25.05.2023

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Saksa
http://www.pilz.com

Lehdistöviesti

Thomas Pilz: Safety ja Security digitaalista automaatiota varten

Ostfildern, 25.05.2023 - **(Puhe on etusijalla)**

Thomas Pilz

Security: Tämä on lakisääteisesti tulossa teollisuuteen ja koneenrakentamiseen

Teollisuusympäristön turvallisuutta koskevissa standardeissa ja laeissa on meneillään radikaali muutos. Sitä ajavat eteenpäin Securityyn ja tekoälyyn liittyvät aiheet. Teollisuudessa yleensä sekä kone- ja laitostekniikassa kolme uutta tai tulevaa lakisääteistä vaatimusta liittyy Security-kysymykseen: EU:n NIS 2 -direktiivi, uusi koneasetus ja kyberkestävyyslaki.
Viime vuoden lehdistötilaisuuden tavoin keskityn nytkin Securityyn ja haluan näyttää teille tänään, miten laajoja vaikutuksia sillä on koko alalle.

NIS 2: Enemmän velvoitteita ja seuraamuksia useammalle yritykselle

NIS (Network and Information Security) on Euroopan unionin direktiivi kyberturvallisuuden vahvistamiseksi. Direktiivi on ollut voimassa vuodesta 2016, ja sitä on tähän mennessä sovellettu kriittisen infrastruktuurin tarjoajiin, kuten energia-, liikenne-, pankki- ja rahoituspalvelut, terveydenhuolto, juomaveden toimitus ja jakelu sekä digitaalinen infrastruktuuri. Näiden alojen palveluntarjoajien oli toteutettava "asianmukaiset varotoimenpiteet" Securityn osalta ja raportoitava vakavista tietoverkkoturvallisuuteen liittyvistä vaaratilanteista. Sen seuraaja on NIS 2, joka tuli voimaan vuoden 2023 alussa ja joka EU:n jäsenvaltioiden on saatettava osaksi kansallista lainsäädäntöään syksyyn 2024 mennessä. Direktiiviä sovelletaan nyt myös muun muassa koneenrakennus- ja autoteollisuudessa ja yrityksissä, joissa on yli 50 työntekijää tai joiden vuotuinen liikevaihto on yli 10 miljoonaa euroa. VDMA:n mukaan tämä koskee noin 9 000 yritystä eri puolilla Eurooppaa. Tulevaisuudessa näiden yritysten on osoitettava, että ne toteuttavat teknisiä, toiminnallisia ja organisatorisia toimenpiteitä suojautuakseen Security-loukkauksilta. Tähän kuuluu ensinnäkin olemassa olevien järjestelmien riskianalyysi myös tuotantoympäristöissä eli OT (Operations Technology). Tämän jälkeen kehitetään ja pannaan täytäntöön erityisiä prosesseja ja toimenpiteitä, kuten salasanasuojaus tai salaus, sekä annetaan työntekijöille lisäkoulutusta. Kyberturvallisuuteen liittyvistä vaaratilanteista on ilmoitettava asianomaisille viranomaisille 24 tunnin kuluessa. Toimitusketjujen nimenomainen huomioon ottaminen on myös uutta. Yhteenvetona voidaan todeta, että NIS 2 koskee nyt useampia yrityksiä, laajentaa velvoitteita ja säätää tiukemmista seuraamuksista. Yrityksiä, jotka eivät ryhdy toimiin, uhkaavat ankarat rangaistukset.

Kyberkestävyyslaki - Security koko tuotteen elinkaaren ajan

Euroopan komissio esitti syyskuussa 2022 asetusluonnoksen, jonka tarkoituksena on lisätä tuotteiden kyberturvallisuutta. Tämä kyberkestävyyslaki on suunnattu sellaisten tuotteiden valmistajille, joissa on digitaalisia elementtejä. Tämä koskee sekä laitteistoa että ohjelmistoja (kuten laiteohjelmistoa). Asetusta sovelletaan sekä kuluttajatuotteisiin että teollisiin sovelluksiin, kuten koneiden ohjausjärjestelmiin, tarkoitettuihin tuotteisiin. Kyberkestävyyslain mukaan markkinoille saa nyt saattaa vain tuotteita, joilla varmistetaan asianmukainen kyberturvallisuuden taso. Lisäksi valmistajien on ilmoitettava asiakkaille tietoturva-aukoista mahdollisimman pian ja suljettava ne. Asetus koskee siis tuotteen koko elinkaarta. Tämä tarkoittaa, että valmistajien on nyt tarjottava ohjelmistopäivityksiä tavanomaisen takuuaikojen jälkeen, jotta myös tulevat uhat voidaan torjua. Odotamme, että asetus hyväksytään vuoden 2024 loppuun mennessä.

Uusi koneasetus - kyberturvallisuus velvollisuutena

Kolmas uusi lakisääteinen Security-vaatimus on EU:n koneasetus. Sen julkaiseminen on lähellä. Koska kyseessä on asetus, sitä ei tarvitse ensin saattaa osaksi kansallista lainsäädäntöä. Konevalmistajilla on 42 kuukautta aikaa täyttää uudet vaatimukset. Koneasetus korvaa aiemman konedirektiivin, ja toisin kuin edeltäjänsä, siinä säädetään kyberturvallisuus pakolliseksi. Kun konedirektiivi koski pelkästään turvallisuutta, asetuksessa Security-suojaustavoite on sisällytetty "olennaisiin terveys- ja turvallisuusvaatimuksiin" kuuluvaan kohtaan "Korruptiolta suojautuminen": Koneen turvatoimintoja ei saa heikentää tahattomalla tai tahallisella väärentämisellä. Toistaiseksi tiedetään, että kyberkestävyyslain vaatimusten noudattaminen johtaa koneasetuksen vaatimustenmukaisuusolettamaan.

Ja nyt: Kenen on huolehdittava mistä?
Mikä on lakivaatimusten merkitys nyt? Haluaisin havainnollistaa riippuvuuksia käyttämällä esimerkkinä sähköntuotantoalaa:
Tähän asti NIS-direktiivi on vaikuttanut ainoastaan sähköntoimittajiin. NIS 2:n myötä myös koneenrakentajien, kuten sähköntuotantolaitteiden (esim. tuuliturbiinien) valmistajien, on tulevaisuudessa noudatettava vaatimuksia. Tuulivoimalan valmistaja puolestaan tarvitsee esimerkiksi Pilzin automaatioratkaisuja, ohjaimia tai antureita. Tietyn koon ylittävät sähkökomponenttien valmistajat kuuluvat myös NIS 2:n piiriin. Ja koska NIS 2:ssa säädetään myös toimittajien huomioon ottamisesta, Pilzin kaltaisen yrityksen on myös huolehdittava turvallisista toimitusketjuista ja asetettava toimittajilleen vaatimuksia. NIS 2 kattaa siis koko toimitusketjun.

Koneiden valmistajien on jo pitkään täytynyt suorittaa vaatimustenmukaisuuden arviointimenettely ja CE-merkintä, jotta ne voivat tuoda koneita Eurooppaan. Nyt uuden koneasetuksen myötä koneenrakentajien on osoitettava, että niiden koneet on suojattu myös manipulointia vastaan. Sähkökomponenttien valmistajaan sovelletaan myös suunnitellun kyberturvallisuuslain tulevia vaatimuksia.

Yhteenvetona: Se, haluaako yritys puuttua Securityyn ja kuinka perusteellisesti, ei ole enää yrityksen harkintavaltaan kuuluva asia. Ei, se on lakisääteinen vaatimus! Yritysten olisi hyvä käsitellä NIS 2 mahdollisimman pian ja tehdä yritykselle kokonaisvaltainen Security-arviointi. Tähän kuuluu esimerkiksi tietoturvallisuuden johtamisjärjestelmän (ISMS) perustaminen, joka on sertifioitu ISO 27001 -standardin mukaisesti.

Koneenrakennusteollisuudessa Industrial Security ei ole vain IT:n tehtävä, vaan olennainen osa suunnittelua ja rakentamista. Securityn toteuttaminen jälkikäteen on aina aikaa vievää ja merkitsee yleensä käyttäjäystävällisyyden, toiminnallisuuden ja tuottavuuden heikkenemistä. Riskinarvioinnissa Safety on nyt liitetty Securityyn. Ei CE-merkintää ilman Securityä!

Digitaalisia elementtejä sisältävien tuotteiden valmistajille IEC 62443 -standardisarja tarjoaa hyvän suunnan. Esimerkiksi standardissa IEC 62443-4-1 kuvataan vaatimukset niin sanotulle "Securityn kehittämisen elinkaariprosessille".

EU on ottanut johtoaseman Security-lainsäädännössä, ja Euroopassa on maailman tiukimmat säännökset. Koordinointi muiden maiden kanssa on kuitenkin jo käynnissä, ja tällaiset lait tulevat myös sinne. Tällä hetkellä esimerkiksi Australia on tiedonvaihdossa EU:n kanssa, ja se todennäköisesti käyttää eurooppalaisia standardeja. Industrial Securityn maailmanlaajuinen yhdenmukaistaminen on näin ollen odotettavissa.

Thomas Pilz

Avoimet viestintästandardit historiallisena tehtävänä

Pilzillä avoimuus ja käyttäjäystävällisyys ovat keskeisiä piirteitä. Haluamme tarjota asiakkaille tuotteita, jotka edustavat uusinta tekniikkaa, ovat helppoja käsitellä ja voidaan sovittaa kaikkiin automaatioarkkitehtuureihin.

Ensimmäisen turvallisen kenttäväyläjärjestelmän SafetyBUS p:n ja turvallisen reaaliaikaisen Ethernetin SafetyNET p:n avulla olemme muokanneet turvallisen teollisuuskommunikoinnin kehitystä. Omien yritysratkaisujen aika on kuitenkin ohi. Teemme kaikkemme luodaksemme alan standardeja. Tämä on historiallinen tehtävä!

OPC UA

Teollisuus on sopinut OPC UA:sta (Open Platform Communications Unified Architecture) teollisuuslaitosten turvallista verkottumista varten. Tämä tiedonsiirtoprotokolla määrittää standardoidun liittymän (IEC 62541) tiedonsiirrolle erilaisten datalähteiden välille. OPC Foundationin jäsenenä Pilzin työntekijät ovat aktiivisia sekä ohjauskomiteassa että Field Level Communication (FLC) -ryhmän teknisissä tiimeissä. Pilzin huomio on työryhmässä, jossa käsitellään Safetyä (Safety over OPC UA).

Täällä on erityisen arvokasta Pilzin tietotaito Publisher/Subscriber-teknologioiden (Pub/Sub) käytöstä toiminnallisesti turvallisten kenttäväyläprotokollien vaatimusten yhteydessä. Verrattuna perinteiseen master/slave-arkkitehtuuriin pub/sub-arkkitehtuurissa tietoja voidaan vaihtaa suoraan osallistujien välillä. Tämän ansiosta OPC UA:ta voidaan käyttää myös vaativiin, hajautettuihin automaatiotehtäviin. Pilzillä on aiheesta paljon kokemusta, koska SafetyNET p on ainut turvallinen Ethernet-pohjainen kenttäväyläjärjestelmä, joka on alusta lähtien tukenut Pub/Sub:ia.

Olemme edistyneet hyvin toiminnalliseen turvallisuuteen liittyvässä työssämme. Konserni työskentelee yhdessä testausviranomaisten kanssa testausmäärittelyjen ja testausjärjestelmien parissa sekä OPC UA Safety -yhteyspinojen sertifioinnin parissa. Versio 1.05 on jo julkaistu.

IO-Link Safety

Anturitasolla automaatio on jo suuri askel eteenpäin avoimuuden suhteen. IO-Link Safety -tiedonsiirtoprotokolla on tulossa kaupallisesti saataville. P2P-tiedonsiirron etuja ovat asennuksen helppous (esim. standardoiduilla kaapeleilla ja rinnakkaiskaapeloinnin poisjäännillä), automatisoitu ja työkalulla tuettu parametrisointi sekä laajennetut diagnosointimahdollisuudet.

Jotta IO-Linkiä voitaisiin käyttää turvallisuuteen liittyviin automaatiotehtäviin, Pilz on työskennellyt intensiivisesti IO-Link-yhteisössä vastaavan laajennuksen ja siihen liittyvien testien ja sertifiointien parissa. Pilzin asiantuntijat johtavat kahta IO-Link Safety -työryhmää (markkinointi ja tekniikka).

Esittelemme ensimmäiset markkinakelpoiset anturit SPS-messuilla marraskuussa. Pilzin lähestymistapa on tarjota täydellinen järjestelmä eli anturit, toimilaitteet ja päämoduulit. Tämä yksinkertaistaa sovellusta asiakkaan kannalta ja lisää suorituskykyä.

Olemme vakuuttuneita siitä, että automaatioratkaisut erottuvat tulevaisuudessa entistä vahvemmin toiminnallisuuksiensa avulla: Miten hyvä käyttöliittymä, miten helppoa käyttö, mitä lisäarvoa se tarjoaa? Täällä on paljon innovaatiovoimaa ja suuri potentiaali uusille sovelluksille.

Thomas Pilz

Turvallisuuden tulevaisuus on dynaaminen

Mitä digitalisaation jatkuminen merkitsee ihmisen ja koneen suojelulle? Mitkä teknologiat täyttävät turvallisuusvaatimukset? Mikä rooli ihmisillä on? Tänään haluamme myös katsoa tulevaisuuteen. Ensin hyvät uutiset: Ihminen on keskipisteessä. Hänen roolinsa jopa vahvistuu.

Ihmiset aktiivisina suunnittelijoina

Esimerkiksi Arena 2036 -hankkeessa "Fluid Production". Pilz työskentelee kumppaneidensa kanssa kehittääkseen ja toteuttaakseen ihmiskeskeisen, kyberfyysisen tuotantokonseptin erityisesti autoteollisuutta varten. Hankkeen ideana on jakaa tuotantolaitokset sijainnin mukaan joustaviin moduuleihin, jotta dynaamisia yksiköitä voidaan muodostaa ja purkaa tarpeen mukaan. Moduulit on suunniteltu siten, että niissä keskitytään ihmisten rooliin tuotantoympäristönsä aktiivisina suunnittelijoina.

Näiden vaatimusten vuoksi halutaan dynaamista turvallisuutta eli turvallisuustoimintojen joustavampaa mukauttamista muuttuviin tuotantoprosesseihin ja niihin liittyviin suojausvaatimuksiin. Ne sallivat esimerkiksi sen, että robottia tai mobiililaitteisiin ei tarvitse pysäyttää heti kun ihminen tulee sen työalueelle ja se voi jatkaa työskentelyä pienennetyllä (ja siten vähemmän vaarallisella) nopeudella – ja voi tulevaisuudessa jopa osata turvallisia väistöstrategioita. Hajautettujen järjestelmien älykkäät anturit ja toimilaitteet huolehtivat siten yhä enemmän ohjausten toiminnoista ja parantavat siten sekä konemoduulien keskinäistä että ihmisten ja koneiden vuorovaikutusta.

Turvallisuus reaaliajassa
Tulevaisuuden tuotantoympäristöjen dynaamiset tilanteet on tarkistettava ja vapautettava reaaliajassa, jotta ihmisen ja koneen suojelu on aina taattu. Iskulause on "reaaliaikainen turvallisuus". On mahdollista, että eri koneet - tai omaisuuserät yleensä - käyttävät tulevaisuudessa yhteisiä turvalaitteita. Tämä on "Shared Safety", jota testaamme SmartFactory KL:ssä. Klassinen CE-merkintä, joka on seurausta vastaavasta vaatimustenmukaisuuden arviointimenettelystä, ei tule kysymykseen, kun turvallisuus ymmärretään näin. Kaikkia asiaan liittyviä omaisuuseriä koskevien tietojen on oltava käytettävissä ajon aikana. Avainsanoja ovat digitaalinen tyyppikyltti ja hallintataso.

Jo mainitussa "Fluid Production" -hankkeessa työskentelemme muiden tulevien aiheiden, kuten ihmisten ja esineiden tunnistamisen (ja siten erottamisen) parissa. Tässä kohtaa tekoälyn käyttö tulee kuvaan mukaan. Mukautuvat tekoälyalgoritmit voivat tunnistaa ja arvioida riskit. "Analoginen" CE-merkintä on perussuojaus. Lisätoimia voidaan kuitenkin ottaa käyttöön riskien minimoimiseksi, turvallisuuden joustavoittamiseksi ja tuottavuuden lisäämiseksi.

Otsikko:

Tekstit ja kuvat voi myös ladata osoitteesta www.pilz.com. Voit siirtyä suoraan asianomaiseen lehdistökeskukseen kirjoittamalla seuraava web-koodi hakukenttään.: **237512**

Pilz-konserni

Pilz-konserni on automaatiotekniikan tuotteiden, järjestelmien ja palvelujen globaali toimittaja. Perheyrityksen pääkonttori sijaitsee Ostfildernissa. Pilz varmistaa ihmisten, koneiden ja ympäristön turvallisuuden kaikkialla maailmassa 2500 työntekijän ja 42 tytäryhtiön voimin. Teknologiajohtaja tarjoaa anturi-, ohjaus- ja käyttötekniikan sisältäviä täydellisiä automaatioratkaisuja – mukaan luettuna järjestelmiä teollisuuden tiedonsiirtoon, diagnosointiin ja visualisointiin. Salkun täydentää kansainvälinen palvelutarjonta, johon sisältyy neuvonta, suunnittelu ja koulutus. Pilz-ratkaisuja käytetään kone- ja laitosrakentamisen lisäksi monilla aloilla, kuten tuulivoimaloissa, rautateillä ja robotiikassa.

www.pilz.com

Pilz sosiaalisessa mediassa

Kerromme some-kanavillamme taustatietoa Pilz-yrityksestä ja ihmisistä ja raportoimme automaatioteknologian uusimmista kehitysvaiheista.

https://www.facebook.com/pilzINT

https://twitter.com/Pilz_INT

https://www.youtube.com/user/PilzINT

https://www.xing.com/companies/pilzgmbh%26co.kg

https://www.linkedin.com/company/pilz

Yhteyshenkilö toimittajille

Martin Kurth
Yritys- ja tekninen lehdistö
+49 711 3409 - 158
publicrelations@pilz.com

Sabine Skaletz-Karrer
Tekninen lehdistö
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de