25.05.2023

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

Tisková zpráva

Thomas Pilz Safety and Security pro digitální automatizaci

Ostfildern, 25.05.2023 - **(Jednou vyslovené slovo platí)**

Thomas Pilz

Security: Týká se ze zákona průmyslu a strojírenství

Normy a zákony v oblasti bezpečnosti průmyslového prostředí procházejí v současné době velkými změnami. Důvodem jsou témata Security a umělá inteligence (AI). Pro průmysl obecně a pro výrobu strojů a zařízení jsou z hlediska Security důležité tři nové, resp. připravované zákonné předpisy: směrnice EU NIS 2, nové nařízení o strojních zařízeních a Cyber Resilience Act.
Stejně jako loni bych se na tomto místě chtěl zaměřit na téma Security a vysvětlit Vám, jak rozsáhlý je jeho vliv na celý průmysl.

NIS 2: Více povinností a více sankcí pro více podniků

NIS ((Bezpečnost sítě a informací) je směrnice Evropské unie, jejím cílem je posílení kyberbezpečnosti. Směrnice existuje již od roku 2016 a dosud platila pro dodavatele v oblasti kritických infrastruktur jako energie, doprava, banky a finance, zdraví, zásobování a rozvod pitné vody a digitální infrastruktura. Dodavatelé v těchto sektorem museli z hlediska Security přijímat „přiměřená preventivní bezpečnostní opatření“ a hlásit rostoucí případy ohrožení kyberbezpečnosti. Nyní nastupuje NIS 2, směrnice, která vstoupí v platnost počátkem roku 2023 a do podzimu 2024 ji členské státy musí integrovat do své národní legislativy. Směrnice nyní kromě jiného platí i v sektoru strojírenství a automobilového průmyslu, zde pro podniky s více než 50 zaměstnanci nebo ročním obratem převyšujícím 10 mil. eur. V celé Evropě směrnice podle údajů VDMA platí pro téměř 9 000 podniků. Tyto podniky budou muset nyní prokazovat, že přijaly technická, provozní a organizačních opatření na ochranu v případech Security. Sem patří jako první analýza rizik stávajících systémů i ve výrobním prostředí, tedy OT (Operations Technology). Pak následuje vypracování a realizace specifických procesů a opatření jako ochrana heslem nebo kódování a samozřejmě další vzdělávání a školení zaměstnanců. Případy ohrožení kyberbezpečnosti musí být příslušným úřadům nahlášeny do 24 hodin. Novinkou je i výslovné zahrnutí dodavatelských řetězců. Celkově vzato se nyní NIS 2 týká více podniků, rozšiřuje povinnosti a předpokládá přísnější sankce. Podnikům, které opatření nepřijmou, hrozí citelné pokuty.

Cyber Resilience Act – Security pro celý životní cyklus produktu

V září 2022 předložila Evropská komise návrh nařízení, které má zvýšit kyberbezpečnost produktů. Cyber Resilience Act je určen pro výrobce produktů s digitálními prvky. Tím je míněn jak hardware, tak i software (např. firmware). Nařízení se vztahuje jak na spotřebitelské produkty, tak i na produkty pro průmyslové využití, například řídící systémy strojů. Podle Cyber Resilience Act smí být do oběhu uváděny pouze produkty, které zaručují přiměřenou úroveň kyberbezpečnosti. Dále budou výrobci povinni co nejrychleji informovat zákazníky o nedostatcích v bezpečnosti a tyto co nejrychleji řešit. Nařízení se týká tedy celého životního cyklu produktu. To znamená, že výrobci musí nyní také i po obvyklé záruční době nabízet aktualizaci softwaru, aby byly odvráceny i budoucí hrozby. Vycházíme z toho, že nařízení bude přijato koncem roku 2024.

Nové nařízení o strojních zařízeních – povinná kyberbezpečnost

Třetím novým zákonným předpisem v oblasti Security je nařízení EU o strojní bezpečnosti. Zveřejnění se očekává v brzké době. Protože se jedná o nařízení, nemusí být nejdříve zahrnuto do národního práva. Výrobci strojů budou mít čas 42 měsíců na to, aby splnili nové požadavky. Nařízení o strojních zařízeních nahrazuje dosavadní směrnici o strojních zařízeních a na rozdíl od ní ukládá kyberbezpečnost jako závaznou. Jestliže se směrnice o strojních zařízeních týkala čistě bezpečnosti (Safety), byl do nařízení zahrnut cíl ochrany Security jako „Protection against corruption“ do „„Essential health and safety requirements EHSR”: Bezpečnostní funkce stroje nesmí být ovlivněny neúmyslným nebo úmyslným falšováním. Dnes je známo, že splnění požadavků z Cyber Resiliance Act vede k domněnce shody v případě nařízení o strojních zařízeních.

A nyní: Kdo a o co se musí starat?
Jaký význam mají nyní zákonné předpisy? Souvislosti bych rád objasnil na příkladu sektoru výroby elektrické energie: Směrnice NIS se dosud týkala pouze dodavatele energie. V případě NIS 2 musí předpisy napříště plnit i výrobce stroje, například výrobce zařízení na výrobu energie (např. větrné elektrárny). Výrobce větrné elektrárny potřebuje řešení automatizace, řídícího systému nebo senzorů, např. od společnosti Pilz. Od určité velikosti spadají do rozsahu směrnice NIC 2 i výrobci elektrických komponent. A protože NIS 2 se vztahuje i na dodavatele, musí si společnost jako Pilz zajistit bezpečný dodavatelský řetězec a přenést požadavky na své dodavatele. NIS 2 tedy pokrývá kompletní dodavatelský řetězec.

Již velmi dlouho musí výrobci strojů absolvovat řízení o posuzení shody, na jehož konci je značka CE. Teprve pak mohou dovážet stroje do Evropy.
Nyní budou výrobci strojů podle nového nařízení o strojních zařízeních muset prokázat, že jejich stroje jsou chráněny i proti manipulaci. A konečně budoucím předpisům plánovaného Cyber Resilience Act bude podléhat i výrobce elektrických komponent.

Souhrnně lze tedy říci: Nyní již nebude na uvážení samotného podniku, zda a nakolik se bude zabývat bezpečností. Bezpečnost se stane zákonným předpisem! Výrobci tedy udělají dobře, jestliže se začnou co nejdříve směrnicí NIS 2 zabývat a provedou ucelený posudek průmyslové bezpečnosti (Security) ve svých závodech. Patří k tomu například vytvoření systému řízení bezpečnosti informací (ISMS) s certifikátem podle normy o bezpečnosti informací ISO 27001.

Ve strojírenství není Security v podobě Industrial Security úkolem pouze pro IT, ale je integrální součástí koncepce a konstrukce. Implementovat Security dodatečně je vždy nákladné a většinou se zásahy nepříjemně dotknou komfortu uživatelů, funkcí a produktivity. Při posuzování rizik tedy dnes k Safety přibývá i Security. Bez Security nelze dosáhnout na značku CE!

A pro výrobce produktů s digitálními prvky představuje dobrou orientační pomůcky řada norem IEC 62443. V podružné normě IEC 62443-4-1 jsou například popsány požadavky na tzv. „Security Development Lifecycle Process“.

EU je oblasti zákonů týkajících se Security průkopníkem a v Evropě budou platit v tomto směru nejpřísnější zákony na celém světě. Již dnes ale probíhají jednání s dalšími zeměmi a i tam na tyto zákony dojde. V současné době např. probíhá výměna informací mezi Austrálií a EU a tamější zákony se budou pravděpodobně opírat o evropské. Lze tedy v případě Industrial Security očekávat celosvětovou harmonizaci.

Thomas Pilz

Otevřené komunikační standardy jako historický úkol

U společnosti Pilz jsou otevřenost a uživatelský komfort důležitou charakteristikou portfólia produktů. Chceme zákazníkům nabízet produkty, které vždy odpovídají aktuálnímu stavu techniky, jsou z hlediska manipulace jednoduché a lze je začlenit do jakékoli architektury automatizace.

Se sběrnicí SafetyBUS p, prvním bezpečným systémem aplikační sběrnice a bezpečným Ethernetem SafetyNET p v reálném čase jsme vytyčili cestu pro vývoj bezpečné průmyslové komunikace. Doba proprietárních firemních řešení však již minula. Ze všech sil se snažíme vytvářet průmyslové standardy. To je historický úkol!

OPC UA

Pro bezpečné propojení průmyslových zařízení napříč různými výrobci se průmysl shodl na OPC UA (Open Platform Communications Unified Architecture). Tento komunikační protokol poskytuje v průmyslovém prostředí standardizované (IEC 62541) rozhraní pro komunikaci mezi různými zdroji dat. Pracovníci společnosti Pilz jsou jako členové OPC Foundation aktivní v řídícím výboru i v technických pracovních skupinách Field Level Communication (FLC). Pilz svou pozornost zaměřil na pracovní skupina, která se zabývá tématem Safety (Safety over OPC UA).

Velmi důležité je naše know-how v oblasti používání technologie Publisher/Subscriber (Pub/Sub) ve spojení s požadavky funkčně bezpečných protokolů aplikační sběrnice. V porovnání s klasickou architekturou Master/Slave dochází u Pub/Sub k přímé výměně dat mezi účastníky. To dovoluje využití OPC UA i pro náročné distribuované automatizační úkoly. Pilz je pro tento účel skutečným expertem, protože naše SafetyNET p je jediným bezpečným systémem aplikační sběrnice na bázi Ethernetu, který se od počátku podporuje Pub/Sub.

Naše práce na tématu funkční bezpečnosti velmi dobře pokračuje. Skupina úzce spolupracuje s kontrolními orgán na specifikaci testu a testovacích systémech i na certifikaci komunikačních stacků pro OPC UA Safety. Verze 1.05 již byla schválena.

IO-Link Safety
Na úrovni senzorů již automatizace ve věci otevřenosti udělala velký krok vpřed. Komunikační protokol IO-Link Safety bude již velmi brzy komerčně dostupný. Komunikace od bodu k bodu nabízí řadu výhod jako například zjednodušenou instalaci (např. standardizovanou kabeláží a odstraněním paralelních kabelů), automatizovanou parametrizaci s podporou nástrojů a rozšířené možnosti diagnostiky.

Aby bylo IO-Link možné využívat i pro úkoly automatizace týkající se bezpečnosti, pracoval Pilz v rámci IO-Link Community intenzivně na příslušném rozšíření o příslušné testy a certifikáty. Experti společnosti Pilz řídí obě pracovní skupiny IO-Link Safety (pro marketing a techniku).

První senzory vhodné pro trh představíme na veletrhu SPS v listopadu. Cílem společnosti Pilz je nabízet kompletní systém, tedy senzory, ovladače a moduly Master. To zákazníkům zjednoduší používání a zvýší výkonnost.

Jsme přesvědčeni o tom, že řešení automatizace se v budoucnu budou stále více lišit svým funkcemi: Jak dobrá jsou uživatelská rozhraní, jak jednoduchá je obsluha, jaké doplňkové výhody se nabízejí? Zde se skrývá možnost výrazných inovací i velký potenciál pro nové aplikace.

Thomas Pilz

Budoucnost bezpečnosti je dynamická

Jaký význam má další digitalizace pro ochranu člověka a stroje? Jaké technologie vyhoví požadavkům na bezpečnost? Jakou roli v tom bude hrát člověk? Chtěli bychom dnes alespoň trochu nahlédnout do budoucnosti. Dobrá zpráva je: Ústředním bodem je člověk. Jeho role bude dokonce ještě posílena.

Člověk jako aktivní tvůrce

Uveďme jako příklad projekt „Fluidní výroba“, Arena 2036. Pilz spolupracuje s řadou partnerů na vývoji a zavádění kyberneticko-fyzické koncepce výroby zaměřené na člověka, zejména pro výrobu automobilů. Myšlenkou projektu je rozložení výrobních zařízení na místně flexibilní moduly, ze kterých bude možné podle potřeby vytvářet dynamické jednotky a znovu je rozdělovat. Moduly jsou navrhovány s hlavním zaměřením na úlohu člověka jako aktivního tvůrce vlastního výrobního postředí.

Z toho vychází požadavek dynamické bezpečnosti, tedy flexibilního přizpůsobení bezpečnostních funkcí měnícím se výrobním procesům a souvisejícím potřebám ochrany. Například nebude muset být nutné, aby došlo k okamžitému zastavení robota nebo mobilní platformy „natvrdo“, jestliže se v pracovním prostoru pohybuje člověk, ale aby tato zařízení mohla dále pracovat se sníženou (a tedy méně nebezpečnou) rychlostí nebo ještě lépe, aby ovládala bezpečnou strategii vyhýbání. Inteligentní senzory a ovladače budou přitom v distribuovaných systémech stále více přebírat řídící funkce, a to povede k lepší interakci nejen strojních modulů navzájem, ale i u člověka a stroje.

Bezpečnost ve správném čase
Dynamické situace v budoucím průmyslovém prostředí musí být prověřovány z hlediska bezpečnosti v reálném čase tak, aby ochrana člověka a stroje byla zaručena v každém okamžiku. Heslem tedy je „Bezpečnost v reálném čase“. Lze si představit, že různé stroje – nebo prostředky obecně – budou bezpečnostní zařízení v budoucnu sdílet. To je „Shared Safety“, kterou zkoušíme ve SmartFactory KL. Klasická značka CE jako výsledek analogového posuzování shody ztrácí při takovém chápání bezpečnosti význam. V době provozu musí být aktuálně k dispozici informace o všech zúčastněných prostředcích, heslem k tomu je digitální typový štítek a digitální obálka komponent výroby.

V již zmíněném projektu „Fluidní výroba“ pracujeme na dalších tématech budoucnosti jako identifikace (a tím rozlišení) člověka a předmětů. Zde se nabízí využití umělé inteligence. Algoritmy AI schopné zaškolení mohou identifikovat a posuzovat rizika. „Analogová“ značka CE přitom představuje základní ochranu. Pro minimalizaci rizik lze samozřejmě zavést další opatření, díky nim bude bezpečnost ještě flexibilnější a bude moci ještě lépe přispívat ke zvýšení produktivity.

Text k obrázku:

You can find texts and images at www.pilz.com also for downloading. To go directly to the relevant internet pages in the press centre, enter the following Web code in the search of the home page.: **237512**

Společnost Pilz

Společnost Pilz je globálním dodavatelem výrobků, systémů a služeb pro automatizační techniku. Rodinný podnik se sídlem v německém Ostfildernu má více jak 2 500 zaměstnanců. Se svými 42 dceřinými společnostmi a pobočkami po celém světě se společnost Pilz stará o bezpečnost lidí, strojů i životního prostředí.
Jako lídr na poli technologií nabízí společnost Pilz kompletní automatizační řešení zahrnující senzoriku, techniku řízení a pohonů včetně systémů pro průmyslovou komunikaci, diagnostiku i vizualizaci. Mezinárodní portfolio společnosti pak završuje nabídka služeb zahrnující poradenství, inženýring a celou řadu odborných školení.
Řešení společnosti Pilz nejsou určena pouze pro strojírenství
a inženýring, nýbrž se s nimi setkáte v celé škále jiných technických oborů, jako jsou například větrné elektrárny, železnice nebo průmysloví roboti.

www.pilz.com

Pilz na sociálních sítích

Na našich kanálech sociálních médií poskytujeme informace o životě firmy Pilz a jejích zaměstnanců. Informujeme o aktuálním vývoji a trendech v automatizační technice.

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

Kontakt na novináře