Auteurs: Ilan Sosnovitch is Global Sales Manager, SIGA OT Solutions (https://sigasec.com/), partner van Aexus. Frank van der Meulen is bereikbaar via frank@aexus-europe.com

Een paradigmaverschuiving in de detectie van cyberdreigingen bij machines en apparatuur in operationele en ICS-omgevingen

De onbetwistbare waarde van LEVEL 0 - elektrische signalen liegen niet

Zonder afbreuk te doen aan het belang van netwerkmonitoring bij bescherming van industrial control systems (ICS) in operational technology (OT) omgevingen, is het essentieel om het belang in te zien van monitoring en detectie van veld- en procesgeoriënteerde afwijkingen op Level 0: de sensoren en actuatoren op apparatuur- en machineniveau. Alleen zo ben je in staat om een OT-systeem holistisch te beschermen.

De term Level 0 is een onderdeel van de purdue enterprise reference architecture (PERA). Dit model beschrijft in een hiërarchische structuur de lagen die van toepassing zijn op procesautomatisering. Het model bevat zes niveaus. Bovenaan op Level 5 bevindt zich de internet DMZ. Level 4 is het bedrijfsnetwerk van de organisatie. Level 3 is de productiezone of het hoofdcontrolecentrum, dat communiceert met human-machine-interface (HMI)-controlepunten op Level 2. Deze HMI's communiceren met Level 1-controllers en Level 0-veldapparatuur. Vanuit cyberperspectief bevatten de Levels 1 tot en met 5 traditionele IT-cyberoplossingen, bestaande uit servers, werkstations, switches, routers en firewalls. Op Level 0 is de omgeving echter significant anders. Controllers (PLCs) dicteren de fysieke ruimte en communiceren met apparatuur door middel van stroom- en voltagesignalen. Daarom moet cybersecurity op Level 0 heel anders worden aangepakt.

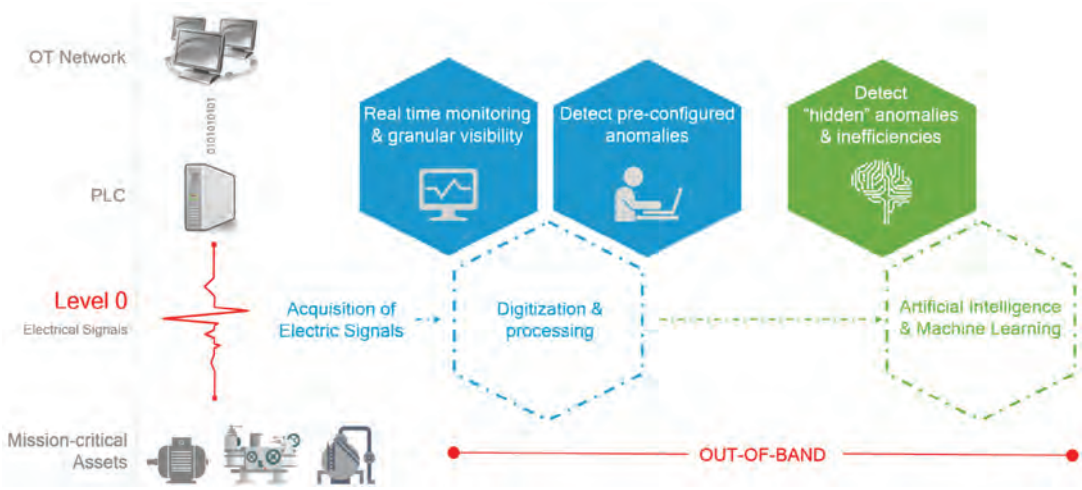
Kwetsbaarheid OT-infrastructuren

Het monitoren van de elektrische signalen, die direct vanaf de kritieke assets worden verzonden, is een zeer waardevolle en betrouwbare manier om kwaadwillende cyberaanvallen op operationele machines en apparatuur te detecteren. In tegenstelling tot intrusion detection solutions op netwerkniveau, die vaak afgeschermd zijn van het eigenlijke proces, kan monitoring en diagnose van ongefilterde en niet te hacken elektrische signalen op Level 0 leiden tot waterdichte bescherming van bedrijfskritieke operationele assets.

Veel cyberaanvallen, zoals Stuxnet, Irongate en de meest recente cyberaanvallen op watervoorzieningen, onderstrepen de kwetsbaarheid van OT-infrastructuren wereldwijd. Omdat monitoring van Level 0 volledig losstaat van het Level 1 netwerk, zorgt dit voor operationele weerbaarheid. Zelfs wanneer cyberaanvallen erin slagen om de logica van ICS controllers te manipuleren. Het belang van Level 0-monitoring is al gevalideerd en weergegeven in recente regelgevende richtlijnen voor kritieke infrastructuur, en door vooroplopende experts en opiniemakers wereldwijd.

OT- versus IT-beveiliging

Control systems maken gebruik van commerciële 'off-the-shelf' human-machine interfaces met communicatienetwerken en daarnaast veldapparatuur (processensoren, actuatoren en aandrijvingen) met hun veldniveau-netwerken. Oorspronkelijk kent cybersecurity in OT-omgevingen een top-downbenadering. Eerst worden digitale muren rond de digitale assets gebouwd, gevolgd door identificatie van malware en netwerkafwijkingen in de IP-netwerken. Dit komt doordat voor IT-afdelingen de beveiliging van procesapparatuur ophoudt bij de netwerklaag. De IT-benadering is uitgebreid om ook control systems te beveiligen, door het monitoren van operational technology (OT) control system ethernet netwerken. Deze benadering is noodzakelijk, maar niet volledig toereikend om control systems veilig te maken en ernstige schade aan OT-apparatuur en machines te voorkomen. Netwerkbeveiliging gaat namelijk nooit in staat zijn om de echte



Aanval op Israëlische watervoorzieningen
Eind april 2020 onderstreepte een Stuxnet-achtige aanval op de Israëlische watervoorzieningen het vitale belang van Level 0-monitoring. Klaarblijkelijk was het doel om het chloorgehalte in de watervoorziening te verhogen door de logica van de PLC te veranderen zonder alarmen te laten afgaan. "… Ze probeerden de chloorniveaus te manipuleren en op hetzelfde moment beheerders een signaal te sturen dat de chloorniveaus naar behoren waren," aldus cybersecurity experts (2). Deze cyberaanvallen markeren de kwetsbaarheid van de water- en energie-infrastructuur wereldwijd.

assets van de OT-architectuur volledig af te schermen: de fysieke apparatuur en processen, of in andere woorden, Level 0-apparatuur. Cybersecurity detectiesystemen voor netwerkafwijkingen gaan ervan uit dat processensoren veilige, geauthentiseerde input bieden. Echter, deze apparaten of apparaat-netwerken kennen geen beveiliging of authenticatie. Sterker nog, verouderde control system apparatuur heeft geen opties voor beveiliging of authenticatie, en toont ook niet welke specifieke control system apparatuur (zoals pompen, ventielen, motoren en relais) kwetsbaar zijn voor netwerkaanvallen. Daardoor kan de IT/OT-benadering geen betrouwbaarheid, weerbaarheid of veiligheidsoverwegingen ondersteunen, noch het systeem dat de control systems vormt veilig maken. Een hardnekkig probleem.

Wie is verantwoordelijk?

Het beschermen van control systems zou gebaseerd moeten zijn op de engineeringprioriteiten veiligheid voor mens & apparatuur en betrouwbaarheid, gevolgd door cybersecurity – daar waar een cyberincident invloed kan hebben op veiligheid en betrouwbaarheid. Verouderde processensoren (zoals druk, niveau, flow, temperatuur, voltage, stroom, enzovoort) zijn mechanische en/of elektrische apparaten die beschikken over faalmodi, maar niet over beveiliging of authenticatie. Voorbeelden waarbij sensoren bijdroegen aan catastrofaal falen zijn onder meer het kernongeval van Three Mile Island, een explosie op de raffinaderij in Texas City, en de tankparkexplosie in Buncefield, in Groot-Brittannië. Grote apparatuur, zoals generatoren, motoren, pompen en relais bevatten 'do not operate' zones die voor beschermingsdoeleinden gebouwd zijn, maar tevens voor catastrofale schade kunnen zorgen. Zo werd de Aurora vulnerability bijvoorbeeld ingezet om apparatuur onjuist te laten werken in deze 'do not operate' zones, wat leidde tot catastrofaal falen, zonder digitale sporen. Uit onderzoek blijkt dat de Aurora vulnerability een netwerk voor een heel lange periode (vele maanden) kan platleggen door kritieke apparatuur te beschadigen (3).
Het realtime monitoren van elektrische eigenschappen van processensoren gaat volledig om de detectie van procesafwijkingen, in plaats van detectie van netwerkafwijkingen. Procesafwijkingen kunnen om allerlei redenen voorkomen, inclusief cyberdreigingen. Als de sensoren die de daadwerkelijke situatie weergeven niet overeenkomen met het netwerk, is het netwerk verdacht. Van cybersecurity ook een engineeringprobleem maken kan voordelen bieden. Een hardnekkig netwerkprobleem wordt oplosbaar, je voorkomt een langdurige schade, verbetert de veiligheid en betrouwbaarheid en je kunt sneller de impact van mogelijke bedreigingen uit apparatuur zelf identificeren. Sensormonitoring kan bovendien helpen de culturele kloof tussen engineering- en beveiligingsorganisaties te overbruggen. Control systems kunnen niet beveiligd worden zonder deze kloof te overbruggen.

Focus OT-engineer vs control system-engineer

Er is een groot verschil tussen hoe OT-engineers naar cybersecurity van

Kritieke infrastructuur security showdown (CISS)
Augustus 2019, Singapore, realtime veldtest van OT-cybersecurity-detectie-tools. Het volledige rapport is recent gepubliceerd (1) en uit de resultaten blijkt dat een Cyber Intrusion Detection Systeem dat op Level 0 monitorde het hoogste scoorde op het gebied van detectie van cyberaanval-afwijkingen in relatie tot het OT-proces. De resultaten laten duidelijk zien dat monitoring van elektrische signalen op Level 0 cruciaal is voor elk cybersecurity-beschermingsplatform in industriële omgevingen. Er zijn veel incidenten, met zowel analoge als digitale sensoren, waarbij onnauwkeurige sensoren voor catastrofaal falen hebben gezorgd. Er is tenminste één incident waarbij een sensor kwaadwillend werd gehackt en het systeem als gevolg daarvan niet meer functioneerde.

control systems kijken en hoe control system-engineers dat doen. Voor control system engineers draait alles om de beveiliging van het netwerk, niet de daadwerkelijke impact op systemen. Wanneer ze malware of netwerkafwijkingen vinden, kunnen ze deze niet direct relateren aan specifieke veldapparatuur, zoals pompen, ventielen, motoren, relais, etc. Wanneer je mij, als OT-engineer, niet kunt uitleggen welke specifieke apparatuur getroffen kan worden en hoe, wat heb ik er dan aan? Bij OT-engineers ligt de focus juist op het proces. Werkt dit zoals ontworpen en treedt er slijtage van de apparatuur op, ongeacht of dat kwaadwillend of onbedoeld is? Verreweg de meeste control system incidenten zijn niet cyber gerelateerd (of tenminste niet identificeerbaar als zijnde cyber) maar het is nog steeds belangrijk om de staat van het proces te weten. Wil OT van waarde zijn voor engineers, dan moet netwerk cybersecurity helpen met deze problemen. De vraag is echter hoe vereisten voor veiligheid en betrouwbaarheid worden beïnvloed door een gebrek aan cybersecurity van processensoren, actuatoren en aandrijvingen. Als je de metingen niet kunt vertrouwen, heb je een probleem. Sensoren, actuatoren en aandrijvingen zijn engineering systemen, geen netwerkapparaten. Ze moeten voldoen aan operationele en designvereisten om processen veilig en betrouwbaar te laten zijn. Cybersecurity is slechts één 'bedreiging' in het voldoen aan design- en operationele vereisten van sensoren.

Het begint allemaal met Level 0

Op dit moment bestaan er geen cybersecurityvereisten voor processensoren, actuatoren en aandrijvingen. Maar zelfs als deze er zouden zijn, lost dat nog steeds niet het probleem op dat een getroffen PLC (of elke andere net entiteit) verkeerde of gemaskeerde informatie heeft, ongeacht welke maatregelen op het gebied van authenticatie of beveiliging zijn getroffen. Deze apparaten hebben een aantal zwakten: de sensoren zelf, de sensornetwerken en de serial-to-ethernet convertors (gateways). Bestaande processensoren zijn mogelijk niet in staat om zelfs minimale cybersecurity te ondersteunen. Als de sensoren zijn gecompromitteerd (wanneer de sensorwaarden of -instellingen 'incorrect' zijn, door onbedoelde of kwaadwillende oorzaak) voordat de gateways de data converteren naar ethernetpakketjes, hebben de PLC en HMI's niet in de gaten dat de sensorwaarden en -instellingen gecompromitteerd zijn. Er zijn een aantal manieren om sensoren elektronisch te compromitteren. De gevolgen daarvan lopen uiteen van een denial-of-service, tot het effectief verwijderen van beveiligingssystemen door manipulatie van sensor-instelpunten. Er vindt momenteel geen cybersecurityonderzoek plaats van de processensor vóór de elektrische signalen ethernet-pakketjes worden. Daardoor is het ook niet duidelijk of een sensor getroffen is met onbedoelde of kwaadwillende redenen. Voor een engineer maakt dat echter niet uit.

Bruikbare inzichten van Level 0

We moeten serieus anders gaan denken over het monitoren van de veiligheid van ICS. Het monitoren van Level 0 combineert cybersecurity en operationele methodologieën, om unieke detectie van elk noemenswaardig procesevent te bieden. Een detectiesysteem voor procesafwijkingen, dat kritieke assets monitort door middel van elektrische signaal gebaseerde geavanceerde analytics, kunstmatige intelligentie en machine learning, als aanvullende en synergetische cyberdetectielaag. In elk end-to-end cyber Intrusion Detection System (IDS) in OT-omgevingen zou dit moeten worden overwogen. Daar waar de aansturing van de elektrische signalen kan worden gehackt of gemanipuleerd, geven de signalen zelf altijd de absolute waarheid weer. Daardoor bieden ze een rijkdom aan informatie om te kunnen zorgen voor operationele betrouwbaarheid, procesoptimalisatie en cyberbeveiliging. Focussen op elektrische signalen, vóór ze zijn geconverteerd naar datapakketjes en zijn gefilterd door de PLC, is vermoedelijk de meest effectieve techniek voor het nauwkeurig identificeren van een operationele afwijkingen, ongeacht de oorzaak.

Monitoring van elektrische signalen op Level 0 gebeurt volledig out-of-band, los van het OT-netwerk en werkt onafhankelijk van het ICS/SCADA-systeem. Dit maakt het de meest veilige en betrouwbare oplossing om afwijkingen te detecteren.

Referenties

(1) https://itrust.sutd.edu.sg/ciss-2019/
(2) https://www.haaretz.com/israel-news/iranian-cyberattack-aimed-to-raise-chlorine-level-in-israeli-water-report-says-1.8886235
https://www.israeldefense.co.il/en/node/43311
www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/
https://www.ynetnews.com/article/H1pA5mM2L
(3) https://blog.trendmicro.com/the-aurora-power-grid-vulnerability-and-the-blackenergy-trojan/
https://www.controlglobal.com/blogs/unfettered/the-aurora-vulnerability-still-being-shunned-by-the-electric-industry-where-is-the-education/