Taustatietoa

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

Heinäkuu 2026

”Zones and Conduits” automaatioverkoissa: security suojaa safetyä

Safety on etusijalla

Ostfildern, heinäkuu 2026 – **Koneasetus asettaa velvoitteen: industrial securityn on suojattava turvallisuuteen liittyviä toimintoja manipuloinnilta – toisin sanoen security on toimivan safetyn edellytys. Mutta miten automaatioverkko voidaan suojata kokonaisvaltaisesti? Standardit, kuten IEC 62443-3-2 ja tuleva EN 50742, antavat tälle suuntaviivat: järjestelmien jakaminen vyöhykkeisiin ja yhteyksien hallinta – periaate, joka toistuu kautta linjan alan järjestöjen ja asiantuntijoiden nykyisissä suosituksissa. Pilz on vakuuttunut siitä, että safetyn ja niin sanotun vakioautomaation johdonmukainen erottaminen toisistaan on avain tehokkaaseen koneturvallisuuteen – kun se toteutetaan Defence-in-Depth-periaatteella ja Zones and Conduits -mallilla.**

Talo voi olla vankasti ja turvallisesti rakennettu: siinä voi olla tukevat seinät, palonkestävät materiaalit, luotettava sähköjärjestelmä ja toimivat hälytyslaitteet. Tällainen rakenteellinen turvallisuus on vertauskuvallinen esimerkki koneiden safetystä, jossa rakenteellisten toimenpiteiden, antureiden ja suojamekanismien tulee estää ei-toivotut vaarat. Tällainen talo pysyy kuitenkin turvallisena vain, jos siihen ei kohdistu mitään tunkeutumisia. Manipuloidut lämmityksen ohjaukset, sabotoidut virtapiirit tai pois päältä kytketyt hälytysjärjestelmät voivat muuttaa objektiivisesti turvallisesti suunnitellun rakennuksen riskiksi. Myös koneiden maailmassa paraskin turvallisuustekninen suunnitteluratkaisu menettää tehonsa,

jos turvallisuuteen liittyviin komponentteihin vaikutetaan luvattomasti tai ne poistetaan luvatta käytöstä.

Securityn roolina on toimia tässä yhteydessä ulkoisena suojana: vankat ovet, suojatut pääsyt, valvotut yhteydet ja esteet, jotka estävät ei-toivotut tunkeutumiset. Security ei siis suojaa itse onnettomuuksilta, vaan siltä, että suojamekanismeja ei voida poistaa toiminnasta – esimerkiksi sellaisten henkilöiden toimesta, jotka pääsevät käsiksi järjestelmään valitsemalla luvattomasti käyttötilan tai tekemällä luvattomia toimenpiteitä. Vasta tällöin safety toimii luotettavasti tehokkaasti – security for safety.

Normatiivisista vaatimuksista ratkaisuehdotukseen

Koneasetuksessa (EU) 2023/1230 securitystä tehdään ensimmäistä kertaa pakollinen edellytys koneiden ja laitteistojen safetyn toimivuudelle: turvatoimintoja ei saa heikentää tahallisella tai tahattomalla manipuloinnilla. Juuri tähän liittyy myös parhaillaan laadittava standardi EN 50742, joka auttaa konkretisoimaan koneasetuksen olennaiset security-vaatimukset. Standardi määrittelee tekniset yksityiskohdat tietojen turmeltumiselta suojautumista varten ja asettaa selkeät vaatimukset laitteistoille, ohjelmistoille ja datalle, jotka voivat vaikuttaa turvallisuuteen liittyviin toimintoihin. Standardi kattaa koko elinkaaren – kehityksestä aina käyttöön ja käytöstäpoistoon saakka. Keskeisessä roolissa on myös jo olemassa oleva IEC 62443 -standardisarja, joka kuvaa teollisten automaatio- ja ohjausjärjestelmien järjestelmällistä kyberturvallisuutta. Se tarjoaa jäsennellyn kehyksen riskianalyyseille, ”Defence-in-Depthille” ja segmentointiperiaatteelle (”Zones and Conduits”), ja se tunnustetaan EN 50742 -standardissa nimenomaisesti vaihtoehtoisena tai täydentävänä lähestymistapana turvallisuuden varmistamiseen. Yhdessä nämä standardit muodostavat security for

safety -konseptin normatiivisen ytimen: ne edellyttävät, että koneen digitaalinen eheys ymmärretään sen toiminnallisen turvallisuuden edellytykseksi ja että sitä suojataan asianmukaisesti.

Miksi ”Zones and Conduits” tekee koneista turvallisempia

Palataan talovertauskuvaan: talon lämmityskeskus edustaa vyöhykettä, ja yhteys älykotiyhdyskäytävään edustaa vastaavaa yhteysväylää. Jos tätä yhteyttä manipuloidaan, koko järjestelmään voidaan vaikuttaa – vaikka tila olisi täydellisesti suojattu. Ratkaisevaa ei siis ole pelkästään yksittäisten alueiden suojaaminen vaan myös näitä alueita yhdistävien väylien turvallisuus. Juuri tässä kohtaa Zones and Conduits -periaate astuu kuvaan. Alueet erotetaan selkeästi toisistaan, ja niiden väliset väylät toteutetaan hallitusti. Aivan kuten talossa, jossa ovet ja niille osoitetut avaimet määräävät, kuka pääsee minnekin, myös teollisuuslaitoksessa sisäinen suojaus (safety) ja ulkoinen suojaus manipulaatioita vastaan (security) kytkeytyvät toisiinsa järjestelmällisesti.

Näin syntyy suojauskonsepti, joka noudattaa Defence-in-Depth-periaatetta: turvallisuutta ei saavuteta yhdellä yksittäisellä esteellä, vaan useilla peräkkäin sijoitetuilla suojauskerroksilla. Jos yksi kerros pettää, seuraava kerros jatkaa suojausta. Nämä kerrostetut tilat muodostavat vyöhykkeitä (Zones), ja niiden välillä on hallittuja tietoväyliä (Conduits). Tällä tavoin estetään se, että yksittäinen haavoittuvuus vaarantaa koko järjestelmän – etenkin kun kyse on safetystä ja siten ihmisten suojelusta.

Pilz noudattaa tätä lähestymistapaa johdonmukaisesti security for safety -periaatteella – safety on securityn tärkein suojelukohde. Kaiken keskiössä on turvata safety, joka puolestaan suojaa ihmisiä. Siksi Pilz erottaa safetyn erilleen koneen yleisestä ohjauksesta eli niin sanotusta vakioautomaatiosta ja vähentää näin turvallisuuteen liittyvien toimintojen altistumista vaaroille. Mitä selkeämmin nämä ”aarteet” erotetaan toiminnallisesti toisistaan, sitä vähemmän lisäsuojatoimenpiteitä tarvitaan niiden luotettavaan suojaamiseen.

Tämän lähestymistavan edut näkyvät koneen koko elinkaaren ajan. Kun safety ja vakiotoiminnot erotetaan toisistaan, vakiotoimintojen päivityksen yhteydessä safety-toimintoja ei tarvitse samalla uudelleensertifioida tai mukauttaa, mikä vähentää selvästi huolto- ja ylläpitotöitä. Lisäksi perinteiset turvaohjaimet tarvitsevat turvallisuuden kannalta kriittisiä päivityksiä huomattavasti harvemmin kuin vakio-ohjaimet, joten erottelu poistaa monia tarpeettomia toimenpiteitä. Erottelu tarjoaa myös teknisiä etuja: itsenäinen safety-järjestelmä, kuten turvallinen PNOZmulti 2 -pienohjaus, voidaan yhdistää vapaasti eri ohjausvalmistajien tuotteisiin, kun taas integroidut järjestelmät ovat usein sidottuja tiettyihin teknologioihin. Samalla erilliset safety-ratkaisut vaikeuttavat hyökkääjien toimintaa, sillä erotetut järjestelmät on murrettava yksi kerrallaan, mikä hankaloittaa huomattavasti manipulointia. Lisäksi vakiojärjestelmä voi olla tarvittaessa verkossa, kun taas varsinaiset safety-toiminnot pysyvät eristettyinä, mikä pienentää merkittävästi sen hyökkäyspinta-alaa.

Safety- ja security-automaation erottelu niin, että kummallakin on optimaalisesti sovitetut turvallisuustasot, parantaa tehokkuutta myös sen ansiosta, että turvallisuus-, ylläpito- ja laajennustoimenpiteiden

suunniteltavuus paranee. Vakio-ohjelmaan tehtävät muutokset eivät tällöin vaadi muutoksia turvallisuuteen liittyvään osaan, mikä vähentää huomattavasti ohjelmointi- ja mukautustyötä. Samalla erottelu vaikuttaa myönteisesti myös ohjelmisto- ja tukikustannuksiin, sillä erillisissä järjestelmissä kertyy usein vähemmän lisenssi- ja palvelumaksuja.

Suojaus erottelulla – osaaminen koulutuksella

Safetyn ja vakioautomaation selkeä erottelu ei takaa ainoastaan teknistä luotettavuutta, vaan se johtaa myös käyttövirheiden vähenemiseen ja vähäisempään koulutustarpeeseen. Koska turvallisuuteen liittyvät toiminnot toimivat omalla laitteistollaan ja on erotettu selkeästi organisatorisesti, ne pysyvät suojattuina myös silloin, kun vakio-ohjelmaan tehdään muutoksia. Virheet päivittäisessä käytössä eivät siten vaaranna safetyä, ja vastuut voidaan määrittää selkeämmin.

Pilz tarjoaa kattavan koulutus- ja palveluohjelman tukeakseen yrityksiä tämän arkkitehtuurin toteutuksessa. Ohjelma käsittää koulutukset ”Industrial securityn perusteet” ja ”CESA – Certified Expert for Security in Automation” sekä Industrial Security Services -palvelut. Ne eivät ainoastaan opasta, kuinka yksittäisistä lohkoista voidaan kehittää vankkoja security for safety -konsepteja, vaan ne menevät paljon pidemmälle: ne näyttävät, kuinka security-riskejä hallitaan järjestelmällisesti ja kuinka kehitetään kokonaisvaltaisia turvallisuuskonsepteja, kuinka IEC 62443 -standardin vaatimukset voidaan sovittaa niihin, kuinka turvallisen koneverkon arkkitehtuuri rakennetaan ja kuinka toteutettujen toimenpiteiden tehokkuutta voidaan arvioida ja jatkuvasti parantaa.

Tämän lähestymistavan ratkaisevana etuna on se, että loppukäyttäjän käyttöhenkilöstön ei tarvitse perehtyä security-asioihin syvällisesti, koska safety-toimintojen suojaus on jo varmistettu arkkitehtuurin suunnittelun kautta. Koulutukset onkin suunnattu ennen kaikkea niille, jotka tekevät security-päätöksiä tai suunnittelevat järjestelmiä – käyttäjät voivat samalla jatkaa työskentelyä turvallisesti tarvitsematta lisäkoulutusta industrial securitystä. Tämä johtaa käytännölliseen roolijakoon, joka yksinkertaistaa laitoksen toimintaa ja parantaa samalla suojaustasoa pysyvästi.

Lisää turvallisuutta selkeän rakenteen avulla – ja oikealla osaamisella

Tehokas security for safety -strategia ei synny yksittäisistä toimenpiteistä, vaan huolellisesti suunnitellusta arkkitehtuurista, selkeistä vastuista ja osaamisen kohdennetusta kehittämisestä. Juuri tässä Pilz astuu kuvaan. Keskittymällä johdonmukaisesti Defence-in-Depthiin ja erottamalla safetyn ja vakioautomaation selkeästi toisistaan Pilz luo perustan kestäville koneille – ja täydentää tätä käytännönläheisillä koulutuksilla ja neuvonnalla, jotta yritykset voivat edetä tällä tiellä varmoin askelin. Tällä tavoin saavutetaan turvallisuustaso, joka ei ainoastaan täytä standardien vaatimuksia, vaan tuottaa jokapäiväisessä käytössä selkeää lisäarvoa: yksinkertaisemmin, kestävämmin ja pysyvästi tehokkaasti.

((Zeichen: 9.640))

Ostfildernissä, on nykyään maailmanlaajuisesti edustettuna 2 500 työntekijän voimin 42 tytäryhtiössä ja sivuliikkeessä.

Teknologiajohtaja tarjoaa täydellisiä automaatioratkaisuja koneen Safetyä ja Industrial Securityä varten. Tuotevalikoimamme sisältää anturi-, ohjaus- ja käyttötekniikan täydellisiä automaatioratkaisuja – mukaan luettuna järjestelmiä teollisuuden tiedonsiirtoon, diagnosointiin ja visualisointiin. Salkun täydentää kansainvälinen palvelutarjonta, johon sisältyy neuvonta, suunnittelu ja koulutus. Pilzin ratkaisuja käytetään kone- ja laitosrakentamisen lisäksi lukuisilla muilla aloilla, kuten intralogistiikassa, pakkaustekniikassa, rautatietekniikassa ja robotiikassa.

www.pilz.com

Pilz sosiaalisessa mediassa:

Sosiaalisen median kanavillamme kerromme taustatietoa Pilzistä ja yrityksessä työskentelevistä ihmisistä ja jaamme uutisia automaatiotekniikan alalta.

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Yhteystiedot lehdistölle:

Martin Kurth
Yritys- ja ammattilehdistö
Puh: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer
Yritys- ja ammattilehdistö
Puh: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman
Ammattilehdistö
Puh: +49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rößle
Ammattilehdistö
Puh: +49 711 3409-7147
e.roessle@pilz.de