20.05.2025

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

Lehdistöviesti

Safetystä, Securitystä ja tekoälystä: Turvallisuus tarvitsee oikeudellisia kehyksiä kaikkialla maailmassa

Ostfildern, 20.05.2025 - **Thomas Pilz, toimitusjohtaja, Pilz GmbH & Co. KG**

(Puhe on etusijalla)

Me kaikki tunnemme CE-merkinnän. Se näkyy sähkölaitteissa, leluissa tai kotitaloustavaroissa, mutta tietysti myös koneissa ja järjestelmissä. Se on lyhenne sanoista "Conformité Européenne". CE-merkki on käytännössä sinetti, joka osoittaa, että Euroopan talousalueella (EU ja EFTA) markkinoille saatetut tuotteet täyttävät olennaiset turvallisuus-, ympäristö- ja terveysvaatimukset. Kiinnittämällä merkin maahantuoja osoittaa, että hän on noudattanut tuotteen turvallisuutta koskevia lakisääteisiä vaatimuksia EU:ssa. Jo 30 vuoden ajan jokainen EU-direktiivien soveltamisalaan kuuluva tuote on vaatinut CE-vaatimustenmukaisuusvakuutuksen.

Näihin direktiiveihin kuuluu myös konedirektiivi, joka on ollut pakollinen vuodesta 1995 lähtien. Konedirektiivi selostaa yhdenmukaiset vaatimukset turvallisuudelle ja terveellisyydelle ihmisten ja koneiden vuorovaikutuksen yhteydessä ja korvaa siten monia koneturvallisuutta koskevia kansallisia asetuksia.

Menestyksekäs CE-malli
Se, mikä alussa oli yrityksille voimanponnistus, on nykyään jotain, mitä kukaan ei halua jättää käyttämättä. CE-merkintä ja konedirektiivi luovat avoimuutta ja luottamusta valmistajien ja käyttäjien välille. Ne ovat siis menestystarinoita. Muualla maailmassa niitä on käytetty ja käytetään edelleen mallina koneturvallisuutta koskevan oikeudellisen kehyksen luomisessa.

Esimerkkinä Brasilia: Siellä on vuodesta 2010 lähtien ollut voimassa kansallinen laki, jossa määrätään koneiden ja laitteiden turvallisuutta koskevista vähimmäisvaatimuksista: Norma Regulamentadora 12 (NR-12) – MÁQUINAS E EQUIPAMENTO. Itse asiassa se sisältää suurelta osin konedirektiivin liitteen I turvallisuusvaatimukset, mukaan lukien tietyntyyppisiä koneita koskevat erityisvaatimukset. Euroopassa tähän lakiin viitataan siksi myös nimellä "Brasilian konedirektiivi".

Ensimmäinen lainsäädäntökehys koneturvallisuudelle Intiassa

Intia on maailman nopeimmin talous, sekin on nyt ottanut käyttöön myös koneturvallisuutta koskevan lainsäädäntökehyksen. Raskaan teollisuuden ministeriö on julkaissut kaksi vastaavaa asetusta. Niin sanotuissa Omnibus Technical Regulations -asetuksissa määritellään turvallisuusvaatimukset erityyppisille koneille ja sähkölaitteille. Niiden tarkoituksena on varmistaa, että koneet täyttävät turvallisuusvaatimukset ennen niiden saattamista markkinoille Intiassa.
Samoin kuin Euroopassa on olemassa pakolliset sertifioinnit ja vaatimustenmukaisuusmerkki. Suurin osa Intian uusista vaatimuksista on nykyisten kansainvälisten standardien mukaisia.

Kaikkien, jotka haluavat harjoittaa vientiä Intiaan, on nimettävä valtuutettu edustaja, jonka kotipaikka on Intiassa. Intialainen tytäryhtiömme voi auttaa yrityksiä täyttämään vaatimukset ja siten viemään tuotteita Intiaan. Pilz Indian työntekijät työskentelevät myös Intian standardisoimisviraston (Bureau of Indian Standard) asiaankuuluvassa komiteassa.

Koneturvallisuuden aihepiiri kehittyy varmasti edelleen Intiassa. Voidaan kuitenkin varmuudella sanoa, että tulevaisuudessa koneita tai tuotteita, jotka eivät ole vaatimustenmukaisia (voisi sanoa, että niissä ei ole Intian CE-merkintää), ei voida tuoda Intiaan. Tämä voi tarkoittaa, että koneita tai tuotteita pidetään Intian tullissa, kunnes toimittaja on toimittanut vaaditut eritelmät.

Turvallisuus: 30 vuotta myöhemmin
Takaisin 90-luvun puoliväliin: Tuolloin Tim Berners-Lee julkisti WWW:n käyttöteknologian CERN-tutkimuskeskuksessa Sveitsissä. Se oli yhteiskunnan ja teollisuuden verkottumisen ja digitalisaation läpimurto.

30 vuotta myöhemmin turvallisuus määritellään eri tavalla. Verkottuminen ja digitalisoituminen tarkoittavat, että tuotteet ja koneet, joissa on digitaalisia elementtejä, altistuvat aivan erilaisille riskeille, jotka liittyvät esimerkiksi tietojen manipulointiin. Euroopan lainsäätäjät ovat reagoineet: CE-merkinnän periaate säilyy ennallaan. Sen ylläpitoa koskevat vaatimukset on mukautettu tekniikan tasolle. Uusi koneasetus on korvannut konedirektiivin vuonna 2023. Haluaisin esitellä lyhyesti kaksi innovaatiota, tekoälyn ja Industrial Securityn.

Voiko tekoäly olla turvallinen?
"Robotti ei saa vahingoittaa ihmistä."
Näin Isaac Asimov muotoili niin sanotun robottilain älykkäille koneille eräässä tieteistarinassaan vuonna 1942. Nyt, 83 vuotta myöhemmin, tekoälyn kehittyminen merkitsee sitä, että ihmisten ja koneiden välisen yhteistyön pelisääntöjä on harkittava uudelleen.
Myös lainsäätäjä on tunnustanut tämän ja ottanut tekoälyä koskevan aiheen huomioon uudessa koneasetuksessa. Siinä puhutaan koneista, jotka kehittävät itseään. Kuinka turvallinen kone voi olla, jos sen reaktiot vaaratilanteissa eivät ole ihmisen vaan algoritmin määrittelemiä? Äärimmäisissä tapauksissa on pohdittava, voiko itseoppiva ohjelmisto mahdollisesti johtaa uuden koneen syntymiseen. Tämä on erittäin mielenkiintoinen aihe paitsi valmistajille myös ilmoitetuille koestuslaitoksille.

Tekoäly ei vaikuta vain koneiden maailmaan. Tekoälyä koskevassa EU:n asetuksessa, niin sanotussa tekoälylainsäädännössä, säädetään yleisesti siitä, mitä tekoälyjärjestelmät saavat ja mitä ne eivät saa tehdä. Asetuksessa kielletään erilaiset tekoälykäytännöt, kuten ihmisten manipulointi. Tämä tarkoittaa, että tekoäly ei saa saada ihmisiä tekemään päätöksiä, jotka aiheuttavat merkittävää haittaa heille itselleen tai muille. Lisäksi tietyt sovellukset, esimerkiksi koulutuksen, kriittisen infrastruktuurin tai lainvalvonnan aloilla, on luokiteltu korkean riskin tekoälyjärjestelmiksi, joiden on täytettävä erityisvaatimukset. Näille korkean riskin tekoälyjärjestelmille on tulevaisuudessa myös hankittava CE-merkintä.

Me Pilzillä pidämme tekoälyasetusta tärkeänä asetuksena, jolla varmistetaan, että mahdollisuuksia voidaan hyödyntää ja että tekoälyn aiheuttamia riskejä vähennetään.

Ei CE-merkintää ilman Securityä
Kyberhyökkäysten ja manipulaation aiheuttamien vahinkojen nopean lisääntymisen vuoksi uudessa koneasetuksessa edellytetään tulevaisuudessa myös suojausta turvallisuustoimintojen, esimerkiksi ohjausjärjestelmien, turmeltumista vastaan, ja siinä asetetaan näin ollen vaatimuksia Industrial Securitylle. Tapahtuman toisessa osassa asiantuntijamme Simon Nutz antaa yksityiskohtaista tietoa siitä, miten yritysten olisi parasta reagoida nyt, jotta ne voivat jatkossakin merkitä tuotteensa CE-merkinnällä. Koneturvallisuuden käsitettä ollaan siis parhaillaan määrittelemässä uudelleen.

Security-lait: All good things come in three
EU on ottanut käyttöön koneenrakennuksen Industrial Securityä koskevat lakisääteiset vaatimukset kolmella tasolla. Koneille, digitaalisia elementtejä sisältäville tuotteille ja yrityksille on omat säädökset.

- Koneisiin sovelletaan koneasetusta.
- Kyberkestävyyslaissa (Cyber Resilience Act, CRA) määritellään kyberturvallisuusvaatimukset tuotteille, joissa on digitaalisia elementtejä.
- Lisäksi EU:n direktiivi toimenpiteistä korkeatasoisen yhteisen kyberturvallisuuden varmistamiseksi unionissa, niin sanottu NIS 2 -direktiivi, koskee lähes kaikkia yli 50 työntekijän yrityksiä.

Tämä on valtava tehtävä teollisuudelle: EU on jo julkaissut kaikki kolme lakia. Kahdessa näistä, nimittäin koneturvallisuusasetuksessa ja CRA:ssa, kello tikittää jo, ja teollisuudella on nyt noin puolitoista vuotta aikaa organisoida tuotekehitys, tuotanto ja tekniikka uudelleen sen mukaisesti, mukaan lukien kaikki asiaan liittyvät prosessit ja tehtävät, kuten koulutus ja dokumentointi. Todellinen mammuttitehtävä - aivan kuten konedirektiivin täytäntöönpano aikoinaan.

Olemme jo puhuneet koneasetuksesta. CRA:ssa edellytetään, että digitaalisia elementtejä sisältävät tuotteet suunnitellaan, kehitetään ja valmistetaan kyberturvallisuutta koskevien perusvaatimusten mukaisesti. Tämä tarkoittaa erityisesti sitä, että nyt vaaditaan riskien arviointia ja varmistamista, haavoittuvuuksien hallintaa, dokumentointia ja raportointivelvoitteita.

Tämä vaikuttaa myös meihin itseemme. Tämän toteuttamiseksi otimme useita vuosia sitten käyttöön IEC 62443-4-1 -standardin mukaisen sertifioidun "securen"-kehitysprosessin tuotekehitysalueillamme, ja saimme sen sertifioitua vuonna 2022. Näin voimme taata, että kehitystyömme on CRA:n mukaista. Pilzin tuotevalikoima on hyvin laaja, ja jokainen tuote oli arvioitava sen selvittämiseksi, missä määrin CRA vaikuttaa siihen ja onko sitä tarvittaessa mukautettava. Tämä arviointi on tehty ja vastaavat toimenpiteet toteutettiin varhaisessa vaiheessa.

Kolmas säädös, EU:n NIS 2 -direktiivi, joka velvoittaa yritykset varautumaan kyberhyökkäyksiin, täytyy vielä saattaa osaksi kansallista lainsäädäntöä. Ja itse asiassa viime vuoden lokakuun 18. päivään mennessä. Tällä hetkellä EU:n 27 jäsenvaltiosta 9 on saattanut täytäntöönpanon päätökseen. Muissa maissa, kuten Saksassa ja Itävallassa, poliittiset olosuhteet estävät usein lakien hyväksymisen.

Security ei ole lakien vuoksi

Pilzin vetoomus: Omasta kokemuksestani Pilziin vuonna 2019 kohdistuneesta kyberhyökkäyksestä voin sanoa, että olisi kohtalokasta odottaa, kunnes poliittisella tasolla päästään sopimukseen ennen kuin security-suojaustoimenpiteet otetaan käyttöön. Kyse ei ole lakisääteisten vaatimusten täyttämisestä vaan yrityksen ja sen olemassaolon turvaamisesta.

Kaikkien uusien vaatimusten myötä herää kysymys, kohtaavatko EU:n lisäksi myös muut markkinat uusia haasteita, kuten tekoälyä tai kyberrikollisuutta. Vastatakseni tähän haluaisin palata CE-merkinnän menestyksekkääseen malliin. Konedirektiivin tapaan voidaan odottaa, että eurooppalaisia lakeja ja standardeja käytetään maailmanlaajuisesti mallina myös tekoälyn ja kyberturvallisuuden alalla. Toisaalta useimmat hallitukset haluavat varmistaa, että niiden kansalaiset ovat mahdollisimman hyvin suojattuja vaaroilta, ja toisaalta koneiden valmistajat ja tuottajat haluavat markkinoida tuotteitaan maailmanlaajuisesti. Tämä tarkoittaa, että myös EU:n ulkopuolisten toimijoiden on täytettävä uudet vaatimukset, jos ne haluavat jatkaa tuontia EU:hun.

Kuten huomaatte, turvallisuudella on monia puolia, jotka vaikuttavat meihin, kumppaneihimme, asiakkaisiimme ja yhteiskuntaan yleensä. Intian uusi lupamenettely ja EU:n uudet tekoäly- ja security-vaatimukset ovat esimerkkejä toimivan markkinayhteistyön merkityksestä. Lait ja kansainväliset standardit ovat tässä avainasemassa. Ne auttavat meitä varmistamaan, että voimme luottaa teknisiin turvamekanismeihin maailmanlaajuisesti.

Otsikko: *Thomas Pilz, Managing Director (Photo: © Pilz GmbH & Co. KG)*

Löydät ladattavia artikkeleita ja kuvia kohdasta:
https://www.pilz.com/fi-INT/company/press/messages/articles/245660

Pilz – The Spirit of Safety

Pilz on globaali automaatiotekniikan tuotteiden, järjestelmien ja palvelujen toimittaja. Turvallisen automaation pioneerina Pilz luo turvallisuutta ihmisille, koneille ja ympäristölle. Vuonna 1948 perustettu perheyritys, jonka pääkonttori sijaitsee Ostfildernissä, on nykyään maailmanlaajuisesti edustettuna 2 500 työntekijän voimin 42 tytäryhtiössä ja sivuliikkeessä. Teknologiajohtaja tarjoaa täydellisiä automaatioratkaisuja koneen Safetyä ja Industrial Securityä varten. Automaatioratkaisut sisältävät anturi-, ohjaus- ja käyttötekniikan – mukaan luettuna järjestelmät 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.

Pilz sosiaalisessa mediassa

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

https://www.facebook.com/pilzINT

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

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

Yhteyshenkilö toimittajille

Martin Kurth
Yritys- ja tekninen lehdistö
+49 711 3409 - 0
publicrelations@pilz.com

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