak badira, hala nola HMI bat, idatzi temporizadorearen edo kontagailuaren balioak profesional bati gramoa:

- ÿ Ez utzi HMI-ri temporizadoreari edo kontagailuari zuzenean idazten, baizik eta pasatzen baliozkotze logika bat
- ÿ baliozkotu aurrezarpenak eta denbora-muga balioak PLCan

Tenporizadorearen eta kontagailuen sarreren baliozkotzea erraza da zuzenean PLCan (paketeen ikuskapen sakona egiteko gai den sareko gailuren beharrik gabe), PLCak sarreraren egoera edo testuingurua zein den "dakielako". "Zer" jasotzen duzun eta "noiz" eskaerak edo leloak jasotzen dituzun balioztatu dezakezu.

ADIBIDEA

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

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

10.000ra iristen denean prozesu bat gelditzea eragiten duen kontagailu bat badago, baina hasieratik 11.000ean ezzarrita badago, baliteke prozesua ez gelditzea.





ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

I/O, temporizadoreak edo aurrezarpenak zuzenean I/O-ra idazten badira, PLCak baliozkotu gabe, PLCareen baliozkotze-geruza saihestu egiten da eta HMI-ri (edo sareko beste gailu batzuei) maila altuago bat esleitzen zaie.

fidagarritasuna

PLCak operadore batek ustekabean temporizadorearen edo kontagailuaren balio okerrak aurrez ezartzen dituenean ere balioztatu dezake.

Mantentzea

Temporizadoreetarako eta kontagailuetarako baliozko tarteak dokumentatuta eta automatikoki balioztatuta edukitzea lagungarria izan daiteke logika eguneratzean.

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICSrako

Taktikoa: TA010 - Prozesuaren kontrola hondatzea

Teknika: T0836 - Parametroa aldatu

ISA 62443-3-3

SR 3.5: Sarreraren baliozkotzea

ISA 62443-4-2

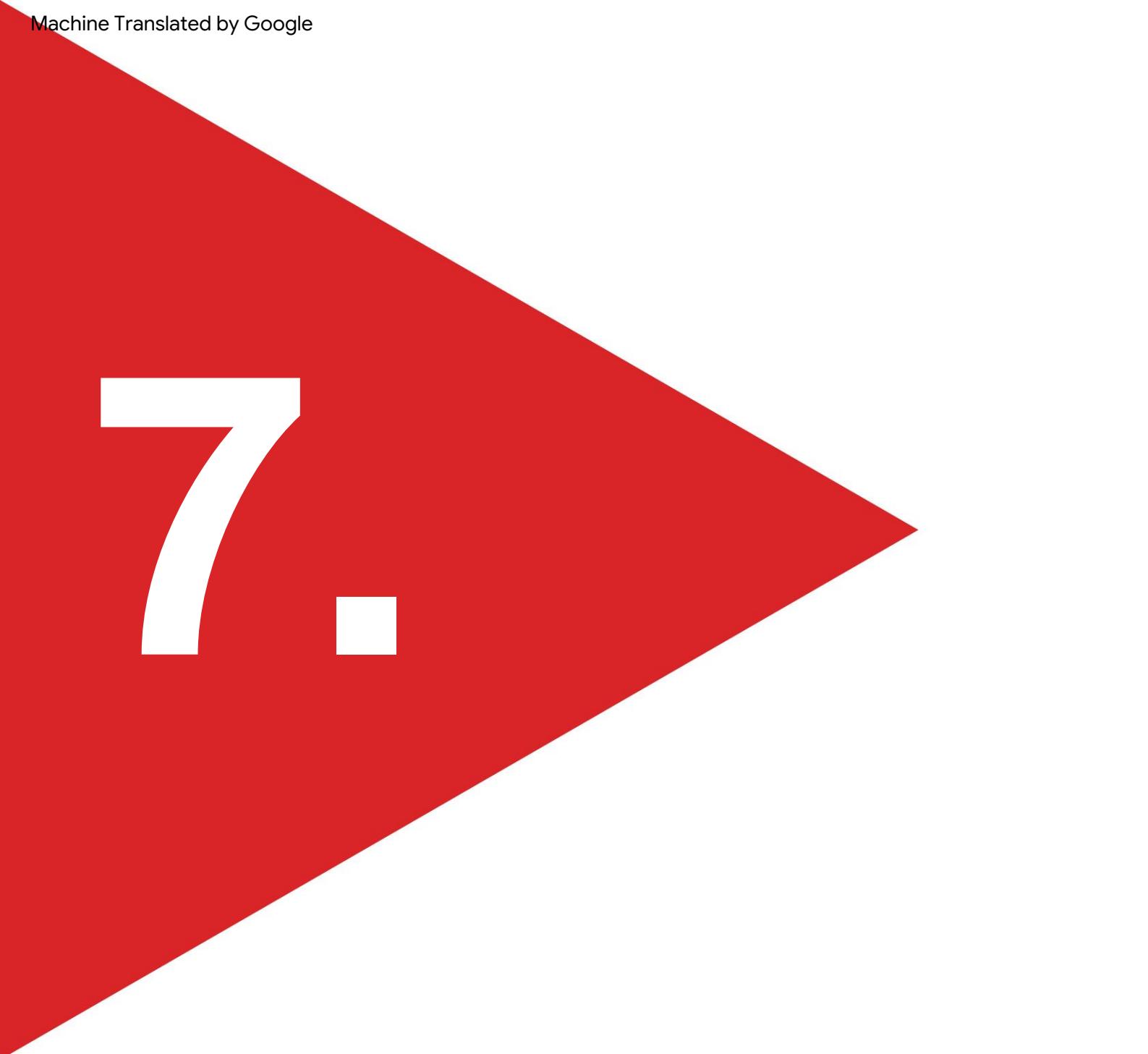
CR 3.5: Sarreraren baliozkotzea

ISA 62443-4-1

SI-2: Kodeketa estandarrak seguruak

SVV-1: segurtasun-eskakizunen proba

7



Parekatutako sarrera/irteeretan baliozkotu eta alerta

Seinaleak parekatuta badituzu, ziurtatu bi seinaleak batera ez daudela baieztagatzen. Eragileari alarma ematen dio fisikoki bideragarriak ez diren sarrera/irteera egoerak gertatzen direnean. Demagun parekatu seinaleak independenteak izatea edo atzerapen-temporizadoreak gehitzea irteerak aldatzea eragingailuentzat kaltegarria izan daitekeenean.



segurtasun helburua

Talde objektiboa

PLC aldagaien osotasuna
erresilientzia

kodea hornitzailea
Integrazio/mantentze-zerbitzuen hornitzailea

ORIENTAZIO

Parekatutako sarrerak edo irteerak fisikoki aldi berean gertatu ezin direnak dira; elkarren esklusiboak dira. Parekatutako seinaleak aldi berean aldarrikatu ezin badira ere akats edo jarduera gaiztorik egon ezean, PLC programatzailuek askotan ez dute baieztapen hori gertatzea eragozten.

Balioztatzea errazagoa da PLCan zuzenean egitea, 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 aldarrikatzen ez direnean, baina azkar aldatzen direnean eragingailuak kaltetzen dituen moduan.

ADIBIDEA

Seinale parekatuen adibideak:

ÿ HASI eta GELDITU

ÿ Irteera eta geldialdi independenteak: konfiguratu irteera eta geldialdia irteera diskretu gisa, piztu eta itzali daitekeen irteera bakarra izan beharrean. Diseinuaren arabera, honek ez du aldibereko tirorik onartzen. Erasotzaile batentzat, askoz zailagoa da bi irteera desberdin konfiguratu behar badira azkar piztea/desaktibatzea.

ÿ Berrabiarazteko temporizadorea: Geldialdi baten ondoren berrabiarazteko temporizadorea gehitzea ere kontuan hartu, abiarazte/gelditzeko seinaleak azkar deskonektatzeko.

ÿ AURRERA eta ATZERA

ÿ IREKI eta ITXI



Kaltegarriak izan daitezkeen seinale parekatuak txandakatzeko adibideak:

PLC/MCC-k sarrera diskretu bat onartzen badu, erasotzaile bati eragingailuei kalte fisikoak eragiteko aukera erraza eskaintzen dio. Kableak aldatzeko kalteak egiteko agertokirik ezagunena MCC bat izango litzateke, baina praktika hau zuzenak aldatzeak kalteak eragin ditzaketan eszenatoki guztietaen aplikatzen da. Irteerak bizkor aldatzeak benetako kalteak eragin ditzakeen kontzeptuaren froga bat izan zen 2007an Idaho Laborategi Nazionalak egindako Aurora sorgailuaren proba, non sinkronizatuta dauden irteerak konmutatzeak etengailuetan kalteak eragin zituen.

ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

1. PLC programek zer egingo den kontuan hartzen ez badute Bi sarrera-seinaleak aldi berean baieztagaten badira, hau eraso-bektore ona da.
2. Baieztagaten ari diren bi sarrera-seinale parekatuak funtzionamendu-txarren bat, programazio-errore bat edo gaiztoren bat gertatzen ari den abisua dira.
3. Horrek eragingailuei kalte fisikoa eragin diezaiekeen eraso-eszenatoki bat eragozten du.

fidagarritasuna

1. Parekatutako sarrera-seinaleek hori adieraz dezakete sentsore bat hautsita edo gaizki kabletuta dagoela edo arazo mekaniko bat dagoela, hala nola, etengailua trabatuta dagoela.
2. Abiarazte eta geldialdia bizkor aldatzea ere akatsez egin daiteke, beraz, nahi gabe eragin daitezkeen kalteak ere saihesten ditu.



Mantentzea

/

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICSrako

Taktikoa: TA010 - Prozesuaren kontrola hondatzea

Teknika: T0836 - Aldatu parametroa, T0806 - Brute Force I/O

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-baldintzen proba

MITRE CWE

CWE-754: ezohiko edo salbuespenezko baldintzen egiaztapen okerra

8.

Baliozkotu HMI sarrerako aldagaiak PLC mailan, ez soilik HMIan

HMI PLC aldagaietarako sarbidea HMIn baliozko balio operatibo batzuetara mugatu daiteke (eta behar da), baina beste egiaztapen gurutzatu batzuk gehitu behar dira PLCan, tarte onargarrietatik kanpoko balioak saihesteko edo ohartarazteko. HMIan programatuta daudenak.



segurtasun helburua

Talde objektiboa

PLC aldagaien osotasuna

kodea hornitzalea

Integrazio/mantentze-zerbitzuen hornitzalea

ORIENTAZIO

Sarrerako baliozketazeak balio operatiboen balioak egiaztatzeak izan ditzake, baita baliozko balioak ere prozesuekin lotutako datu motei dagokienez.

PLC aldagai batek mugetatik kanpo dagoen balio bat jasotzen badu, eman PLC logika honi

- ÿ Prozesuan negatiboki eragiten ez duen aldagai horren **balio lehenetsi** bat sartu, eta hori abisu adierazle gisa erabil daiteke, edo
- ÿ Sartu balio horri **azken balio zuzena** eta erregistratu gertaera gero aztertzeko.

ADIBIDEA

1. adibidea

Eragiketa batek erabiltzaileak balbularen presioaren balio bat sartu behar du HMI batean. Eragiketa honetarako baliozko tarteak 0tik 100era bitartekoak dira, eta erabiltzailearen sarrera HMIko erabiltzailearen sarrera funtziotik PLCko V1 aldagaira pasatzen da. Orduan,

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

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

Honek erantzun positiboa ematen du ustezko balio seguru batetik aldagai horren sarrera baliogabe bati.





2. adibidea

Eragiketa batek erabiltzaileen sarrera behar du neurtzeko atalaseak beti INT2 datu-barruti batean egon behar duen aldagai batean. Erabiltzailearen sarrera HMIk V2 aldagaira pasatzen da PLCan, hau da, 16 biteko datu-erregistro batera.

1. V2 aldagaiaaren HMI sarrerak -32768 eta 32767 (dec.) programako tarte mugatua du HMIn.
1. PLCak datu-mota gurutzatutako kontrol logika du, gainezkatzea aldaia (V3) monitorizatzen duena, PLC memoria-egituraren V2 ondoren dagoena:

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 (Proporcionala, Integrala, Deribatua Kontrolatzalea) unitate koherenteetara edo gordinetara, kontrol-arazoak eragiten dituzten eskalatze-akatsak ezabatzeko. Eskalatze desegokiak nahi gabeko tratu txarrak sor ditzake.





ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

1. HMlek normalean motaren bat eskaintzen duten bitartean sarreraren baliozkotzea, operadore gaizto batek aldatutako paketeak sortu edo erreproduzi ditzake kanpoko eraginetarako irekita dauden PLC aldagaien balio arbitrarioak bidaltzeko (HMI batetik emandako balioetarako irekita, adibidez).
2. PLC protokoloak protokolo "ireki" gisa merkaturatzen dira eta publiko orokorrari kaleratzen dira, beraz, "ireki" protokoloetako informazioa erabiliz malwarea sortzea hutsala izan daiteke garatzea. PLC aldagaien mapaketa normalean trafikoaren analisiaren bidez gerta daiteke eraso baten ezagutza-faseetan, horrela intrusoari trafiko gaiztoa helburura bideratzeko eta, horrela, prozesu bat baimendu gabeko tresnekin manipulatzeko behar den informazioa emanet. Datu horiek prozesuan implementatu aurretik PLCari emandako balioak gurutzatzeak baliozko datu-barrutiak bermatzen ditu eta memoria-kokapen horietan baliorik gabeko balio bat arintzen du, prozesatzen zehar mugaz kanpoko balio bat detektatzen denean barruti seguruak behartuz. . du

PLC eskanearaztea.

fidagarritasuna

/

Mantentzea

/



ERREFERENTZIAK

estandarra / esparrua	mapaketa
MITRE ATT & CK ICSrako	Taktikoa: TA010 - Prozesuaren kontrola hondatzea 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-baldintzen proba
MITRE CWE	CWE-1320: Mugetatik kanko seinale-mailaren babes desegokia

9.

Baliozkotu aholkuak

Baliozkotu zeharkaketak array-aren muturrak pozoituz hesi-zutoinetan akatsak hautemateko.



segurtasun helburua

Talde objektiboa

PLC aldagaien osotasuna

kodea hornitzalea

Integrazio/mantentze-zerbitzuen hornitzalea

ORIENTAZIO

Zeharkakoa erregistro baten balioa beste erregistro batean erabiltzea da. Iradokizunak erabiltzeko arrazoi asko daude.

Beharrezko zeharkaketen adibideak hauek dira:

- ÿ Maiztasun Aldakorreko unitateak (VFD), maiztasun desberdinatarako ekintza desberdinak abiarazten dituztenak. konsultak bilaketa-taulak erabiliz.
- ÿ Martxaren denboraren arabera zein ponpa abiarazi behar den erabakitzea egungo gezurra.

PLCek ez dute normalean “matrizearen amaiera” banderarik, beraz, ideia ona da softwarean bat sortzea; helburua PLCaren ezohiko/planifikatu gabeko eragiketak saihestea da.

ADIBIDEA

PROGRAMAZIOA JARRAIBIDE ZERRENDA (IL)

Planteamendua funtzio-bloke gutxi batzuetan bihur daiteke eta agian beste aplikazio batzuetarako berrerabili daiteke.

1. Sortu array-maskara bat

Egiaztatu matrizeak tamaina bitarra duen. Tamaina bitarra ez bada, sortu maskara bat eskala bitarrean hurrengo tamainan. Adibidez, 5 erregistro behar badituzu (tamaina ez bitarra):

[21 31 41 51 61]

definitu 8ko array bat:

[xx 21 31 41 51 61 x]

Ondoren, hartu indizearen balioa zeharkarako biltzeko; adibide honetan, 3 da.



Abisua: indizea 0tik hasten da!

[21 31 41 51 61]

_____ ^

Aurkibidea: 3

gehitu offset bat amaiera pozoitua konpentsatzeko. 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, arrayaren tamainaren berdina den maskara batekin.

Adibide honetan, matrizearen tamaina 8 da, beraz indizea 7 da, beraz, maskara 0x07 izango litzateke. Maskarak ziurtatzen du lor dezakeen indize maximoa 7 dela, adibidez:

6 ETA 0x07 itzuliko litzateke

6,7 ETA 0x07 78 itzuliko litzateke

ETA 0x07 0,9 itzuliko litzateke

ETA 0x07k 1 itzuliko luke.

Horrek ziurtatzen du beti matrizeko balio bat bideratzen duzula.

2. Txertatu pozoitutako muturrak

Amaiera pozoitzea aukerakoa da. Inguruko manipulatuak pozoitu gabe harrapa ditzakezu, baina pozoitzeak hesi-zuten akatsak harrapatzen laguntzen du, zentzurik ez duen balio bat berreskuratzen duzulako.

Kontua da matrizeko 0 indizean balio ez duen balio bat egon behar dela, -1 edo 65535 bezalakoa. Hau da "amaiera pozoitua". Era berean, arrayko azken elementuetan gauza bera egiten duzu:

Beraz, goiko arrayrako, pozoitutako bertsioa honelakoa izan daiteke:

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





3. Zeharkako helbide-balioen erregistroa maskararik gabe

Ondoren, erregistratu zeharkako helbidearen balioa ETA maskararik eta desplazamendurik gabe:

adibide honetan, 51 erregistratuko zenuke 3 indizerako.

[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: zeharka zuzena

Lehenik eta behin, desplazamendua:

$$\text{Indizea} + \text{Desplazamendua} = 3 + 2 = 5$$

Bigarrena, maskara:

$$5 \text{ ETA } 0x07 = 5$$

Hirugarrena, zeharkako egiaztapena

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

_____ ^

Desplazamendua barne indizea: 5

Balioa = 51 erregistratutako balioaren berdina da, beraz, dena ondo dago.

4b. B kasua: Helbide manipulatua

Orain zeharkako manipulatua baduzu, esan 7, ikus dezagun zer gertatzen den:

Lehenik eta behin, kalte-ordaina:

$$\text{indizea} + \text{desplazamendua} = 7 + 2 = 9$$



**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 pozoitutako amaiera-puntuia ere adierazten du, beraz, zure zeharkakotasuna manipulatuta dagoela jakingo zenuke.

5. Exekutatu Scheduler Fault/Alerta

Balidatutako balio hau erregistratutakoaren desberdina bada, badakizu zerbait gaizki dagoela. Sortu softwarearen kalitatearen alarma.

Ondoren, egiaztu zeharkako balioa. Pozoitutako balio bat bada, beste softwarearen kalitatearen alarma piztu beharko luke. Hau hesi-zutoin akastunaren seinale da.





ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

PLC gehienek ez dute matrizeen mugetatik kanpo indizeak kudeatzeko funtziorik. Bi **agertoki arriskutsu** egon daitezke zeharkako akatsen ondorioz:

Lehenik eta behin, zeharkatze batek erregistro okerra irakurtzera eramatzen badu, programa balio okerrak erabiliz exekutatuko da.

Bigarrenik, zeharkatze txar batek erregistro okerrean idazteria eramatzen badu, programak gorde nahi dituen kodeak edo balioak gainidazten ditu. Bi kasuetan zeharkako akatsak detektatzeko zailak izan daitezke eta ondorio larriak izan ditzakete. Giza akatsak eragin ditzakete, baina maltzurrez ere txertatu daitezke.

fidagarritasuna

Programazioan giza akats ez-maltzurrak identifikatzen ditu.

Mantentzea

/

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICSrako

Taktikoa: TA010 - Prozesuaren kontrola hondatzea

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: Zifratze Estandar Seguruak

SVV-1: Segurtasun-baldintzen proba

MITRE CWE

CWE-129: Array-indizearen baliozkotze okerra

10.

Esleitu izendatutako erregistro-blokeak funtziaren arabera
(irakurtzea/idatzi/balioztatzeko)

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



segurtasun helburua

Talde objektiboa

PLC aldagaien osotasuna

kodea hornitzalea

Integrazio/mantentze-zerbitzuen hornitzalea

ORIENTAZIO

Aldi baterako memoria, scratch pad memoria bezala ere ezagutzen dena, erraz ustiatzen den memoria-eremua da praktika hau jarraitzen ez boda. Adibidez, mugaz kanpo dagoen "Modbus" erregistro batean idazteak aldi baterako kalkuluetarako erabiltzen diren memoria-erregistroak gainidaztea ekar dezake.

Orokorrean, erregistro-memoria beste gailu batzuek PLC sarearen bidez atzi dezakete irakurtzeko eta idazteko eragiketak egiteko. Erregistro batzuk HMI batek irakur litzake, eta beste batzuk SCADA sistema batek, etab. Aplikazio jakin baterako erregistro-matrizetan espezifikoak izateak ere errazten du (kontrolagailuan edo kanpoko suebaki bat erabiliz) beste gailu/HMI batetik irakurtzeko soiliak konfiguratzeari.

Izendatutako erregistro-blokeek zentzua duten funtzionen adibideak hauek dira:

ÿ irakurketa

ÿ Idatzi (HMI / kontrolagailu / kanpoko beste gailu batetik)

ÿ Eskriturak baliozkotzea

ÿ kalkuluak

Erregistroetan kanpoko idazketak onartzen direla ziurtatzeak memoria nagusia berrezartzeko akatsak saihesten laguntzen du, mugaz kanpoko exekuzioengatik edo asmo maltzurengatik. Izendatutako erregistro-bloke hauek I/O idazketarako, temporizadoreetarako eta kontagailuetarako buffer gisa erabil daitezke, buffera guztiz idatzita dagoela egiaztatuz (ez dauka datu zaharrik eta ez da berriak) eta buffer-eko datu guztiek baliozkotuz.

Testuingurua:

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



ADIBIDEA

Praktika hau aplikatu ezean gerta daitekeenaren adibideak:

Planteamendua funtziobloke gutxi batzuetan bihur daiteke eta agian beste aplikazio batzuetarako berrerabili daiteke.

(Erreferentzia: g. P. H. Sandaruwan, PS Ranaweera, Vladimir A. Oleshchuk, PLC segurtasuna eta azpiegitura kritikoen babesa):

ŷ Siemens-ek normalean scratchpad memoria erabiltzen du gonbidapen-eremuan 200.0-tik 255.7-ra. Eremu horretan bit bat aldatzen bada, PLC-k matxura larria izateko probabilitatea dago bit edo byte horren garrantziaren arabera.

ŷ Demagun erasotzaile bat PLC sareko makinetako batera sar daitekeela eta makina hori memoria erregistratzeko balio arbitrarioak idazteko gai den harra batekin kutsa dezakeela.

Erregistroaren memoria-balioak arbitrarioki aldatzen direnez, presioaren balioa alda dezakezu.

ŷ Exekuzio-logikak balio berri bat ezarriko du aldaketaren arabera, eta horrek sistemak segurtasun-marjinak gainditzea eragin dezake eta, agian, hutsegitea eragin dezake.

Praktika honen aplikazioaren adibideak:

ŷ Segurtasun-eremu bat dagoen agertoki batean (baina DCS-k irakur dezake), suebakiak "idazketa" saiakera guztiak erregistra ditzake erregistro hauek IRAKURTZEKO BAKARRIK direla segurtasun-eremuan.

ŷ Beste agertoki batean, baliteke erregistro batzuk idazteko modukoak izatea, eta erregistro batzuk irakurtzeko soilik, baina erregistro guztiak IRAKURTZEKO BAKARRIK array bakarrean edukitzeak erraztu egiten du kontrolagailuan (edo suebaki batean) konfiguratzea.



ZERGATIK?

Onuragarria...?

Segurtasuna

Kontrolatzailearen datuen babesia errazten du funtziaren arabera (irakurtzea/idatzi/balioztatzea).

Protokoloa ezagutzen duten suebakien lana errazten du: arauak simplifikatu egiten dira, oso argi baitago HMIak zein erregistro-bloketan sar dezakeen. Suebaki-arau (simpleagoak) kudeaketa errazten du.

Barne memorian baimenik gabeko aldaketak egitea erraz ustiatzen den ahultasun bat da (By-pass Logiko Erasoa).

PLC errutinen sarrerak eta irteerak behar bezala balioztatzen direnean, edozein aldaketa (aktore gaizto baten ondorioz edo akatsen bidez) erraz hauteman daiteke sekuentzia logikoan denbora luzez egon eta gero eragiketan erroreak bota/arazoak sortu beharrean. .

fidagarritasuna

Irakurketa eta idatzeta azkarrago egiten ditu transakzio kopurua murrizten delako.

Baimendutako aldaketek eta programazio akatsek ere akatsak sor ditzakete aldi baterako memoria babestuta ez badago.

Mezu luzeetan sare- eta komunikazio-erroreek nahi gabeko akatsak sor ditzakete datuak prozesatu aurretik baliozkotasuna egiaztatzen ez badute.

Mantentza

Aldi baterako memorian idaztea eragiten duten akatsak programatzeak akatsak aurkitzea zaildu dezake, beraz, arazoa saihestu daiteke idazketetarako erregistro espezifikoak esleituta.



ERREFERENTZIAK

estandarra / esparrua	mapaketa
MITRE ATT & CK ICSrako	<p>Taktikoa: TA009 - Erantzunaren inhibizio funtzioa, TA010 - Hondatze-prozesuaren kontrola</p> <p>Teknika: T0835 - Irudiaren I/O parametroa , T0836 - Aldatu manipulatzea</p>
ISA 62443-3-3	<p>SR 3.4: Softwarea eta informazioaren osotasuna</p> <p>SR 3.5: Sarreraren baliozkotzea</p> <p>SR 3.6: Irteera deterministikoa</p>
ISA 62443-4-1	<p>SD-4: Diseinu seguruaren praktika onak</p> <p>SI-1: Segurtasunaren Ezarpenaren Berrikuspena</p> <p>SI-2: Kodeketa Estandar Seguruak</p> <p>SVV-1: segurtasun-eskakizunen proba</p>
ISA 62443-4-2	<p>CR 3.4: Softwarearen eta informazioaren osotasuna</p> <p>CR 3.5: Sarreraren baliozkotzea</p> <p>CR 3.6: Irteera deterministikoa</p>
MITRE CWE	<p>CWE-787: Idatzi mugetatik kanpo</p> <p>CWE-653: Konpartimentazio nahikoa</p>

11.

Sinesgarritasun egiaztapena ezartzea

Prozesua neurketa desberdinak gurutzatuz
egiaztatzea ahalbidetzen duen sinesgarritasuna egiazatzeko
moduan.



segurtasun helburua

Talde objektiboa

I/O balioen osotasuna

kodea hornitzalea

Integrazio/mantentze-zerbitzuen hornitzalea

ORIENTAZIO

Sinesgarritasun fisikoa erabiltzeko modu desberdinak daude neurketak balioztatzeko:

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 alternatiboen erabilera ere esan dezakete (ikus adibideak).

ADIBIDEA

a) Denboraren araberako neurriak eta integratuak alderatu

ÿ Dosifikatzale-ponpa eta deposituaren maila-neurgailua: aldaketa bolumetrikoa kauaren berdina izan behar du integratutik.

ÿ Erregailua galdara batean: gehitutako bero kalorikoa tenperatura igoeraren berdina izan behar du.

b) Konparatu neurketa iturri desberdinak

ÿ Erabili airearen abiadura, horizonte artifiziala, abiadura bertikala eta altitudea hegazkinean hegazkinaren igoera/jaitsiera fenomenoa neurtzea.

ÿ Datu-erregistratzale autonomoen prozesu-parametroen balioak (4-20 mA-ko begiztekin edo errele-kontaktuekin lotuta eta komunikazio-kanal bereizietatik transmitituta) SCADA sistemako datuekin (PLC eta HMI bidez "normal bezala" iristen diren) eta alertak alderatzea. desbideratzeetan eta zehaztapenetatik kanpoko balio nabarmenetan.



ZERGATIK?

Onuragarria...?	Zergatik?
Segurtasuna	Manipulatutako balioen kontrola errazten du (sentsore guztiak aldi berean manipulatzen ez direla suposatuz).
fidagarritasuna	Sarrera gisa hondatutako/okerrak diren neurketak onartzea eragozten du edo identifikatzen ditu (ekintza gehiago egiteko).
Mantentzea	Baztertu azkarrago hutsegiteen arrazoi fisiko posibleak.

ERREFERENTZIAK

estandarra / esparrua	mapaketa
MITRE ATT & CK ICSrako	Taktika: TA010 - Prozesuaren kontrola hondatza Teknika: T0806 - Brute Force I/O
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
MITRE CWE	CWE-754: Ezohiko baldintzen egiaztapen okerra edo apartekoa

12.

Egiaztatu sarrerak sinesgarritasun fisikoan oinarrituta

Ziurtatu operadoreek praktikoa edo fisikoki bideragarria dena soilik sartu dezaketela prozesuan. Ezarri temporizadorea eragiketa baterako fisikoki izan behar duen iraupena duen. Kontuan izan desbideraketak daudenean abisatzea.

Era berean, jakinarazi ustekabeko geldialdia dagoenean.



segurtasun helburua

Talde objektiboa

I/O balioen osotasuna

Integrazio/mantentze-zerbitzuen hornitzalea

ORIENTAZIO

a) Aurreikusitako iraupen fisikoak egiaztatu

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

Irtenbide simple bat denbora pasako alerta bat izan liteke. Hau erabilgarria izango litzateke sekuentzia/pausoak gidatutako zereginetarako.

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

Baldintza goizegi edo beranduegi betetzen bada, urratsa iraungi.

b) Espero den jarduera fisiko errepikakorra kontrolatu

Sinesgarritasun fisikoaren egiaztapenak fisikoki nekez aktibitatearen abisua ere esan nahi du: gertakarien ziklo erregularra eta errepikakorra espero bada (adibidez, multzoak, eguneko ereduak), jarduerarik gabeko temporizadore batek abisua emango du zerbait gertatzen bada. balio analogikoa) denbora gehiegi gelditzen da.

ADIBIDEA

a) Aurreikusitako iraupen fisikoak kontrolatu

- ÿ Presa baten atek denbora jakin bat behar dute guztiz itxita igarotzeko.
itxita guztiz ireki arte

- ÿ Saneamendu-zerbitzu batean, hobi heze batek denbora pixka bat behar du betetzeko

b) Programatutako errepikapen-jarduera fisikoa kontrolatu

- ÿ Fabrikazio-prozesuak edo kanalizazio-dosiak aldizka txandakatu behar ditu kontrol-eremuak edo funtzionamendu-moduak.
- ÿ Udal hondakin-uren araztegiak normalean eguneko zikloa dute
jarduera / sarrera-eredua.



c) Mugatu operadorearen sarrera ezarpenak praktiko/fisikoki posible denera.

ÿ Adibidez, Oldsmar (Florida) kasuak a) normalean behar dena baino milaka aldiz gehiago eta b) fisikoki ezinezkoa den operadore bat sartzea ahalbidetu zuen. Saiatu funtzionamendu-mugak PLC kodean ezartzen ahal den guztietan HMI scriptak erabili beharrean.

ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

1. Desbideratzeek eragingailu bat jada bazegoela adieraz dezakete korritze-egoera baten erdian edo norbait I/O faltsutzen saiatzen ari dela, adibidez, errepikapen-eraso bat eginez.
2. Inaktiboen alertak erraz egiten du sistema edo gailuaren manipulazioaren ondorio izan daitezkeen izoztutako edo behartutako balio konstanteak kontrolatzea.

fidagarritasuna

1. Desbideratzeek roaren abisua goiztiarra ematen ditzu akats elektriko edo mekanikoen ondorioz eztula.
2. Inaktiboen alertak neurketak edo sistemaren kontrol-begiztak adierazten laguntzen du gailu fisikoaren hutsegite batengatik edo kontrol-algoritmo logikoaren arazoengatik edo huts egindako sarrera edo operadore-erroreengatik huts egin dezaketen (beraz, estatikoak).

Mantentzea



ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICSrako

Taktikoa: TA010 - Prozesuaren kontrola hondatzea

Teknika: T0806 - Brute Force I/O

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

MITRE CWE

CWE-754: Ezohiko baldintzen egiaztapen okerra edo

apartekoa

13.

Desgaitu beharrezkoak ez diren/erabiltzen
ez diren komunikazio-atak eta protokoloak

PLC kontrolagailuek eta sareko interfaze-moduluek, oro har, lehenespenez gaituta dauden hainbat komunikazio-protokolo onartzen dituzte. Desgaitu aplikazioak behar ez dituen ataka eta protokoloak.



segurtasun helburua

Talde objektiboa

Gogortzea

Integrazio/mantentze-zerbitzuen hornitzalea

ORIENTAZIO

Lehenespenez gaitzen diren ohiko protokoloak, adibidez, HTTP, HTTPS, SNMP, Telnet, FTP, MODBUS, PROFIBUS, EtherNet/IP, ICMP, etab.

Praktika onena PLCareen eta beste sistemaren osagaien arteko beharrezko komunikazioak deskribatzen dituen datu-fluxuaren diagrama bat garatzea da.

Datu-fluxuaren diagramak PLCareen ataka fisikoak zein sare logikoak konektatzen dituen erakutsi behar ditu. Ataka fisiko bakoitzeko, beharrezkoak diren sare-protokoloen zerrenda identifikatu behar duzu 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 du. Erasotzaile batek baimenik gabeko komunikazioetarako erabili ezin dituela ziurtatzeko modurik errazena guztiz desgaitzea da.

fidagarritasuna

PLC bat ezin bada ataka edo protokolo jakin baten bidez komunikatu, horrek (okerreko) trafikoaren potentziala ere murrizten du, gaiztoa izan ala ez, eta horrek komunikazio-paketeen ondorioz PLCa huts egiteko aukera murrizten du.

Mantentzea

Erabiltzen ez diren atakak eta protokoloak desgaitzeak mantentze-lanak errazten ditu PLCaren konplexutasun orokorra murriztuz. Ez dagoena ez da kudeatu edo eguneratu beharrik.

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICSrako

Taktikoa: TA005 - Aurkikuntza

Teknikoa: T0808 - Kontrol-gailuaren identifikazioa, **T0841** - Network Services Scan, **T0854 - Konexioen** zenbaketa eta serieak

ISA 62443-3-3

SR 7.6: Sarearen eta segurtasunaren konfigurazio-ezарpenak

SR 7.7: Gutxieneko funtzionaltasuna

ISA 62443-4-2

EDR 2.13: Diagnostiko eta proba fisikoen interfazeen erabilera

ISA 62443-4-1

SD-4: Diseinu seguruaren praktika onak

SI-1: Segurtasun Aplikazioaren Berrikuspena

SVV-1: Segurtasun-baldintzen proba

14.

Mugatu hirugarrenen datuen interfazeak

Mugatu hirugarrenen interfazeetarako eskuragarri dauden konexio eta datu motak. Konexoak eta/edo datu-interfazeak ondo definitu eta mugatuta egon behar dira, beharrezkoa den datu-transferentziarako irakurtzeko/ idazteko gaitasuna soilik uzteko.



segurtasun helburua

Talde objektiboa

Gogortzea

Integrazio/mantentze-zerbitzuen hornitzailea

ORIENTAZIO

Zenbait kasutan, kable luzeak edo datu-truke zabalak direla eta, interkonektatutako datu-konexioek negozio kasu hobea eskaintzen dute bi alderdi ezberdinaren arteko kable bidezko datu-trukeak baino.

Ahal den neurrian, honako printzipio hauek kontuan hartu eta jarraitu behar dira hirugarrenen datuen truke-interfazea diseinatzean eta ezartzean:

ÿ Erabili komunikazio-modulu dedikatu bat, hirugarrenen PLCA edo datuak trukatzeko ekipoetara zuzenean konektatuta, edo erabili sare-ekipo dedikatua alderdi bakoitzaren sare nagusitik fisikoki bereizita.

ÿ Konektatutako gailuen MAC helbidea normalean eskuragarri dago ICS Ethernet gaitutako edozein gailuren sistema-aldaagaietan, gailuaren identitatea faktore anitzeko ikuspegia erabiliz (IP helbidea + MAC fabrikatzailearen kodea = ICS gailua). Praktika hau ez da inongoa, MAC eta IP helbideak faltsu daitezkeelako, baina ICS sistema eta gailu fidagarrien arteko komunikazioen muga igotzen du.

ÿ Hirugarrenen interfazeetarako protokolo bat hautatzen duzunean, aukeratu protokoloa minimizatzen duen hirugarrenen gaitasuna jabearren sisteman datuak idazteko.

ÿ Aukeratu hirugarren bati jabearren PLCA edo datuak trukatzeko ekipoak konfiguratzea eragozten dion konexio-metodo eta konexio-ataka.

ÿ Hirugarrenak ezin izan behar du berariaz definitu ez den datuetan irakurri edo idatzi. zuk eta eskuragarri jarri.

ÿ Erabili zaintzako temporizadore bat komunikazioa kontrolatzeko, arriskuan egon ez dadin. bidali aginduak PLC batera akats moduan.

ÿ Serie-konexioa: Erabili komunikazio-modulu dedikatu bat hirugarrenen interfaze bakoitzeko datu-matrize mugatu batekin. Ziurtatu jabearren konexioaren aldea abiarazlea dela eta hirugarrena erantzuna dela.



ÿ Ethernet/IP: PLC batzuek komunikazio-moduluei suebaki gisa funtzionatzea ahalbidetzen diente eta paketeen ikuskapen sakona (DPI) egin dezakete, edo komunikazio-moduluen interfazeak mugatu ditzakete datu-trukea aurrez definitutako azpimultzo batera mugatzeko. Ezaugarri hauek erabilgarri badaude eta Ethernet/IP protokoloa erabiltzen bada, ziurtatu funtzioak gaituta eta konfiguratuta daudela.

ÿ Eragiketa- edo kontratu-baldintzek jabeari aurrekoan egitea eragozten diotenean, kontuan hartu "datuen kontzentrazio" PLC bereizi bat erabiltzea (proxy/DMZ gisa ere ezagutzen dena) datuak gordetzeko eta jabea idazketa/berridazketatik babesteko. . Ziurtatu PLC honen atzoko planoa ezin dela hirugarren saretik zeharkatu.

ADIBIDEA

- ÿ Zaintza Automatikoko Transferentzia Unitateak (LACT), ekoizle edo petrolio eta gasbideen konpainia baten eta enpresen artean informazioaren neurketa, egoera eta baimenak partekatzen dituzten sareko edo serieko konexioak dituzten ekoizle edo petrolio eta gasbideen konpainia baten artean trukatzen diren hidrokarburoak edo ura transferitzen eta neurten dituztenak. .
- ÿ Eskualdeko edateko uraren hornitzalea (importatzailea) desbideratzeko uraren emaria partekatzen duena tokiko udalerri bateko ur plantara entregatzen dena.



ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

1. Mugatu hirugarrenen sare eta ekipoekiko esposizioa.
2. Autentifikatu kanpoko gailuak faltsutzea ekiditeko.

fidagarritasuna

Aldaketak edo sarbideak egiteko gaitasuna mugatzen du, nahita edo nahi gabe, hirugarrenen kokapen edo ekipoetatik.

Mantentzea

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICS

Taktikoa: TA010 - Prozesuaren kontrola hondatza
Teknika: T0836 - Parametroa aldatu

ISA 62443-3-3

SR 7.6: Sarearen eta segurtasunaren konfigurazio-ezarpenak
SR 7.7: Gutxieneko funtzionaltasuna

ISA 62443-4-2

SR 7.6: Sarearen eta segurtasunaren konfigurazio-ezarpenak
SR 7.7: Gutxieneko funtzionaltasuna

ISA 62443-4-1

SD-4: Diseinu seguruaren praktika onak
SI-1: Segurtasun Aplikazioaren Berrikuspena
SVV-1: Segurtasun-baldintzen proba

15.

Definitu prozesu-egoera seguru
bat PLC berrabiarazten bada

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



segurtasun helburua

Talde objektiboa

erresilientzia

kodea hornitzalea

Integrazio/mantentze-zerbitzuen hornitzalea

ORIENTAZIO

Zerbaitek PLC bati lan-prozesu baten erdian berrabiarazteko agintzen badio, programak arin hastea espero beharko genuke prozesu gutxieneko etenaldiarekin. Ziurtatu kontrolatzen duzun prozesua berrabiarazteko segura dela.

Ezinezkoa bada PLCa segurtasunez berrabiarazteko ezartzea, ziurtatu gertakari horren berri ematen dizula eta ez duela komando beririk igortzen. Halaber, kasu horretarako, ziurtatu Eragiketa Prozedura Estandarrek (SOP) eskuzko kontrolak konfiguratzeko argibide oso argiak dituztela, PLCak prozesua behar bezala abiarazteko.

Era berean, dokumentatu hegaldiak kontrolatzeko sistemaren abiarazte, itzaltze, egoera egonkorreko egiaztapen eta berrabiarazi prozedura guztiak.

ADIBIDEA

/



ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

Ezabatu ustekabeko portaera posiblea:

PLC baten eraso-bektorerik oinarrizkoena kraskatzea eta/edo berrabiaraztea da. PLC askorentzat ez da hain zaila egitea, PLC askok ezin baitute ustekabeko sarrera edo trafiko gehiegi aurre egin. Exekutatzen ari den bitartean kontrolagailuaren ekintzei buruzko hainbat diagnostiko dauden arren, abian den prozesu batekin abiarazteak nola kudeatzen dituen askotan ez dago argi. Hau ezohikoa izan daiteke, baina oinarrizko eraso-bektorea da erasotzaile baten portaera gaitza kontuan hartuta.

fidagarritasuna

Saihestu ustekabeko

atzerapenak: PLC bat piztu ondoren, egoera-makina prozesua abiarazterik uzten ez duten baldintza batzuk dituen egoera batean abiarazten bada, eta operadoreak ezin du sistema normalizatu, teknikari batek PLCaren programan sartu beharko luke. behartu baldintzak nahi den egoerara joan daitezen eragiketa hasteko. Horrek atzerapenak eta produkzioa galtzea eragin dezake.

Mantentzea

/

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICS

Taktikoa: TA009 - Inhibit Erantzun Funtzioa

Teknika: T0816 - Gailua berrabiarazi/Itzali

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-baldintzen proba

16.

Laburbildu zikloaren denborak
PLCa eta HMIn joera

Laburtu PLCareen ziklo-denbora 2-3 segundoz behin eta jakinarazi HMI-ri grafiko batean bistaratzeko.



segurtasun helburua

Talde objektiboa

Gainbegiratzea

Integrazio/mantentze-zerbitzuen hornitzailera

ORIENTAZIO

Ziklo-denborak normalean PLC bateko sistema-aldagaiak dira eta PLC kodean laburbiltzeko erabil daitezke. Laburpena egin behar da batez besteko, gehienezko eta gutxieneko ziklo-denborak kalkulatzeko.

HMIk balio horien joera ezarri behar du eta aldaketa nabarmenak egonez gero alerta.

Ziklo-denbora PLCareen logikaren iterazio bakoitza kalkulatzeko behar den denbora da. Iterazioak eskailera-diagramen (LD), funtziobloke diagramen (FBD), instrukzio-zerrenda (IL) eta testu egituratuaren (ST) konbinazioa dira. Osagai logiko hauek Funtzio Sekuentzial Plakekin (SFC) lotu daitezke.

Ziklo-denborak konstanteak izan behar dira PLC batean, aldaketarik ez badago, adibidez:

- ÿ sare-ingurunea

- ÿ PLC logika

- ÿ prozesua

Hori dela eta, ezohiko ziklo-denbora aldaketak PLCareen logika aldatu den adierazle izan daitezke eta, beraz, informazio baliotsua ematen dute osotasuna egiazatzeko.

Grafiko batean denboran zehar balioak bistaratzeko modu intuitiboa eskaintzen du balio absolutuak soilik erabilgarri egongo balira ikustea zailago litzatekeen anomaliei arreta erakartzeko.

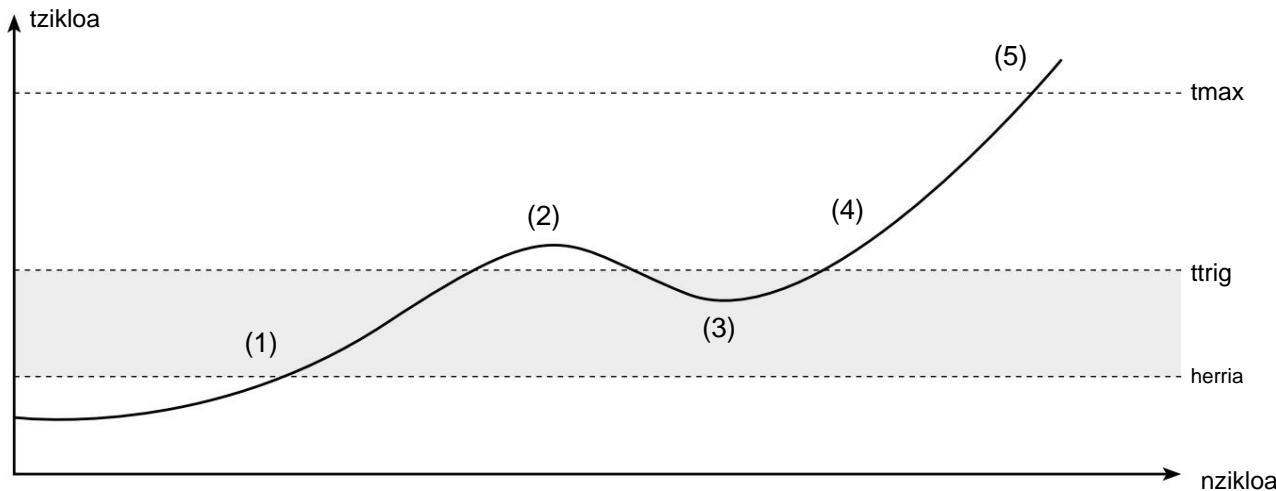
ADIBIDEA

PLC askok "ziklo-denbora maximoa" kontrola dute hardware mailan. Ziklo-denborak gehienezko balioa gainditzen badu, hardwareak PUZa STOP-ean jartzen du (5).

Jakina, erasotzaileak horretaz jakitun dira eta posible den eraso-kodea ahalik eta txikiena mantenduko dute ziklo-denbora orokorrean eragina gutxitzeko. Ziklo-denbora kontrolatzeko beste programa batean, erreferentzia-ziklo-denbora tref oinarrizko ziklo-denbora gisa definitzen da.

Gorabehera txikiak naturalak direnez, beharrezkoa da atalase onargarria (1,3) definitzea. Zikloaren gainbegiratzea aktibatu egiten da (2,4) atalasea gainditzen bada.

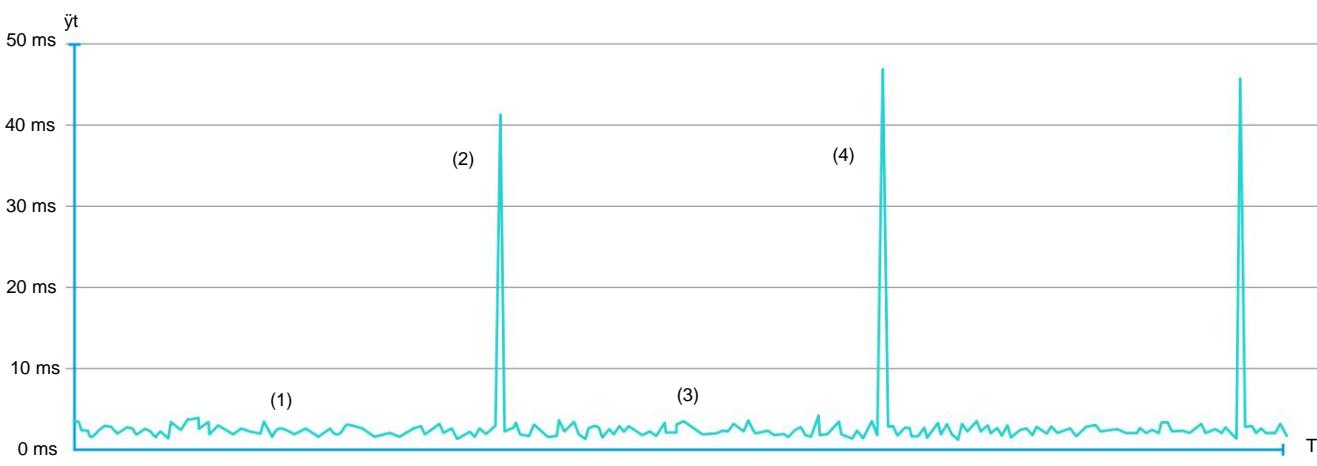




Erreferentzia-denboraren edozein desbideratze erregistro-fitxategi batean gorde daiteke honela:

	Data	UTC ordua	desbideraketa
1	2019-11-22	09:05:50.021	40.821 ms
2	2019-11-22	09:06:00.069	44.391 ms
3	2019-11-22	09:06:10.120	44.994 ms
4	2019-11-22	09:06:20.166	40.561 ms
5	2019-11-22	09:06:30.211	40.725 ms

Ziklo-denborak HMIan erregistratzen badira, PUZaren karga astunak ikusten dira 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)-n exekutatzen da eta horrek ziklo-denbora handitzen du.



09:18:57 09:18:58 09:18:59:19:00 09:19:02 09:19:04 09:19:05 09:19:06 09:19:07 09:19:09 09:19:10 09:19:11 09:19:12 09:19:14 09:19:15 09:19:16 09:19:18 09:19:19:21 09:19:23 09:19:25 09:19:27 09:19:28 09:19:29 09:19:32



ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

PLCen aurkako erasoen artean, logika aldatzea, programa berri bat aktibatzea, kode berria probatzea, prozesu-formula berri bat kargatzea, logika osagarria txertatzea mezuak bidaltzeko edo funtzioren bat aktibatzeko dira.

PLC gehienentzat, osotasun kriptografikoen egiaztapen tradizionalak ez dira bideragariak. Hala ere, komeni da goiko aldaketa logikoren bat gertatzen bada abisatzea.

Ziklo-denborak nahiko konstanteak direnez zirkunstantzia normalean, ziklo-denboraren aldaketak goiko osagai logikoetako batean logika aldatu izanaren adierazle ona dira.

fidagarritasuna

Ikusi segurtasuna, baina kausa ez-maltzurengatik.

Mantentzea

/

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICS

Taktikoa: TA002 - Exekuzioa

Teknika: T0873 - Project File Infection

ISA 62443-3-3

SR 3.4: Softwarea eta informazioaren osotasuna

ISA 62443-4-2

EDR 3.2: Kode maltzurren aurkako babesia

MITRE CWE

CWE-754: ezohiko edo salbuespenezko baldintzen egiaztapen okerra

17.

Grabatu funtzionamendu-denbora PLCa eta bere joera HMIan

Grabatu PLCaren funtzionamendu-denbora noiz berrezarri zen jakiteko. Diagnostikorako HMI-n egonkortasunaren joera eta grabazioa.



segurtasun helburua

Talde objektiboa

Gainbegiratzea

Integrazio/mantentze-zerbitzuen hornitzalea

ORIENTAZIO

Egin jarraipena PLC-ren denboraren jarraipena

- ÿ PLCan bertan (funtzio-denbora PLCko sistemaren aldagaia bada)
- ÿ PLCan bertan MIB-2 / SNMP implementazioren bat badu
- ÿ kanpotik, adibidez, SNMP bidez

PLCak MIB-2-rekin SNMP badu, oso ohikoa dena, "sysUp TimeInstance(0)" funtzionamendu-denboraren OID 1.3.6.1.2.1.3 da. Exekutatu denbora berrezartzeak PLC berrezartzeko adierazle garrantzitsuak dira. Ziurtatu HMIak PLC berrezartze motaren berri ematen duela.

Errore-kodeekin erlazionatutako funtzionamendu-denbora diagnostiko onak dira.

ADIBIDEA

/



ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

PLC baten eraso-bektorerik oinarrizkoena kraskatzea eta/edo berrabiaraztea da. PLC askorentzat ez da hain zaila egitea, PLC askok ezin baitute ustekabeko sarrera edo trafiko gehiegi aurre egin. Beraz, ustekabeko berrabiarazteak PLCa ezohiko ekintzak aurkitzen ari den adierazle izan daitezke.

fidagarritasuna

PLC berrezartzeak ere onak dira akatsen kasuan diagnostikatzeko eta zein PLCTan lan egiten den eta zein ordutan kontrolatzeko.

Mantentzea

/

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICS

Taktikoa: TA009 - Inhibit Erantzun Funtzioa

Teknika: T0816 - Gailua berrabiarazi/Itzali

ISA 62443-3-3

SR 7.6: Sarearen eta segurtasunaren konfigurazio-ezarpenak

ISA 62443-4-2

SR 7.6: Sarearen eta segurtasunaren konfigurazio-ezarpenak

MITRE CWE

CWE-778: Erregistro nahikoa

18.

Grabatu PLC geldialdi gogorrak eta joera horiek HMIen

HMI alarma-sistemek PLCa berrabiarazi aurretik konsulta ditzaten akatsen edo itzaltzeen ondorioz PLC gogor gelditzeko gertaerak gordetzen ditu. Denbora sinkronizazioa datu zehatzagoak lortzeko.



segurtasun helburua

Talde objektiboa

Gainbegiratzea

Integrazio/mantentze-zerbitzuen hornitzalea

ORIENTAZIO

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

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

PLC gehienek ere gertaerak sortzen dituzten eskaneatu-lehen funtzio mota bat dute.

PLC ekipamendu ia guztiak nolabait duten portaera da. Funtsean, bandera bat edo gehiago da, edo "esnatu ondoren" PLC baten lehen eskanean exekutatzen den errutina izendatua. Lehenengo eskaneatu hau erregistratu eta jarraipena egin behar da.

ADIBIDEA

/



ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

Erregistroek gorabeheraren bat gertatuz gero arazoak konpontzeko aukera ematen dute. PLC bat martxan jarri aurretik, batez ere arazoak izan ondoren, garrantzitsua da fidagarria dela ziurtatzea.

fidagarritasuna

Erregistroak arazketa-iturri onak dira, gertaera maltzurrez sortu ez bada.

Mantentzea

/

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICS

Taktikoa: TA009 - Inhibit Erantzun Funtzioa

Teknika: T0816 - 1. Gailua berrabiarazi/Itzali

ISA 62443-3-3

SR 7.6: Sarearen eta segurtasunaren konfigurazio-ezarpenak

ISA 62443-4-2

SR 7.6: Sarearen eta segurtasunaren konfigurazio-ezarpenak

MITRE CWE

CWE-778: Erregistro nahikoa

19.

Kontrolatu memoriaren erabilera PLCa eta bere joera HMIan

Neurtu eta eman memoria-erabileraren oinarrizko lerroa ekoizpen-ingurunean implementatutako kontrolagailu bakoitzarentzat eta HMI-n joera.



segurtasun helburua

Talde objektiboa

Gainbegiratzea

Integrazio/mantentze-zerbitzuen hornitzalea

Aktiboen jabea

ORIENTAZIO

Logikaren kode-lerroak handitzeak memoria-kontsumoa areagotu dezakeenez exekuzio-denboran, PLC programatzailleei gomendatzen zaie oinarrizko lerroetik edozein desbideratzeen jarraipena egitea eta gertaera honi alarma-klase bat eskaintza.

ADIBIDEA

Rockwell Allen Bradley PLC-ean, kontrolagailu bat oinarri-lerro bat egin daiteke eta memoria-erabileraren jarraipena egin daiteke RS Logix 5000 atazak monitorizatzeko tresna erabiliz. I/O eta Ladder/Tag memoria joerak erabiliz jarraipena egin daiteke.



ZERGATIK?

Onuragarria...?

Zergatik?

Segurtasuna

Memoriaren erabilera handitzea PLCA hondatutako kodea exekutatzen ari den adierazle izan daiteke.

fidagarritasuna

Exekutatzen diren programen memoria-erabileraren jarraipena egitea erabilgarria izan daiteke memoria-kontsumo osoa eta PLC kontrolagailuaren akats-egoera saihesteko.

Mantentzea

Memoria-erabileraren jarraipena erabil liteke kontrolatzale gainbegiratuaurentzat eskaneatzeko denborarik onena sintonizatzeko eta aurkitzeko, baina baita egoera txarrekin lotutako arazoak eta arazoak konpontzeko ere.

ERREFERENTZIAK

estandarra / esparrua

mapaketa

MITRE ATT & CK ICS

Taktikoa: TA002 - Exekuzioa

Teknika: T0873 - Project File Infection

ISA 62443-3-3

SR 3.4: Softwarea eta informazioaren osotasuna

ISA 62443-4-2

EDR 3.2: Kode maltzurren aurkako babesia

20.

Programa negatibo faltsu tranpa eta positibo faltsuak alerta kritikoetarako

Identifikatu alerta kritikoak eta ezarri tranpa bat alerta horientzat.

Konfiguratu tranpa abiarazte-baldintzak kontrolatzeko eta edozein
desbiderapenen alerta-egoera kontrolatzeko.



segurtasun helburua

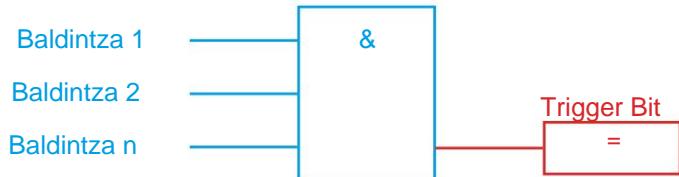
Talde objektiboa

Gainbegiratzea

Integrazio/mantentze-zerbitzuen hornitzalea

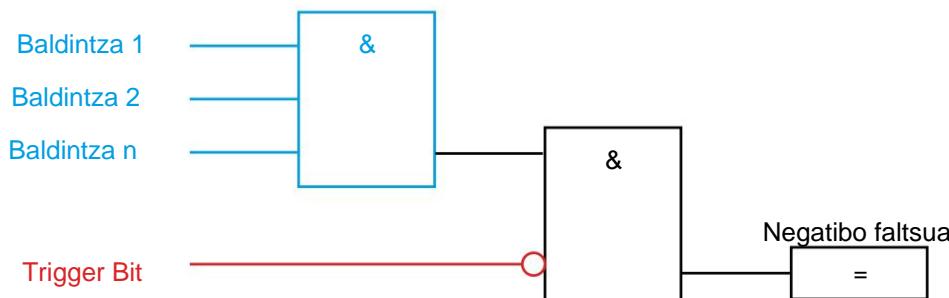
ORIENTAZIO

Kasu gehienetan, alerta-egoerak boolearrak dira (Egia, Gezurra) eta baldintza jakin batzuek abiarazten dituzte, behean erakusten den moduan. Esate baterako, "gainpresioa" alertaren aktibazio-bitak EGIA bihurtzen da, 1. baldintza "presio-interruptora 1", 2. baldintza "presio-sentsorearen atalase kritikoaren balioa", n. arte, EGIA bada.



Eraso bat ezkutatzeko, etsai batek alerta gaitzeko bit ezabatu eta negatibo faltsu bat eragin dezake.

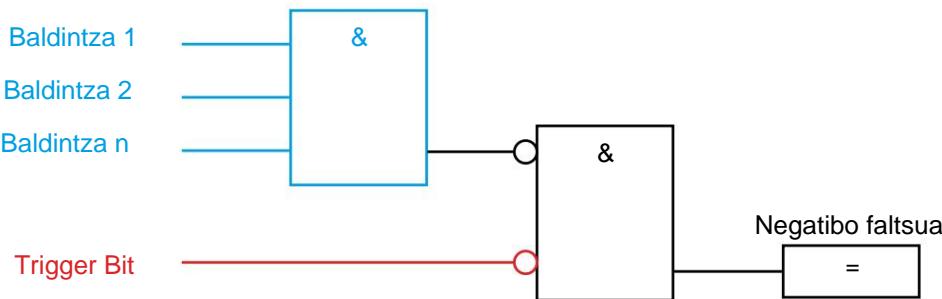
Tranpa negatibo faltsu batek abiarazte-bitaren eta abiarazle-bitaren baldintzak kontrolatzen ditu. Konfigurazio simple honenkin, negatibo faltsu bat detektatzen da. Ikusi hurrengo irudia:



Beste kasu batzuetan, aurkari batek positibo faltsuak sor ditzake nahita, prozesuko operadorearen arreta kentzeko.



Negatibo faltsuko tranparen modu berean, positibo faltsuak ere detekta daitezke alertaren abiarazte-bitaren jarraipena eginez eta abiarazte-baldintzak betetzen diren ala ez. Baldintzak EZ badira betetzen, baina abiarazte-bitak aktibo badago, positibo faltsu bat detektatzen da: Ikusi irudi hau:



ADIBIDEA

1. adibidea: Siemens-ek bere Siemens S7-1200/1500 produktuetan funtziogunetan web zerbitzari bat eskaintzen du, adibidez, PLCarenen egoera, ziklo-denbora edo estaldura-erregistroak bistaratzea. Datu-taulak eta aldagaiai ikusteko eta aldatzeko aukera ere baduzu. Web zerbitzarirako sarbide-eskubideak PLCarenen hardware-konfigurazioan alda daitezke. Gaizki konfiguraturako sarbide-eskubideen kasuan, aurkari batek PLCarenen aldagai eta datu-blokeetara sar lezake. Positibo faltsu bat sortzeko, etsaiak alerta-gaitzko bit bat hautatzen du eta egoera aldatzen du.

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

3. adibidea: autobusen injekzio-eraso batek alerta positibo faltsu bat bidal diezai oike maila altuko SCADA bezero batik.



ZERGATIK?

Onuragarria...?	Zergatik?
Segurtasuna	Aurkari batek bere erasoa nahastu izanak eragindako alerta-mezuen negatibo faltsuak edo positibo faltsuak arintzen ditu (hau da, kode faltsuak, bus injekzioa, PLC eskuragarri dauden egoera-taulen manipulazioa web zerbitzari seguruetan).
fidagarritasuna	/
Mantentzea	/

ERREFERENTZIAK

estandarra / esparrua	mapaketa
MITRE ATT & CK ICS	Taktikoa: TA009 - Erantzunaren inhibizio funtzioa Teknika: T0878 - Alarma kentzea
ISA 62443-3-3	SR 3.5: Sarreraren baliozkotzea
ISA 62443-4-2	CR 3.5: Sarreraren baliozkotzea
ISA 62443-4-1	SI-1: Segurtasun Aplikazioaren Berrikuspena
MITRE CWE	CWE-754: Ezohiko baldintzen egiaztapen okerra edo apartekoia

Proiektuari buruz PLC programazio segurua

Urte askotan, kontrolagailu logiko programagarriak (PLC) ez dira seguruak izan diseinuz. Hainbat urtetan IT praktika onen pertsonalizazioak eta aplikazioak protokolo seguruak, komunikazio zifratuak, sarearen segmentazioa, etab. Hala ere, orain arte, arreta gutxi jarri zaio PLCen (edo SCADA/DCS) ezaugarriak segurtasunerako erabiltzeari edo PLCak segurtasuna kontuan hartuta nola programatu. Proiektu honek - egungo Ordenagailu Secure Kodetze Praktiketan inspiratua - hutsune hori betetzen du.



NORK IRAKURRI ETA INPLEMENTATU BEHAR DITU PLCAREN KODETZE SEGURAKO PRAKTIKAK?

Praktika hauek ingeniarientzat diseinatu dira. Proiektu honen helburua softwarea sortzen duten ingeniariei jarraibideak ematea da (eskailera-logika, funtzio-diagramak, etab.) industria-kontrol-sistemen segurtasun-jarrera hobetzen laguntzeko. Praktika hauek PLC/DCS-n natiboki eskuragarri dauden funtzionaltasunaz baliatzen dira. Praktika hauek ezartzeko hardware edo software-tresna gehigarri gutxi behar dira. PLC programazio eta funtzionamenduaren lan-fluxu arruntean sartu daitezke guztiak. Segurtasun-esperimentzia baino gehiago behar da, babestu beharreko PLCak ondo ezagutzea, haien logika eta azpiko prozesua praktika hauek ezartzeko.

ZEIN DA ZERRENDA HONEN IRISMENA / NOLA DEFINITZEN DA PLC KODEA?

20 PLC Secure Kodeketa Praktiken zerrendaren esparruan sartzeko, praktikek PLC batean zuzenean egindako aldaketak sartu behar dituzte. Dokumentu honetan ikusten duzuna PLC kodeketa seguruko praktika potentzialen kopuru handiagoaren 20 aukeraketa da. Arkitektura orokorrarekin, HMiekin edo dokumentazioarekin lotutako aurretiazko praktika osagarriak ere badaude. Hauek ez dira PLC kodeketa seguruaren esparruan sartzen, baina etorkizuneko PLC ingurune seguruen zerrendan egon daitezke.

ZEIN DITU PLC SEGURUAK KODETZEKO PRAKTIKAK APLIKATZEAREN ABANTAILAK?

Praktika hauek erabiltzeak segurtasun-onurak ditu argi eta garbi, batez ere eraso-azalera murrizten duelako edo segurtasun-intzidentziaren bat gertatuz gero arazoen ebaZen azkarrago ahalbidetuz. Hala ere, praktika askok segurtasunaz harago abantaila gehigarriak dituzte. Batzuek, gainera, PLC kodea fidagarriagoa egiten dute, arazketa eta mantentze errazago, komunikatzeko errazagoa eta, agian, simpleagoa baita. Gainera, PLC kodetze-praktiek erabiltzaileei erasotzaile gaitz bat izanez gero laguntzeaz gain, PLC kodea sendoagoa egiten dute ustekabeko konfigurazio okerretan edo giza akatsei aurre egiteko.



NOR DAGO PROIEKTU HONEN ATZEAN?

Jake Brodskyren S4x20 hitzaldiarekin hasi zen dena “Secure Coding Practices for PLCs”.

Konferentziaren ostean, Dale Petersonek Top 20 proiektuari ekin zion. Jake Brodskyk eta Sarah Fluchsek hainbat ordu eman zituzten telefonoz Jake-k proposatutako PLC kodeketa seguruko praktikak paperean jartzen. Gero, Dale, Jake eta Sarah plataforma bat sortu zuten top20.isa.org webgunean, ISA GCAren laguntzarekin, ICS ingeniaritzarik eta segurtasun komunitateen ekarpen gehigarriak egituratzeko eta biltzeko.

Eztabaidak eta praktiken testuak finkatzeak, bai eta 20 praktika garrantzisenen zerrenda prestatzeak ere urtebete irauen zuen gutxi gorabehera; prozesua bizkortu zen Vivek Ponnadari esker, edukiak ekarpenak egiteaz eta berrikustearaz gain, ohiko deialdiak antolatu baitzituen praktikei buruzko iruzkin guztiak konpondu arte; Mohamed Abdelmoez Sakesli, estandar-erreferentzia guztiak ahalegin handiz gehitu zituena, MITRE CWE taldea, azken momentuan CWE erreferentziak eman zituena, Sarah, orain irakurtzen ari zaren dokumentua osatu zuena, eta Jake, Dale , John Cusimano, Dirk. Rotermund, Josh Ruff, Thomas Rabenstein, Gus Serino, Walter Speth, Agustín Valencia Gil-Ortega, Marcel Rick-Cen eta Al Ratheesh R, ohiko deietan ekarpenak eman zituztenak.



EMAILEEN ZERRENDA

PLC Secure Coding Proiektua komunitatearen benetako ahalegina da eta izaten jarraitzen du, PLC eta segurtasunari buruzko denbora eta ezagutza eskuzabaltasunez partekatzen duten hainbat laguntzailerik gabe posible izango ez zena. Guztira 943 erabiltzailek eman dute izena plataforman eztabaideatzeko eta ekarpenak egiteko. Jarraian izendatzea espresuki onartu zuten guztien zerrenda alfabetikoa da. Eskerrik asko proiektu honi laguntzeko ardura hartu duzuen guztioi.

Aagam Shah	Heiko Rudolph	Miguel Angel Fria
Adam Paturej	Isiah Jones	Mohamed Abdelmoez Sakesli
Agustin Valencia Gil-Ortega	Jacob Brodsky	Luna Eluvangal Chandran
Aitor Garcia Alminana	Javier Perez Quezada	Nahuel Iglesias
Alec Summers	JD Bamford	Nalini Kanth
Al Ratheesh. R	Joe Weiss	NarasHMia S. Himakuntala
Andreas Falk	John Cusimano	Omar Morando
Anton Shipulin	John Hoyt	Oscar J. Delgado-Melo
Arkaitz Gamino	John Powell	Päivi Brunou
carlos olave	John Kingsley	Peter Donnelly
Chris van den Hooven	Joseph J. Januszewski	Peter Jackson
Chris Sistrunk	Josh Ruff	Ravindra Deshakulakarni
Christos Alexopoulos	Josie Houghton	Rick Booij
Cris DeWitt	Jozef Sulwinski	Robert Albach
Dale Peterson	Juan Pablo Angel Ispilua	Rushi Purohit
Dene Yandle	Khalid Ansari	Sarah Fluchs
Dennis Verschoor	Marc Weber	Sergei Biberdorf
Dirk Rotermund	Marcel Rick-Cen	Stephan Beirer
Edorta Echave García	Martin Huddleston	Steve Christey Coley
Gananand Kini	Massimiliano Zonta	Thomas Rabenstein
George Alex Holburn	Matthew Loong	Tim Gale
Gus Serino	Matthew Mueller	Vivek Ponnada
Hakija Agic	Michael Thompson	Vytautas Butrimas
Hector Medrano	Michal Stepien	Walter Speth



Esker bereziak erakunde horiei, eskuzabaltasunez proiektu-taldeari erabiltzeko azpiegiturak eskaini zizkiontenak, hala nola domeinuak, hostinga eta web diseinua eta



Copyright (c) 2021 admeritia GmbH, Langenfeld/Rhineland, Alemania

Honen bidez, baimena ematen zaio, dohainik, "Datuak enkriptatzeko 20 praktika seguruenen kopia bat lortzen duen pertsonari". "PLC Top 20 Secure Coding Practices" mugarik gabe aurre egiteko, besteak beste, baina ez mugatu gabe, erabiltzeko, kopiatzeko, aldatzeko, batu, argitaratu, banatu, azpilizentzia edo/edo saltzeko eskubideak barne. "PLC Top 20 Secure Kode Praktiken" kopiak, eta "PLC Top 20 Secure Kode Praktikak" ematen zaizkien pertsonei horretarako baimena eman, baldintza hauetan betez:

Goiko copyright-oharra eta baimen-ohar hau "PLC Top 20 Secure Coding Practices"-en kopia guztietan edo zati garrantzitsuetan sartuko dira.

"PLC Top 20 Secure Kode Praktikak" "BELEAN" EMATEN DIRA, INOLAKO BERMErik GABE, EZ ASAZITZIK EZ INPLIZITARIK. SALGAITASUN, HELBURU BATEKO EGOKITASUN ETA URRATZE EZKO BERMEAK BARNE, BAINA MUGATU EZ. EGILEAK EDO ESKUBIDEEN TITULARRAK EZ DUTE EZIN EGINDAKO ERREKLAMAZIO, KALTE EDO BESTE ERANTZUKIZUNAREN ERANTZUKIZUN IZANGO, ALA KONTRATU, ALEGRE EDO BESTELAKO EKINTZA, "Top 20 Coding Practices Secure PLC-REN ERATORTZEN, HANDIK EDO HORRETARAKO ERABILTZEN." EDO ERABILERA EDO BESTE TRATAZIOA "PLC kodetze-praktika nagusienetako 20".



- 📍 Delizieen pasealekua, 30 - 2.a. 28045 Madril
- 📞 +34 910 910 751
- ✉️ info@cci-es.org
- 🌐 www.cci-es.org
- 💻 blog.cci-es.org
- 🐦 @info_cci
- linkedin www.linkedin.com/in/centrociberseguridadindustrial



↳ <https://plc-security.com/>
↳ @securePLC