

Informace ze společnosti

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

Červenec 2026

Strana 1 z 7

„Zones and conduits“ v automatizačních sítích: Security chrání bezpečnost

Bezpečnost má nejvyšší prioritu

Ostfildern, červenec 2026 – **Nařízení o strojních zařízeních to stanoví jako povinnost: Industrial Security má chránit funkce relevantní z hlediska bezpečnosti před neoprávněnou manipulací – bezpečnost je tedy předpokladem pro funkční bezpečnostní systémy. Jak ale lze zajistit komplexní zabezpečení automatizační sítě? Normy jako IEC 62443-3-2 a připravovaná norma EN 50742 udávají směr: oddělit systémy do zón, kontrolovat propojení – tento princip se prolíná všemi aktuálními doporučeními asociací a odborníků. Pilz je přesvědčen, že důsledné oddělení bezpečnosti od takzvané standardní automatizace je klíčem k účinné strojní bezpečnosti – opírající se o princip „Defence-in-Depth“ a realizované prostřednictvím přístupu „Zones-and-Conduits“.**

Dům může být postaven pevně a bezpečně: se stabilními stěnami, ohnivzdornými materiály, spolehlivou elektroinstalací a funkčními poplašnými zařízeními. Tato konstrukční bezpečnost je příkladem bezpečnosti strojních zařízení, u nichž mají konstrukční opatření, senzorika a ochranné mechanismy zabránit nechtěným rizikům. Takový dům však zůstane bezpečný pouze tehdy, pokud nedojde k žádným cíleným zásahům. Manipulace s ovládacími prvky topení, sabotáže elektrických obvodů nebo deaktivace poplašných systémů mohou proměnit objekt, který byl z hlediska bezpečnosti navržen správně, v rizikové místo. I ve světě strojů ztratí i ta nejlepší bezpečnostní konstrukce svůj smysl, pokud dojde k neoprávněnému

zásahu do bezpečnostních komponent nebo k jejich vyřazení z provozu.

Security v tomto kontextu plní roli vnější ochrany: robustní dveře, zabezpečené přístupy, monitorovaná spojení a bariéry proti nežádoucím zásahům Security tedy nechrání před samotnými nehodami, ale před tím, aby byly ochranné mechanismy vyřazeny z provozu – například osobami, které k nim získají přístup neoprávněným výběrem provozního režimu nebo neoprávněnými úkony. Jen tak může bezpečnost spolehlivě fungovat – security pro bezpečnost.

Od normativního zadání až po návrh řešení

Nařízení o strojních zařízeních (EU) 2023/1230 poprvé stanoví zabezpečení jako závaznou podmínku pro funkční bezpečnost strojů a zařízení: bezpečnostní funkce nesmějí být narušeny ani úmyslnou, ani neúmyslnou manipulací. Právě na to navazuje připravovaná norma EN 50742, která pomůže konkretizovat základní bezpečnostní požadavky nařízení o strojních zařízeních. Norma definuje technické podrobnosti týkající se ochrany před poškozením a stanoví jasné požadavky na hardware, software a data, které mohou ovlivnit funkce související s bezpečností. Norma pokrývá celý životní cyklus – od vývoje přes provoz až po odstavení z provozu. Klíčovou roli zde hraje také již existující řada norem IEC 62443, která popisuje systematickou kyberbezpečnost pro průmyslové automatizační a řídicí systémy. Poskytuje strukturovaný rámec pro analýzy rizik, „Defence-in-Depth“ i princip segmentace („Zones and Conduits“) a je v normě EN 50742 výslovně uznána jako alternativní nebo doplňkový přístup k zajištění bezpečnosti. Tyto normy společně tvoří normativní jádro koncepce „Security for Safety“: vyžadují, aby byla digitální

integrita strojního zařízení chápána jako předpoklad jeho funkční bezpečnosti a aby byla odpovídajícím způsobem chráněna.

Proč „Zones and Conduits“ zvyšuje bezpečnost strojních zařízení

Zpět k obrázku domu: Topenářská místnost představuje zónu, připojení k bráně Smart Home Gateway pak příslušnou spojovací trasu. Pokud dojde k manipulaci s tímto připojením, lze ovlivnit celé zařízení – i když je místnost dokonale chráněna. Rozhodující proto není jen zabezpečení jednotlivých prostor, ale také bezpečnost tras, které je spojují. Právě v tomto bodě přichází ke slovu princip „Zones and Conduits“. Jednotlivé prostory jsou od sebe jasně odděleny a přechody mezi nimi jsou promyšleně řešeny. Stejně jako v domě, kde dveře a přidělené klíče určují, kdo kam smí vstoupit, i v průmyslovém závodě se strukturovaně prolíná vnitřní ochrana (bezpečnost) a vnější ochrana proti neoprávněné manipulaci (security).

Vzniká tak koncepce ochrany, která se řídí principem „Defence-in-Depth“: bezpečnost není zajištěna jedinou bariérou, ale několika za sebou řazenými ochrannými vrstvami. Jakmile se překoná jedna vrstva, další odolá. Tyto stupňovité prostory tvoří zóny, zatímco mezi nimi se nacházejí kontrolované průchody zvané „conduits“. Tímto způsobem se zabrání tomu, aby jediná slabina ohrozila celý systém – zejména pokud jde o bezpečnost a tedy o ochranu lidí.

Společnost Pilz důsledně uplatňuje tento přístup pod názvem „Security for Safety“; bezpečnost je hlavním cílem ochrany. V centru pozornosti stojí ochrana bezpečnosti, která zase chrání lidi. Proto společnost Pilz Safety odděluje bezpečnostní systém od obecného řízení strojů, tzv. standardní automatizace, a tím snižuje riziko ohrožení bezpečnostních funkcí. Čím jasněji jsou tyto „poklady“

funkčně odděleny, tím méně dodatečných bezpečnostních opatření je zapotřebí k jejich spolehlivé ochraně.

Výhody tohoto přístupu se projevují po celou dobu životního cyklu strojního zařízení. Pokud jsou bezpečnostní a standardní funkce odděleny, není při aktualizaci standardních funkcí nutné souběžně recertifikovat nebo upravovat bezpečnostní funkce, což výrazně snižuje nároky na údržbu a servis. Klasické bezpečnostní řadiče navíc vyžadují aktualizace kritické pro bezpečnost podstatně méně často než standardní řadiče, takže díky tomuto oddělení odpadá mnoho zbytečných zásahů. I z technologického hlediska přináší oddělení řadu výhod: Samostatný bezpečnostní systém, jako je například bezpečný malý řídicí systém PNOZmulti 2, lze libovolně kombinovat s produkty různých výrobců řídicích systémů, zatímco integrované systémy jsou často vázány na konkrétní technologie. Zároveň samostatná bezpečnostní řešení zvyšují překážky pro útočníky, protože oddělené systémy je třeba napadnout jednotlivě, což manipulaci výrazně ztěžuje. K tomu je třeba připočítat, že standardní systém může být v případě potřeby online, zatímco samotné bezpečnostní funkce zůstávají izolované, čímž se výrazně snižuje jeho zranitelnost.

Kromě toho toto oddělení automatizace bezpečnosti a zabezpečení s optimálně sladěnými úrovněmi zabezpečení zvyšuje efektivitu díky lepší plánovatelnosti bezpečnostních, údržbových a rozšiřovacích opatření. Změny ve standardním programu pak nevyžadují zásahy do části související s bezpečností, což výrazně snižuje nároky na programování a přizpůsobení. Zároveň má toto oddělení pozitivní účinek na náklady na software a podporu, protože v samostatných systémech jsou licence a servisní poplatky často nižší.

Ochrana díky oddělení – kompetence díky školení

Jasně oddělení bezpečnostní a standardní automatizace zajišťuje nejen technickou spolehlivost, ale také méně chyb při obsluze a nižší nároky na školení. Jelikož funkce související s bezpečností běží na samostatném hardwaru a jsou organizačně jasně odděleny, zůstávají chráněny i v případě, že dojde k změnám ve standardním programu. Chyby v běžném provozu tak neohrožují bezpečnost a odpovědnosti lze jasněji přiřadit.

Aby společnost Pilz pomohla podnikům s implementací této architektury, nabízí rozsáhlý program školení a služeb. Mezi ně patří školení “Základy Industrial Security” a “CESA – Certified Expert for Security in Automation” a také služby v oblasti Industrial Security. Nejenže ukazují, jak lze z jednotlivých stavebních kamenů vyvinout robustní koncepcí „Security-for-Safety“, ale jdou ještě mnohem dál: Ukazují, jak systematicky řídit bezpečnostní rizika a vyvíjet komplexní bezpečnostní koncepcí, jak zařadit požadavky normy IEC 62443, jak vybudovat architekturu bezpečné strojní sítě a jak vyhodnocovat a průběžně zlepšovat účinnost přijatých opatření.

Rozhodující výhodou tohoto přístupu je, že obsluha u konečného uživatele nemusí být podrobně seznámena s bezpečnostními otázkami, protože ochrana bezpečnostních funkcí je již zajištěna samotnou architekturou systému. Školení jsou proto určena především těm, kteří přijímají rozhodnutí v oblasti bezpečnosti nebo navrhují systémy – přičemž obsluha může i nadále pracovat bezpečně, aniž by musela absolvovat další školení v oblasti Industrial Security. Tím vzniká praktické rozdělení rolí, které zjednodušuje provoz zařízení a zároveň trvale zvyšuje úroveň ochrany.

Větší bezpečnost díky přehledné struktuře – a správnému know-how

Účinná strategie Security for Safety nevzniká na základě jednotlivých opatření, ale díky promyšlené architektuře, jasnému rozdělení odpovědností a cílenému rozvoji kompetencí. Právě v tomto bodě vstupuje do hry společnost Pilz. Díky důslednému zaměření na princip Defence-in-Depth a jasnému oddělení bezpečnostní a standardní automatizace vytváří společnost Pilz základ pro odolné stroje – a doplňuje jej praktickými školeními a poradenstvím, aby podniky mohly touto cestou sebevědomě kráčet. Tak vzniká úroveň bezpečnosti, která nejen splňuje standardní požadavky, ale v každodenním provozu přináší znatelnou přidanou hodnotu: je jednodušší, odolnější a má trvalý účinek.

((Počet znaků: 9.640))

Pilz – The Spirit of Safety

Pilz je celosvětovým dodavatelem produktů, systémů a služeb v oblasti automatizační techniky. Jako průkopník bezpečné automatizace zajišťuje Pilz bezpečnost lidem, strojům i životnímu prostředí. Rodinná firma s hlavním sídlem v Ostfildern byla založena roku 1948. Dnes zaměstnává ve 42 dceřiných společnostech a pobočkách rozptýlených po celém světě 2 500 pracovníků a pracovníků.

Dodavatel prvotřídní technologie nabízí ucelené koncepce pro bezpečnost a Industrial Security strojních zařízení. Naše řešení zahrnují senzorické produkty, řídicí techniku a pohony – včetně systémů pro průmyslovou komunikaci, diagnostiku a vizualizaci. Portfólio doplňuje mezinárodní nabídka služeb, jejíž součástí jsou konzultace, inženýrské služby a školení. Řešení společnosti Pilz se uplatňují kromě sektoru výroby strojů a zařízení v celé řadě dalších oborů, mimo jiné v intralogistice, obalovém průmyslu a železniční technice nebo robotice.

www.pilz.com

Pilz na sociálních sítích

Na sociálních sítích se dozvíte zajímavé informace ze zákulisí života firmy a jejích pracovníků a najdete zde aktuality z oblasti automatizační techniky.



www.pilz.com/facebook



www.pilz.com/xing



www.pilz.com/youtube



www.pilz.com/linkedin

Kontakt pro tisk:

Martin Kurth

Podnikový a odborný tisk
Tel: +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

Odborný a podnikový
tisk
Tel: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

Odborný tisk
Tel: +49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rößle

Odborný tisk
Tel: +49 711 3409-7147
e.roessle@pilz.de