ročník XXVIII • ISSN 1335-2237

atp journal

7/2021

PRIEMYSELNÁ AUTOMATIZÁCIA A INFORMATIKA

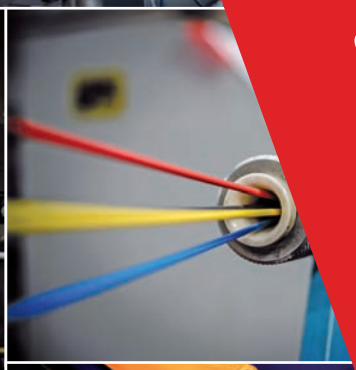
Útoky na priemyselné ciele rastú

VUKI
SINCE 1950

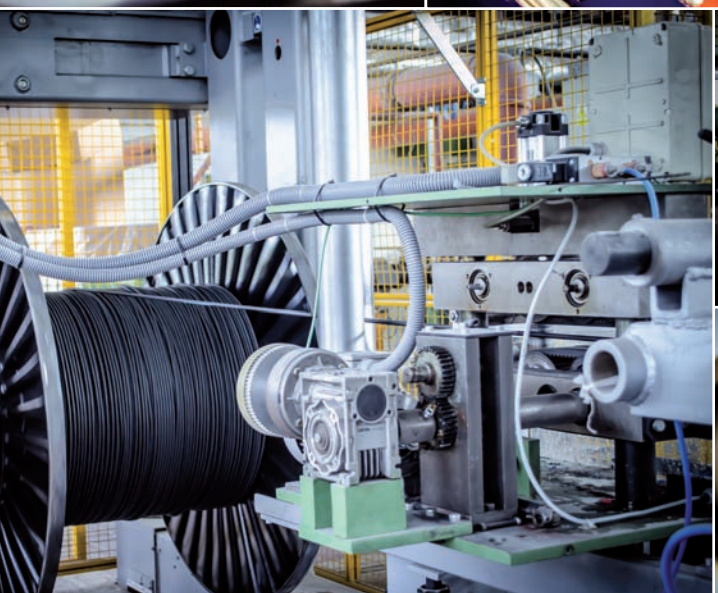
VUKI a.s.

Navrhujeme káble už viac ako 70 rokov…

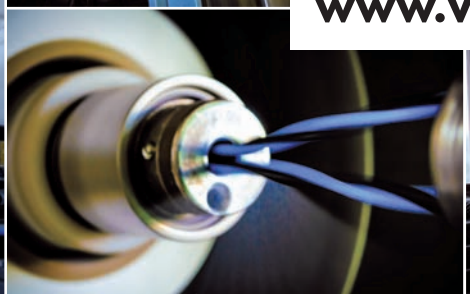
Vyrábame káble na Slovensku
pre najrôznejšie priemyselné aplikácie
rýchlejšie, ako ich viete inštalovať.



… keď chcete viac ako len kábel



www.vuki.sk



Čo keď to budete práve vy?

Skôr ako sa do prostredia výrobných a spracovateľských prevádzok začali inštalovať siete, či už drôtové, alebo bezdrôtové, a zariadenia sa začali pripájať k internetu, boli priemyselné riadiace systémy prirodzene chránené „vzduchovou medzerou“, čo znamenalo, že nikto nemohol len tak ľahko narušiť každodennú prevádzku. Moderné priemyselné riadiace systémy však teraz spolupracujú s rôznymi sieťami a zariadeniami a predstavujú množstvo bezpečnostných slabín. Zaspalo zabezpečenie dobu?

V polovici decembra minulého roku odhalil FireEye rozsiahly útok, ktorý sa šíril prostredníctvom komerčnej softvérovej aplikácie SolarWinds, do ktorej útočníci nainštalovali tzv. zadné dvere. Zasiahnutá bola celá štvrtina severoamerických spoločností z oblasti sieťových odvetví. Ďalší prípad je z mája tohto roku, keď bol na priemyselné riadiace systémy spoločnosti Colonial Pipeline podľa viacerých odborných subjektov podniknutý doteraz najrozsiahlejší kybernetický útok na priemyselné zariadenia v histórii. Útočníci sa do systémov dostali cez odchytené heslo, ktoré forenzný tím našiel na darknete. Ešte horšie dopadol jeden z celosvetovo najväčších spracovateľov mäsa a výrobca mäsových výrobkov, ktorého zasiahol ransomvér ako služba (RaaS) z dielne neslávne známej hackerskej skupiny REvil. Útočníci si takto vymohli od výrobcu, ktorý musel odstaviť niekoľko svojich prevádzok, značné množstvo peňazí.

Ako si môžu byť teda jednotlivé priemyselné odvetvia či podniky isté, že práve ony sa nestanú terčom útoku, keď niektoré typy škodlivého softvéru sa môžu prebudiť až po dlhšom čase? Nová norma ISA/IEC 62443-3-2: Posúdenie bezpečnostných rizík pre návrh systému definuje súbor technických opatrení, ktoré majú podniky zavádzať na základe procesu posudzovania rizika nového alebo existujúceho priemyselného riadiaceho systému alebo IIoT systémov. Stanovuje tiež spôsob identifikácie a použitia bezpečnostných protiopatrení na zníženie tohto rizika na únosnú mieru. Ešte lepšie je spojiť sa z kompetentnými odborníkmi z oblasti kybernetickej bezpečnosti priemyselných riadiacich systémov.
My sme to tiež urobili a tak vám opäť môžeme priniesť zaujímavé inšpirácie. A to nielen z tejto oblasti.

Anton Gérer
šéfredaktor

PARTNERSKÉ ORGANIZÁCIE ATP JOURNAL

IEEE Czechoslovakia Section · MESA INTERNATIONAL Driving Operations Excellence EUROPE · ISA · NÁRODNÉ CENTRUM ROBOTIKY · ZAP · SKSI · ZEPSR Zväz elektrotechnického priemyslu Slovenskej republiky

INOVATO

FESTIVAL INOVÁCIÍ

INOFEST

23. - 24.09.2021 Online

www.inovato.sk/eventy/inofest/ info@inovato.sk

“Každá kríza môže byť dobrá. Pretože vás prebudí.” Ryan Reynolds

Do čoho investovať v najbližších 3 rokoch?

Workshopy a panelové diskusie

Financovanie inovácií / Energetika / eMobilita / Agro a technologické trendy

Aká bezpečnosť v prevádzke, taká pohoda v celom podniku

Meniace sa obchodné modely, zvýšený tlak na náklady a nové regulačné požiadavky urýchľujú potrebu zbližovania prevádzkových (OT) a informačných technológií (IT). Priemyselný internet vecí (IIoT) zabezpečuje takú úroveň prepojiteľnosti a viditeľnosti zariadení v reálnom čase, akú sme si doteraz ani nevedeli takmer predstaviť. Zároveň sa však dramaticky zvyšuje riziko kybernetickej bezpečnosti. Konvenčná bezpečnosť nestačí na ochranu pred množiacimi sa kybernetickými hrozbami pre OT aj IT systémy. Ako reagovať na výzvy v oblasti kybernetickej bezpečnosti pre automatizačné a riadiace technológie, sme sa v exkluzívnom interview porozprávali s Miroslavom Kořenom, generálnym riaditeľom spoločnosti Kaspersky pre východnú Európu.

Skúsme na úvod vysvetliť, v čom je rozdiel medzi kybernetickou bezpečnosťou v prostredí výrobných a priemyselných podnikov, príp. podnikov spadajúcich do tzv. sieťových odvetví, a v „štandardnom kancelárskom" prostredí.

Útoky na priemyselné systémy majú potenciál byť mimoriadne zničujúce. Nie je to len kvôli veľmi citlivým informáciám, ktorými priemyselné organizácie disponujú, ale aj preto, že pri týchto systémoch je najvyššou prioritou neprerušovaná prevádzka a každá minúta prerušenia prevádzky či hocijaká chyba je citeľná. Navyše distribučné spoločnosti zohrávajú kľúčovú úlohu v kritickej infraštruktúre a pri dodávkach energie, plynu alebo pitnej vody si nemôžu dovoliť žiaden výpadok. To odlišuje priemyselnú kybernetickú bezpečnosť od iných oblastí – a preto je spolupráca so správnym poskytovateľom zabezpečenia taká dôležitá. V našej spoločnosti považujeme koncept Adaptive Security Architecture (ASA) vytvorený agentúrou Gartner za najefektívnejší model na vybudovanie postupov kybernetickej bezpečnosti pre priemyselné podniky. Zahŕňa štyri typy opatrení týkajúcich sa jednotlivých štádií potenciálneho kyberbezpečnostného incidentu: prevenciu, detekciu, reakciu a predvídanie. Unikátnou vlastnosťou tohto modelu je schopnosť proaktívne reagovať na hrozbu a chrániť technický proces pred akýmkoľvek druhom incidentu. Patria sem cielené útoky, obvyklé infekcie malvérom, chyby softvéru a hardvéru, dokonca aj zlyhanie ľudského faktora. Úroveň kybernetickej bezpečnosti spoločnosti je odvodzovaná od toho, v ktorej fáze ASA sa nachádza. Jednoduché kopírovane modelu ASA, ktoré bolo pôvodne navrhnuté pre tradičnú korporátnu kybernetickú bezpečnosť, však nepomôže účinne chrániť priemyselný podnik. Pri použití tohto rámca v reálnych podmienkach v danom podniku treba totiž vziať do úvahy špecifiká prevádzkových technológií (OT), všetky technické osobitosti zavedených procesov a ľudský faktor.

V súčasnosti sú už aj na Slovensku k dispozícii rôzne legislatívne nástroje či inštitúcie, ktoré pokrývajú oblasť kybernetickej bezpečnosti. Na ktoré z nich by sa mal zamerať priemyselný podnik?

Najdôležitejšou inštitúciou je samozrejme Národný bezpečnostný úrad (NBÚ), ktorý je relevantný pre všetky spoločnosti vo všetkých priemyselných odvetviach. Zohráva kľúčovú úlohu pri stanovovaní štandardov a stratégie kybernetickej bezpečnosti, riešení incidentov, poskytovaní certifikácií a pod. Aj keď NBÚ odvádza skvelú prácu, neznamená to, že si spoločnosti môžu oddýchnuť a stopercentne sa spoľahnúť na jeho pomoc. Je v ich záujme zabezpečiť sa a v prípade potreby si pomôcť kompetenciami NBÚ. Pokiaľ ide o štandardy kybernetickej bezpečnosti, odporúčam ISO/IEC 27001, aby sa zaistilo zabezpečenie informácií o spoločnosti a tiež používanie certifikovaných produktov a služieb podľa zákona EÚ o kybernetickej bezpečnosti.

Ako sa v súčasnosti vyvíja stav v oblasti kybernetických útokov na priemyselné podniky? Sú viac ohrozené ako v minulosti? Ktoré skutočnosti prispievajú najväčším podielom k tomuto trendu?

Zo štatistík ICS CERT našej spoločnosti vyplýva, že percento priemyselných riadiacich systémov (ICS), na ktorých boli zistené škodlivé objekty, stále narastá a v roku 2020 ich počet dosiahol celosvetovo podiel 38,55 %. Spoločnostiam v našom regióne strednej a východnej Európy sa darí o niečo lepšie s počtom napadnutých ICS v roku 2020 na úrovni 30,5 %, avšak ani tu nevidím dôvod na stratu ostražitosti. Znamená to totiž pravdepodobne len to, že priemyselné podniky v našom regióne nie sú tak často v hľadáčiku kybernetických zločincov. Najbežnejším typom kybernetického útoku na priemyselné spoločnosti, ktorý sme zistili v roku 2020, bol ransomvér. Tieto typy útokov sú čoraz sofistikovanejšie a cielenejšie. Priemyselné spoločnosti sa stávajú čoraz viac „digitálnymi" a takisto viac investujú do inteligentných technológií, nových automatizovaných systémov či zavádzania Priemyslu 4.0. To v skutočnosti eliminuje rozdiel medzi prostredím IT a OT, ktoré sa tradične využívalo na zabránenie tomu, aby sa kybernetické hrozby vôbec dostali do blízkosti priemyselných riadiacich systémov.

Ktoré zariadenia v rámci priemyselných podnikov sú najčastejším terčom útokov?

Posledných šesť mesiacov roku 2020 sa nieslo v znamení zvýšenia percentuálneho podielu útokov na niekoľko priemyselných odvetví vrátane automatizácie budov, automobilovej výroby, energetiky, ropy a zemného plynu, aj keď najväčší nárast (7,8 percentuálneho bodu) nastal v sektore ICS. Nie je prekvapením, že ICS sa stávajú čoraz častejším cieľom, pretože majú priame a nepriame pripojenie k rôznym systémom na úrovni prevádzky aj celého podniku, z ktorých niektoré môžu dokonca patriť iným priemyselným podnikom. Aj keď má systém na úrovni operátorských počítačov viac prístupových práv a menej obmedzení (ako je napríklad kontrola aplikácií či zariadení) ako priemerný počítač s ICS, disponuje širšou útočnou plochou.

Techniky útokov na priemyselné riadiace a informačné systémy sú rôzne. Na čom sú založené? Čo je indikátorom toho, že systém alebo zariadenie boli napadnuté?

Vo všeobecnosti čelia priemyselné riadiace systémy dvom hlavným útočným vektorom. Kyberzločinci môžu získať prístup k priemyselnej infraštruktúre cez hraničné externé siete (napr. podnikovú sieť s ERP, ktorá si v súvislosti s prediktívnou údržbou vymieňa údaje s priemyselnými sieťami) alebo sa môžu pokúsiť preniknúť priamo do domény ICS využitím nepozornosti zamestnancov alebo podplatenia niekoho vnútri podniku. Pracovník napríklad môže priniesť infikovanú USB jednotku alebo osobné zariadenie do izolovanej siete. Je dôležité uvedomiť si, že v dnešnej dobe existuje len veľmi málo skutočne izolovaných sietí, dokonca aj v rámci kritických infraštruktúr. Priemyselné siete „vďačia" za svoju zvýšenú konektivitu nesprávnym konfiguráciám a nízkemu povedomiu zamestnancov – zamestnanci môžu aj nevedome prepojiť takúto izolovanú sieť. Podľa našich skúseností a výskumov je 90 % prípadov kyberbezpečnostných incidentov spôsobených chybou človeka, pričom najčastejšou z nich je podľahnutie phishingovému útoku. Svoju úlohu zohráva aj modernizácia infraštruktúry – priemyselný internet vecí predpokladá externú dostupnosť priemyselných sietí až na úrovni zariadení v teréne.

Čo by malo stáť na začiatku procesu budovania účinnej ochrany pred kybernetickým útokom v rámci priemyselného podniku?

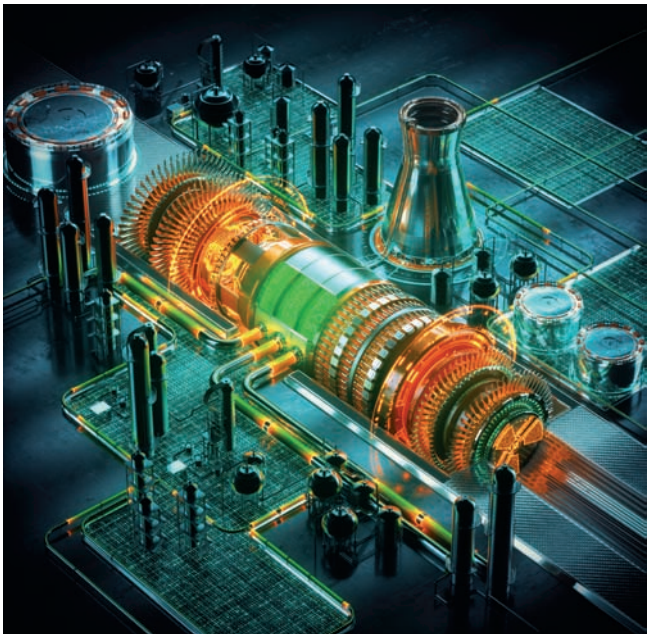
Správne opatrenia pre ICS v oblasti kyberbezpečnosti pre priemyselný podnik by sa mali vždy začínať ochranou priemyselných koncových bodov, aby sa zabránilo náhodným infekciám a sťažilo sa prípadné plánované narušenie. Ďalším krokom by malo byť monitorovanie OT siete a detekcia anomálií, aby bolo možné identifikovať škodlivé aktivity na úrovni programovateľných logických automatov (PLC). Nakoľko akákoľvek reťaz je len taká silná, ako jeho najslabšia časť, alebo v tomto prípade najzraniteľnejší článok, je tiež nevyhnutné pripraviť školiace programy pre zamestnancov zamerané na znižovanie týchto incidentov a minimalizovať ľudské chyby. Na záver je dôležité mať k dispozícii špecializované odborné služby, či už zabezpečené interne, alebo ako riadené služby, na preskúmanie infraštruktúry, vykonávanie odborných analýz alebo na zmiernenie dosahu prípadného incidentu.

Predstavuje vybudovanie účinnej ochrany významnejšie zásahy do existujúcej IT infraštruktúry priemyselného podniku? Čo všetko z hľadiska SW/HW komponentov tvorí ochranný „štít" proti kybernetickým útokom?

To vo veľkej miere závisí od samotnej organizácie, stavu jej infraštruktúry a potrieb, ako aj od odvetvia, v ktorom pôsobí. V našej spoločnosti pevne veríme, že prístup k priemyselnej kybernetickej bezpečnosti by mal byť iba holistický – od predpovedania potenciálnych vektorov útokov cez špecializované priemyselné technológie na prevenciu a detekciu až po proaktívnu reakciu na kybernetický incident. To je najvyššia záruka nepretržitého a bezpečného fungovania, čo je aj ultimátnym cieľom, o ktorý sa snaží každá organizácia.

Aké dôsledky môže mať kybernetický útok v prostredí priemyselného podniku?

Na jednej strane môže ísť o stratu cenných údajov, no najhorším scenárom je narušenie priemyselných procesov. V závislosti od citlivosti priemyselného podniku môže takýto incident viesť k strate



peňazí, napr. vo forme odstávky technológie, alebo dokonca k fyzickým škodám v reálnom svete. Z najznámejších útokov môžem spomenúť napríklad hackerský útok na oceliarne v Nemecku v roku 2014, ktorý narušil riadenie vysokej pece, na Ukrajine zas v rokoch 2015 a 2016 spôsobili útoky na rozvodný systém výpadky elektriny, ktoré sa dotkli tisícok spotrebiteľov. Netreba opomenúť ani nedávny útok na Colonial Pipeline, ktorý paralyzoval dodávky pohonných látok v USA.

Ako by mal priemyselný podnik postupovať, ak zistí, že v jeho sieťach a zariadeniach sa objavili neočakávané zmeny, situácie, príp. že ich údaje či citlivé informácie boli zneužité a hackeri požadujú zaplatiť „výkupné“?

Ak je požadované výkupné, dôrazne odporúčame jeho nevyplatenie. Najpádnejším dôvodom takéhoto odporúčania je skutočnosť, že neexistuje žiadna záruka, že prístup k súborom bude po zaplatení obnovený. Musíte mať na pamäti, že máte do činenia so zločincami. Preto je lepšie osloviť špecializovaných poskytovateľov bezpečnostných služieb, ktorí môžu okamžite poslať svojich odborníkov a podniknúť potrebné kroky priamo na mieste. Avšak kyberbezpečnostný trh trpí nedostatkom vysoko kvalifikovaných odborníkov. A tento nedostatok je ešte väčší v priemyselnej sfére, kde musí byť bezpečnostný expert zdatný nielen v oblasti informačnej bezpečnosti, ale aj v priemyselných riadiacich systémoch. To je pravdepodobne dôvod, prečo mnoho organizácií nemá kapacity na zvládnutie takýchto situácií samostatne – totiž aby podnik zvládol alebo vyšetril incident vo vlastnej réžii, to vyžaduje veľa prostriedkov a úsilia. Ďalším spôsobom, ako získať pomoc s digitálnou forenznou analýzou a reakciou na incidenty, je zapojenie tímu špecialistov na kybernetické incidenty (CERT). No nájsť špecialistu aj na ICS je ešte náročnejšie. Tu by som rád zdôraznil jednu vec – použitie špecializovaného nástroja na sledovanie priemyselnej bezpečnosti v každom prípade dokáže uľahčiť forenznú analýzu. Vo väčšine prípadov protokoly používané v rámci systémov ICS/SCADA nestačia na identifikáciu vektora útoku a na jeho dôkladné prešetrenie.

Nie je nič výnimočné, že svoj podiel na kybernetickom ohrození podniku majú aj jeho interní zamestnanci. Ako by teda mala vyzerať správne nastavená bezpečnostná politika pre túto kategóriu?

Správne nastavené pravidlá a procesy sú určite základným krokom, ale často nie sú dostatočne účinné pri zvyšovaní povedomia o postupoch priemyselnej kyberbezpečnosti medzi všetkými zamestnancami. Na základe našich skúseností najefektívnejším spôsobom, ako prostredníctvom vzdelávania zvýšiť povedomie a prevenciu, sú školenia zahŕňajúce aj prvky hry. Simulované cvičenia a školenia zamerané na zvyšovanie povedomia o kyberbezpečnosti sú mimoriadne dôležité pre všetkých zamestnancov zodpovedných za prevádzku automatizovaných systémov.

Ako ovplyvnila pandémia správanie podnikov a ich prístup k otázke kybernetickej bezpečnosti?

Samotná technológia nie je schopná vyriešiť všetky problémy. Spoločnosti roky čelia neschopnosti budovať podnikové bezpečnostné systémy, konkrétne najímaním nových talentov – a to začalo mať priamy vplyv na škody spôsobené skutočnými narušeniami kyberbezpečnosti. V dôsledku pandémie mnoho spoločností zmenilo spôsob fungovania – podľa prieskumu, ktorý sme realizovali minulý rok vo viac ako 330 priemyselných spoločnostiach a organizáciách po celom svete, až 30 % respondentov potvrdilo, že prešlo na model vzdialenej pracovnej sily. Kyberbezpečnostné procesy sa dostali pod tlak a prechádzali skutočným záťažovým testom. 14 % organizácií v prieskume uviedlo, že museli prepracovať svoje kyberbezpečnostné koncepty a len 7 % uviedlo, že ich stratégia kybernetickej bezpečnosti bola počas pandémie dostatočná. Zvýšenie počtu zamestnancov pracujúcich vzdialene zvýšilo počet pokusov o OT skenovanie siete počas pandémie. Výsledkom toho bolo, že spoločnosti uznali potrebu posilniť postupy kybernetickej bezpečnosti počas výnimočných situácií.

Je otázka kybernetickej bezpečnosti nákladnou záležitosťou pre podnik? Ako sa dajú náklady na vybudovanie účinnej ochrany optimalizovať?

Vzhľadom na to, že v roku 2020 dosiahli priemerné náklady za narušenie bezpečnosti podniku približne 0,9 milióna eur, sú investície do kybernetickej bezpečnosti vždy výrazne nižšie ako možná strata, ktorú by mohol úspešný kybernetický útok spôsobiť. A netreba zabúdať, že okrem finančných nákladov dochádza aj k poškodeniu reputácie a dôvery. Náklady na kybernetickú bezpečnosť tvoria vždy tri zložky: kapitálové (Capex), prevádzkové (Opex) a osobné (Personal). Takže napríklad investície do hardvéru a softvéru zároveň vyžadujú aj investície do ľudí potrebných na ich prevádzku a starajúcich sa o bezpečnosť. Po dôkladnom vyhodnotení súčasného stavu kybernetickej bezpečnosti spolu s analýzou potrieb a požiadaviek existuje priestor na optimalizáciu nákladov. Navrhujem využiť tzv. Paretov princíp, čiže zamerať sa na najvyššie priority a zabezpečiť aspoň najdôležitejšie časti podniku.

Aké prínosy pre koncového používateľa predstavuje spolupráca medzi výrobcami priemyselných automatizačných, riadiacich a IT systémov s tvorcami riešení z oblasti kybernetickej bezpečnosti?

Je zrejmé, že ide o nepretržitú a spoľahlivú dostupnosť či dodávku príslušného produktu alebo služby, ako aj o istotu, že sa ich údaje zdieľané s výrobcom nedostanú do zlých rúk. To je obzvlášť dôležité pre dodávateľov tretích strán a všetky takto prepojené subjekty. Okrem toho sa v priemysle dosiahlo veľa inovácií v oblasti automatizácie, internetu vecí, rozšírenej reality a ďalších technologických trendov. Tieto nové technológie neotvárajú iba nové obzory, predstavujú tiež nové vektory potenciálnych kybernetických útokov. Preto je dôležité, aby všetky strany úzko spolupracovali na zabezpečení toho, že každú inováciu bude možné používať bezpečne.

O tom, že kybernetickú bezpečnosť by nemal podceňovať žiadny podnik z akejkoľvek oblasti priemyslu, snáď netreba nikoho presviedčať. Aký by bol váš záverečný odkaz k tejto téme?

Ako som už spomenul, čoraz väčší prechod priemyselných spoločností aj do digitálneho priestoru vytvára tlak na ich ochranu pred kybernetickými útokmi. Som veľmi rád, že tento veľmi dôležitý proces je sprevádzaný zvýšeným povedomím o potrebe zabezpečiť tieto prevádzkové procesy aj pred kybernetickými hrozbami. Aby ste to mohli urobiť čo najlepšie a najefektívnejšie, je veľmi dôležité zvoliť si spoľahlivého a renomovaného partnera v oblasti kyberbezpečnosti s vhodnými produktmi, znalosťami, skúsenosťami a podporou. Naša spoločnosť ponúka klientom svojich 24 rokov skúseností v oblasti kybernetickej bezpečnosti, aby mohli bezpečne využívať výhody digitalizácie a technologického pokroku.

Ďakujeme za rozhovor.

Anton Gérer

Foto: Mondi SCP

Unikátne riešenie riadenia pohyblivých zariadení cez WiFi

Čo všetko je dôležité pre to, aby priemyselný podnik fungoval efektívne a bez zbytočných prestojov? Mnohí manažéri by za nevyhnutné predpoklady určite označili spoľahlivé stroje, včasnú dodávku surovín a energií aj zabezpečenie pracovnej sily. Málokto by možno vyzdvihol komunikačný systém slúžiaci na prepravu paliet s tovarom z automatickej baliacej linky do skladu. Príklad spoločnosti Mondi SCP, a. s., ktorá v Ružomberku vyrába papier a celulózu, však ukazuje, aký význam v súčasnosti komunikačné technológie zohrávajú nielen v živote ľudí, ale aj vo výrobných podnikoch.

Spoločnosť Mondi SCP so sídlom v Ružomberku je súčasťou Mondi, globálneho lídra v oblasti výroby obalov a papiera, ktorá zamestnáva približne 26 000 pracovníkov vo viac ako 30 krajinách. Je to najväčší integrovaný závod na výrobu celulózy a papiera v Slovenskej republike s výrobnou kapacitou 560 000 ton nenatieraného papiera, 66 000 ton obalového papiera a okolo 100 000 ton vysušenej buničiny určenej na predaj. Najnovšia investícia do nového papierenského stroja na výrobu kartónu s výrobnou kapacitou 300 000 ton ročne výrazne zvyšuje ponuku produktov pre udržateľné obalové riešenia používané v aplikáciách obalov z vlnitej lepenky popri už existujúcej silnej základni produktov z nenatieraného bezdrevného papiera.

Frustrujúce výpadky

Priemysel je dnes do značnej miery automatizovaný a inak to nie je ani v prípade Mondi SCP. Finálne zabalené palety prepravuje z výrobnej haly do automatického regálového skladu v podniku v súčasnosti dvanásť autonómnych koľajových vozíkov, ktoré riadi centrálny softvérový systém. Samotné vozíky sú osadené viacerými snímačmi, ktoré kontrolujú prítomnosť balíkov a tiež snímajú polohu vozíka v reálnom čase. Vozíky s centrálou po mnoho rokov komunikovali cez priemyselnú zbernicu PROFIBUS, pričom údaje sa prenášali cez kontaktnú komunikačnú zbernicu Wampfler. Takýto systém je už však do veľkej miery zastaraný a vyžaduje pomerne komplikovanú údržbu. Navyše ak sa zastaví jeden vozík, zostanú stáť aj všetky ostatné, pričom nájsť skutočnú príčinu výpadku býva zložité. Vzhľadom na nepretržitú výrobu sa nová zabalená produkcia začne hromadiť v baliacom priestore.

Manažment podniku sa preto rozhodol zastaraný komunikačný systém s problémovou údržbou nahradiť novým moderným stabilným riešením, ktoré spĺňa najvyššie kvalitatívne i bezpečnostné kritériá. Dôveru vložil do spoločnosti Soitron, ktorá má bohaté skúsenosti s navrhovaním bezdrôtových sietí v priemyselnom aj v kancelárskom prostredí.

Spoľahlivo v reálnom čase

Soitron v rámci tohto projektu predstavil v ružomberských papierňach inovatívne riešenie na bezdrôtovú WiFi komunikáciu autonómnych koľajových vozíkov, postavené na komunikačnej zbernici PROFINET. Tá sa v porovnaní s predošlou platformou PROFIBUS vyznačuje napríklad päťnásobne rýchlejšou reakciou na úrovni pod

100 milisekúnd, čo zaručuje komunikáciu medzi vozíkmi a centrálnym riadiacim systémom v reálnom čase.

Prenos dát cez sieť je šifrovaný, čiže dobre zabezpečený. Z pohľadu spoľahlivosti prevádzky a zabezpečenia kontinuity procesov je však dôležitejšie, že systém je navrhnutý redundantne. „Znamená to, že pri výpadku jedného prístupového bodu dokážu jeho úlohy prevziať okolité prístupové zariadenia. Podnik má aj redundantné prepínače, takže prípadná porucha jedného sieťového prvku nespôsobí nefunkčnosť siete," vysvetľuje Roland Rais, špecialista na siete v spoločnosti Soitron.

Priemyselný ethernetový riadený prepínač Cisco IE4000

Komunikácia v sieti PROFINET je trvale monitorovaná analyzátorom PROFINET-Inspektor.

Spoľahlivosť komunikácie zaručujú aj prístupové body a sieťové komponenty od spoločnosti Cisco, určené do priemyselného prostredia, ktoré odolávajú vode, prachu a nečistotám a dokážu fungovať aj pri extrémne nízkej či vysokej teplote. Pridaním priemyselného komunikačného prístupového bodu Cisco na samotný vozík bolo potrebné osadiť ho výkonnejším, 24 V DC napájacím zdrojom. Komunikácia pritom prebieha na dvoch frekvenciách – 2,4 a 5 GHz.


Priemyselný bezdrôtový prístupový bod Cisco Industrial Wireless 3702

Komunikácia pod dohľadom

Svoj podiel na riešení tohto projektu mala aj spoločnosť ControlSystem, s. r. o., ktorá sa zamerala práve na komunikačný systém na úrovni priemyselných zberníc PROFINET a PROFIBUS. „Pri návrhu riešenia sme vychádzali z požiadaviek zákazníka, ktorými boli možnosť postupnej implementácie nového systému počas prevádzky a dosiahnutie minimálne takej rýchlosti výmeny údajov na zbernici, ako mal pôvodný systém," konštatuje Ján Snopko, konateľ ControlSystem, s. r. o.

Z tohto dôvodu sa rozhodli ponechať pôvodné decentralizované systémy umiestnené vo vozíkoch postavené na CPU a V/V moduloch Wago. Tie boli doplnené o prevodník protokolov Proxy PN/DP, čo umožňuje postupné pripájanie vozíkov do novej siete, ako aj prípadný núdzový návrat do pôvodného riešenia. Z rovnakého dôvodu bol upravený aj HW a SW riadiaceho systému Simatic S7-400 tak, aby okrem nového CPU s rozhraním PROFINET zostala možnosť prevádzkovať aj pôvodnú komunikáciu PROFIBUS.

Vzhľadom na dôležitosť dopravy produktov pre plynulosť výroby je komunikácia v sieti PROFINET trvale monitorovaná analyzátorom PROFINET-Inspektor. „Namerané parametre komunikácie sú dôležité pre skrátenie času odstránenia poruchy, ako aj pre skoré rozpoznanie komunikačných problémov ešte pred výpadkom niektorej z pripojených staníc," konštatuje J. Snopko.

Tandem so spoločnosťou Cisco

Koncept bezdrôtovej komunikačnej siete v priemyselnom prostredí cez zbernicu PROFINET, v ktorej musia pohyblivé objekty v reálnom čase komunikovať a prechádzať medzi viacerými prístupovými bodmi, je jedinečná novinka v celosvetovom meradle. Samotná spoločnosť Cisco po ukončení projektu v Mondi SCP pripravila takzvaný Cisco Validated Design, čiže akési usmernenia (guidelines) na návrh tohto typu riešení. „Informácie získané pri našom testovaní a finalizácii riešenia smerovali do laboratórií Cisco a pomáhali firme pri tvorbe validovaného dizajnu," dodáva R. Rais.

Prirodzene neznamená to, že so základnými pravidlami na návrh komunikácie pohyblivých objektov sú návrh a realizácia obdobných riešení triviálne. Nestačí nakúpiť špičkový hardvér. Treba mať aj pokročilé znalosti sieťovej problematiky – od najvhodnejšieho umiestnenia zariadení cez voľbu typu kabeláže až po konfiguráciu a odladenie komunikačných tokov, prípadne integráciu do existujúcej podnikovej siete. „Návrh komunikačného riešenia nikdy nebude rovnaký, aj keby sme použili rovnaké hardvérové komponenty," objasňuje R. Rais.

Aj voľba hardvéru však býva u každého zákazníka iná. Napríklad v Mondi SCP využil Soitron protokol Cisco PRP (Parallel Redundancy Protocol) implementovaný v bezdrôtovom prostredí a jeho nasadenie odladil tak, aby spĺňal požiadavky systému, ktorý zákazník používal.


Foto: Mondi SCP

Protokol paralelnej redundancie (PRP) cez bezdrôtové pripojenie umožňuje rozdelenie prevádzky na dve paralelné bezdrôtové pripojenia, aby sa dosiahla najvyššia úroveň odolnosti pri rôznych priemyselných IoT implementáciách. Tým sa zabezpečuje nepretržitá konektivita a minimalizácia výpadkov v priemyselnom prostredí. Riešenie je založené na štandarde 802.11, ktorý otvára možnosti spolupráce s inými systémami.

Linyu Lu, Cisco,
Technical Marketing Engineer – IoT Wireless

Bez narušenia výroby

Po preukázaní životaschopnosti a spoľahlivosti v rámci pilotného konceptu nasadilo Mondi SCP nový bezdrôtový komunikačný systém na riadenie autonómnych vozíkov do ostrej prevádzky. Podľa R. Raisa sa dá obdobné riešenie implementovať aj bez celkovej odstávky vozíkov: „Keďže riadiaci systém zostáva ten istý a údaje do neho môžu plynúť cez obidva protokoly, môžeme vozíky vybavovať potrebnými zariadeniami postupne, jeden po druhom."

Uvedené riešenie možno podľa R. Raisa nasadiť nielen na autonómne vozíky, ale teoreticky aj na iné technológie, ako napr. portálové žeriavy, ktorých pohyb a polohu treba monitorovať v reálnom čase. A pritom nemusí ísť len o riešenie postavené na zberniciach PROFINET a PROFIBUS, pretože protokol Cisco PRP implementovaný v bezdrôtovom prostredí možno prepojiť aj s inými sieťami a protokolmi.

Spoľahlivý a bezpečný komunikačný systém je základným prvkom pri maximálnom využití dostupných výrobných kapacít a uspokojení potrieb našich zákazníkov zabezpečením stabilnej internej logistiky. Nasadená technológia jednoznačne prispela k zlepšeniu prevádzkových procesov.

Jaroslav Jaroš, Mondi SCP,
IT Manager

Priemyselné podniky dnes majú vďaka novým technológiám možnosť vniesť do mnohých prvkov výroby vrátane logistických vozíkov na prepravu tovaru skutočnú inteligenciu. Zariadenia nemusia plniť len základné úlohy – pomocou senzorov dokážu zbierať užitočné údaje o svojom okolí aj o sebe. Môžu dať napríklad včas vedieť, že majú opotrebovanú niektorú súčiastku. Ak však majú byť akékoľvek stroje či zariadenia v priemysle múdre, potrebujú nevyhnutne spoľahlivú komunikačnú sieť, aby dokázali komunikovať a odovzdávať svoju múdrosť ukrytú v údajoch nepretržite a okamžite ďalej.

Ďakujeme spoločnosti Mondi SCP, a. s., za možnosť realizácie reportáže a Rolandovi Raisovi zo spoločnosti SOITRON, s. r. o., a Jánovi Snopkovi zo spoločnosti ControlSystem, s. r. o., za poskytnuté technické informácie.

Anton Gérer

„Réžisti"

Keď sa vo firme znižujú náklady, často sa hľadajú režijní pracovníci – skladníci, manipulanti, zoraďovači, údržbári, upratovačky, asistentky a rôzni iní pomocní pracovníci. Všimli ste si, že procesy aj prácu v podniku delíme na hlavné a obslužné? A k ľuďom v tých obslužných sa niekedy správame ako k poskokom a sluhom? Manažéri s konzultantmi radi redukujú „réžistov" a myslia si, že tak zvyšujú výkonnosť firmy. V skutočnosti ju znižujú.

Pri návšteve firmy Toyota v Japonsku si spomínam na niektoré otázky našich ľudí. V jednej sa niekto pýtal japonského manažéra, koľko má „réžistov". Chcel počuť nejaké percento k počtu pracovníkov, ktorí „tvoria hodnotu". Japonec nechápal našu otázku a po vysvetlení nám odpovedal, že ich je toľko, koľko treba – aby bol plynulý tok. Mal pravdu. Tých „réžistov" tam mali oveľa viac, ako sme boli zvyknutí z našich firiem. A produktivitu mali oveľa vyššiu ako my. Práve vďaka tomu. Rýchli a kvalitní zoraďovači a údržbári zaistia vysoké využitie a výkon kľúčových strojov. Spoľahliví skladníci a manipulanti dokážu zabezpečiť plynulý tok montážnej linky. Dobre organizované sestričky dokážu zaistiť plynulý tok pacientov cez kvalifikovaných lekárov. Podobný problém vzniká u právnikov, konštruktérov, vývojárov, programátorov alebo projektantov.

Kamarátova dcéra robí lekárku v Japonsku. Keď som túto krajinu navštívil, videl som všade snahu o plynulý tok. V hoteli už mali pripravené kľúče, aby sme nečakali. Keď sa niekde vytvoril rad, hneď niekto riešil úzke miesto. Procesy vo výrobných fabrikách pripomínali orchester. Vďaka „réžistom". V našich podnikoch manažéri behajú s tabuľkami a redukujú „nadbytočných réžistov". Za dobré čísla dostanú prémie. V Japonsku manažéri namiesto „réžistov" riešili plynulý tok a dosahovali vysokú produktivitu a zisk. Slovenská lekárka v Japonsku má tri sestričky – na administratívu, organizačné a medicínske záležitosti. U nás som ešte nevidel tri sestričky na jedného lekára. Ani by to nemuseli byť zdravotné sestry, ale manažérky toku pacientov. Aj preto je produktívne využitie lekárov u nás pod 30 %. Možno preto ich je nedostatok a musí sa u nich tak dlho čakať. Zákazníci dnes vyžadujú hlavne kvalitné služby. Mali by sme sa preto namiesto redukovania „réžistov" zamerať na plynulý tok.

Ján Košturiak
IPA Slovakia, s.r.o.

IIoT a rozšírená realita v drevospracujúcom priemysle

Vo svete podnikania si nikto nemôže dovoliť stagnovať. Lídri podstatne skôr získajú skúsenosti a sú ochotní posúvať hranice, aby narušili dlho zaužívané priemyselné normy. V nasledujúcej reportáži sa dozviete, ako zavedená spoločnosť na výrobu zariadení na spracovanie dreva využívala inovatívne technológie a partnerstvá na transformáciu svojich vlastných prevádzok a revitalizáciu celého odvetvia.

Spoluprácu a inovácie má BID vo svojej DNA

Ak niekto pozná hodnotu spolupráce, je to BID Group. S viac ako 35-ročnými skúsenosťami je BID jedným z najväčších integrovaných dodávateľov inovatívnych riešení na kľúč pre drevospracujúci priemysel. Spoločnosť BID Group poskytuje kompletnú škálu zákaznícky orientovaného inžinieringu, inovatívnych zariadení, digitálnych technológií, inštalácií na kľúč a popredajných služieb. Od jednotlivých až po niekoľko vzájomne prepojených výrobných liniek poskytuje BID svojim zákazníkom inteligentné vybavenie a prepojené továrne.

Snaha čeliť zásadným výzvam celého odvetvia

Drevospracujúci priemysel nedokázal prijať zmeny s rovnakou rýchlosťou a prispôsobivosťou, ako iné výrobné odvetvia. Ak sa na vstupe procesov nachádzajú suroviny tak viariabilné, ako je napr. drevo, schopnosť nájsť a štandardizovať technológiu s preukázanou pridanou hodnotou bola pre priemysel ako celok výzvou. Ak jednotliví výrobcovia navyše nemôžu mať pod kontrolou vlastnosti rozhodujúceho materiálu na vstupe, ako môže celé odvetvie štandardizovať technológie?

Najvyššie náklady pre akýkoľvek drevospracujúci podnik sú na vstupné suroviny, takže udržanie dostatku hodnotného dreveného vlákna je pre ziskovosť rozhodujúce. V tomto odvetví priemyslu má každý typ surového dreveného vlákna jedinečné vlastnosti, ako je veľkosť, tvar alebo obsah vlhkosti, ktoré majú vplyv na spôsob jeho spracovania. Neustále sa mení aj dopyt na trhu pre konkrétne konfigurácie. Aj pri optimálnom zhodnotení materiálu bránia vyššiemu výkonu prevádzky na pílenie dreva faktory, ako neplánované odstávky, strata produktivity a problémy s kontrolou kvality. Mnohí prevádzkovatelia píl investovali veľké prostriedky do vybavenia a tieto investície sa musia v súvahe prenášať viac ako desať rokov. Aktíva podniku sa časom stanú menej spoľahlivými a operátori si musia zvoliť medzi zle fungujúcim vybavením alebo ďalšími veľkými finančnými investíciami.

Napriek týmto prekážkam videla spoločnosť BID príležitosť narušiť tento neutešený súčasný stav – to by však neprišlo bez riešenia dlhodobých výziev. Vďaka technológiám cloudu a priemyselného internetu vecí (IIoT), ktoré transformujú výrobné prevádzky v iných priemyselných odvetviach, spoločnosť BID stavila na potenciál kombinovať najmodernejšie technológie s hlbokými znalosťami odvetvia a pripraviť tak pôdu na digitálnu transformáciu v drevospracujúcom priemysle.

Transformácia so správnymi partnermi

Spoločnosť vedela, že chce využiť cloudové pripojenie a IIoT, a preto na začiatku celého procesu uzavrela partnerstvo s malou firmou na vývoj softvéru, aby vytvorila platformu na zhromažďovanie a sledovanie prevádzkových údajov. No navrhnutá platforma nepriniesla očakávané výsledky a nedokázala poskytnúť požadované impulzy potrebné na posun vpred. Nakoniec si v BID Group uvedomili, že firme zaoberajúcej sa vývojom softvéru chýbali znalosti drevospracujúceho odvetvia a že je potrebný nový plán. Prehodnotením svojho prístupu sa spoločnosť BID snažila vybudovať tím strategických partnerov, z ktorých každý má odborné znalosti vo vlastných oblastiach. Spoločnosť sa už v minulosti zúčastnila na podujatí PTC 2019 LiveWorx a uvedomila si, že riešenia PTC zodpovedajú ich obchodným modelom a vízii rastu. Chris Wells, hlavný viceprezident spoločnosti BID pre popredajné služby, servis a spoľahlivosť, bol prekvapený prístupom PTC ku kontinuite podnikania a správe životného cyklu produktu. „Len čo sme začali myslieť na celý životný cyklus produktu, všetky tieto nástroje zrazu pridali obrovskú hodnotu riešeniam, o ktorých uvažujeme," hovorí Ch. Wells.

Spoločnosť tiež vedela, že kompletný tím bude vyžadovať ďalších strategických partnerov. Okrem PTC sa obrátili na dlhoročného partnera Rockwell Automation, a to pre jeho odborné znalosti prevádzkovej technológie a rozsiahlu ponuku HW a SW vrátane analytiky, MES, automatizácie, priemyselného riadenia, snímačov a sietí. Okrem ľahko programovateľného softvéru bola nevyhnutnosťou aj životnosť produktu. Pretože na pílach nepracuje veľa technikov na plný úväzok, spoľahlivý hardvér s dlhou životnosťou a kultúra spolupráce spoločnosti Rockwell Automation boli rozhodujúcimi faktormi, ktoré prispievajú k minimalizácii neočakávaných prestojov.

Udržiavanie vzťahov s existujúcimi partnermi bolo pre BID rovnako dôležité – a umožňovala to schopnosť bezproblémovej integrácie PTC s iným softvérom. Napríklad BID integrovala PTC technológiu IIoT do Grafana Labs na analýzu a monitorovanie postavenú na otvorenej platforme a zároveň využila nástroj Influx Data na zabezpečenie viditeľnosti zásobníkov, snímačov a systémov v reálnom čase. Vďaka PTC Cloud Services získala navyše spoločnosť BID podporu v oblasti správy a bezpečnosti údajov od spoločnosti PTC spolu s infraštruktúrou poskytovanou spoločnosťou Microsoft Azure. BID sa tak dostala do pozície, keď môže využiť svoje skúsenosti výrobcu pôvodných zariadení spolu s poprednými technologickými partnermi, aby mohli pomôcť svojim zákazníkom v oblasti spracovania dreva v úsilí o digitálnu transformáciu.

Digitálne prepojenie zariadení

Ako podnik zameraný na zákazníka mala spoločnosť BID jasné ciele: znížiť neplánované prestoje a nastaviť novú úroveň využitia a výkonnosti aktív, aby zákazníci mohli čo najlepšie využiť svoje investície. Pri pilotnom projekte u jedného zo svojich zákazníkov

začali používať PTC ThingWorx, end-to-end priemyselnú IoT platformu ako komunikačný základ na prepojenie ich inteligentných prevádzok. Platforma umožnila spoločnosti BID získať prehľad o produkcii a stave aktív pomocou analýzy údajov v reálnom čase a bohatej škály prehľadov a reportov z výroby. Spoločnosť BID tiež využila ThingWorx na implementáciu prediktívnych analýz pri údržbe a optimalizácii spoľahlivosti.

V rámci tohto pilotného projektu dokázala spoločnosť BID zlepšiť celkovú spoľahlivosť výrobných procesov a zariadení. Pridali výstrahy do svojich vysokorýchlostných ložísk a na úrovni komponentov použili ďalšie monitorovanie, alarmové a analytické údaje, aby identifikovali abnormálne podmienky a lepšie sledovali stav technických prostriedkov. Čo je dôležité, spoločnosť BID dokázala prejsť z reaktívneho na preventívny a proaktívny prístup k servisu a údržbe, čo viedlo k bezprecedentnej spoľahlivosti zariadenia.

Vďaka týmto vylepšeniam bola spoločnosť BID schopná rýchlo poskytovať svojim zákazníkom prepojenie ich prevádzok. Prvotná implementácia priniesla neuveriteľné výsledky vrátane dvojciferného vylepšenia ukazovateľa celkovej efektívnosti zariadení (OEE).

Potvrdený úspech priniesol aj vylepšenú ponuku pre zákazníkov

Aj keď bol úspech transformácie prevádzok na kľúč od spoločnosti BID pôsobivý, boli si vedomí, že existuje veľká trhová príležitosť na digitálnu transformáciu prevádzok, ktoré boli len čiastočne vybavené ich hardvérom. Spoločnosť mala deväť zákazníkov, ktorí využívali výlučne jej zariadenia a riešenia, ale ďalších 400, v ktorých videli potenciál na presadenie sa. Cieľom pritom bolo nezameriavať sa tak na predaj svojich zariadení, ale viac na prepájanie a servis existujúcich prevádzok na spracovanie a pílenie dreva. Na základe tohto predpokladu spoločnosť BID oslovila ďalších zákazníkov, ktorí mali rôznorodé vybavenie svojich prevádzok. Spoločnosť predstavila OPER8™, riešenie IIoT poskytujúce prehľady v reálnom čase, ktoré optimalizujú obnovu a produktivitu drevených vlákien pri súčasnom zvýšení predaja. Na základe poznatkov získaných z vlastných skúseností s OPER8™ mohla spoločnosť prísť na trh s balíkom riešení určených na digitálnu transformáciu prevádzok zákazníkov a pomôcť im pripojiť ich existujúce prevádzky na spracovanie a pílenie dreva. Zákazníci prijali toto riešenie nad očakávania.

„OPER8™ poskytuje technické znalosti potrebné na perfektné monitorovanie spoľahlivosti a výkonu píl," hovorí Dan Bowen, generálny riaditeľ Biewer South, Biewer Lumber. „Poskytuje prehľad, ktorý nám pomáha monitorovať všetky procesy a vykonávať úpravy v reálnom čase, aby sme zaistili, že pracujeme v rámci vopred stanovených ukazovateľov a udržujeme efektivitu výroby. OPER8™ poskytuje pílam komplexný balík, ktorý monitoruje spoľahlivosť strojov, generuje alarmy, keď je proces mimo svojich hraničných stavov, a sleduje kontrolu kvality vo všetkých častiach linky," dodáva D. Bowen.

Skúsenosti spoločnosti BID v odvetví spracovania dreva prispeli k schopnosti ponúknuť zákazníkom transformačné riešenia. „Naše topánky sú plné pilín – pri rozhovoroch so zákazníkmi okamžite prinášame odborné znalosti z odvetvia," uvádza s humorom Steven Hofer, výkonný viceprezident pre stratégiu a rozvoj podnikania. „V tomto odvetví nie je žiadne iné riešenie, do ktorého by bolo možné pripojiť toľko rôznorodých zariadení na spoločnú platformu, ako je to v prípade OPER8™. Ukázali sme to aj na príklade využitia radu produktov a technológií spoločnosti PTC," dodáva.

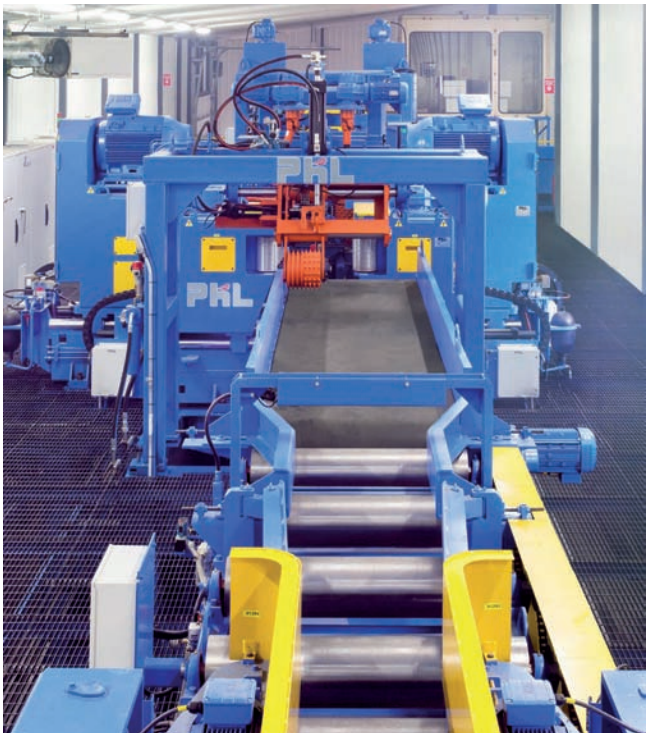
Posun smerom k rozšírenej realite rozširuje možnosti popredajných služieb

Na základe zmien, ktoré boli postavené na IIoT, rozpoznala spoločnosť BID príležitosť posunúť svoje prevádzky na vyššiu úroveň využitím rozšírenej reality (RR). Nielen v rámci svojich prevádzok, ale aj v prevádzkach svojich zákazníkov začína RR zlepšovať popredajné služby, jeden z najdôležitejších aspektov podnikania, ktorý neustále zvyšuje príjmy.

V BID rozpoznali najmä podstatnú výzvu poskytnúť rýchle a presné služby na míle vzdialenému zákazníkovi, ktorých má spoločnosť viac než dosť – a to najmä pri núdzových alebo rozsiahlejších opravách. V týchto situáciách vedú tradičné spôsoby služieb, ako sú telefónne hovory, textové správy a e-maily, k dlhším čakacím lehotám a k neplánovaným prestojom zákazníkov. Pretože cestovanie je pre prevádzkových technikov BID čoraz náročnejšie, stala sa RR jednoznačne použiteľným riešením.

Pomocou Vuforia Chalk, nástroja na vzdialenú pomoc a spoluprácu na diaľku, môžu teraz prostredníctvom RR poskytovať presné a podrobné pokyny zákazníkom v reálnom čase, kdekoľvek a kedykoľvek to bude potrebné. Zákazníci si môžu aplikáciu jednoducho stiahnuť a spojiť sa so servisnými technikmi spoločnosti BID a vyriešiť neočakávané problémy. Kombináciou zvuku a videa v reálnom čase s technológiou RR umožňuje Chalk servisnému technikovi prezerať prostredie a vybavenie koncového zákazníka a písať poznámky priamo na obrazovku. Pretože digitálne poznámky tohto nástroja bežia v rámci RR, „držia sa" miesta a prostredia, do ktorého sú nakreslené, čo pomáha zákazníkovi ľahko sledovať a dokončiť kroky smerujúce k vyriešeniu problému. „Chalk je obzvlášť užitočný nástroj na poskytovanie diagnostiky zákazníkom na diaľku," hovorí Alistair Cook, generálny riaditeľ spoločnosti BID Group. „Vďaka nasadeniu pokrokových technológií môžeme pokračovať v rozvoji tohto odvetvia, aby sme nemuseli kvôli poskytnutiu služby toľko cestovať. Používanie nástroja Chalk je obrovskou výhodou pre všetkých zúčastnených."

Chalk tiež dramaticky zmenil spôsob, akým sa odborníci na servis v spoločnosti BID navzájom spájajú počas hovorov, ktoré iniciuje



zákazník požadujúci servis. V mnohých prípadoch vycestuje miestny servisný technik BID k používateľovi kvôli údržbe alebo oprave. Pomocou nástroja Chalk sa technik môže spojiť so vzdialeným odborníkom, ktorý ho bude viesť, ak narazí na neznáme problémy, ktoré sám nedokáže vyriešiť. Chalk pomáha pracovníkom v prvej línii získať prístup k cenným znalostiam odborníkov BID z daného odvetvia bez ohľadu na to, kde sa nachádzajú.

Rozšírená realita zdôrazňuje víziu spoločnosti v oblasti neustáleho učenia sa

Posun smerom k RR bol obrovský z toho hľadiska, ako sa BID pozerá na spokojnosť zákazníkov. „Technológia RR spoločnosti PTC mení náš pohľad na to, ako pristupujeme k celkovému procesu popredajných služieb," objasňuje S. Hofer. Mnoho zákazníkov si podľa neho všimlo rozdiel v denných pracovných postupoch. „Je zrejmé, že schopnosť rýchleho prechodu na vzdialené diagnostické a servisné služby bola neuveriteľne dôležitá," pokračuje S. Hofer. „Tento typ technológie môže fungovať a možno ho rýchlo nasadiť a pridať obrovskú hodnotu."

Ak sa pozrieme ešte ďalej, investícia do RR technológie prináša ešte ďalší úžitok. Pomôže spoločnosti rozvíjať príležitosti na vzdelávanie a rozvoj pre jej zákazníkov aj zamestnancov. Tradičné metódy školení zahŕňajú veľa papierových príručiek, ktoré sa skôr prikláňajú k suchému čítaniu. No nedávna investícia do programu Vuforia Expert Capture umožní spoločnosti BID vytvoriť knižnicu podrobných virtuálnych manuálov typu „krok za krokom" a štandardných prevádzkových postupov, ktoré pomôžu zrýchliť školenia týkajúce sa rôznych zariadení a procesov. Pomocou aplikácie Expert Capture budú ich servisní odborníci schopní vykonať a zaznamenať sériu servisných postupov a zverejniť hotové pokyny na prezeranie internými technikmi a koncovými zákazníkmi pomocou rôznych mobilných a handsfree zariadení vrátane inteligentných okuliarov Microsoft HoloLens. Koncový používateľ potom môže pri vykonávaní úlohy postupovať podľa pokynov a dokončiť kroky sám. To zníži počet servisných zásahov, pretože zákazníci budú mať ľahko dostupné pokyny, ktoré ich oprávnia vykonávať v prípade potreby viac vlastnej údržby a opráv.

Spoločnosť BID skúma ďalšie možnosti zlepšenia služieb popredajného servisu a zvyšovania výnosov s RR, od ponuky doplnkových služieb a inštruktážnych materiálov pre jednotlivé prevádzky až po prístup na portál s mesačným predplatným. V súlade so svojím dlhodobým modelom služieb bude BID naďalej vyvíjať úsilie na lepšie poskytovanie služieb zákazníkom – najmä prostredníctvom RR. „Rozšírená realita je o reakcii. Pevne veríme, že ak chceme byť úspešní, obchodovanie s nami musí byť jednoduché – a AR to umožňuje," hovorí Ch. Wells. Vysvetľuje, že poskytovanie rýchlej a ľahkej starostlivosti o zákazníka – alebo posilnenie vedomostí zákazníkov o ich zariadeniach – prináša z dlhodobého hľadiska výhody každému. „Ide o čas a peniaze. Neexistuje žiadny iný spôsob okrem RR, ktorý nás dostane tam, kde chceme."

Zostať verný hodnotám

Spoločnosť BID prešla významnou digitálnou transformáciou vo svojom vnútri, ako aj v službách ponúkaných zákazníkom. S plánmi na vybudovanie úplne nových závodov, poskytovanie vzdialeného monitorovania a vytváranie skúseností zo služieb zameraných na zákazníka nepochybne nie je nedostatok príležitostí rozširovať sa o nové technológie. Pri ďalšom rozširovaní cesty digitálnej transformácie sa BID bude naďalej spoliehať nielen na produkty a riešenia PTC, ale aj na ľudí za nimi. S tímom zákazníckej podpory spoločnosti PTC, ktorý poskytuje nepretržité vedenie a podporu, využíva spoločnosť BID svoje technologické úspechy a napreduje pred konkurenciou.

Najdôležitejšie je, že BID sa bude aj naďalej pozerať do minulosti, aby mohla byť lídrom v budúcnosti. „Začínali sme ako spoločnosť so základnými hodnotami týkajúcimi sa budovania tímov svetovej triedy a poskytovania najlepších služieb pre našich zákazníkov," hovorí S Hofer. „Budeme pokračovať v inováciách a narúšaní tradícií tohto odvetvia, aby sme mohli zostať verní týmto hodnotám – pretože naši zákazníci dávajú smer našej ceste." Vďaka lepšej podpore zákazníkov a interných tímov prostredníctvom digitálnej transformácie vytvoril BID základ poskytovania výnimočných výsledkov v rekordnom čase. Ide o zmeny, ktoré zásadne transformujú nielen ich podnikanie, ale aj drevospracujúci priemysel ako celok – a BID už na túto výzvu nemôže byť viac pripravený.

Zdroj: BID Group uses PTC's IIoT and augmented reality solutions to digitally transform the wood processing industry. PTC Inc. Prípadová štúdia. [online]. Citované 23. 5. 2021. Dostupné na: https://www.ptc.com/en/case-studies/bid-group-drives-digital-transformation-with-iot.

-tog-

Výrobca nábytku zabezpečil sieť na úrovni riadiacich systémov

Táto spoločnosť je najväčším výrobcom v nábytkárskom priemysle v USA. Hlavná výrobná prevádzka sa rozkladá na ploche viac ako 370 000 m^2, zamestnáva 2 000 pracovníkov a suroviny získava z celého sveta. Ochrana najdôležitejších priemyselných zariadení pred kybernetickými hrozbami je zložitá z mnohých dôvodov. Spoločnosť si na riešenie tejto výzvy vybrala Check Point.

Potreba zabezpečenia priemyselných riadiacich systémov (ICS)

Spoločnosť uvádza na trh viac ako 40 rôznych produktových radov. Pri ich výrobe sa spolieha na stovky jedinečných priemyselných strojov a riadiacich systémov, ako sú systémy SCADA a PLC. Všetky tieto systémy a procesy musia byť monitorované, aby sa zabezpečila optimálna kvalita výroby a prevádzkyschopnosť.

„Vznikajúce hrozby sa čoraz viac zameriavajú na narušenie výrobných procesov alebo prevzatie kontroly nad nimi získaním prístupu prostredníctvom SCADA a PLC," uviedol odborník IT oddelenia tohto výrobcu. „Pretože sa IT a operačné technológie (OT) zbližujú, je nevyhnutné okrem systémov IT zabezpečiť aj kybernetickú bezpečnosť pre systémy OT." Ochrana ICS na úrovni prevádzky tradičnými bezpečnostnými opatreniami je zložitá. Na rozdiel od IT prostredia, piliny, výkyvy teploty, vibrácie a elektromagnetické rušenie spôsobujú, že prostredie prevádzky je nepriateľské voči tradičnej elektronike. Celková koncepcia takejto výrobnej prevádzky a rozvrhovanie priestoru je zvyčajne ťažiskovo orientované na výrobné zariadenia a technológie, čo sťažuje inštaláciu ďalších zariadení určených napr. na riešenie bezpečnosti.

Vytvorenie bezpečnej hranice

Technik z oddelenia IT bol oboznámený s riešeniami Check Point a po vyhodnotení niekoľkých možností si spoločnosť vybrala na zabezpečenie svojich výrobných prevádzok odolné zariadenia Check Point 1200R. Tie poskytujú osvedčené integrované zabezpečenie v náročnom prostredí a na komplexné pokrytie podporujú širokú škálu protokolov špecifických pre priemysel. Obsahujú aj firewall novej generácie, IPS, kontrolu aplikácií, antivírus, antibot na plnohodnotnú obranu systémov ICS, ako aj sieťové mosty medzi systémami OT a IT. „Zariadenia Check Point 1200R dokonale zapadajú do nášho prostredia," uviedol technik. „Vďaka možnosti montáže na DIN lištu bolo ich nasadenie jednoduché a nákladovo efektívne. Jednoducho sme ich pripevnili na DIN lišty a sú automaticky napájané cez systémy OT. Eliminovala sa potreba budovania väčšieho priestoru alebo prevádzkovania drahej elektrickej kabeláže. "

Spoločnosť tiež používa zariadenie na správu kybernetickej bezpečnosti Check Point R80, aby mala pod kontrolou 50 zariadení Check Point 1200R nasadených vo viacerých výrobných prevádzkach po celom svete. Check Point R80 konsoliduje systémy, pravidlá a správu do jednotnej konzoly kvôli jednoduchosti správy.

Ochrana systémov a ľudí

Zariadenia Check Point 1200R sú nasadené medzi sieťami IT a OT, aby monitorovali všetku komunikáciu smerujúcu dovnútra a von z výrobných zariadení spoločnosti. Zariadenia používajú na detekciu prichádzajúcich hrozieb pre SCADA a riadiace siete firewall bránu novej generácie a IPS. „Od nasadenia R80 a odolných zariadení 1200 sme nemali žiadne bezpečnostné incidenty," uviedol IT technik. „Funkcie antibot a antimalware spoločnosti Check Point nám tiež pomáhajú zabezpečiť, aby boli zamestnanci chránení pred nehodami, ktoré by mohli vyplynúť z prevzatia kontroly nad priemyselným zariadením."

Nie je potrebný žiadny ďalší personál

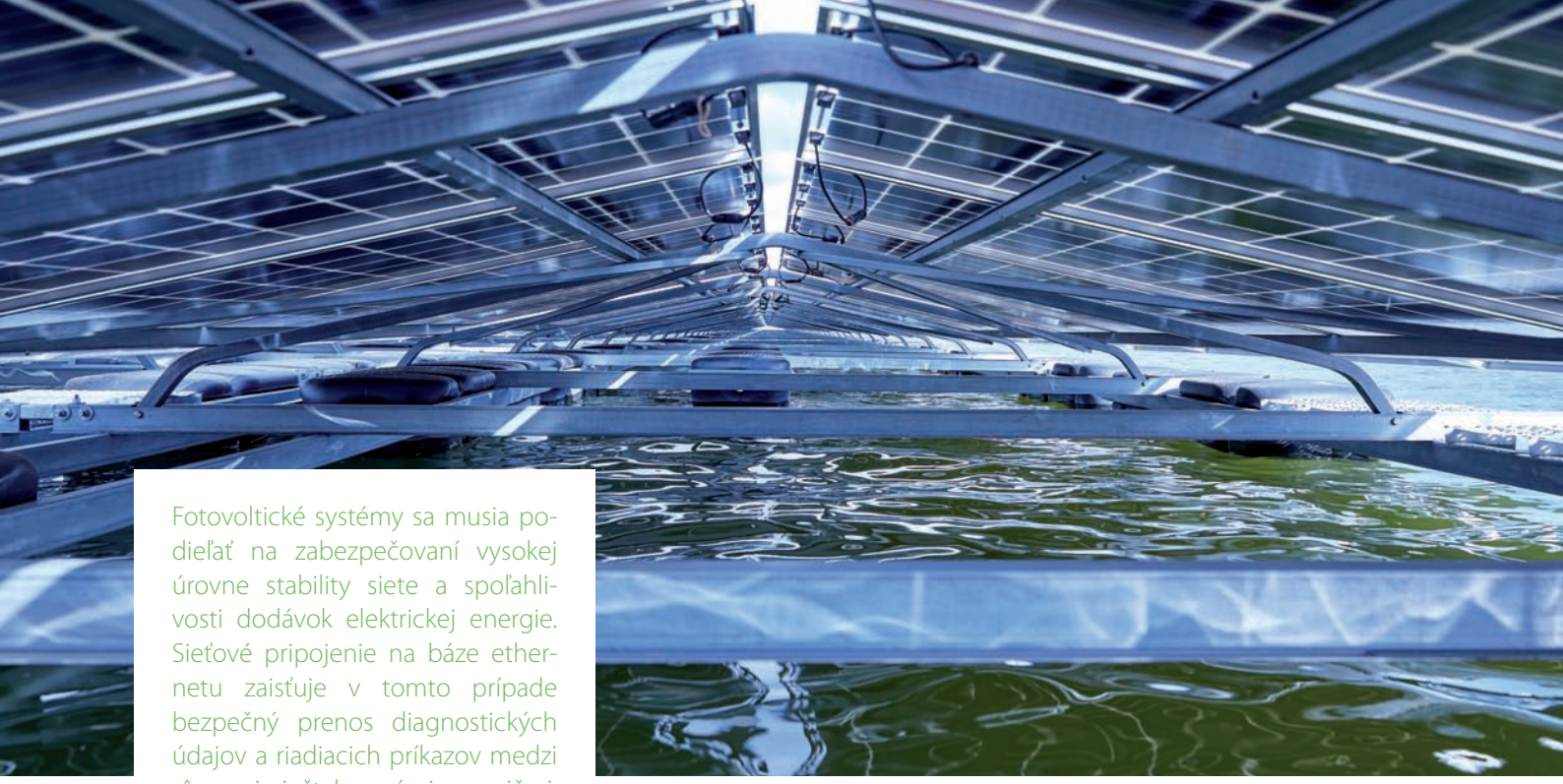
Správa kybernetickej bezpečnosti Check Point R80 beží ako virtuálny stroj a všetky údaje potrebné na správu celého prostredia prezentuje pre kompetentných na jednej obrazovke. Členovia tímu sa nemusia prihlásiť do každého zariadenia zvlášť, čo šetrí hodiny času. Funkcia súbežnej správy umožňuje prihlásenie viacerých správcov súčasne, čo zvyšuje efektivitu. Všetky zmeny pravidiel možno pred inštaláciou skontrolovať, aby sa tak ešte viac znížilo riziko. „Nemuseli sme kvôli tomu zamestnávať ďalších odborníkov," vysvetľuje IT technik. „Systémy Check Point sú prístupné pre správcov, takže ich sledovaním nemusíme tráviť hodiny týždenne. Sledujeme hrozby, ale ich správa a riešenie sú mimoriadne jednoduché."

Dobrá rada

Spoločnosť má teraz istotu, že ich kritické systémy a zamestnanci sú chránení. Zariadenia Check Point 1200R chránia tisíce zariadení v jej sieti, a teda aj výrobných zamestnancov. „Máme pokoj, keď vieme, že sme chránení," povedal IT technik. „Mojou radou ostatným výrobným IT tímom je pozrieť sa na Check Point a chrániť tak svoje OT investície. Hrozby a nové útoky sa zameriavajú na priemyselné riadiace systémy a ďalšie hardvérové zariadenia – v hre je príliš veľa, aby sme ostali nepripravení."

Zdroj: Furniture manufacturer secures its ICS network, keeping employees safe and operations running with Check Point rugged appliances and cyber security management. [online]. Citované 10. 5. 2021. Dostupné na: http://www.checkpoint.com/downloads/customer-stories/furniture-manufacturer-security-management-case-study.pdf.

-tog-



Fotovoltické systémy sa musia podieľať na zabezpečovaní vysokej úrovne stability siete a spoľahlivosti dodávok elektrickej energie. Sieťové pripojenie na báze ethernetu zaisťuje v tomto prípade bezpečný prenos diagnostických údajov a riadiacich príkazov medzi rôznymi inštalovanými meničmi, transformačnými stanicami, bodmi pripojenia do siete a monitorovacími systémami – či už prostredníctvom káblového pripojenia, alebo bezdrôtovej komunikácie.

Keď je prioritou vysoká úroveň stability siete

Fotovoltické systémy (FVS) ako zdroje využívajúce obnoviteľnú energiu výrazne prispievajú k uspokojeniu globálne rastúceho dopytu po energii. Plánovanie, výstavba a správa veľkých FVS však vyžaduje obrovské množstvo odborných znalostí a skúseností. Spoločnosť Zebotec GmbH so sídlom v nemeckom Konstanci sa za posledných 15 rokov v tejto oblasti etablovala a stala sa jedným z popredných svetových nezávislých systémových integrátorov riadenia fotovoltických elektrární. Zebotec je súčasťou BayWa r. e. Group, ktorá v roku 2009 spojila rôzne spoločnosti zaoberajúce sa využívaním obnoviteľných energetických zdrojov. K činnostiam mníchovskej spoločnosti patrí okrem iného návrh, výstavba a marketing FV elektrární (FVE) v rámci sektora riadenia solárnych projektov. V týchto projektoch sa spoločnosť Zebotec okrem iného stará aj o systémy na monitorovanie a riadenie. Rozsah služieb zahŕňa aj budovanie efektívnych ethernetových sietí, ktoré sa používajú na prepojenie jednotlivých častí systému a na výmenu údajov (obr. 1).

Obr. 1 Spoločnosť Zebotec GmbH so sídlom neďaleko Bodamského jazera sa špecializuje na monitorovacie a riadiace technológie pre fotovoltické systémy.

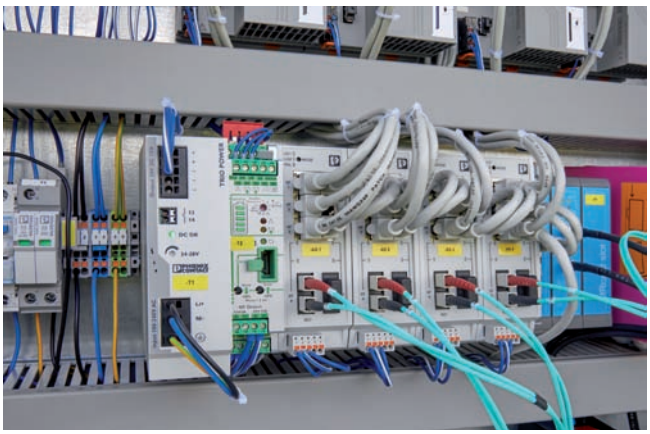
VLAN zabraňujú nežiaducej komunikácii medzi rôznymi časťami systému

Ethernetové siete nainštalované vo fotovoltických systémoch sa používajú na prenos diagnostických údajov zaznamenaných v meničoch, meteorologických staniciach, teplotných snímačoch namontovaných v transformačných staniciach a zariadeniach na meranie energie. Zasielanie riadiacich údajov na pripájanie zdroja do prenosovej sústavy kladie vysoké nároky na bezpečnú realizáciu tejto komunikácie, pretože ak prijímač neprijíma riadiace hodnoty spoľahlivo, zdroj sa pripojí do sústavy neriadene, čo by mohlo ohroziť stabilitu siete.

Najmä pri sieťovom prepojení jednotlivých transformačných staníc preto treba zohľadniť určité špecifické skutočnosti. Dobrým príkladom je 45-megawattový pozemný systém v holandskom Oosterwolde de Boer, ktorý realizovala spoločnosť Zebotec a holandská pobočka spoločnosti BayWa r. e., GroenLeven. Prvou výzvou bolo prekonanie veľkých vzdialeností medzi stanicami v tomto systéme. Druhou bola skutočnosť, že ethernetové káble boli uložené v káblových kanáloch s veľmi malou vzdialenosťou od AC a DC káblov. Kvôli tejto blízkosti môže pri používaní klasických medených káblov (skrútenou dvojlinkou) vzniknúť elektromagnetické rušenie, ktoré môže v horšom prípade viesť k strate údajov. Aby sa tomu zabránilo, museli by byť medené káble vybavené špeciálnym tienením alebo uložené osobitne. Kvôli dĺžke káblov a možnosti vplyvu elektromagnetickej indukcie sa Zebotec rozhodol použiť káble optických vlákien, ktoré sa vďaka svojej odolnosti proti elektromagnetickému rušeniu a chybám osvedčili ako vhodné riešenie pre túto aplikáciu (obr. 2).

Zebotec tiež nainštalovala do centrálneho bodu pripojenia k sieti riadené prepínače od Phoenix Contact, aby sa ešte viac zvýšila stabilita siete. Do prepínačov sa privádzajú údaje ethernetovým prenosom z transformačných staníc zapojených do niekoľkých liniek.

Obr. 2 Pri sieťovom prepojení jednotlivých transformačných staníc inštalovaných na zemi bolo potrebné zvážiť rôzne špecifiká.



Obr. 3 Riadené prepínače radu 2200 sa vyznačujú okrem iného rôznymi mechanizmami redundancie a bezpečnostnými funkciami.

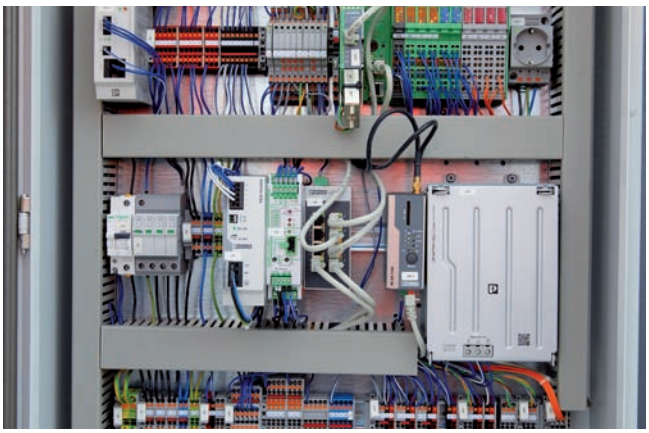
V tejto topológii je každá linka nakonfigurovaná ako samostatná virtuálna sieť (VLAN). To zabraňuje rôznym častiam systému v tom, aby nechtiac vymieňali údaje medzi sebou, a zbytočným dátovým tokom, čím sa zlepšuje efektivita komunikácie. Zebotec tiež vytvoril redundantné sieťové štruktúry, najmä vo veľkých systémoch a zvyčajne vo forme kruhovej topológie pomocou protokolu RSTP (Rapid Spanning Tree Protocol), aby sa dosiahla ešte vyššia úroveň bezpečnosti pri zlyhaní. Tento koncept znamená, že je zabezpečený prenos dát medzi všetkými časťami systému, a to aj v prípade poruchy spojenia v jednej linke tvorenej optickými vodičmi. Zebotec v tejto aplikácii využil riadené prepínače série FL SWITCH 2200, aby zabezpečil potrebnú funkčnosť redundancie (obr. 3).

Plávajúce transformačné stanice možno pripojiť k sieti prostredníctvom siete WLAN

Zebotec bol konfrontovaný s ďalšou výzvou týkajúcou sa pripájania nového typu FV systémov. Popri veľkých, samostatne stojacich systémoch začala spoločnosť nedávno spolupracovať so spoločnosťou BayWa r. e. v oblasti FVE umiestnených na vodných plochách, ktoré nie sú určené na rekreačné účely alebo nie sú v ochrannom pásme. Transformácia nevyužitých jazier na vysoko efektívne fotovoltické systémy prináša viaceré výhody: prispievajú napríklad k znižovaniu emisií CO_2, majú vysokú účinnosť výroby elektrickej energie vďaka efektu vodného chladenia a zabraňujú konfliktom, ktoré sa často vyskytujú pri FVE umiestnených na zemi a vyžadujú odkúpenie či vyvlastnenie pôdy. Jedným z príkladov je plávajúci systém Bomhofsplas s výkonom 27 MW ukotvený na dne štrkoviska blízko mesta Zwolle v Holandsku (obr. 4).

Z dôvodu umiestnenia na jazere by bola kabeláž transformačných staníc a bodu pripojenia k sieti zložitá a nákladná. Zebotec sa preto

Obr. 4 Fotovoltický systém Bomhofsplas, ktorý pláva na štrkovisku neďaleko Zwolle, má množstvo výhod.



Obr. 5 Komponenty FL WLAN 5100 možno nakonfigurovať ako klientov, opakovače alebo prístupové body.

rozhodla pre bezdrôtové ethernetové siete: WLAN klienti nainštalovaní v každej transformačnej stanici nadväzujú spojenie s prístupovými bodmi WLAN namontovanými v staniciach blízko pobrežia. Transformačné stanice, ktoré sú samy osebe ďaleko od brehu, sú spojené pomocou opakovačov s prístupovým bodom, čím sa zabezpečila spoľahlivá komunikácia. Kľúčovým faktorom v tejto aplikácii bola vysoká spoľahlivosť a odolnosť použitých komponentov WLAN. Zebotec použila zariadenia FL WLAN 5110 od spoločnosti Phoenix Contact (obr. 5).

Tieto priemyselné zariadenia možno nakonfigurovať ako klientov WLAN, opakovače alebo prístupové body. To poskytlo spoločnosti Zebotec ako systémovému integrátorovi flexibilitu najskôr skonštruovať rozvádzače pre všetky transformačné stanice tak, aby boli

Obr. 6 Na trafostanici sú inštalované všesmerové antény.

identické, a potom nakonfigurovať konečnú topológiu siete WLAN do príslušného systému. Na každej transformačnej stanici sú na výmenu údajov medzi zariadeniami FL WLAN 5110 nainštalované dve všesmerové antény. Vzhľadom na väčšie vzdialenosti použila Zebotec smerové bezdrôtové antény na pripojenie prístupových bodov k zariadeniu FL WLAN 5110 nainštalovanému na zemi na mieste pripojenia rozvodnej siete. Všetky anténne káble sú chránené prepäťovou ochranou od spoločnosti Phoenix Contact, čím je zaručená bezpečnosť samotného FV systému (obr. 6).

Obr. 7 Werner Neff, generálny riaditeľ spoločnosti Zebotec GmbH, bol ohromený trvanlivosťou a spoľahlivosťou komponentov a systémov Phoenix Contact.

Moderné sieťové riešenie má perspektívu do budúcnosti

Systémový integrátor so sídlom v Konstanci má doteraz vynikajúce skúsenosti s riadenými aj neriadenými prepínačmi a s komponentmi WLAN od spoločnosti Phoenix Contact. „To bol jeden z dôvodov, prečo sme sa rozhodli pre komponenty infraštruktúry, pretože tieto zariadenia sú, priemyselné', a teda dostatočne odolné, aby uspokojili naše vysoké požiadavky na dostupnosť na vysokej úrovni," vysvetľuje Werner Neff, generálny riaditeľ spoločnosti Zebotec GmbH. Preto bude spoločnosť inštalovať tieto sieťové koncepty aj v budúcich projektoch FVE (obr. 7).

Platí to aj pre oblasť riadiacej techniky. Spoločnosť Zebotec už roky používa na spracovanie diagnostických a riadiacich údajov v rámci svojich FV systémov riadiace systémy AXC 3050 a ILC 191, ako aj zbernicové spojovacie členy (V/V moduly) z produktovej rodiny Inline. Zebotec ako partner spoločnosti Phoenix Contact v oblasti riešení využívajúcich obnoviteľné zdroje energie je tiež jednou z prvých spoločností na svete, ktorá používa novú otvorenú riadiacu platformu PLCnext Technology.

Marek Slezák

PHOENIX CONTACT, s.r.o.
Námestie Mateja Korvína 1
811 07 Bratislava
Tel.: +421 2 3210 1470
obchod.sk@phoenixcontact.com
www.phoenixcontact.sk

Riešenie prevádzkovej kybernetickej bezpečnosti v priemyselnej praxi chemického podniku

Nárast digitalizácie v priemysle poskytuje detailnejšie údaje z priebehu automatizovaných procesov. Ich analýza umožňuje následnú optimalizáciu výroby. Nevyhnutnou samozrejmosťou je dnes prepojenie priemyselných systémov a informačných technológií, ale aj prelínanie ich kybernetického zabezpečenia.

Jedna z významných spoločností z oblasti chemického priemyslu na Slovensku prešla niekoľkými etapami výstavby a transformáciou. Pôvodný výrobný program sa postupne rozširoval o špeciálne produkty organickej a anorganickej chémie. Dopyt po možnosti sledovania prevádzok technológiami z diaľky v priebehu rokov rástol, pričom súčasná pandemická situácia a čoraz rozšírenejšia práca z domu tento tlak iba zvyšuje.

Ako sa spoločnosti KFB Control, s. r. o., podarilo poskytnúť zákazníkovi z chemického priemyslu spoľahlivé riešenie na monitorovanie celej prevádzky v rámci riadiacich a procesných sietí? Prečo bolo riešenie od Nozomi Networks ideálnym nástrojom na zabezpečenie celej výrobnej automatizácie, vám lepšie predstaví v prípadovej štúdii Ľuboslav Palkoci, Sales Manager zo spoločnosti KFB Control, s. r. o.

Aké výzvy ste museli prekonať z hľadiska kybernetickej bezpečnosti v OT u zákazníka pôsobiaceho v priemyselnom prostredí?

Bežnou praxou pri nasadzovaní, úpravách, ale aj modernizácii OT je projektový princíp. Dôsledkom toho je rozmanitosť riadiacich systémov nasadených v jednotlivých prevádzkach aj rozmanitosť ich dodávateľov/realizátorov. Legitímnou snahou vlastníka je takúto rozmanitosť redukovať, napríklad štandardizáciou požiadaviek na dokumentáciu. Keď si však uvedomíte, že životnosť OT je 20 – 30 rokov, je jasné, že projektová dokumentácia nedáva ucelený a reálny obraz, aká je aktuálna vyťaženosť technológie, čo všetko je jej súčasťou, čo s čím komunikuje, kto má k čomu prístup a podobne.

Prečo si vybrali riešenie od Nozomi Networks?

Nozomi Networks bezproblémovo integruje komplexné riešenie a za posledných 12 mesiacov je na špici rebríčka spoločnosti Gartner/Products In Operational Technology (OT) Security Market. Spokojnosť zákazníkov s nasadením riešení od lídra v zabezpečení kybernetickej bezpečnosti pre priemyselné automatizačné a riadiace systémy je ďalšou doménou Nozomi Networks.

> *Nasadenie produktov Guardian a CMC je len prvý krok vo vzťahu k implementácii ZoKB. Riešenie od Nozomi Networks sa ukazuje ako vhodné na množstvo nedostatkov, a preto s ním určite počítame aj v budúcnosti.*

Ako prebiehal proces implementácie?

Ide o pasívnu technológiu s minimálnym dosahom na samotnú prevádzku. Nasadenie je vďaka zabudovanej inteligencii relatívne jednoduchá záležitosť, konfigurácia je možná aj vo virtuálnom prostredí. Po inštalácii a prepojení fyzických zariadení umiestnených v priemyselných rozvádzačoch prebieha centrálny manažment celého systému z jedného miesta.

Aké výzvy sa očakávajú v tejto oblasti v budúcnosti?

Na budúcnosť sa netreba pozerať ako na niečo, čo je veľmi ďaleko. To, čo tu dnes máme nastavené z hľadiska zákona o kybernetickej

bezpečnosti, je presne tá budúcnosť, čo nás čaká. Budúcnosť je naplnenie toho, čo DNES máme zadefinované, čomu sa treba DNES venovať. Podniky realizujú kroky na celkové zlepšenie naplnenia tohto zákona, ale veľkou výzvou je nedostatočná pripravenosť a dostupnosť ľudských zdrojov. Každý podnik sa na to do istej miery môže pripraviť vypracovaním rozdielovej analýzy alebo správou o zhode s požiadavkami ZoKB.

Výzvy

Zákazníkovi chýbala ucelená znalosť zariadení, ich vzájomného prepojenia a výmeny informácií medzi prevádzkami, systémami a segmentmi siete. Preto bolo náročné posúdiť celkový stav kybernetickej bezpečnosti a zabezpečiť tak potrebné úkony. Technický pracovník musel získať fyzický prístup k zariadeniu na potrebný servisný zásah, čo predstavovalo riziko infiltrácie škodlivého obsahu alebo zámerne upraveného kódu.

Kľúčové výhody Nozomi Networks:
- vyspelá inteligencia odhaľovania zraniteľností a hrozieb v prepojení na Nozomi LAB,
- silný integrovaný query editor a reportovací nástroj,
- integrácia s firewallom, čo pri jasných pravidlách znamená včasné eliminovanie hrozieb a zníženie potenciálnej škody,
- podpora integrácie so systémami SOC a SIEM vo vlastných štruktúrach.

Dosiahnuté výsledky:
- automatizovaný up to date asset invertory list s podrobnosťami o zariadeniach,
- kompletná vizualizácia siete v reálnom čase najlepšia vo svojej triede,
- implementovaný nástroj automatickej detekcie kybernetických incidentov s informáciami na ich nahlasovanie.

O spoločnosti KFB Control, s. r. o.

Spoločnosť bola založená v roku 1999 ako inžinierska skupina skúsených pracovníkov z oblasti automatizácie a informačných technológií. Dnes má zákazníkov už po celom svete a jej činnosť je postavená na troch divíziách. Jadrom jej práce je oblasť automatizácie technologických procesov, druhou divíziou je fyzická bezpečnosť a v tretej divízii sa venujú softvérovým aplikáciám a cyber security.

O spoločnosti Nozomi Networks

Švajčiarsky výrobca Nozomi Networks sa pýši titulom lídra v oblasti kybernetickej bezpečnosti industriálnych systémov a systémov SCADA. Poskytuje inovatívnu technológiu na monitorovanie a hodnotenie priemyselných riadiacich systémov, a to na fyzickom zariadení alebo vo virtuálnom prostredí. To sa pasívne pripojí do priemyselnej siete bez narušenia prevádzky. Sleduje celú prevádzku v rámci kontrolných a procesných sietí a analyzuje ju na všetkých úrovniach vrstiev OSI. Využíva techniky umelej inteligencie a strojového učenia na vytvorenie podrobných profilov správania pre každé zariadenie podľa stavu, aby sa rýchlo zistili kritické hodnoty.

KFB Control s.r.o.

Stará Vajnorská 37, 831 04 Bratislava
Tel.: +421 2 32 161 700
office@kfb.sk
www.kfb.sk

Prvý priemyselný Wi-Fi 6 modul umožňujúci náročné aplikácie Priemyslu 4.0

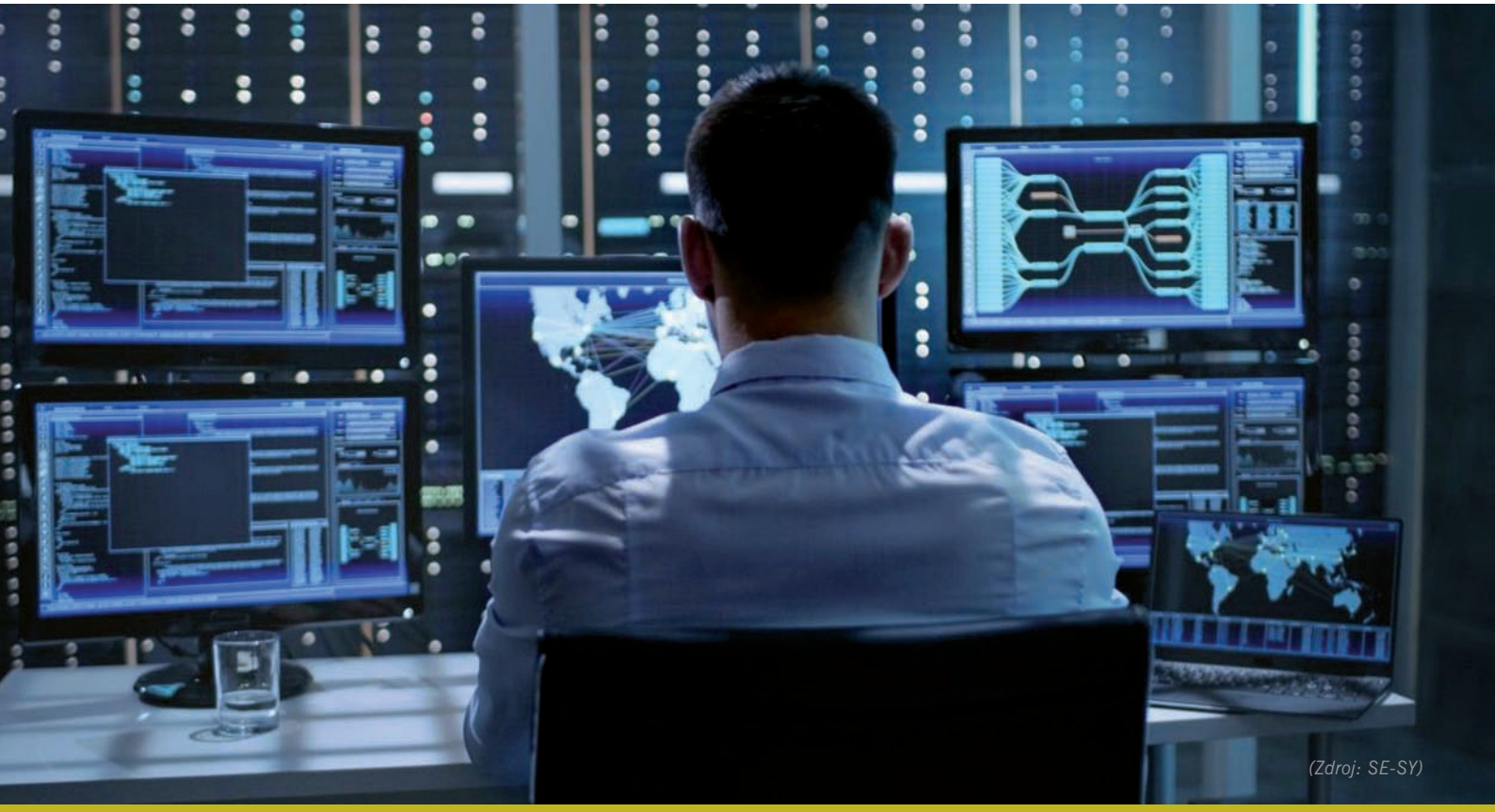
V oblasti digitalizácie narastajú požiadavky na efektívnejšie bezdrôtové sieťové riešenia. Siemens preto rozširuje svoje portfólio sieťových komponentov pre priemyselné riešenia IWLAN a predstavuje prvý priemyselný klientský modul na trhu Scalance WUM766-1, ktorý spĺňa najnovší štandard bezdrôtovej siete LAN IEEE 802.11.ax (Wi-Fi 6). Umožňuje tak spoľahlivé a vysoko výkonné bezdrôtové pripojenie, dokonca s krytím IP65.

Kombinácia klientských modulov IWLAN s novými prístupovými bodmi Scalance WAM766-1 umožňuje používateľom implementovať náročné aplikácie Priemyslu 4.0, ako sú automaticky riadené vozíky (AGV) alebo diaľkovo ovládané žeriavy. Pri rýchlosti prenosu dát 1 201 Mbit/s môžu prístupové body prepojiť veľké množstvo mobilných zariadení v stiesnených priestoroch, ako sú napríklad systémy v oblasti logistiky.

Sieťové komponenty IWLAN možno tiež použiť mimo rozvádzača, napr. v železničnej doprave a v priemyselných aplikáciách v náročnom prostredí, a to vďaka špecifickým schváleniam na priemyselné použitie a kompaktnej a odolnej konštrukcii s krytím IP65. Špecifické mobilné zariadenia v sieťach IWLAN možno navyše deaktivovať pomocou funkcie režimu spánku v kombinácii s digitálnym V/V. To pomáha šetriť energiu a predlžovať životnosť a cykly údržby mobilných zariadení IWLAN napájaných z batérií. Vďaka tomu možno tiež napríklad dosiahnuť energeticky efektívnejšiu prevádzku autonómnych vozíkov (AGV).

Nové komponenty sú vybavené aj funkciou určenou najmä pre tzv. priemyselnú oblasť s iPRP (z angl. Industrial Parallel Redundancy Protocol) na redundantnú dátovú komunikáciu cez WLAN s maximálnou dostupnosťou pre kritické služby. Túto funkciu môžete aktivovať pomocou vymeniteľného pamäťového média CLP, ktoré umožňuje jednoduchú výmenu zariadení v prevádzke vďaka možnosti ukladania konfigurácie nastavení daného zariadenia aj firmvéru. Po výmene náhradného prístupového bodu IWLAN alebo klienta ich CLP jednoducho prenesie. Výmenu tak zvládne aj nezaškolená obsluha.

www.siemens.sk



(Zdroj: SE-SY)

SASE: novovznikajúci koncept kybernetickej bezpečnosti

Dôverné informácie o zamestnancoch, aktívach, podniku. To všetko a ešte oveľa viac uniklo za posledný rok zo systémov priemyselných podnikov po celom svete. A čo je závažnejšie? Že identifikácia narušenia bezpečnosti IT môže trvať aj mesiace, a preto je pravdepodobné, že o mnohých únikoch tieto podniky ani samotné obete nevedia. V mnohých prípadoch sa hacker nesnaží ukradnúť iba osobné údaje, ale akékoľvek údaje, ktoré by mohol speňažiť alebo zneužiť. Ako možno týmto únikom predísť?

Pandémia koronavírusu spôsobila revolúciu v spôsobe pracovania. Zamestnanci, ktorým to práca povoľuje, pracujú z domu, aby chránili nielen seba, ale aj svoje okolie pred nákazou. Počítače v domácnostiach však môžu byť často nakazené malvérom či ransomvérom a ľahko sa stávajú cieľom a obeťou phishingových útokov.

Na druhej strane stojí podnik, ktorý vníma potrebu zvýšenej ochrany údajov popri zrýchľovaní digitalizácie a zintenzívňovaní kybernetických útokov. Dobrým znamením je aj to, že sa dostáva do centra pozornosti aj v podnikoch, ktoré jej doteraz nevenovali adekvátnu pozornosť.

Popri práci z domu je často potrebné externé pripojenie do podnikovej siete, ktoré môže byť v prípade nepripravenosti zraniteľné. VPN alebo siete MPLS doteraz plnili svoje prístupové funkcie, ale ich bezpečnosť a výkonnosť sú otázne vo svete, v ktorom dominuje práca z domova, prechod na hybridný cloud a čoraz častejšie využívanie softvérových aplikácií ako služby – SaaS.

Čo je to SASE?

Secure Access Service Edge (SASE) je novovznikajúci koncept kybernetickej bezpečnosti, ktorý konzultačná spoločnosť Gartner opísala v správe The Future of Network Security in the Cloud z augusta 2019. Koncept spája sieťové pripojenie a bezpečnostné funkcie do jednej ponuky v cloude.

Kým sa pozrieme na prednosti SASE, je dôležité pochopiť, čo stojí za týmto novým pojmom. Existujúce sieťové prístupy a technológie už jednoducho neposkytujú úrovne bezpečnosti a kontroly prístupu, ktoré digitálne podniky potrebujú. Tieto podniky požadujú okamžitý a nepretržitý prístup pre svojich používateľov bez ohľadu na to, kde sa nachádzajú. S nárastom počtu vzdialených používateľov a SaaS aplikácií, presunu údajov z dátového centra do cloudových služieb a väčšieho prenosu smerujúceho do verejných cloudových služieb vznikla potreba nového prístupu k bezpečnosti sietí.

SASE definuje trend v oblasti informačných technológií, pri ktorom dodávatelia kybernetickej bezpečnosti začali spájať sieťové a bezpečnostné funkcie dodávané ako jednotná cloudová služba. SASE kombinuje softvérovo definované WAN (SD-WAN) s bezpečnostnými funkciami, ktoré sa poskytujú ako služba cez cloud a sú spravované prostredníctvom jedinej cloudovej riadiacej konzoly. SASE poskytuje možnosti SD-WAN a na zaistenie bezpečnostných a ďalších funkcií vyžaduje minimálny hardvér a prostriedky ako:

- firewall ako služba (FWaaS),
- Cloud Access Security Brokers (CASB),
- zabezpečené webové brány,

- Zero Trust Network Access (ZTNA),
- zabezpečenie koncového bodu.

Stručne povedané, SASE kombinuje sieťové pripojenie a zabezpečenie tak, aby vyhovovalo požiadavkám novodobých digitálnych podnikov. Umožňuje zabezpečiť prístup ľubovoľného koncového zariadenia k ľubovoľnej aplikácii alebo službe v ľubovoľnej sieti. Hoci je SASE pomerne novým konceptom, pandémia koronavírusu posilnila potrebu zostavovať také plány trvalo udržateľného fungovania podnikov, ktorých súčasťou bude flexibilný, bezpečný vzdialený prístup odkiaľkoľvek, kedykoľvek, pre veľký počet používateľov, a to aj z neznámych zariadení.

Ako funguje SASE?

Platformy SASE môžu integrovať SD-WAN, FWaaS, CASB, zabezpečené webové brány, nulovú dôveru prístupu do siete, zabezpečenie koncového bodu a zabezpečený prístup k podnikovým zdrojom bez ohľadu na to, kde sídlia zamestnanci, kancelárie, dátové centrá a cloudové aplikácie. Architektúra SASE sa spolieha na sieť prístupových bodov označovaných aj ako PoP (Points of Presence) s poskytovaním dohľadu a presmerovania namiesto použitia inšpekčných nástrojov umiestnených v dátovom centre. SASE je v podstate novým balíkom technológií, ktorý môže identifikovať citlivé údaje alebo malvér so schopnosťou dešifrovať obsah prenosovou rýchlosťou s nepretržitým monitorovaním relácií.

Rozhodujúce vlastnosti modelu SASE

Medzi vlastnosti, vďaka ktorým je SASE inovatívny a jedinečný, patrí to, že na pripojenie distribuovaných PoP používa službu SD-WAN so súkromnou, tzv. backbone sieťou. Týmto spôsobom sa k internetu pristupuje iba pri pripojení k tejto súkromnej sieti, čím sa zabráni rizikám oneskorenia. SASE pripája okrajové zariadenia a softvérových agentov k tejto sieti pomocou sprostredkovateľov prístupu a šifrovania, takže slúži ako náhrada VPN a zjednodušuje sa správa siete.

Model SASE je tiež zameraný na používateľa alebo identitu a udeľuje prístup na základe polohy používateľa a zariadenia. Presadzovanie podnikových zásad je jednotné, ale distribuované. Distribuuje sa tiež kontrola paketov, trasovanie, šifrovanie a dešifrovanie prenosu. Viaceré inšpekčné nástroje, ako napríklad vyhľadávanie škodlivého softvéru a tzv. sandboxy, pracujú paralelne, čo zvyšuje výkon siete. SASE ako také nielenže spája používateľov a zariadenia, ale tiež ich chráni pred útokmi DDoS a inými hrozbami v sieti.

SASE je v konečnom dôsledku cloudová architektúra, ktorá využíva cloudové zdroje bez konkrétnych hardvérových požiadaviek. V ideálnom prípade to nezahŕňa reťazenie služieb a konzola má zvyčajne viacerých klientov. Pomáha IT pracovníkom kontrolovať a presadzovať bezpečnostnú politiku podniku prostredníctvom jednej konzoly, čím zjednodušuje operácie.

Ako môže SASE pomôcť?

Model zabezpečenia SASE môže podniku pomôcť niekoľkými spôsobmi:

- Úspora nákladov: Namiesto nákupu a správy viacerých produktov využitie jednej platformy zníži náklady a zdroje IT.
- Znížená zložitosť: IT infraštruktúru možno zjednodušiť minimalizáciou počtu bezpečnostných produktov, ktoré musí IT tím spravovať, aktualizovať a udržiavať.
- Zvýšený výkon: Vďaka cloudovej infraštruktúre sa môžete ľahko pripojiť kdekoľvek k rôznym zdrojom. Prístup k aplikáciám, internetu a podnikovým údajom je k dispozícii globálne.
- Zero Trust: Prístup Zero Trust ku cloudu odstraňuje pri pripájaní používateľov, zariadení a aplikácií nutnosť využívania technológií a postupov zameraných na kontrolu dôvery. Riešenie SASE poskytne úplnú ochranu relácie bez ohľadu na to, či je používateľ v podnikovej sieti alebo mimo nej.

(Zdroj: CSO Online)

- Prevencia hrozieb: Vďaka komplexnej kontrole obsahu integrovanej do riešenia SASE môžete ťažiť z väčšej bezpečnosti a viditeľnosti svojej siete.
- Ochrana údajov: Implementácia zásad na ochranu údajov v rámci SASE pomáha predchádzať neoprávnenému prístupu a zneužitiu citlivých údajov.

SASE je kľúčom k digitálnej transformácii

Práve rok 2020 bol rokom, keď SASE zaznamenalo rast. Asi najväčším dôvodom bola pandémia COVID-19, keď rôzne priemyselné aj nepriemyselné podniky umožnili pracovať svojím zamestnancom z domova.

Transformácia digitálneho podnikania priniesla dopyt po väčšej schopnosti rýchlo a presvedčivo reagovať a škálovateľnosti so zníženou zložitosťou. Podniky zisťujú, že musia poskytovať konzistentný a bezpečný, globálne dostupný prístup k aplikáciám a službám bez ohľadu na to, kde sa používatelia (či už sú to zamestnanci, zákazníci alebo partneri) nachádzajú alebo aké zariadenia používajú. Riešenie SASE ponúka podnikom úplne nový model pripojenia používateľov a zariadení, ktorý je rýchly a flexibilný, jednoduchší a bezpečnejší. Pomocou cloudového modelu sa podniky, ktoré adoptujú SASE, ocitnú na ceste k digitálnej transformácii.

Ak sa chcete o SASE dozvedieť viac, prečítajte si správu spoločnosti Gartner: Budúcnosť sieťovej bezpečnosti je v cloude (The Future of Network Security Is in the Cloud).

Zdroje

[1] What Is Secure Access Service Edge (SASE)? McAfee. [online]. Citované 8. 6. 2021. Dostupné na: https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-sase.html.

[2] What Is SASE? Palo Alto Networks. [online]. Citované 8. 6. 2021. Dostupné na: https://www.paloaltonetworks.com/cyberpedia/what-is-sase.

[3] Protecting Data with a SASE Solution. Palo Alto Networks. [online]. Citované 8. 6. 2021. Dostupné na: https://www.paloaltonetworks.com/cyberpedia/protecting-data-with-a-sase-solution.

Petra Valiauga

Riešenie nepretržitého napájania do 3 kVA, keď pár minút nestačí

So zvyšujúcim sa počtom IT zariadení narastá potreba ich zálohovania od niekoľko desiatok minút až po niekoľko hodín. Spoločnosť A2B ponúka individualizované zákaznícke riešenia pri zachovaní minimálnych rozmerov inštalovaných aplikácií.

Kabinet s dvoma UPS 19“, s bajpasom a zásuvkami na napájanie záťaží

Bežné malé zdroje UPS s výkonom do 3 000 VA ponúkajú čas zálohovania pár minút. V závislosti od typu zariadenia možno čas zálohovania predlžovať prídavnými batériovými modulmi, no výrazným obmedzením je málo výkonný zabudovaný nabíjač v kombinácii s internými batériami.

Základ riešení s predĺženým časom zálohovania

Riešením je použitie zdroja UPS so silnejším nabíjačom bez interných batérií. V takomto vyhotovení zdroj UPS neobsahuje zabudované batérie a v uvoľnenom priestore je osadený výkonnejší nabíjač. Dostupné sú rôzne vyhotovenia zdrojov UPS ako tower alebo 19“ rack vrátane kompaktnej verzie s hĺbkou len 380 mm. Aký čas zálohovania teda získame? V závislosti od použitých batérií možno bežne dosiahnuť čas zálohovania rádovo v hodinách.

Ako vyberáme batérie?

Bežné batériové moduly obsahujú malé batérie zaradené podľa Eurobat ako General Purpose so životnosťou tri až päť rokov (pri 20 °C). Ak namiesto 19“ batériových modulov uložíme batérie na policu v kabinete, na samostatný stojan či do batériového kabinetu, tak máme širokú škálu možností riešenia batérií.

Prvým aspektom výberu je životnosť batérií. Bežne staviame riešenia na batériách zaradených podľa Eurobat minimálne do kategórie Long Life so životnosťou 10 až 12 rokov (pri 20 °C). Pre podmienky s vyššou teplotou okolia ponúkame vysokoteplotné batérie s očakávanou životnosťou až do 10 rokov pri teplote okolia 35 °C. Pri zvýšených nárokoch na bezpečnosť inštalácie batérií používame osadenie batérií na izolované batériové stojany, ako aj použitie batérií s puzdrom zo samozhášavého plastu.

Z dôvodu zvýšenia spoľahlivosti uprednostňujeme vyskladať výslednú kapacitu minimálne z dvoch paralelne zapojených batériových reťazcov. Takto je aj pri poruche jedného batériového reťazca zabezpečená ochrana technológie (s redukovaným časom zálohovania). Zároveň možno počas prevádzky zdroja UPS vykonávať servisné činnosti na jednom batériovom reťazci.

Batérie v kabinete s batériovými odpojovačmi

Zvlášť kritické aplikácie

Vo veľmi kritických aplikáciách možno použiť dvojvetvové napájanie, kde má každá vetva vlastný zdroj UPS aj príslušné batérie. Zariadenia, ktoré nemajú možnosť dvojvetvového napájania, možno pripojiť cez ATS alebo STS prepínač.

Čo v prípade opravy alebo výmeny zariadenia?

Zariadenie možno vybaviť samostatným externým manuálnym bajpasom. Pri výmene zariadenia sa prepne pripojená technológia na napájanie priamo zo siete a samotný zdroj UPS možno následne kompletne odpojiť.

Batériový kabinet pre rôzne typy batérií

Správne príslušenstvo pre každú aplikáciu

Konkrétne aplikácie vyžadujú špecifické riešenia, kde práve dodané príslušenstvo výrazne ovplyvňuje možnosti zostavy zdroja UPS:

- karta alarmových relé – či už na signalizáciu alarmov do nadradeného PLC, alebo na zopnutie uzatváracej armatúry pri výpadku siete,
- karta SNMP – pre IT aplikácie vrátane podpory VMware,
- rozhranie Modbus TCP alebo Modbus RTU,
- snímače prostredia – meranie teploty a vlhkosti vrátane možnosti spínania núdzového prevetrávania pri dosiahnutí nastavenej teploty,
- vzdialený displej – bežne využívaný v medicínskych aplikáciách na vyvedenie stavu UPS do blízkosti personálu vykonávajúceho kritický úkon.

Nami realizované riešenia zahŕňajú zálohovanie celoslovenskej siete internetu vecí (IoT), ako aj dodávku zdrojov UPS so seizmickou odolnosťou do atómovej elektrárne.

Ing. Peter Švolik

A2B, s.r.o.
Horská 1
Považský Chlmec
010 03 Žilina
Tel.: +421 41 5000 490
a2b@a2b.sk
www.a2b.sk

Beamex predstavuje revolúciu v kalibrácii teploty

Spoločnosť Beamex predstavuje lepší spôsob vykonávania kalibrácie teploty pomocou nového revolučného a všestranného riešenia Beamex MC6-T. Je to najnovší člen mimoriadne úspešnej a medzi odborníkmi uznávanej rodiny Beamex MC6 zahŕňajúcej dokumentačný kalibrátor a komunikátor MC6, kalibrátor a komunikátor pracovnej stanice MC6 Workstation a iskrovo bezpečný prevádzkový procesný kalibrátor a komunikátor MC6-Ex certifikovaný podľa ATEX, IECEx a noriem platných v Severnej Amerike.

Lepší spôsob kalibrácie teploty

„Spoločnosť Beamex už viac ako 40 rokov rozvíja svoje znalosti a know-how v oblasti merania teploty. Nedávno sme komplexnejšie pochopili termodynamiku a riadiace systémy teploty. To nám umožnilo spojiť naše skúsenosti s návrhom kalibrátorov, kalibráciou teploty a odbornými znalosťami v oblasti merania teploty, ktoré vyvrcholili predstavením špičkovej kalibračnej teplotnej piecky kombinovanej s multifunkčným prevádzkovým kalibrátorom a komunikátorom Beamex MC6, čo pozoruhodne zjednodušuje kalibráciu teploty," vysvetľuje Antti Mäkynen, produktový manažér Beamex.

MC6-T je najnovším členom mimoriadne úspešnej a medzi odborníkmi rešpektovanej rodiny Beamex MC6.

Výkonný a všestranný charakter MC6-T je dôkazom toho, že jediné zariadenie môže poskytovať vysoko presné referenčné merania a simulácie teploty, tlaku a elektrických signálov, ako sú odpor, mA, mV, V, impulzy a frekvencia, spolu s komunikátorom HART, Profibus PA a FOUNDATION Fieldbus. „So všetkou touto funkčnosťou môže MC6-T nahradiť mnoho jednotlivých zariadení, ako je napr. teplotný blok, kalibrátor teploty a tlaku, prevádzkový komunikátor, datalogger. Na trhu nie je nič, čo by malo túto kombináciu funkčnosti," vysvetľuje A. Mäkynen. „Model MC6-T štandardne prináša zákazníkom jednoduché použitie v spojení so spoľahlivými bezpečnostnými prvkami chrániacimi ľudí a pracovisko," dodáva.

Kombinácia vynikajúceho teplotného a metrologického výkonu, skráteného času kalibračného cyklu a špeciálneho vyhotovenia odolného okolitým podmienkam predstavuje niekoľko jedinečných vlastností. Ponúka tiež schopnosť kalibrovať krátke a prírubové sanitárne snímače. Pri tradičných tepelných suchých pieckach to spravidla nie je možné. MC6-T je k dispozícii v dvoch rôznych modeloch: MC6-T150 na kalibráciu nižšej teploty (-30 až 150 °C) a MC6-T660 na kalibárciu vysokej teploty (50 až 660 °C). Kombináciou MC6-T so softvérom Beamex bude proces kalibrácie teploty plne automatizovaný, a teda aj bezpapierový. S týmto druhom integrovaného kalibračného riešenia možno čas strávený kalibráciou znížiť až o 50 %, čo šetrí peniaze a súčasne zvyšuje kvalitu záznamov.

MC6-T je k dispozícii v dvoch rôznych modeloch: MC6-T150 na kalibráciu nižšej teploty a MC6-T660 na kalibráciu vysokej teploty.

O spoločnosti Beamex

Beamex je popredný svetový poskytovateľ kalibračných riešení, ktorého cieľom je vytvoriť lepšie spôsoby kalibrácie pre globálny spracovateľský priemysel. Beamex ponúka komplexnú škálu produktov a služieb: od prenosných kalibrátorov po pracovné stanice, kalibračné príslušenstvo, kalibračný softvér, odvetvové riešenia a profesionálne služby. Prostredníctvom dcérskych spoločností, pobočiek a rozsiahlej siete nezávislých distribútorov spoločnosti Beamex sú jej produkty a služby dostupné vo viac ako 80 krajinách. Spoločnosť Beamex má po celom svete viac ako 12 000 zákazníkov.

Pozrite si video o automatickej kalibrácii teplotného snímača Pt100 pomocou Beamex MC6-T660.

Kalibrátory, s.r.o.

Nové sady 988/2
602 00 Brno
Tel.: +420 703 132 620
info@kalibratory.sk
www.kalibratory.sk

Dokumentačný kalibrátor a jeho prínosy v prevádzkovej praxi

Bežnou praxou vo výrobných podnikoch je pravidelná kalibrácia prístrojov v celom závode. V rámci výrobných prevádzok, kde je presnosť prístroja rozhodujúca pre zabezpečenie kvality produktu, bezpečnosti alebo prepravy, nie je kalibrácia každých šesť mesiacov – alebo ešte častejšie – neobvyklá. Kľúčový posledný krok v akomkoľvek kalibračnom procese – dokumentácia – je však často zanedbávaný alebo prehliadaný pre nedostatok zdrojov a času alebo pre tlak každodenných činností. Mnoho výrobných závodov je tak pri zabezpečovaní rýchlej a presnej kalibrácie prístrojov a zdokumentovaní výsledkov v náležitej kvalite a s cieľom získať úplnú nadväznosť často pod tlakom. Cieľom samotnej kalibrácie je zistiť, aký presný je prístroj alebo snímač. Aj keď je dnes väčšina prístrojov veľmi presná, regulačné orgány musia často vedieť, s akou presnosťou konkrétne prístroje pracujú a či sa časom táto presnosť neodchýli od stanovenej tolerancie.

Asi sa zhodneme na tom, že pre väčšinu z nás nie je dokumentácia vo všeobecnosti nejakou vzrušujúcou pracovnou náplňou. No pri kalibrácii prevádzkových prístroje je dôležité zdokumentovať jej výsledky, inak je táto činnosť len zbytočným úsilím. Nebolo by skvelé, keby namiesto manuálneho dokumentovania výsledkov kalibrácie pomocou pera a papiera robil celú dokumentáciu automaticky kalibrátor? Znie to zaujímavo? V tomto príspevku budem hovoriť o dokumentačných kalibrátoroch, ktoré práve toto dokážu.

Čo je dokumentačný kalibrátor?

Dokumentačný kalibrátor je ručné elektronické komunikačné zariadenie schopné kalibrovať rôzne procesné signály, ako sú tlak, teplota a elektrické signály vrátane frekvencie a impulzov, a automaticky dokumentovať výsledky kalibrácie ich prenosom do plne integrovaného softvéru na správu kalibrácie. Niektoré kalibrátory dokážu čítať výstupy vysielačov HART, Foundation Fieldbus alebo Profibus, môžu sa dokonca použiť na konfiguráciu inteligentných senzorov. Kalibrátor je testovacie zariadenie, ktoré je dostatočne presné na to, aby ste ho mohli použiť na kalibráciu procesných nástrojov. Musí mať platnú kalibráciu podľa národných noriem, aby ste mohli vykonať kalibráciu prevádzkových nástrojov s náležitou nadväznosťou.

Ďalším typom je tzv. nedokumentujúci kalibrátor. Je to zariadenie, ktoré neuchováva žiadne údaje, resp. aj keď dokáže zaznamenať údaje o kalibrácii z prístrojov, nie je integrované do systému riadenia kalibrácie. Výsledky kalibrácie sa musia ručne zadať do samostatnej databázy, tabuľkového alebo papierového záznamu.

Ako dokáže kalibrátor vytvárať dokumentáciu?

Kalibrátor vytvorí dokumentáciu, ak dokáže počas kalibrácie uložiť výsledky kalibrácie do svojej pamäte, takže ich netreba zaznamenávať manuálne. Dokumentačný kalibrátor by mal byť schopný komunikovať s kalibračným softvérom, aby mohol výsledky kalibrácie prenášať elektronicky zo svojej pamäte do kalibračného softvéru. Komunikácia by mala fungovať aj opačne, to znamená, že kalibračný softvér by mal byť schopný odosielať do kalibrátora informácie o úlohách, ktoré treba vykonať.

Ako sa líši proces kalibrácie pri použití dokumentačného kalibrátora od použitia nedokumentujúceho kalibrátora?

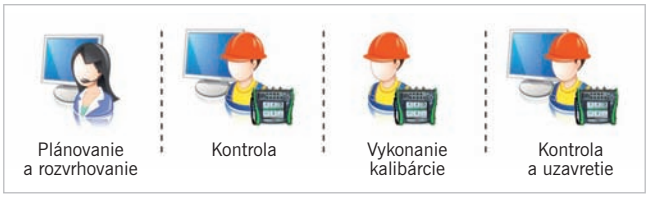
Obr. 1

Proces kalibrácie bez dokumentačného kalibrátora

Ak nemáte k dispozícii dokumentačný kalibrátor, kalibrácia sa zvyčajne vykonáva podľa nasledujúceho postupu (obr. 1):

1. Nástroj na plánovanie a časové rozhvrhovanie vám oznámi, že je čas kalibrovať určité prístroje.
2. Pracovný príkaz vytlačíte na papier a distribuujete príslušnému oddeleniu/osobe.
3. Poverený technický pracovník ide do prevádzky a urobí kalibráciu.
4. Pracovník zdokumentuje výsledky kalibrácie v tlačenej forme – zapíše ich na papier.
5. Po dokončení kalibrácie možno pracovný príkaz uzavrieť.
6. Výsledok je skontrolovaný/overený.
7. Výsledky kalibrácie sa archivujú.

Hovoríte, že nearchivujete papierové výsledky, ale máte kalibračný softvér? Ak máte kalibračný softvér, do ktorého po návrate z prevádzky zadávate výsledky ručne, ide len o ďalší proces, pri ktorom sa môžu vniesť do kalibrácie chyby. Navyše s tým strávite nie krátky čas, takže nejde o veľmi dobrý a efektívny proces.



Obr. 2

Proces kalibrácie s dokumentačným kalibrátorom

Ak používate dokumentačný kalibrátor spolu so systémom riadenia kalibrácie, ktorý ho podporuje, proces je podstatne efektívnejší (obr. 2):

1. Realizácia kalibrácie a s tým súvisiace úkony sú plánované v softvéri na správu kalibrácií (alebo v systéme riadenia údržby, ku ktorému je kalibračný softvér pripojený).
2. Pracovné príkazy sa posielajú elektricky do dokumentačného kalibrátora.
3. Kalibráciu vykonáte pomocou dokumentačného kalibrátora a výsledky sa automaticky uložia do pamäte kalibrátora.
4. Nakoniec výsledky z kalibrátora dostanete elektronicky do svojho softvéru na správu kalibrácie, pričom sa automaticky ukladajú do databázy (systém riadenia údržby je na to automaticky upozornený).

A je to! Vykonali ste kalibráciu a dokumentácia sa urobila automaticky!

Prečo používať dokumentačný kalibrátor? Aké sú jeho výhody?

Použitím dokumentačného kalibrátora sa výsledky kalibrácie automaticky ukladajú do pamäte kalibrátora počas kalibrácie. Technik nemusí zapisovať žiadne výsledky na papier, čo celý proces výrazne zrýchľuje a následne znižuje náklady. Zlepší sa tiež kvalita a presnosť výsledkov kalibrácie, pretože bude menej chýb spôsobených ľudským faktorom.

Výsledky kalibrácie sa automaticky prenášajú z pamäte kalibrátora do počítača/databázy. To znamená, že technik nemusí tráviť čas prenosom výsledkov z poznámkového bloku do konečného úložiska v počítači; opäť sa šetrí čas a peniaze.

Ako ukazujú predchádzajúce kroky a obrázky, proces kalibrácie je dosť odlišný s kalibrátormi, ktoré dokumentáciu vytvárajú automaticky, alebo bez nich. Zhrňme teda hlavné výhody používania dokumentačných kalibrátorov:

- Kalibrácia trvá oveľa menej času, a preto šetrí vaše zdroje, čas a peniaze.
- Kvalita, konzistencia a spoľahlivosť výsledkov sú lepšie, pretože nedochádza k chybám spôsobeným ručným zápisom výsledkov kalibrácie.
- Postup kalibrácie vedie používateľov a zaručuje jednotný proces.
- Výsledky sa automaticky ukladajú do databázy, nie je potrebné ručné prepisovanie ani archivácia papierových výsledkov.
- Softvér na správu kalibrácií môže byť tiež integrovaný do systému riadenia údržby, čo umožňuje bezpapierový tok pracovných príkazov medzi týmito dvoma systémami.

Kto by mal používať dokumentačný kalibrátor?

Prečo by ste teda mali používať dokumentačné kalibrátory a kedy máte z ich používania najväčšie výhody? Väčšinu výhod získate v nasledujúcich prípadoch:

- Ak urobíte veľa kalibrácií, ušetríte viac času a peňazí vďaka efektívnejšiemu procesu kalibrácie.
- Ak ste spoločnosť, ktorej činnosť spadá pod regulované odvetvia, alebo chcete iba profitovať zo zlepšenej kvality kalibračných údajov a jednotného procesu s automatizovanými funkciami.
- Ak chcete zvýšiť účinnosť svojho kalibračného procesu.
- Ak sa chcete ubezpečiť, že proces kalibrácie spĺňa požiadavky vášho systému kvality alebo externých auditov.
- Ak chcete využiť efektívnejší proces kalibrácie.

Záver

Kalibrácia prevádzkových prístrojov je len jednou z mnohých činností súvisiacich s údržbou vo výrobnom závode. Posledná vec, ktorú chcete urobiť, je vykonávať zbytočné kalibrácie alebo používať časovo náročné a neúčinné kalibračné postupy. Navyše ako každý podnik aj vy chcete mať istotu, že všetky dôležité kalibrácie sa naozaj zrealizujú a že budete ďalej efektívne fungovať s minimálnymi prestojmi pri zachovaní predpísanej kvality produkcie a zhody so všetkými internými predpismi, legislatívou a bezpečnosťou. Venujte teda kalibrácii a spôsobu jej výkonu takú pozornosť, akú si v modernej dobe digitalizácie zaslúži.

Zdroje

[1] What is a documenting calibrator and how do you benefit from using one? Beamex Oy Ab. [online]. Citované 10. 6. 2021. Dostupné na: https://blog.beamex.com/what-is-a-documenting-calibrator-and-how-do-you-benefit-from-using-one.

[2] The Benefits of Using a Ducumenting Calibrator. Beamex Oy Ab. White Paper. [online]. Citované 10. 6. 2021. Dostupné na: https://resources.beamex.com/documenting-calibrator?hsCtaTracking=dbc8a83e-d91e-4f3d-b7fe-a758a128dccb%7C4f18ee09--d0e0-4124-93a2-e5638cb1d678.

www.kalibratory.sk

ABB L&W Autoline

Nová generácia automatizovaného systému na testovanie papiera.

V procese výroby papiera má nezastupiteľnú úlohu jeho testovanie. Proces, počas ktorého vzniká, je zložitý a nie vždy bezchybný. V každej výrobnej fáze preto treba venovať náležitú pozornosť požiadavkám na kvalitu finálneho produktu. Nová generácia automatizovaného testovacieho systému spoločnosti ABB prináša aj do tejto oblasti nové možnosti.

Automatizovaný testovací systém ABB L&W Autoline je až 10-krát rýchlejší oproti manuálnemu testovaniu, čo umožňuje rýchlu redukciu nekvalitného produktu. Systém, ktorý zvládne všetko od prípravy vzorky až po záverečný test report, radikálne znižuje závislosť od manuálneho testovania. Umožňuje sústrediť sa tak na neustále a udržateľné zlepšovanie kvality a zároveň znižovať náklady na kontrolu kvality.

Autoline S

S cieľom intuitívneho ovládania obsahuje L&W Autoline jedinečné vizuálne rozhranie dotykovej obrazovky, ktoré vyžaduje minimálne zaškolenie. Špeciálny dizajn zabezpečuje najspoľahlivejší systém podávania vzorky na trhu. Ťahá vzorky cez tester tak, aby nedošlo k ich zaseknutiu. Veľkoobjemové ukladanie informácií umožňuje identifikáciu trendov kvality v čase. Vizualizácia v reálnom čase poskytuje priamu spätnú väzbu operátorom v prevádzke aj v celom závode.

ABB Autoline je dostupný v dvoch veľkostiach: L&W Autoline S je pre menšie závody a pre tých, ktorí začínajú s automatizovaným testovaním, L&W Autoline L je väčšia jednotka navrhnutá s ohľadom na rozsiahlejšie testovacie požiadavky.

Systém L&W Autoline je modulárny a umožňuje viac ako 20 kombinácií testovacích modulov. Všetky jeho merania vyhovujú normám ISO a TAPPI.

Príklad testovacích modulov:
- pevnosť v ťahu,
- gramáž/plošná hmotnosť,
- odolnosť proti ohybu,
- pevnosť v pretlaku,
- belosť papiera,
- lesk,
- drsnosť,
- hrúbka,
- absorpcia,
- obsah vlhkosti,
- vzdušná priepustnosť,
- povrchová topografia a ďalšie.

Autoline L

Kľúčové vlastnosti:
- Modulárne vyhotovenie – škálovateľné riešenie umožňuje výrobcom papiera zvoliť si moduly, ktoré vyhovujú ich potrebám.
- Jedinečné podávanie papiera – nový dizajn zaisťuje spoľahlivé a bezproblémové podávanie vzorky.
- Možnosť duálneho testu – testovanie dvoch prúžkov súčasne skracuje čas testu.
- Veľkokapacitné úložisko dát – ukladanie veľkého objemu nameraných údajov na identifikáciu trendov kvality v priebehu času.
- Reportovanie v reálnom čase – poskytuje operátorom priamu spätnú väzbu prostredníctvom sledovania kvality produktu v reálnom čase.
- Kľúčové informácie o kvalite – systém spravidla hlási viac ako 100 dôležitých parametrov kvality na pozícii CD (priečny profil).
- Automatická registrácia vzoriek – zaregistruje vzorku podľa čiarových kódov z dôvodu testovacej postupnosti, pričom špecifikácia druhu papiera sa vyberá automaticky.
- Automatická distribúcia informácií – ľahký prístup ku kvalitným informáciám v celom závode.
- Intuitívne rozhranie – na používanie dotykovej obrazovky je potrebné len minimálne školenie.
- Jednoduchá inštalácia a údržba – modulárny dizajn umožňuje údržbu a inštaláciu jednoduchšie ako kedykoľvek predtým. Integrovaná diagnostika dáva možnosť spoločnosti ABB pripojiť sa a vyriešiť problém na diaľku.

V dnešných papierňach a baliarňach sú náklady na implementáciu automatizovaného testovania vyvážené mnohými výhodami. Typická návratnosť investícií je menej ako dva roky. Dosiahnuteľná je prostredníctvom podrobných správ o kvalite a rýchlejšou optimalizáciou procesov. Zaistenie konkurenčnej výhody vyplýva z komplexných, presných a rýchlych výsledkov testov, ktoré sa dajú ľahko dosiahnuť automatizovaným testovaním papiera.

Ján Kováčik

ABB, s.r.o.
Tuhovská 29
831 06 Bratislava
www.abb.sk

UDC2800 – nový výkonný PID regulátor teploty od fy Honeywell

V portfóliu firmy Honeywell je UDC2800 najvýkonnejším jednoslučkovým PID regulátorom teploty. Kombinuje všetky funkcie starších modelov a mnoho ďalších výhod: vyšší výkon riadenia procesu, vylepšený displej, rýchlejšie konfigurovanie, vyššia presnosť, rýchlejšia ethernetová komunikácia a ľahká obsluha.

Oblasti použitia

PID regulátor UDC2800 sa používa hlavne v priemysle tepelného spracovania, v letectve, vo farmaceutickom, sklárskom, potravinárskom či keramickom priemysle. Ďalej ho možno použiť na reguláciu vo vykurovacích a sušiacich peciach, kotloch, ohrievačoch, klimatických komorách a pod.

Vlastnosti a výhody

S presnosťou vstupu 0,15 % sa UDC2800 radí medzi špičku jednoslučkových regulátorov. 100 ms vzorkovacia frekvencia univerzálneho vstupu patrí v súčasnosti medzi najrýchlejšie, aké sa na trhu v tomto segmente regulátorov vyskytujú. K dispozícii je aj funkcia Accutune III na automatické ladenie PID parametrov. Regulátor tak neustále reaguje na zmeny v procese, čím zabezpečuje presnú reguláciu. Efektívne hlásenie alarmov procesu umožňuje rýchlu reakciu na tieto poruchy.

Prostredníctvom aplikácie a pripojenia cez Bluetooth možno PID regulátor teploty konfigurovať veľmi ľahko a rýchlo. Intuitívne vyhotovenie s plnofarebným 3,5“ TFT displejom uľahčuje čítanie údajov. Štandardom sú rôzne sieťové a komunikačné rozhrania ako RS-485, ethernet 10/100M s protokolom Modbus. Programová regulácia v čase môže mať až 64 segmentov. Používateľ má k dispozícii štyri súbory PID parametrov a žiadanej hodnoty. Regulátor UDC2800 môže mať dva univerzálne vstupy: RTD, TC, mV, mA a relatívnu vlhkosť. Krytie IP66 umožňuje nasadenie v najťažších priemyselných prostrediach.

Regulátor UDC2800 pomáha s vyššou presnosťou a rýchlejšie reaguje na zmeny v technologickom procese, čím optimalizuje reguláciu, minimalizuje odpad a znižuje celkové náklady.

MARSEM

MARSEM s.r.o.

Akreditovaný distribútor fy Honeywell
Furdekova 7
851 04 Bratislava
Tel.: +421 903 228 570

Česká firma ZAT finišuje s dodávkami pre francúzske jadrové elektrárne

Príbramská spoločnosť ZAT dodá do projektu modernizácie jadrových elektrární vo Francúzsku 58 rozvádzačov osadených vlastným riadiacim systémom. Systém KCF od českého výrobcu riadiacich systémov bude tak zabezpečovať diagnostické a informačné funkcie na dvadsiatich blokoch ôsmich jadrových elektrární vo Francúzsku.

Dodávku skríň riadiaceho systému v hodnote 80 miliónov korún firma ZAT realizuje pre francúzsku spoločnosť Framatome (predtým Areva NP) s termínom ukončenia v roku 2024. „K dnešnému dňu sme do jadrových elektrární vo Francúzsku dodali 90 % zariadení. Aktuálne prebieha výroba a kompletizácia skríň riadiaceho systému pre posledné tri jadrové bloky," hovorí Ivo Tichý, člen predstavenstva ZAT.

Prvé dve dodávky boli určené pre tréningové centrá, ďalšie už mierili do jednotlivých elektrární. Procesu výroby a montáže systému KFC predchádzala kvalifikácia prototypových skríň v akreditovaných skúšobniach, ktorá overila ich funkčnosť aj pri náročných vonkajších podmienkach, ako je seizmicita, elektromagnetická kompatibilita, teplota a vlhkosť.

„Pre spoločnosť Framatome boli dôležité predovšetkým naše kompetencie a referencie v dodávkach do jadrovej energetiky a schopnosť prispôsobiť sa miestnej legislatíve a požiadavkám francúzskeho jadrového dozoru," doplňuje Karel Stočes, riaditeľ marketingu a obchodu pre jadrovú energetiku, a dodáva: „V rámci realizácie sme museli zohľadňovať aj prísnu normatívu prevádzkovateľa jadrových elektrární vo Francúzsku. Konkrétne išlo o štandardy zabezpečenia kvality vrátane príručky RCC-E. Všetky dokumenty samozrejme odovzdávame aj vo francúzskom jazyku."

Realizácia projektu od fázy projektovania, výroby až po skúšky zariadení prebieha vo výrobnom závode v Příbrami. Súčasne s prepojovacími testami sa tu robí aj kontrola kvality vyrobených KCF skríň. Na záverečných skúškach funkčnosti sa zúčastňujú aj zástupcovia zákazníka.

Bezpečnosť je priorita – aj v preprave

Nielen výroba a testovanie podliehajú prísnym pravidlám bezpečnosti a kvality. Rozvádzače s riadiacim systémom sú umiestnené, montované a skúšané v špeciálnej miestnosti s riadeným prístupom dostupným len pracovníkom ZAT a zákazníka. Sú tiež balené podľa špeciálnych predpisov, prevoz do Francúzska zaisťuje zaplombované vozidlo s hydraulickou plošinou. „Jednotlivé rozvádzače sú osadené nárazovými snímačmi, ktoré pri preprave zariadení zaznamenajú prípadný náraz," doplňuje K. Stočes.

Jadrové elektrárne, do ktorých česká firma ZAT systémy KCF dodáva, patria do koncernu EDF (Électricité de France), ktorý sa zaoberá výrobou a distribúciou elektriny. Aktuálna modernizácia sa týka jadrových elektrární Paluel, Cattenom, St. Alban, Penly, Flamanville, Belleville, Nogent-Sur Seine a Golfech s reaktormi typu PWR s výkonom 1 300 MW. „Vo Francúzsku je teraz v prevádzke 58 jadrových blokov. Aj naďalej sa chceme podieľať na ich modernizácii, v súčasnosti sme v spoločnosti EDF v procese kvalifikácie vybraného dodávateľa. Pravdepodobne v polovici roka bude zavŕšená externým auditom," dopĺňa I. Tichý.

ZAT v jadrovej energetike

Spoločnosť ZAT patrí medzi popredných dodávateľov riadiacich systémov pre energetiku a priemysel vo svete. Technológiu a know-how českej firmy nájdete v 30 percentách jadrových elektrární v EÚ a 10 percentách vo svete. Najúspešnejšími produktmi ZAT sú riadiace systémy, bezpečnostný systém ovládania pohonov regulačných kaziet reaktora a regulačný systém výkonu jadrového reaktora. Riadiace systémy firma nasadzuje na primárnej i sekundárnej časti veľkých a malých jadrových reaktorov aj na ďalšie jadrové technológie vrátane súvisiacich služieb.

Okrem Francúzska má ZAT rozpracované dodávky riadiaceho systému v jadrovej elektrárni vo Fínsku, v Maďarsku, Arménsku, na Slovensku a v Českej republike. „Máme potrebné kompetencie a referencie na modernizáciu systémov kontroly a riadenia v už prevádzkovaných aj novostavaných jadrových elektrárňach s rôznymi typmi reaktorov. Chceme sa tiež zapojiť do dodávateľských modelov v rámci ponúk všetkých potenciálnych dodávateľov pri výstavbe nových jadrových blokov v Českej republike," uzatvára I. Tichý. ZAT je členom Aliancie českej energetiky, ktorej cieľom je práve zapojenie českého priemyslu do dostavby jadrovej elektrárne v Českej republike.

www.zat.cz

Rýchlejšia cesta k net zero

Globálne Centrum excelentnosti pre net zero transformáciu bude poskytovať jedinečné služby z deviatich lokalít v Európe, Severnej Amerike a v Ázii. Spoločnosť Atos potvrdila svoju pozíciu lídra v oblasti bezpečných a dekarbonizovaných digitálnych technológií. Svojim zákazníkom poskytuje najkomplexnejšie, end-to-end dekarbonizačné možnosti na trhu, aby umožnila a urýchlila ich cestu k net zero.

Nová ponuka „Od A po Zero“ (A to Zero) obsahuje kompletné portfólio podporované dvoma novými integrovanými dátovými platformami. Zahŕňa stratégiu pre klimatické zmeny, nastavenie cieľov, kalkulácie emisií, hodnotenia digitálnej dekarbonizácie, znižovanie uhlíkových emisií, ako aj inovatívne priemyselné riešenia, ako sú digitálne dvojčatá, dohody o úrovni dekarbonizácie alebo nízkouhlíkové dátové centrá. Neutralizovať a kompenzovať emisie CO_2 pomáha klientom dobrovoľné vyvažovanie uhlíka založené na prírodných riešeniach.

Ponúkať a podporovať ju bude globálne Centrum excelentnosti pre net zero transformáciu v rámci deviatich lokalít: päť z nich bude v Európe (Paríž, Lyon, Barcelona, Londýn, Mníchov), dve v Severnej Amerike (New York a Montreal) a dve v Ázii (Chennai a Singapur). Centrum zákazníkom umožní naplno využiť globálne zručnosti, zdroje a sieť viac ako 200 expertov Atosu na vytvorenie vlastnej cesty k tomu, aby sa stali odolnými, net zero spoločnosťami. Vzhľadom na rozmach net zero emisných stratégií Atos plánuje rozšíriť svoj net zero transformačný tím na 500 expertov do konca roka 2022.

„Neprejde ani deň bez toho, aby nejaká organizácia neohlásila svoju ambíciu dosiahnuť net zero. Dokazuje to, že globálne úsilie o uhlíkovo neutrálnu ekonomiku dosiahlo bod zlomu. Atos bol medzi priekopníkmi, ktorí razili cestu boja s klimatickými zmenami v rámci firiem; spoločnosť svojou ambíciou ‚net zero do roku 2028‘ nastavila vo svojom odvetví tie najvyššie dekarbonizačné štandardy. Naša ponuka, Od A po Zero‘ ťaží zo silného odhodlania a dlhoročnej práce na znižovaní našich vlastných emisií skleníkových plynov a z návrhov inovatívnych riešení s nízkym vplyvom na prostredie. Sme radi, že zlepšujeme a rozširujeme naše dekarbonizačné možnosti, aby sme lepšie podporovali cestu našich zákazníkov k net zero,“ vysvetľuje Elie Girard, CEO spoločnosti Atos.

Portfólio sa delí do troch kategórií.

Biznisové poradenské služby
Ponúkajú organizáciám ucelený prístup k vytváraniu úspešných stratégií pre net zero transformáciu, pričom zohľadňujú špecifické výzvy odvetví a podnikania. Cieľom týchto služieb je:
- porozumieť strategickým ambíciám zákazníka;
- merať uhlíkové emisie s využitím uznávaných odolných metodológií a digitálnu uhlíkovú stopu pomocou hodnotenia digitálnej dekarbonizácie;
- efektívne spravovať dáta s reportingovými protokolmi na mieru a implementáciou IT systémov;
- určiť stratégiu a nastaviť ciele – definovaním cieľov založených na vedeckých poznatkoch, implementáciou odporúčaní TCFD (Task Force on Climate-related Financial Disclosures) a definovaním akčných plánov na zmiernenie klimatických rizík.

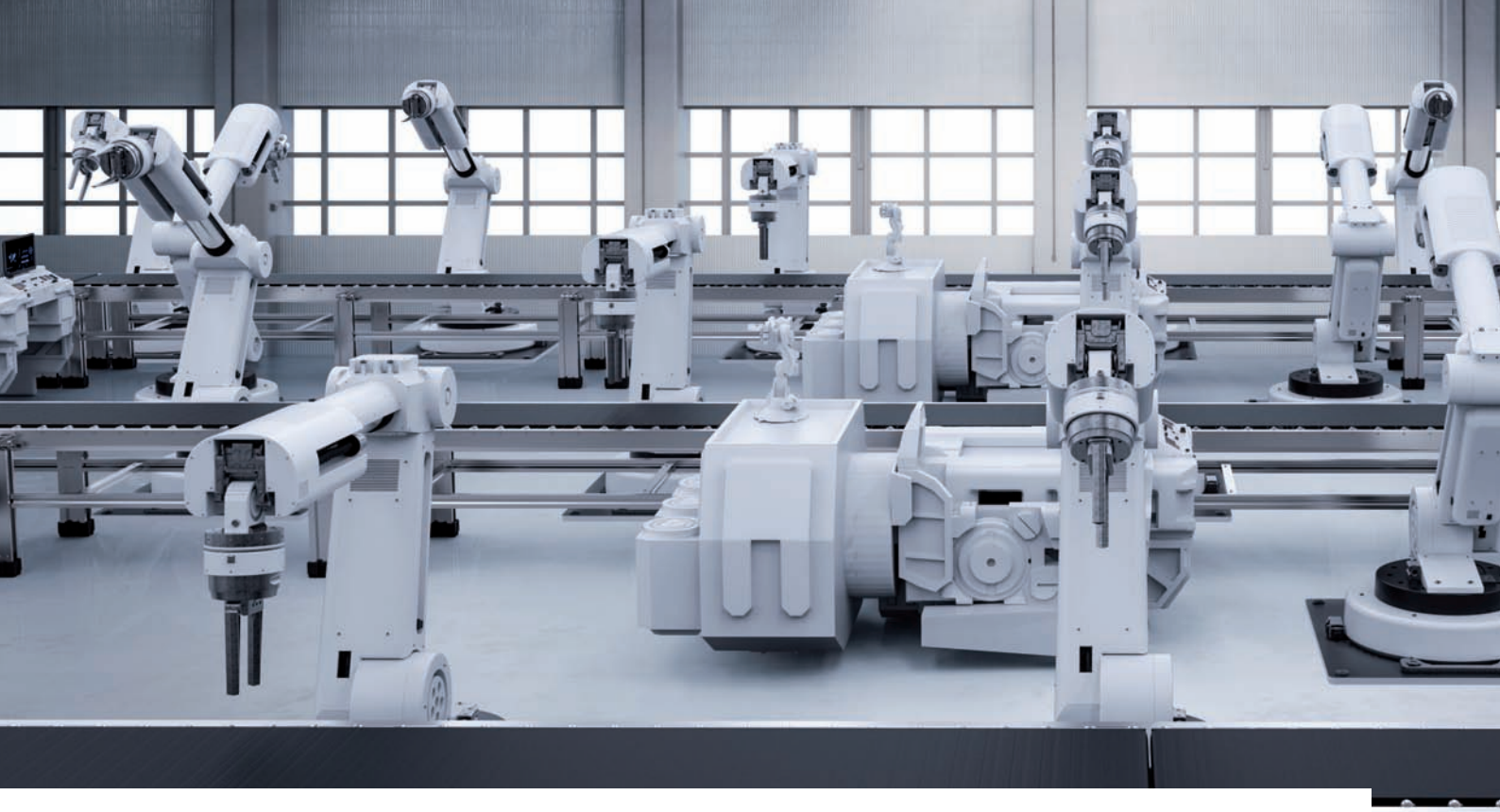
Digitálne zelené poradenstvo a platformy
Ponúkajú organizáciám príležitosť znižovať emisie a účinky na životné prostredie prostredníctvom:
- inovatívnych a udržateľných digitálnych riešení (cloud, digitálne pracovisko, smart budovy, IoT, HPC mobilita a riešenia dodávateľského reťazca) a dohody o úrovni dekarbonizácie;
- opatrení na zvyšovanie energetickej účinnosti, využívania obnoviteľnej energie, akčných plánov znižovania emisií a nástrojov na oceňovanie uhlíka;
- platformy Atos Digital Decarbonization Platform, komplexnej ponuky, ktorá podnikom a organizáciám umožňuje využívať digitálne technológie na zjednodušenie a automatizáciu zbierania, kalkulácie, reportovania, dátovej analýzy a vizualizácie emisií naprieč hodnotovým reťazcom. Jedinečná platforma ponúka aj nový pohľad na optimalizáciu obchodného rozhodovania, založený na dátach a predvídateľnosť.

Prírodné riešenia uhlíkovej kompenzácie a neutralizácie
Tie organizáciám umožnia:
- posunúť sa smerom k net zero na základe vedecky overených cieľov zameraných na znižovanie emisií, a to prostredníctvom najlepších projektov na vyvažovanie uhlíka na celom svete, čím sa zaistí jedinečný prístup k riadeniu rizika a strategickej komunikácii organizácií a výsledky posilnené digitálnymi inováciami;
- pod názvom Going4Zero využívať automatizované online služby na mieru, merať emisie uhlíka, sledovať trajektóriu znižovania emisií a vyberať a riadiť aktivity, zamerané na vyvažovanie uhlíka. Going4Zero okrem toho zabezpečuje komunikáciu o klimatických akciách s kľúčovými účastníkmi, napríklad zákazníkmi, a ponúka široké možnosti vzdelávacích a praktických riešení spoločnostiam bez ohľadu na ich veľkosť a vyzretosť v otázkach ochrany životného prostredia;
- vyvinúť vlastný projekt zameraný na vyvažovanie uhlíka.

Ponuka net zero transformácie od Atosu ťaží z 15-ročných skúseností spoločnosti EcoAct pri pomoci firmám s implementáciou pozitívnych zmien v reakcii na klimatické a uhlíkové výzvy a odborných znalostí spoločnosti Atos získaných pri pomoci firmám pri inováciách a prijímaní digitálnych riešení. To ešte posilňujú ambície skupiny odomknúť uhlíkovo neutrálnu ekonomiku s digitálnymi technológiami.

Atos IT Solutions and Services s.r.o.

Pribinova 19
811 09 Bratislava
Tel.: +421 2 6852 6801
sylvia.zazova@atos.net
https://atos.net/sk/



Tri trendy, ktoré zmenia výrobné prevádzky

Takmer pred desiatimi rokmi zaviedlo nemecké spolkové ministerstvo školstva a výskumu termín na opísanie zmeny, ktorá sa teraz šíri naprieč výrobným priemyslom: Industrie 4.0. Ten sa dnes bežnejšie uvádza v podobe anglického ekvivalentu Industry 4.0 (a slovenského Priemysel 4.0, pozn. red.). Táto zmena sa niekedy nazýva štvrtá priemyselná revolúcia a opisuje ďalší krok transformácie automatizačnej technológie pre výrobu.

Rovnako ako tretia priemyselná revolúcia, aj Priemysel 4.0 sa točí okolo používania robotiky a zariadení využívajúcich počítačové systémy. Hlavne sa však vyznačuje zvýšeným zameraním na vzájomné prepojenie systémov a úplné využitie údajov, ktoré každý automatizovaný subsystém generuje a zhromažďuje. Dôraz na komunikáciu je dôvod, prečo Priemysel 4.0 začína čoraz viac pokukávať po koncepte priemyselného internetu vecí (IIoT). Roboty a obrábacie stroje sa vďaka analýze dát, komunikácii a riadeniu v reálnom čase stávajú „kyberfyzikálnymi systémami“, ktoré dokážu oveľa inteligentnejšie reagovať na zmeny podmienok.

Zameranie na aspekty informačných technológií (IT) prenesených na úroveň priemyselných riadiacich systémov neznamená, že sa Priemysel 4.0 spolieha len na automatizáciu. Mnoho výrobných postupov a činností stále vyžaduje ľudskú interakciu. Na rozdiel od minulosti, keď boli roboty inštalované vnútri bezpečnostných klietok, ďaleko od zamestnancov prevádzky, trendy v súčasnosti smerujú k používaniu cobotov, t. j. robotov a nástrojov, ktoré spolupracujú priamo s ľuďmi. To má uľahčiť prechod na oveľa flexibilnejšiu prevádzku, kde sú výrobné bunky schopné rýchlo a efektívne meniť operácie. Táto schopnosť umožňuje bunkám reagovať na náhle zmeny v dopyte, aby mohli v prípade potreby pracovať s rôznymi produktmi a variantmi. To zase vyvoláva potrebu buniek reagovať na oveľa bohatšiu skupinu dátových tokov a podľa nich aj vykonávať plánovanie.

Obrábacie stroje a roboty boli doteraz zväčša konštruované tak, aby reagovali na okolnosti vyskytujúce sa okolo nich, aby pomocou zabudovaných senzorov zisťovali, či sú porušené definované obmedzenia, alebo v niektorých prípadoch monitorovali svoj vlastný stav pomocou analýzy, napríklad vibrácií. Očakáva sa, že schopnosť vlastného monitorovania sa v nasledujúcich rokoch začne čoraz viac využívať, aby sa zabránilo neočakávaným poruchám a aby sa zefektívnila činnosť údržby.

V scenári Priemyslu 4.0 môžu strojné zariadenia reagovať na údaje produkované susednými jednotkami alebo externými vstupmi, čo im umožňuje rýchlo zvládnuť meniace sa podmienky. Procesy môžu prispôsobiť časy zahrievania a sušenia tak, aby vyhovovali meniacemu sa obsahu vlhkosti v materiáloch alebo vlhkosti prostredia. Zníženie odchýlok spôsobených meniacimi sa podmienkami znamená, že sa zlepší kvalita výstupu a pri priaznivých podmienkach aj schopnosť šetriť energiu.

Niektoré výrobky dostupné v súčasnosti na trhu poskytujú nové možnosti pre konkrétne typy strojov. Napríklad Motion Terminal VTEM od spoločnosti Festo je prvý ventil so schopnosťou spúšťať aplikácie, ktoré vyladia prevádzku pre rôzne situácie. Kontrola kvality je hlavným zameraním programovateľných uťahovacích nástrojov HS-Technik od spoločnosti Panasonic. Zabudované snímače zaznamenávajú a vyhodnocujú hodnoty krútiaceho momentu a uhla upevnenia, ktoré sú rozhodujúce pre kontrolu kvality v aplikáciách s vysokou výkonnosťou.

Trend č. 1 – simulácia a digitálne dvojčatá

Analytická spoločnosť GlobalData vo svojich prieskumoch zistila, že koncept digitálneho dvojčaťa sa začína presadzovať čoraz častejšie. Podporou digitálnej reprezentácie každého dodávaného fyzického produktu, ktorý obsahuje väčšinu údajov zo snímačov získaných počas výroby a počas jeho životnosti, uľahčuje digitálne dvojča meranie efektívnosti fyzického produktu. Kľúčom vytvorenia konceptu digitálneho dvojčaťa je technológia simulácie. Namiesto toho, aby sa simulácia digitálneho dvojčaťa spoliehala výlučne na

nejaké charakteristické vzory v údajoch zo snímačov, môže na základe zaznamenávaných údajov poukázať na potenciálne problémy, čo pomáha nielen pri zabezpečovaní vysokej dostupnosti výroby a zefektívnení údržby zariadení, ale aj pri návrhu nových výrobkov.

Adrian Lloyd z agentúry Interact Analysis poznamenáva, že simulácia digitálnych dvojčiat pomáha nielen pri vývoji nových produktov, ale aj pri výrobných linkách, ktoré ich používajú. Príkladom bol automobilový start-up VinFast. V spolupráci so spoločnosťou Siemens použila automobilka simuláciu usporiadania prevádzok na zlepšenie priepustnosti a produktivity ešte skôr, ako boli jednotlivé strojné zariadenia fyzicky nainštalované, čo prinieslo výrazné úspory oproti tradičným metódam používaným pri výstavbe tohto typu výrobných liniek.

Spoločnosť Schneider Electric označuje myšlienku využitia simulácie pri vývoji výrobných liniek ako „inžiniering od nuly“, čím rozširuje koncepciu aj na programovanie jednotlivých častí riadiacich systémov. Namiesto viazania výrobnej kapacity na programovanie a testovanie teraz možno experimentovať a konfigurovať riadiace systémy Modicon a AVEVA vo virtuálnom prostredí. Techniky digitálneho dvojčaťa spájajú virtuálne modely s fyzickými systémami. V prípade potreby zmeny sa programovanie jednoducho prevedie z jedného do druhého.

Podľa spoločnosti ABB prístupy virtuálneho uvedenia do prevádzky skracujú celkový čas inžinieringu o 20 %, znižujú kapitálové výdavky o 25 % a skracujú čas potrebný na školenie o polovicu. Na podporu tohto prístupu poskytuje spoločnosť ABB riešenie virtuálneho uvedenia do prevádzky v rámci konceptu Ability, ktoré podporuje nielen konfiguráciu v digitálnom prostredí, ale ponúka aj rozhrania virtuálnej reality na podporu efektívneho a včasného školenia operátorov.

Trend č. 2 – inteligentné snímače sú všade

Použitie snímačov sa bude rozširovať v rámci aj mimo prevádzok. Dodávatelia, ako sú Omega a Omron, poskytujú širokú paletu snímačov, ktoré okrem iného využívajú techniky indukčnej, optickej, magnetickej, tlakovej a laserovej triangulácie. Vďaka dopytu po presnom meraní analytická skupina Mordor Intelligence predpovedá, že globálny trh so snímačmi internetu vecí (IoT) porastie od roku 2020 do roku 2025 kumulovaným ročným prírastkom okolo 24 %. Podľa štúdie spoločnosti Ericsson z roku 2021 bude k internetu pripojených 28 miliárd zariadení, z toho takmer 16 miliárd budú IoT zariadenia a veľká časť z nich bude umiestnená vo výrobe.

V dnešnom prostredí je bežným modelom to, že veľká časť údajov zo snímačov sa posiela do cloudu. Pretože počet snímačov narastá, je podpora tohto modelu náročná. Na analýzu údajov bude potrebné zabezpečiť ich lokálne spracovanie a z toho odvodiť nejaké informácie ešte skôr, ako sa niekam odošlú. Mali by sa nechať len tie informácie, ktoré sa viažu k nejakým zásadnejším zmenám stavu a až tie by sa mali poslať na hĺbkovú analýzu do cloudu. Pre tento prístup bude rozhodujúci vysokovýkonný a lacný výpočtový hardvér s edge funkcionalitou, ktorý je už teraz k dispozícii od popredných dodávateľov v rôznych formách.

Spoločnosť Omron začlenila umelú inteligenciu do svojej riadiacej platformy Symaec, zatiaľ čo Opto22 poskytuje vysokovýkonné výpočty na riadenie v reálnom čase v blízkosti prevádzky prostredníctvom rodiny modulov groov.

Trend č. 3 – bezpečnosť aj v heterogénnom prostredí

Ako sa zvyšujú možnosti výpočtov na okrajových zariadeniach siete a pripojených moduloch snímačov, stáva sa bezpečnosť pre implementátorov kľúčovým problémom. Všadeprítomná konektivita reprezentovaná IIoT poskytuje hackerom mnoho cieľov útoku. Prítomnosť viacerých komunikačných štandardov v rámci prevádzky zvyšuje celkovú zložitosť poskytovania ochrany.

V rámci boja proti riziku napadnutia musia vývojári venovať osobitnú pozornosť rizikám a mechanizmom boja proti útokom. Súčasťou riešenia je využitie skúseností z IT sveta v prostredí prevádzkových technológií. V IT priestore je dnes bežné šifrovanie údajov nielen pri prenose, ale aj keď sú v pokoji, pričom treba zabezpečiť, aby všetky kódy spustené v sieti boli podpísané schváleným dodávateľom. Výrobcovia musia ďalej zabezpečiť, aby bolo možné aktualizovať softvér a firmvér, keď sa nájdu chyby zabezpečenia. Dodávatelia, ako napríklad Schneider Electric, vyvinuli stratégie, ktoré majú výrobcom pomôcť pri zabezpečení a poskytnúť zákazníkom architektúru, ktorá sa s týmito problémami vyrovná. Ďalší dodávatelia implementujú do svojich produktov ochranné mechanizmy, aby zabezpečili výrobcom možnosť zostaviť si vlastnú bezpečnú architektúru.

Všetko prepojené

V súhrne možno povedať, že systémy priemyselnej automatizácie a riadenia sa rýchlo rozvíjajú na viacerých frontoch, pretože výrobcovia začínajú využívať výhody flexibility a schopnosti, ktoré prinášajú technológie Priemyslu 4.0. Aj keď bezpečnosť a ďalšie problémy prinášajú výzvy, vďaka vylepšeniam technológií bude výroba efektívnejšia a bude lepšie zvládať dopyt a požiadavky zákazníkov. Dôkladným výberom vhodnej technológie a využitím škálovateľných platforiem môžu podniky uľahčiť svoju digitálnu transformáciu. V tomto smere je vhodné obrátiť sa na osvedčených globálnych distribútorov, ako je napríklad Farnell, ktorí môžu poskytnúť prístup k špičkovému produktovému portfóliu na trhu, silnej sieti dodávateľov, spoľahlivej distribúcii a technickej podpore, a to bez ohľadu na veľkosť firmy.

Cliff Ortmeyer

globálny vedúci technického marketingu
Farnell
www.farnell.com

Ochrana obvodov MaR vo výbušnom prostredí (3)

Ďalšie kritériá výberu zvodičov na ochranu obvodov MaR pred prepätím v prostredí s nebezpečenstvom výbuchu.

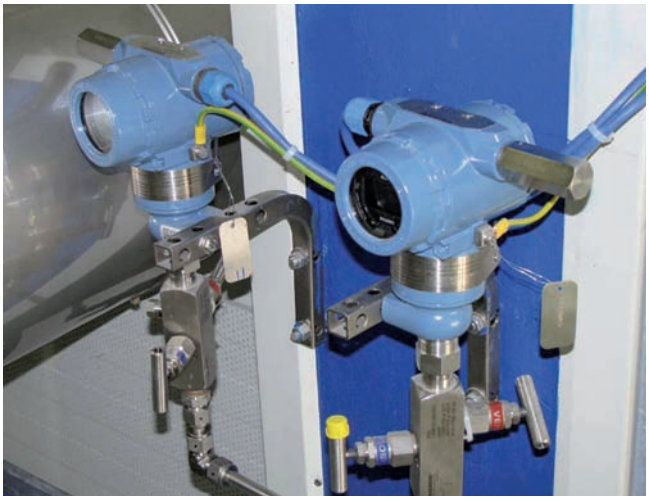
V prostredí s nebezpečenstvom výbuchu sa najčastejšie používajú iskrovo bezpečné obvody. To znamená, že iskra, ktorá pri možnej poruche vznikne na vedení alebo v elektrickom zariadení, do ktorého vedenie vstupuje, nebude mať dostatočnú energiu na to, aby zapálila horľavý plyn alebo prach v prostredí. Aby sa zamedzilo nepresnostiam v meraní z dôvodu unikajúcich prúdov, sú tieto obvody najčastejšie navrhované ako galvanicky oddelené. Iskrovo bezpečné obvody s meracou slučkou 4 – 20 mA sa v závislosti od izolačnej pevnosti použitých snímačov a galvanických oddeľovačov (bariér) voči zemi rozdeľujú na obvody na „plávajúcom“ potenciáli a obvody, ktoré sa považujú na uzemnené. Ak je izolačná pevnosť vedení privedených do zariadenia voči zemi väčšia ako 500 V AC, považujeme ju za meraciu sústavu na „plávajúcom“ potenciáli. Nainštalované zvodiče prepätia nesmú túto izolačnú pevnosť vodičov voči zemi ovplyvňovať. Ak je izolačná pevnosť medzi vodičmi meracieho, iskrovo bezpečného obvodu a zemou menšia ako 500 V AC, musia sa použiť zvodiče, ktorých úroveň ochrany pri impulznom prúde 10 kA (tvar impulzu 8/20 μs) je pod hodnotou izolačnej pevnosti „uzemneného“ zariadenia, napr. Up vodič/zem ≤ 35 V.

Iskrová bezpečnosť. Typ ochrany – kategória ia, ib alebo ic?

Izolačná bariéra a zvodič prepätia sú inštalované v zóne 1. Pre túto zónu je pre meracie obvody 4 – 20 mA typ ochrany s iskrovou bezpečnosťou ib postačujúci. Zvodiče, ktoré sú certifikované ako typ ochrany s iskrovou bezpečnosťou ia, spĺňajú najprísnejšie požiadavky, a preto sú vhodné aj do obvodov s požadovanou iskrovou bezpečnosťou ib a ic.

Maximálne prípustné hodnoty L_o a C_o

Pred uvedením iskrovo bezpečného obvodu do prevádzky musí byť predložený dôkaz o vnútornej bezpečnosti meracieho obvodu vo forme výpočtu. V praxi to znamená, že pre každý iskrovo bezpečný obvod musí byť vykonaný výpočet, ktorý zohľadňuje nahromadenú

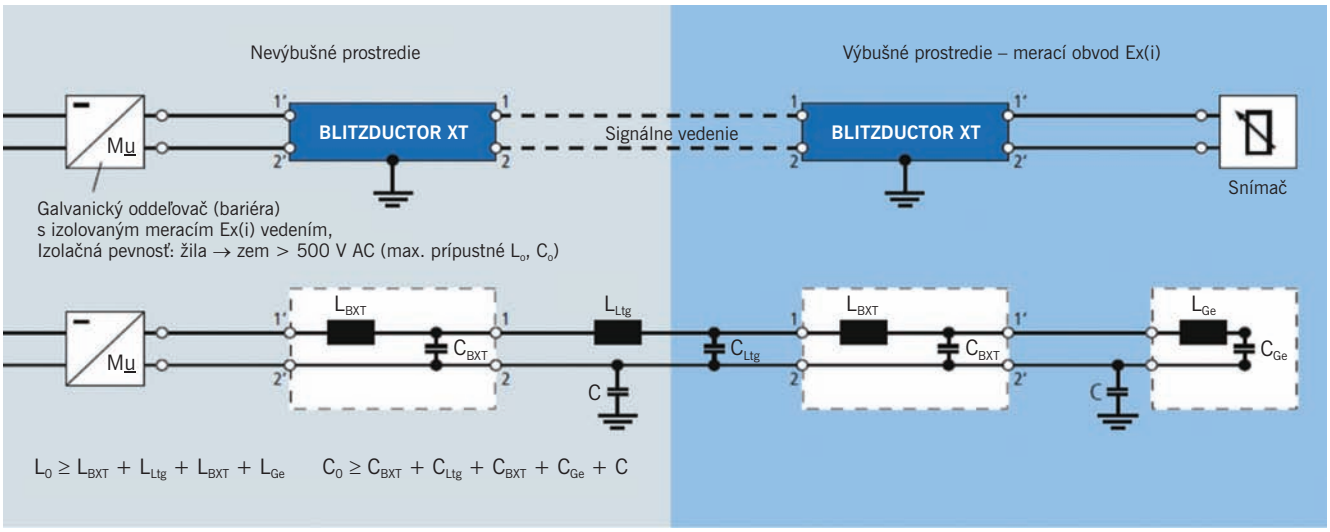


Obr. 6 Ochrana tlakomera v prostredí Ex zvodičom prepätia DEHNpipe konštrukčne vyvinutá na montáž priamo na tlakomer od výrobcu DEHN SE + Co KG.

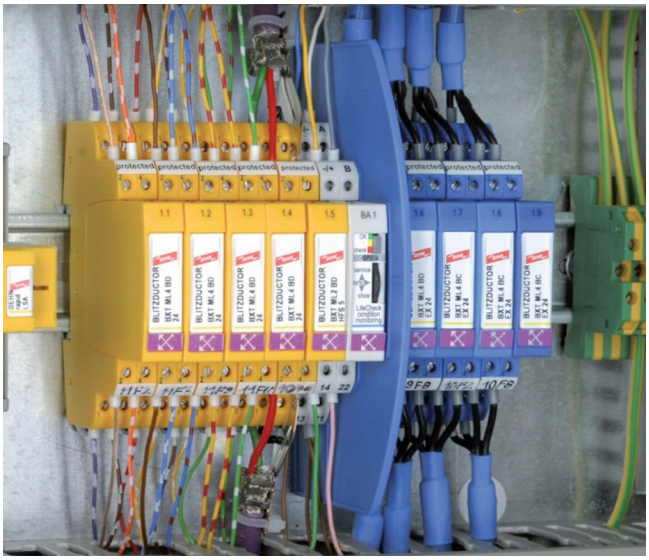
energiu v zariadeniach inštalovaných v tomto obvode a energiu v samotnom káblovom vedení. Tu máme na mysli vlastnú kapacitu a indukčnosť vedenia a nainštalovaných prístrojov (napr. snímače, zdroje, prevodníky a zvodiče prepätia). Zvodič prepätia Blitzductor BXT ML4 BD EX 24 od výrobcu DEHN SE + Co KG použitý v našom príklade má certifikáciu ATEX/IECEx a je určený na inštaláciu do iskrovo bezpečných obvodov 4 – 20 mA. Má zanedbateľnú vlastnú kapacitu a indukčnosť. Pri výpočte teda netreba počítať s energiou, ktorá môže byť nahromadená v tomto zvodiči.

Maximálne hodnoty napätia U_i a prúdu I_i

Galvanický, iskrovo bezpečný oddeľovač má jasne definované technické parametre, aby bola aplikácia skutočne iskrovo bezpečná. Je to hlavne napájacie napätie U_o a maximálny skratový prúd I_o. Tieto



Obr. 5 Príklad výpočtu C_o a L_o v iskrovo bezpečnom obvode Ex(i)



Obr. 7 Zvodiče prepätia Blitzducktor XT inštalované na vstupe vedení 4 – 20 mA do rozvádzača MaR. Modré zvodiče pre obvody Ex(i).

hodnoty musia byť zohľadnené aj pri výbere správneho zvodiča. Menovité napätie zvodiča U_c alebo maximálne prípustné napätie U_i zvodiča musí mať minimálne takú hodnotu, aké je maximálne napätie napájacieho zdroja na prázdno. V prípade menovitého prúdu musí minimálna hodnota zvodiča dosahovať hodnotu maximálneho skratového prúdu, ktorý môžeme v meracom obvode očakávať v prípade poruchy. Zvodič môže zlyhať aj vtedy, keď pri pretekaní maximálneho skratového prúdu dôjde k jeho nebezpečnému oteplení. Oteplenie zvodiča je teda tiež jeho dôležitý technický parameter a musí byť bezpodmienečne zohľadnený pri špecifikácii vhodného zvodiča.

Koordinácia zariadenia na ochranu pred prepätím a koncovým zariadením

Technický štandard NAMUR NE 21 špecifikuje požiadavky na odolnosť a elektromagnetickú kompatibilitu elektrických zariadení procesnej a laboratórnej techniky. Signálové vstupy takýchto zariadení musia mať minimálnu odolnosť 0,5 kV medzi žilami vedenia (priečne napätie) a 1 kV vodiče vedenia voči zemi. Skúšobné metódy, priebeh skúšky a skúšobné impulzy sú opísané v základnej norme STN EN 610 00-4-5. Podľa amplitúdy skúšobného impulzu, ktorý bol bez poškodenia aplikovaný na skúšanom zariadení, dostane zariadenie pridelenú triedu odolnosti voči rušeniu EMC. Trieda 1 znamená najnižšiu a trieda 4 najvyššiu odolnosť. Trieda odolnosti sa zvyčajne uvádza v technickej dokumentácii k zariadeniu alebo ju výrobca vyznačí priamo na zariadení. Tam, kde existuje riziko poškodenia zariadenia z dôvodu blesku (prepätie, prúd, energia), treba tieto hodnoty obmedziť zvodičmi pod deklarovanú odolnosť zariadenia procesnej techniky. Firma DEHN SE + Co KG na svojich zvodičoch a v dokumentácii uvádza označenie, ktoré zariadenia a s akou triedou odolnosti je zvodič prepätia schopný ochrániť. Nájdete tam napríklad údaj P1, ktorý znamená, že zvodič je schopný ochrániť aj tie najcitlivejšie zariadenia procesnej a meracej techniky.

Jiří Kroupa

j.kroupa@dehn.sk
www.dehn.cz

Informácie o teplote v rozvádzači cez IIoT

Optimálne rozloženie prístrojov a inteligentné monitorovanie stavu zabraňujú teplotnému poškodeniu v rozvádzači. Inteligentný ochranca rozvádzača IM18-CCM od spoločnosti Turck prenáša údaje o stave priamo do sveta IT.

Údaje týkajúce sa stavu rozvádzača umožňujú používateľom predchádzať poruchám a zvyšovať tak dostupnosť ich zariadenia.

Nadmerné hromadenie tepla v rozvádzačoch môže mať hneď niekoľko dôvodov. Vývojári a konštruktéri môžu často vopred minimalizovať nebezpečenstvo vyplývajúce z nesprávne usporiadaných zariadení alebo zlého vetrania. Vzhľadom na externé faktory a anomálie zariadení umiestnených v rozvádzači treba zabezpečiť sledovanie špecifických ukazovateľov a hodnôt klímy vnútri rozvádzača. Zariadenie spoločnosti Turck s označením IM18-CCM teraz poskytuje inteligentné riešenie na spracovanie údajov zo snímačov cez ethernet v rámci priemyselného internetu vecí (IIoT).

Umiestnenie čoraz výkonnejších zariadení do čoraz menších priestorov je známkou technologického pokroku. Z hľadiska rozvádzača znamená kompaktný dizajn moderných zariadení menšie vonkajšie rozmery alebo možnosť umiestniť väčší počet elektronických súčiastok. Inovácie však majú aj svoju odvrátenú stránku. V tomto prípade pre všetkých, ktorí musia dávať pozor na možné vedľajšie účinky zvyšujúcej sa miniaturizácie technológie, ako je napríklad hromadenie tepla. Najmä extrémne alebo nepravidelné teplotné podmienky v rozvádzači môžu spôsobiť výpadok napájania alebo dokonca poruchu jednotlivých zariadení. Okrem efektívneho rozmiestnenia jednotlivých zariadení sú preto čoraz dôležitejšie aj inteligentné riešenia na monitorovanie stavu vnútri rozvádzača. IM18-CCM, najnovší kompaktný monitor klímy a ochrana dverí od spoločnosti Turck, prináša monitorovanie stavu dokonca aj do sveta IT prostredníctvom siete ethernet.

Z vyššieho tepla vzniká hneď niekoľko rizík

Vyššia hustota rôznych zariadení, spotreba energie a s ňou súvisiace vyššie generované teplo v rozvádzači nevyhnutne zvyšuje straty a znižuje účinnosť. Myslí sa tým podiel spotrebovanej elektriny, ktorá sa nemôže použiť v procese, ale je rozptýlená elektronickými zariadeniami vo forme tepla. Ak sú komponenty rozvádzača usporiadané tak, že sa vytvárajú horúce miesta, alebo je zle zabezpečené prúdenie studeného vzduchu, vzniká niekoľko rizík súčasne. Presné meracie prístroje môžu v niektorých prípadoch stratiť svoju presnosť, môže sa znížiť životnosť komponentov alebo v tom najhoršom scenári môže dôjsť k výpadku činnosti. Zložité systémy, ako napríklad riadiace systémy, sú obzvlášť citlivé na teplo. Väčšina PLC má maximálnu prevádzkovú teplotu 55 °C. To je iba približne 15 °C nad „komfortnou teplotou“ mnohých rozvádzačov.

Zistite anomáliu skôr, ako bude neskoro

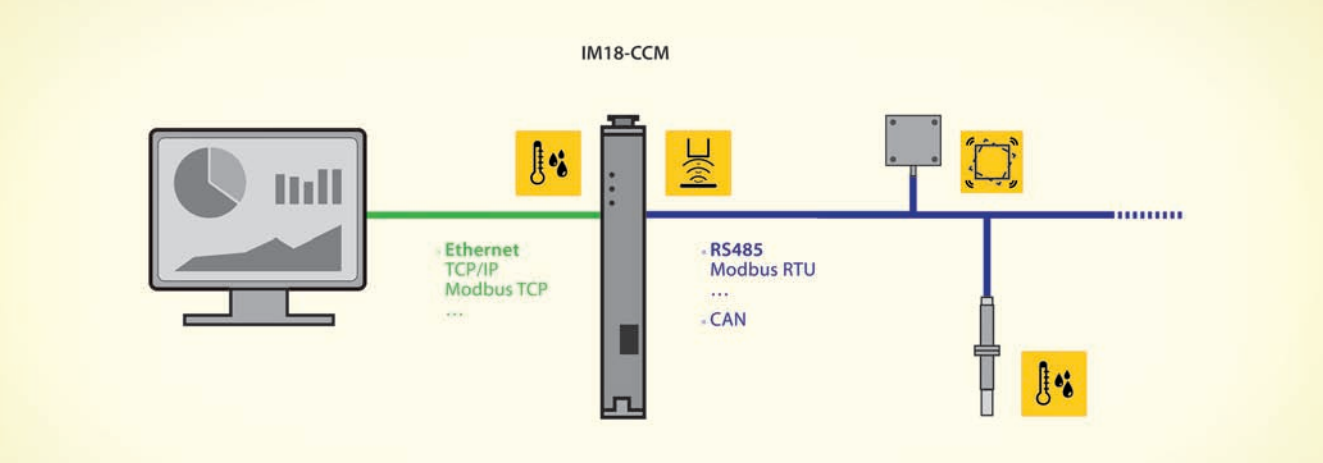
Ak je už rozvádzač osadený komponentmi, možno ešte aj v tejto fáze čiastočne znížiť riziko vzniku tepla. Usporiadanie zariadení do stredne veľkých blokov, ktoré zabraňujú vzniku prekážok v prúdení vzduchu spôsobených nevhodne položenými káblami alebo káblovými

„Ochranca“ rozvádzača Turck IM18-CCM prenáša namerané hodnoty cez ethernet do IT sietí a môže ich dokonca vzdialene posielať.

trasami, a inštalácia komponentov citlivých na teplo čo najbližšie k spodnej časti skrinky – to sú len niektoré z vhodných praktík, vďaka ktorým môžu prevádzkovatelia dosiahnuť dobré teplotné pomery vnútri rozvádzača. Aj pri optimálnej topológii alebo vetraní pomocou klimatizačných systémov má však zmysel permanentne elektronicky monitorovať klimatické podmienky v rozvádzači. To umožňuje technikom údržby včas spozorovať akékoľvek anomálie, aby sa zabránilo poruchám, najmä keď sú zariadenia umiestnené v geograficky vzdialených rozvádzačoch. To platí napríklad pre vonkajšie priestory, kde je dôležitým faktorom počasie.

Monitorovanie tri v jednom na DIN lište

Pred niekoľkými rokmi pridala spoločnosť Turck do svojho portfólia produkty IM12-CCM a IMX12-CCM (na umiestnenie do Ex prostredia) ako ľahko rozšíriteľné riešenie monitorovania stavu. Kompaktné zariadenia sú namontované na DIN lište a vybavené tromi zabudovanými snímačmi na monitorovanie teploty, vlhkosti vzduchu a po otvorenia dverí. IM(X)12 používa konfigurovateľnú funkciu hraničnej hodnoty na následné odoslanie signálu, ak sa vyskytnú hodnoty nad alebo pod definovanými hraničnými hodnotami. To by potom konkrétne naznačovalo, že zariadenie sa prehrialo, v rozvádzači dochádza ku kondenzácii vlhkosti alebo dvere neboli správne zatvorené.



Bezproblémové spojenie medzi OT a IT: IM18-CCM od spoločnosti Turck umožňuje pripojenie externých snímačov a prenos nameraných hodnôt do systémov vyššej úrovne cez ethernet.

Model IM12-CCM je vybavený interným záznamníkom údajov s časovou značkou a uchováva údaje až dva roky. To umožňuje používateľom tiež dlhodobo detegovať plazivé zmeny a odstraňovať ich príčiny. Rozhranie umožňuje prevádzku dvoch „ochrancov" rozvádzačov v režime master/slave, čo umožňuje monitorovať správne zatváranie dverí a ďalšie hraničné hodnoty súčasne v dvoch bodoch v rozvádzači. Master spracuje dáta od slave a odošle signál do riadiaceho systému. Štandardné zariadenie IM12-CCM sa dodáva s dvoma spínacími kontaktmi a rozhraním IO-Link. Režim rýchleho učenia umožňuje používateľovi ľahko nastaviť hraničné hodnoty v prevádzke. Alternatívne možno parametre nastaviť pomocou IO-Link alebo FDT nástroja, ako je napr. PACTware.

Spoločnosti by mimochodom nemali monitorovať stav dverí iba kvôli sledovaniu zmien teploty a vlhkosti. Digitálne systémy, najmä v takzvaných kritických infraštruktúrach (CRITIS), ako sú dodávky elektriny a vody, musia byť spoľahlivo a transparentne chránené pred neoprávneným prístupom. To stanovuje zákon o bezpečnosti IT. Zariadenia CCM spoločnosti Turck s ich bezpečnými ovládacími funkciami ponúkajú v tejto oblasti skvelý výkon. Vďaka týmto zariadeniam je každý rozvádzač vhodný na použitie v kritických infraštruktúrach bez akýchkoľvek veľkých výdavkov.

Ďalšie kroky: prepojenie výrobnej úrovne a sveta IT

Turck IM18-CCM posúva všetko o krok ďalej, pretože umožňuje nielen lokálne zobrazenie monitorovania stavu rozvádzačov, ale aj prenos dát do sveta IT. Úzke 18 mm zariadenie odosiela namerané hodnoty zo snímačov do systémov vyššej úrovne prostredníctvom svojho ethernetového rozhrania. Teoreticky môžu byť prenášané až do cloudu, čo umožní pracovníkom údržby prístup k aktuálnym údajom o klíme kedykoľvek prostredníctvom mobilných terminálov. Hranica medzi úrovňou prevádzky a IT infraštruktúrou sa tak postupne stráca. To znamená, že používatelia môžu analyzovať údaje z výroby priamo zo svojho kancelárskeho stola.

Z hľadiska výstupných údajov to predstavuje ďalšie možnosti pre tvorcov prevádzok aj pre ich samotných prevádzkovateľov. Pri zbere nameraných hodnôt je tak k dispozícii viac voľnosti: rozhranie RS485 (Modbus RTU alebo CAN) umožňuje v prípade potreby pripojiť k IM18-CCM (okrem troch už nainštalovaných snímačov) ďalšie externé zariadenia, ako sú napríklad snímače vibrácií. Napríklad na získanie ideálneho teplotného obrazu rozvádzača by sa mohlo nainštalovať viac snímačov teploty v jeho rôznych častiach, čím by sa eliminovala potreba ďalších zariadení na monitorovanie klímy v rozvádzači. Údaje z troch snímačov teploty často stačia na získanie presného celkového obrazu aj vo veľkých rozvádzačoch.

Flexibilita v aplikáciách na mieru

Úlohy monitorovania stavu sú často rovnako individuálne ako softvérové riešenia mnohých výrobcov alebo používateľov zariadení. Otvorená linuxová platforma zariadení IM18-CCM preto poskytuje

Rad IM-CCM od spoločnosti Turck ponúka riešenia monitorovania stavu pre koncových používateľov a výrobcov OEM.

možnosť inštalovať vlastné aplikácie. To umožňuje programátorom vložiť do zariadenia špecifické aplikácie, napríklad na zisťovanie rosného bodu alebo umožnenie prirodzeného zvýšenia teploty na začiatku letných mesiacov. Niektorí používatelia si tiež môžu želať nahrať svoje vlastné rozhranie na pripojenie sa do cloudu – vizualizácia trendov alebo odoslanie alarmu potom prebehne v systéme vyššej úrovne.

Viac rozhraní, viac pamäte

Teplota, vlhkosť vzduchu, ale aj bezpečnosť rozvádzačov sú faktory, ktoré hrajú dôležitú úlohu v každom návrhu konceptu prevádzky. Pri správnom usporiadaní prístrojov a účinnom vetraní môžu návrhári zabezpečiť základ optimálnej dostupnosti elektronických komponentov. Okrem „ochrancov" rozvádzačov sú k dispozícii aj kompaktné a ľahko ovládateľné nástroje na monitorovanie stavu, ktoré kedykoľvek poskytujú informácie o kritických nameraných hodnotách.

V nadväznosti na osvedčené zariadenia radu IM12 prináša nový rad IM18-CCM prepojenie aj k IIoT, čo poskytuje priestor na zákaznícke riešenia na mieru. Ktokoľvek, kto si želá ešte väčšiu škálu rozhraní, bude môcť tento rok využiť druhú verziu zariadenia – pribudne ďalší ethernetový vstup, univerzálne V/V, USB a ďalšia pamäť.

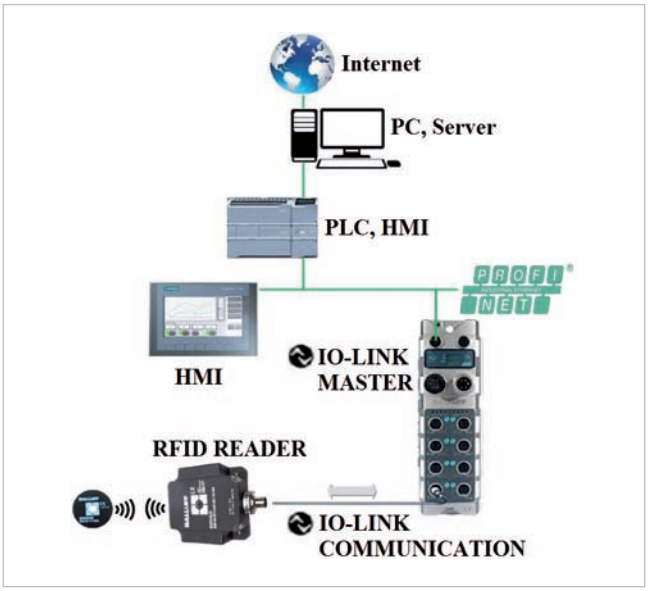
Marpex, s.r.o.

Športovcov 672
018 41 Dubnica nad Váhom
Tel.: +421 42 444 0010 – 1
info@marpex.sk
www.marpex.sk

Možnosti integrácie zariadenia IO-Link Master prostredníctvom webového servera

Článok opisuje možnosti integrácie zariadenia IO-Link Master (na základe konkrétneho typu, od spoločnosti Balluff) a porovnáva tento proces s ostatnými výrobcami s ohľadom na spoľahlivosť konfigurácie a využiteľnosť jednotlivých funkcií. Môžeme konštatovať, že takmer každé zariadenie IO-Link Master možno štandardne monitorovať cez webový server a zodpovedajúcu IP adresu. Rozsah monitorovania samozrejme závisí od konfigurácie portov IO-Link, typu zariadenia i samotného výrobcu. Nami predkladaný postup bol testovaný na senzoroch a akčných členoch, ktoré sú súčasťou automatizovaného systému FESTO FMS 500 s cieľom monitorovania prediktívnej údržby.

IO-Link predstavuje štandardizovanú technológiu komunikácie, ktorá sa zameriava na priame prepojenie inteligentných snímačov s akčnými členmi priemyselnej automatizácie (napr. s PLC) prostredníctvom priemyselnej komunikačnej siete. Inteligentné senzory, ktoré nevyžadujú vysoké náklady na prevádzku, však nemôžu používať štandardné komunikačné protokoly. Dôvodom je cyklická komunikácia v reálnom čase za súčasného prenosu malého množstva dát. Preto využívajú charakter komunikácie IO-Link, ktorá je typu point-to-point, čiže je realizovaná medzi dvoma bodmi. Ako taká vznikla s cieľom digitálnej náhrady analógových alebo spínaných výstupov. Charakterovo nejde o systémovú zbernicu, ale používa sa pod úrovňou týchto zberníc s cieľom jednoduchého pripojenia sa na priemyselné zbernice. Konečným cieľom je pritom zlepšenie výkonnosti automatizovaného systému, pretože procesné dáta a ich diagnostika môžu byť súčasne dostupné mnohým distribuovaným systémom a tiež môžu byť zdieľané na webe. V zásade topológia technológie IO-Link vyžaduje zariadenie IO-Link Master, ktoré má niekoľko portov IO-Link Master [1]. Zariadenie IO-Link sa potom na Master port pripája trojžilovým netieneným káblom s maximálnou dĺžkou 20 m pomocou štandardných eurokonektorov M5, M8 alebo M12. Nevyžaduje sa už žiadna ďalšia kabeláž, nakoľko týmto jedným prepojením sa prenáša dátová komunikácia aj napájacia energia pre pripojené zariadenie IO-Link (obr. 1).



Obr. 1 Princíp zberu dát na báze technológie IO-Link

Štruktúra komunikácie predstavuje hviezdu, kde centrálnym prvkom je zariadenie IO-Link Master, ktoré riadi a nadväzuje komunikáciu s ostatnými komponentmi IO-Link. Zariadenie IO-Link Master funguje vlastne ako komunikačná brána k nadradenej priemyselnej zbernici. Výhody používania IO-Link sa delia do troch oblastí:

- Zjednodušená a rýchla inštalácia – prepojenia sa realizujú trojžilovým alebo štvoržilovým káblom so štandardnými konektormi M5, M8 alebo M12, čo urýchľuje zapojenie a znižuje vznik chýb pri inštalácii. Jednoduchšia kabeláž znižuje náklady a zlepšuje prehľadnosť.
- Diagnostická funkcia – komponent IO-Link má autodiagnostické funkcie a pomocou rozhrania IO-Link poskytuje informácie o svojom stave nadradeným systémom. Vďaka takýmto informáciám sa môže predísť nečakanej poruche.
- Parametrizácia – IO-Link umožňuje vykonávať nastavovanie parametrov počas chodu. Pre každý komponent IO-Link možno zálohovať parametre priamo v zariadení IO-Link Master, ktoré sa automaticky nahrajú v prípade, že starý komponent bude nahradený novým.

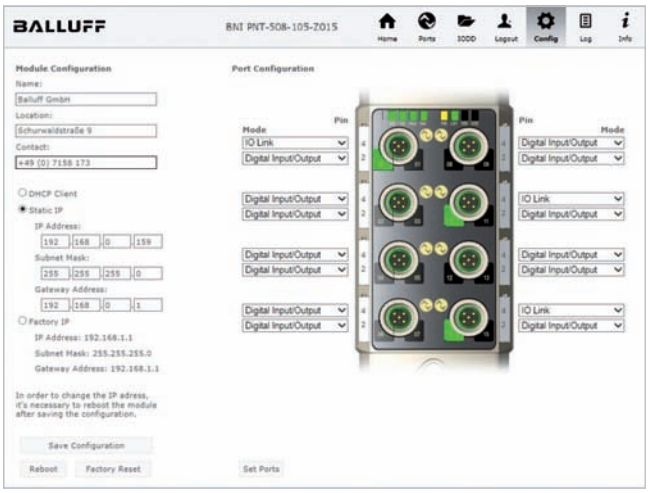
Integrácia zariadenia IO-Link Master

Diagnostiku dát (získaných pomocou RFID, resp. inou technológiou) možno v súčasnosti riešiť aj komplexným softvérom výrobcu, ktorý umožňuje zber týchto dát a ich samotnú distribúciu naprieč podnikovými informačnými systémami. Obyčajne tento softvér zabezpečuje riadenie a zber údajov medzi jednotlivo pripojenými zariadeniami IO-Link [2]. Súčasťou takéhoto softvéru (na úrovni SCADA) je tiež filtrácia, agregácia a priradenie významu údajom získaným pomocou technológie RFID (či inej). Ďalšou a treba povedať, že jednoduchšou metódou diagnostiky a získavania dát je integrácia a následná konfigurácia zariadenia IO-Link Master v zodpovedajúcom prostredí (napr. prostredníctvom webového servera, obr. 2).

Podružné činnosti získavania dát zahŕňajú oživenie čítacieho zariadenia (napr. na princípe RFID) či tvorbu vizualizácie prostredníctvom panela HMI. Metodický postup čítania, zápisu a následného spracovania získaných dát až po ich následné zdieľanie pomocou webového servera predpokladá nasledujúce kroky:

- Pridanie zariadenia IO-Link Master pre nový projekt. Krok obsahuje výber zodpovedajúceho zariadenia z hardvérového katalógu, inštaláciu súboru GSD a kontrolu dostupnosti predmetného zariadenia IO-Link Master v novom projekte.
- Vytvorenie spojenia (napr. s PLC). Tento krok možno charakterizovať ako realizáciu spojenia PROFINET a konfigurácie IP adresy zariadenia IO-Link Master.

- Nastavenie portov IO-Link Master. Činnosť predpokladá zobrazenie dostupných portov IO-Link a kontrolu ich aktuálneho nastavenia (štandardné nastavenie alebo nastavenie IO-Link).
- Pridanie zariadenia na zber dát (napr. čítačka RFID). V tomto kroku je potrebné nastavenie konkrétneho typu snímacieho zariadenia. Zároveň je vhodné zjednotiť nastavenie pre vstupné a výstupné byty pridanej čítačky RFID (aby vždy začínali z rovnakej adresy).
- Kompilácia a nahranie hardvérovej konfigurácie (napr. do PLC). Úspešnosť kroku je dokumentovaná rozsvietením zelenej LED na zariadení IO-Link Master, resp. zeleným blikaním zodpovedajúceho portu IO-Link, na ktorom je pripojené snímacie zariadenie (napr. čítačka RFID).

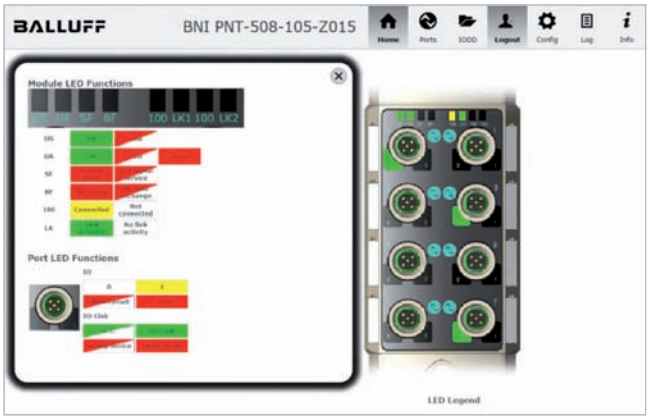


Obr. 2 Konfigurácia zariadenia IO-Link Master prostredníctvom webového servera

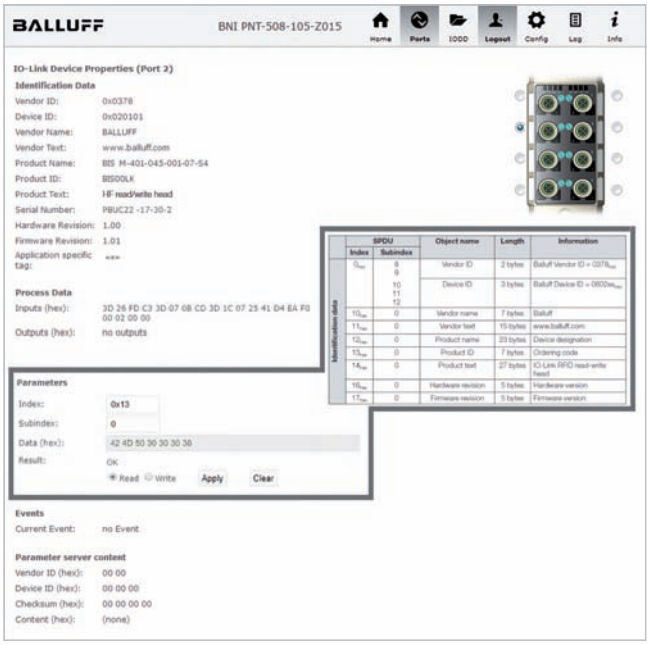
- Softvérová konfigurácia snímacieho zariadenia. Táto konfigurácia je založená na knižniciach pre dané zariadenie a ich kopírovaní do nového projektu. Konfigurácia obsahuje tagy PLC, tabuľku WATCH (so zaujímavými údajmi, ako sú dáta na zápis, prečítané dáta, informácie o tom, či zápis alebo čítanie dát prebehlo bez chyby alebo s chybou a pod.), dátové či programové bloky.
- Organizácia hlavného bloku „MAIN“. Krok obsahuje priradenie a opis významu pre jednotlivé vstupy a výstupy hlavného bloku a tabuľky WATCH.
- Monitorovanie v online režime. Pomocou nakonfigurovanej tabuľky WATCH skontrolujeme potrebné parametre (nastavenie hodnôt na čítanie, resp. zápis údajov, napr. pre zariadenie RFID).
- Kontrola spustenia, čítania, resp. zápisu dát (napr. prostredníctvom funkcie DATALOGGER) z automatizovaného pracoviska na báze technológie RFID (či inej). Krok zahŕňa aj možnosť nulovania či resetovania procesu.

Konfiguračný proces zariadenia IO-Link Master

Konfiguračný proces bol realizovaný priamo na automatizovanom výrobnom systéme FESTO FMS 500. Cieľom tohto konfiguračného procesu bolo experimentálne overenie a následné testovanie spoľahlivosti parametrizácie s dôrazom na využiteľnosť jednotlivých funkcionalít spolu s možnosťou optimalizácie samotného procesu v závislosti od výrobcu zariadenia IO-Link Master. Na tieto činnosti nadväzuje získanie, spracovanie a agregácia dát o stave automatizovaného pracoviska v reálnom čase. Jedným z dôvodov je potreba monitorovania procesov s cieľom prediktívnej údržby, ako aj stratégie digitálnej transformácie Slovenska [3]. Súčasný manažment prediktívnej údržby totiž vyžaduje zdieľanie dát o stave automatizovaného pracoviska v spoločnej i vzdialenej ethernetovej sieti, čo možno realizovať vďaka webovému serveru.



Obr. 3 Príklad spojenia so zariadením IO-Link Master prostredníctvom webového servera

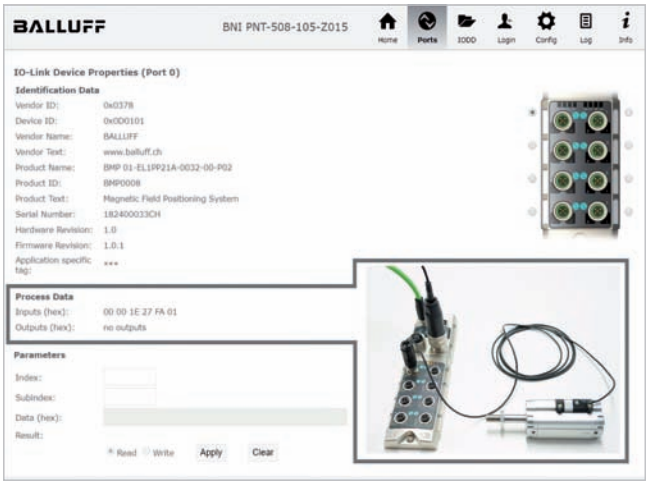


Obr. 4 Monitorovanie parametrických dát na vybranom porte zariadenia IO-Link Master

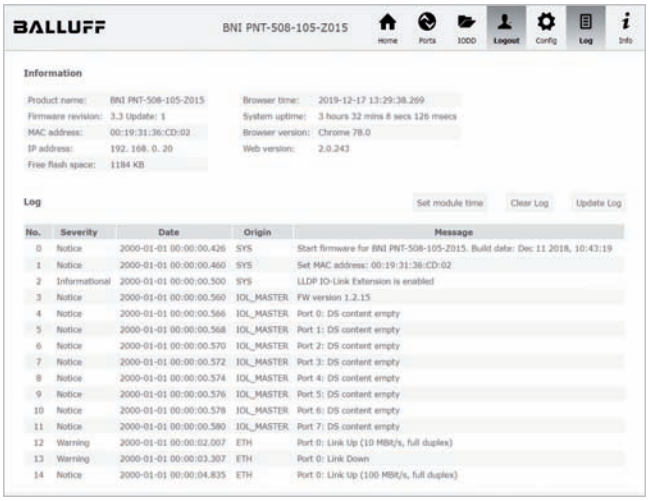
Prístup k monitorovacím a diagnostickým funkciám zariadenia IO-Link Master bol realizovaný prostredníctvom protokolu SNMPv1, ktorý je založený na IP adresácii cez ethernetovú sieť. Prístup je zabezpečený prostredníctvom prehliadača SNMP alebo bežných aplikácií na správu siete (obr. 3). Predpokladom je korektná sieťová konfigurácia (maska podsiete, Gateway adresa, meno zariadenia, podporované webové prehliadače).

Priamo v zariadení IO-Link Master je integrovaný webový server, nie je potrebná ďalšia inštalácia softvérového produktu tretích strán. Prostredníctvom zadania IP adresy pristupujeme k dátam. Vieme ich čítať, ale aj zapisovať konfiguračné parametre zariadenia IO-Link [4]. Indexy parametrov a subindexy potrebné na selekciu dát vybraného zariadenia IO-Link Master sú opísané v návode k zariadeniu (indexácia sa realizuje s ohľadom na konvencie IO-Link). Dialóg s prístupom k parametrickým dátam prostredníctvom karty „Port“ ilustruje obr. 4.

Na druhej strane procesné dáta sa zbierajú prostredníctvom zariadenia IO-Link Master a prenášajú z pripojeného zariadenia IO-Link (napr. zo senzora) cyklickým spôsobom v dátových rámcoch (obr. 5). Veľkosť týchto dát je špecifikovaná daným typom pripojeného zariadenia IO-Link. V závislosti od toho môžu mať tieto procesné dáta veľkosť od 0 do 32 bajtov (pre každý vstup a každý výstup). Zloženie prenášaných dát nie je fixné a závisí od zariadenia Master. Dátami rozumieme merané parametre, identifikačné dáta či diagnostické informácie. Dáta môžu byť zapísané do zariadenia (Write – zápis) alebo získané zo zariadenia (Read – čítanie).



Obr. 5 Nastavenie procesných dát na vybranom porte zariadení IO-Link Master



Obr. 6 Zaznamenané udalosti s časovou značkou na vybranom zariadení IO-Link Master

Obr. 7 Nahranie súboru IODD pre pripojené zariadenie IO-Link Master

Na karte „Log“ sú všetky udalosti zariadenia IO-Link Master zaznamenané a datované časovou značkou, čo umožňuje rýchlo diagnostikovať všetky udalosti alebo chyby systému, ktoré sa môžu na zariadení vyskytnúť.

Príklad histórie udalostí v zariadení IO-Link Master je na obr. 6. Všetky zmeny či varovania sú tiež zaznamenávané (napr. ak bolo zariadenie odpojené a znovu pripojené, resp. nastala nejaká zmena v nastavení parametrov IP adresy a pod.). Webový server umožňuje aj nastavenie systémového času zariadenia IO-Link Master pomocou Set module time. Parametre a procesné údaje sú k dispozícii na karte IODD (obr. 7). Prístup k nim je možný iba pomocou prihlasovacieho mena a hesla na zariadení Master. Každý súbor IODD pre zariadenie IO-Link sa nachádza na webovej stránke výrobcu. Stiahnutie príslušného adresára obsahuje nielen súbor xml s potrebnými údajmi, ale aj obrázky produktu. Stiahnuté súbory by mali byť premenované podľa presného typu zariadenia IO-Link (napr. BA0D0101.xml, BA0D0101.png).

Porovnanie konfiguračného procesu zariadenia IO-Link Master s ostatnými výrobcami

Porovnávanie a hodnotenie zariadení IO-Link Master bolo realizované jednak s ohľadom na konfiguračný proces a jeho jednotlivé kroky, jednak z pohľadu možností monitorovania, nastavovania i zbierania dát pomocou pripojených zariadení IO-Link (ako je napr. senzor, akuátor či hlava RFID).

Komunikačné protokoly

Čo sa týka komunikačných protokolov, podpora výrobcov je rôzna. Spoločnými a najčastejšie podporovanými komunikačnými protokolmi sú PROFINET a PROFIBUS, keďže, ako je známe, komunikácia IO-Link bola primárne určená práve pre tento typ komunikačných protokolov (Balluff GmbH, Pepperl + Fuchs SE, IFM electronic GmbH, Baumer Group, Turck GMBH a iní výrobcovia). Tu sa však podpora výrobcov nekončí, v súčasnosti je už poskytované a podporované široké spektrum komunikačných protokolov, počnúc ethernetom a končiac CC-Link (ETHERNET, PROFINET, PROFIBUS, ETHERCAT, CC-Link). Výhodou týchto multiprotokolových zariadení IO-Link je ľahká integrácia do rôznych priemyselných sietí bez potreby nákupu ďalších špecializovaných podporných modulov. Možno ho teda využívať v rôznych komunikačných prostrediach.

Konfigurácia

Niektorí výrobcovia (napr. Pepperl + Fuchs SE) používajú pri konfigurácii a samotnom nastavovaní komunikácie otočné prepínače, ktoré sa nachádzajú priamo na zariadení IO-Link Master, takže možno pohodlne a ľahko nastaviť potrebný protokol či adresu zariadenia. Ďalšou užitočnou funkciou zariadenia IO-Link Master je automatické a intuitívne zapamätanie si posledného nastavenia použitej komunikačnej zbernice. Tu sa však možnosti konfigurácie nekončia. Takmer všetci výrobcovia (aspoň v určitej forme) umožňujú flexibilnú konfiguráciu (adresáciu) zariadenia IO-Link Master prostredníctvom webového servera. Táto možnosť je veľmi obľúbená a používaná pre jej široké možnosti parametrizácie, monitorovania i poskytovania diagnostických údajov pripojených zariadení IO-Link. Prístup na Master je umožnený cez štandardný webový prehliadač, resp. cez obslužný softvér výrobcu (napr. spoločnosť IFM: LR Device software – LINERECORDER). Samotný proces konfigurácie vyžaduje dostupnosť súborov IODD, ktoré poskytujú výrobcovia ku každému zariadeniu IO-Link. Tieto súbory sú potrebné na nastavovanie zariadenia aj na zobrazovanie a aktualizáciu parametrov v čitateľnom jazyku cez prehliadač. Ako potvrdzujú výrobcovia, ďalšia konfigurácia zariadenia či „portu“ už nie je potrebná.

Monitoring parametrických dát

Prihlásenie (prostredníctvom webového servera) na zariadenie IO-Link Master umožňuje monitoring parametrických dát a zobrazovanie stavov jednotlivých portov. Komunikáciou point-to-point, ktorá umožňuje výmenu dát v reálnom čase, je zabezpečená dostupnosť a presnosť získaných údajov z pripojených zariadení IO-Link. Ďalšou výhodou je vzdialené monitorovanie, ľahké a rýchle nastavenie (parametrizácia) zariadenia Master, identifikácia správneho komunikačného portu a pripojených zariadení IO-Link. Bez komunikácie IO-Link by informácia musela (niekoľkonásobne) prechádzať A/D konverziou a kým by sa dostala na spracovanie (napr. do PLC), stratila by na význame. Tu však treba spomenúť jednu zaujímavosť, niektorí výrobcovia neumožňujú plný prístup k pripojeným zariadeniam IO-Link či všetkým funkciám zariadenia Master. To je používateľovi dovolené až po riadnom zakúpení (platnej a plnej verzie) licencovaného softvéru od poskytovateľa. Monitoring parametrických dát má podporu aj pri otvorených (vlastných softvérových) programoch, ale niektorí výrobcovia uprednostňujú samozrejme svoje fabrické (uzavreté) produkty. Open source programy však mnohokrát umožňujú efektívnejšiu spoluprácu (a možnosti) v kombinácii s ľubovoľným hardvérom.

Nastavenie procesných dát

Rozsah nastavenia procesných dát vo veľkej miere závisí od pripojeného zariadenia IO-Link a možností, resp. schopností samotného zariadenia Master. Všetci výrobcovia však podporujú cyklickú výmenu dát medzi zariadením Master a pripojeným zariadením IO-Link (Slave). Rozdiely pri takejto výmene dát sú najmä v reakčnom čase a rýchlosti ich aktualizácie (súvisí to najmä s množstvom dát, ale aj pripojeným zariadením). V nadväznosti na ich spracovanie treba počítať s optimalizáciou, grafickou vizualizáciou i exportom, napr. vo forme MS Excel tabuľky. Konečným cieľom spracovania procesných dát je jednoduché a jasné zobrazenie procesných hodnôt. Z pohľadu obsahu procesných dát treba špecifikovať výrobcu a typ pripojeného zariadenia IO-Link a na základe toho definovať, či budú procesné dáta obsahovať informácie o vstupoch/výstupoch, o pozícii lineárneho vedenia, o hodnotách tlaku snímača či z hlavy RFID.

Zaznamenané a datované udalosti (stavy, eventy, poruchy)

Všetky zmeny vplývajúce na činnosť a výkon pripojených zariadení IO-Link aj na samotné zariadenie Master sú zaznamenávané a logované pre potreby nadradených systémov (napr. pre PLC), resp. diagnostiky a prediktívnej údržby automatizovaného pracoviska. Procesná postupnosť zberu týchto zmien sa začína od pripojených zariadení a postupuje na zariadenie Master. Príkladom zmien môže byť napr. pripojenie/odpojenie zariadenia, prehriatie či skrat. Rozsah monitorovacích zmien závisí od výrobcu zariadenia IO-Link. Rozhodujúcimi údajmi sú často chybové kódy, problémy konfigurácie, problémy s prístupom na zariadenie Master a pod.

Záver

Monitorovanie procesných aj diagnostických dát technológiou IO-Link poskytuje široký rozsah nepretržitej spätnej väzby o zdraví, funkčnosti a stave pripojených zariadení IO-Link (senzor, hlava RFID apod.) i samotného zariadenia Master. Treba však zohľadniť špecifiká jednotlivých výrobcov, najmä čo sa týka úrovne zhromažďovania zbieraných dát, ktoré sa v ďalších procesoch musia nevyhnutne upravovať do zrozumiteľnej formy (číselná, grafická, vizuálna reprezentácia). Možnosti spracovania dát sa neobmedzujú iba na tzv. fabrické riešenia, keďže protokol IO-Link je otvorený a nezávislý od priemyselnej zbernice. Navyše podporuje kombinované využitie fabrického hardvéru a nezávislého softvérového spracovania dát.

Poďakovanie

Tento príspevok vznikol vďaka podpore v rámci projektu VEGA 1/0330/19 Výskum a návrh algoritmov a systémov pre fúziu rôznorodých dát v multisenzorových architektúrach.

Literatúra

[1] Vagaš, M. – Galajdová, A. – Šimšík, D.: IO-Link field parameterization for data collection based on RFID technology. In: Cybernetics & Informatics (K&I): 30th International Conference. Velké Karlovice, Czech Republic. p. 1 – 6. ISBN 978-1-7281-4381-1.

[2] e-F@ctory. Mitsubishi Electric systémy pre monitorovanie a riadenie procesov. [online]. Dostupné na: https://simap.sk/eafctory/.

[3] Stratégia digitálnej transformácie Slovenska 2030. [online]. Dostupné na: https://www.mirri.gov.sk/sekcie/informatizacia/digitalna-transformacia/strategia-digitalnej-transformacie-slovenska-2030/index.html.

[4] Balluff. S IO-Link k vylepšeniu kvality procesov. Dostupné na: https://www.balluff.com/local/sk/industries-and-solutions/solutions-and-technologies/io-link/.

doc. Ing. Marek Vagaš, PhD.
prof. Alena Galajdová, PhD.

Technická Univerzita v Košiciach
Strojnícka fakulta
Katedra automatizácie a komunikačných rozhraní
Park Komenského 8
042 00 Košice
Tel.: +421 55 602 3163
marek.vagas@tuke.sk

EtherCAT (2)

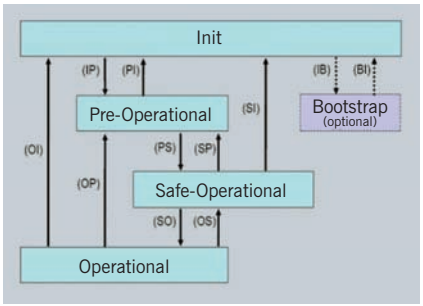
Výber správnej komunikačnej technológie je dôležitý a určuje to, či sa výkon riadenia dostane k prevádzkovým zariadeniam a akčným členom a aké zariadenia pritom možno použiť. V seriály článkov si predstavíme technológiu priemyselného ethernetu EtherCAT.

V predchádzajúcej časti seriálu *(ATP Journal 5/2021)* sme sa venovali začiatkom vzniku zbernice EtherCAT, organizácii EtherCAT Technology Group, metóde spracovania rámcov On the Fly, topológii tejto zbernice, skladbe rámcov (frame), synchronizácii, diagnostike a lokalizácii porúch, ako aj výhodám zbernice EtherCAT. V tejto časti sa budeme venovať opisu ďalších vlastností, ktoré čitateľom pomôžu správne pochopiť fungovanie EtherCAT-u. Hlavnou témou je stavový automat EtherCAT-u (tzv. EtherCAT State Machine), ďalej spomenieme jednotlivé protokoly, ktoré EtherCAT vie do seba zahrnúť, a opíšeme ich význam a možnosti použitia. Nadviažeme aj na informácie z predchádzajúceho dielu a detailne opíšeme synchronizačné skupiny (Sync Units), predovšetkým prácu s nimi, ich význam aj zmysel použitia.

EtherCAT State Machine (ESM)

Stavový automat EtherCAT-u je definovaný základnými stavmi Init, Pre-OP, Safe-OP a Operational. Špeciálnym stavom je BootStrap, ktorý slúži na prenos firmvéru. Základné pravidlá fungovania ESM sú zhrnuté v nasledujúcich bodoch:

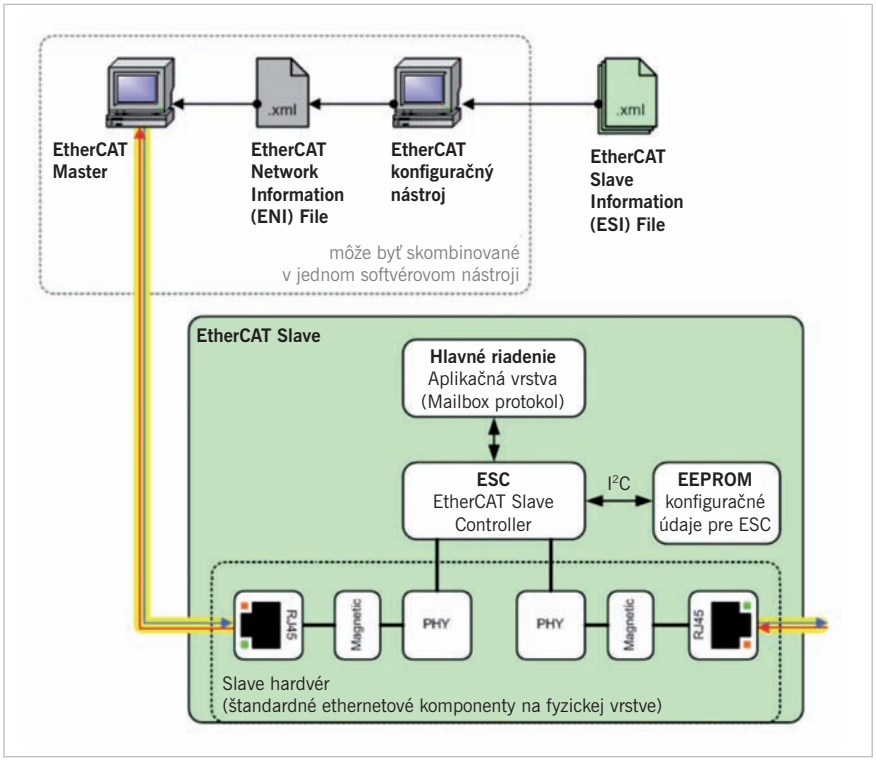
- EtherCAT Slave nasleduje stav svojho EtherCAT Master,
- EtherCAT Slave nemôže zotrvávať vo „vyššom“ stave než jeho master,
- master odovzdáva jednotlivým slave požiadavky, v akom stave sa majú nachádzať,
- master kontroluje, či sú všetky slave v príslušnom stave,
- smerom hore vedie cesta len pomocou prechodov cez jednotlivé kroky (vynechanie stavu nie je možné),
- smerom nadol je zmena možná na akýkoľvek nižší stav priamo (stavy možno preskakovať),
- stav je pretrvávajúca vlastnosť EtherCAT Slave (nežiaduce zmeny sú zaznamenané ako poruchy),
- dôležité sú prechodové deje medzi jednotlivými stavmi.



Obr. 5 Schéma EtherCAT State Machine

Pri zmene stavu treba splniť príslušné požiadavky, ktoré prechod do nasledujúceho stavu podmieňujú. Poruchy nastávajú spravidla počas prechodových dejov. Preto si na pochopenie diagnostiky jednotlivé stavy opíšeme a v poslednom diele tohto seriálu na uvedené informácie nadviažeme.

Pre názornosť je dobré pripomenúť si typickú schému EtherCAT Slave, ktorá už bola uvedená v predchádzajúcom diele tohto seriálu. Z pohľadu funkcie EtherCAT je hlavným prvkom EtherCAT Slave Controller (ESC). Naň je naviazaná pamäť typu EEPROM. Záleží na type ESC a celkovom riešení EtherCAT Slave, ale samotnú funkciu EtherCAT Slave spravidla riadi ďalší mikroprocesor. To je ďalší procesor, s ktorým treba vytvoriť komunikáciu. Všetky opísané časti majú svoju nezameniteľnú úlohu a internú nadväznosť jedna na druhú a celkovo externú nadväznosť z pohľadu komunikácie celého zariadenia EtherCAT Slave voči EtherCAT Master. Jednoducho povedané, najskôr treba pomocou pamäti EEPROM inicializovať ESC a spustiť jeho väzbu na EtherCAT Master. Potom treba sprevádzkovať komunikáciu ESC s mikroprocesorom



Obr. 6 Schéma EtherCAT Slave

a opäť aj túto väzbu pomocou prostredníka ESC sprístupniť pre EtherCAT Master. To je v skratke a laicky opísané fungovanie tohto procesu, ktorý je v princípe zastrešovaný spomínaným stavovým automatom, teda EtherCAT State Machine.

Ako už bolo povedané, zariadenie slave rešpektuje či nasleduje stav svojho mastera. Preto je tiež logické rozlišovať aj stavový automat EtherCAT-u z hľadiska EtherCAT Master a EtherCAT Slave, pretože pre každého z nich daný stav znamená iné činnosti, iné odpovede, iné detegované chyby a pod.

Init

Z hľadiska EtherCAT Master ide o kompletnú inicializáciu predovšetkým adresných registrov a ak je implementovaný, inicializuje sa aj mechanizmus distribuovaných hodín. V komunikácii medzi master a slave vyčíta master z ESC VendorID kód produktu, prípadne sériové číslo. Všetko bolo pôvodne uložené v pamäti EEPROM.

Z hľadiska EtherCAT Slave dochádza k vytvoreniu internej komunikácie medzi ESC a mikroprocesorom (tzv. Host Controller). O túto dátovú výmenu sa starajú dve synchronizačné jednotky, SyncManager0 a SyncManager1, ktoré sú súčasťou EtherCAT Slave Controller. Pre mailbox komunikáciu tieto dve jednotky oddelene komunikujú vstupné a výstupné údaje z mailbox komunikácie. Dátová časť je však pre obe spoločná. Master má prístup len k registrom EtherCAT Slave Controller.

Ak sú na EtherCAT použité distribuované hodiny na synchronizáciu údajov, práve v stave Init dochádza ku kontrole a nastaveniu príslušných časových offsetov zmeraných pomocou minimálne 15 000 rámcov EtherCAT, ktoré za týmto účelom prejdú topológiou ešte za stavu Init.

Pre-Operational (Pre-OP)

Počas prechodu z Init do Pre-OP dochádza ku kontrole, či bola interná mailbox komunikácia vytvorená korektne. Dochádza k parametrizácii komunikácie procesných dát, nakoľko pri zmene nastavenia mohol byť zmenený rozsah procesných dát. Mapovanie procesných dát spadá pod mechanizmus Fieldbus Memory Management Unit (FMMU) a je realizovaný zvyšnými dvoma Sync Manager EtherCAT Slave Controller. Každý z týchto Sync Manager sa stará o výmenu jednej skupiny dát. Inými slovami, vstupné a výstupné procesné dáta sú od seba oddelené, pretože SyncManager 2 komunikuje výstupné dáta a SyncManager 3 komunikuje vstupné dáta. Na rozdiel od mailbox komunikácie sú na vstupné a výstupné procesné dáta vymedzené dve samostatné pamäťové oblasti.

Funkčný stav Pre-OP znamená úplne funkčnú mailbox komunikáciu od EtherCAT Master po mikroprocesor (Host Controller). Túto komunikáciu sprostredkúva EtherCAT Slave Controller. Procesné dáta v tomto stave ešte nie sú komunikované.

Safe-OP (Safe-Operational)

Prechodom z Pre-OP do Safe-OP nadobudne platnosť adresácia a overí sa jej funkčnosť nastavená v predchádzajúcom stave. Reč je predovšetkým o kontrole nastavení a plnej funkčnosti jednotlivých Sync Managers. Funkčný Safe-OP mód znamená kompletný a funkčný prenos mailbox komunikácie a vstupných procesných dát. Hodnoty vstupných procesných dát sú cyklicky aktualizované. Popri tom sú do EtherCAT Slave doručené aj hodnoty výstupných procesných dát, zostávajú však v bezpečnom stave a nie sú prenášané na fyzické výstupy. Ak je použitá synchronizácia pomocou mechanizmu distribuovaných hodín, potom je už v stave Safe-OP plne funkčná.

Operational (OP)

Prechod do stavu Operational prakticky znamená, že už prenášané, teda známe hodnoty výstupných procesných dát začnú byť razom prenášané aj na fyzické výstupy daného EtherCAT Slave. Stav OP zodpovedá plne funkčnému zariadeniu EtherCAT Slave. Kompletne sa prenáša všetka komunikácia vrátane výstupných procesných dát. Pre diagnostiku funkčného stroja je kontrola tohto stavu pri všetkých zariadeniach v topológii základným ukazovateľom. Treba podotknúť, že stav Operational je nutnou podmienkou funkcie zariadenia a vzťahuje sa na problematiku ESM. Neznamená to však, že zariadenie v stave OP nemôže detegovať iný typ poruchy. Preto treba brať stav Operational z pohľadu diagnostiky v súvislosti so všetkými ostatnými ukazovateľmi.

Bootstrap

Ide o špeciálny režim prístupný iba zo stavu Init. Slúži na aktualizáciu firmvéru daného EtherCAT Slave. Neprenášajú sa žiadne procesné dáta. Funkčná je len mailbox komunikácia, predovšetkým pre protokol FoE (File over EtherCAT).

Protokoly EtherCAT (CoE, EoE, FSoE, AoE, SoE…)

Ďalšou dôležitou vlastnosťou EtherCAT-u je možnosť integrovať do dátového priestoru EtherCAT Frame aj iné protokoly. Táto vlastnosť nie je bezpredmetná, ide o praktické rozšírenie. Konfiguráciu, diagnostiku a prístup k registrom slave zariadenia zabezpečuje acyklická komunikácia, ktorá je založená na mailbox protokole. Mailbox protokol je potvrdzovaná, spoľahlivá a diagnostikovaná komunikácia.

Vzhľadom na potrebu obslúžiť veľmi široké spektrum slave zariadení (od digitálnych signálov cez analógové a enkodérové signály až po servomenič a safety zariadenie) a šírku rôznych typov aplikačných vrstiev boli definované nasledujúce komunikačné protokoly. Mailbox komunikácia nie je povinná pre všetky typy slave zariadení, na jednoduché a základné spracovanie digitálnych signálov nie je potrebná vôbec. Mailbox komunikácia neznamená ucelený balíček. Vždy podľa typu zariadenia a individuálnych potrieb EtherCAT Slave sú implementované len konkrétne typy protokolov.

CoE (CANopen over EtherCAT)

Prostredníctvom CoE je v rámci EtherCAT plne implementovaná CAN Open komunikácia definovaná štandardom EN 50325-4, ktorý definuje Object Dictionary, PDO mapping (Process Data Objects) a komunikáciu SDO (Service Data Objects). Podporované je aj rozšírenie štandardu CAN Open, napr. implementovaného profilu CiA 402 na riadenie servomeničov.

EoE (Ethernet over EtherCAT)

Vďaka EoE možno prostredníctvom procesných dát EtherCAT prenášať štandardné ethernetové správy, teda čokoľvek zo sveta IT založeného na spojení TCP/IP. Prakticky takýto prenos dát zodpovedá použitiu tunelov. Ethernetové zariadenia sú s topológiou EtherCAT prepojené pomocou tzv. switchportov, ktoré vedia fragmentovať a defragmentovať ethernetové správy „do“, prípadne „z“ EtherCAT Frame. EtherCAT Master a switchport tvoria druhú (linkovú) vrstvu modelu OSI, keď sú ethernetové správy odosielané na konkrétne MAC adresy jednotlivých zariadení, možno prenášať tiež akékoľvek internetové dáta (webové servery, e-maily, FTP spojenia…).

SoE (SERCOS over EtherCAT)

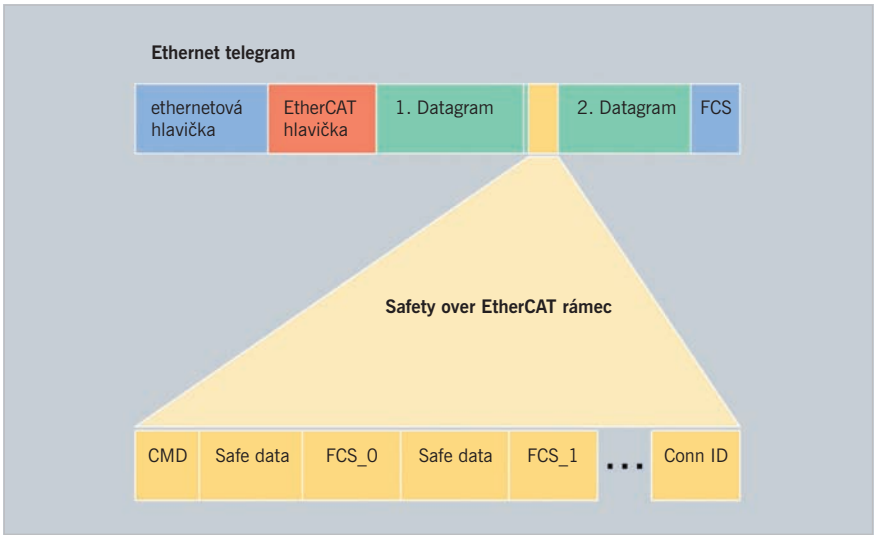
SERCOS je uznávaný komunikačný štandard vo svete motion aplikácií. Mailbox komunikácia môže pomocou SoE zahŕňať aj servisný prístup k parametrom a funkciám servomeničov.

FoE (File over EtherCAT)

Prenos súborov pomocou dát EtherCAT má význam predovšetkým pri prenose firmvéru do zariadenia EtherCAT. Zariadenia EtherCAT Slave spravidla nemajú implementované žiadne ďalšie rozhranie. Preto je aj FoE ďalším dôležitým protokolom, pretože bez ďalšieho rozhrania by aktualizácia firmvéru nebola možná.

FSoE (Fail Safe over EtherCAT)

Z hľadiska strojnej bezpečnosti je integrácia prenosu dát pre certifikované bezpečnostné zariadenie úplne zásadná. O tento prenos sa stará protokol FSoE, ktorý svoj názov dostal podľa základného bezpečnostného princípu Fail Safe. Certifikované bezpečnostné zariadenie, či už to sú rôzne skenery alebo servomeniče s integrovanými bezpečnostnými funkciami, musí voči Safety CPU prenášať dáta bezpečnou cestou. Priemyselné zbernice samotné sú so svojou chybovosťou o rád vyššie, než súčasné najvyššie štandardy vyžadujú. Preto možno do takej zbernice implementovať mechanizmus, ktorý zabezpečí spoľahlivý a kontrolovateľný prenos dát do pripojeného bezpečnostného zariadenia.



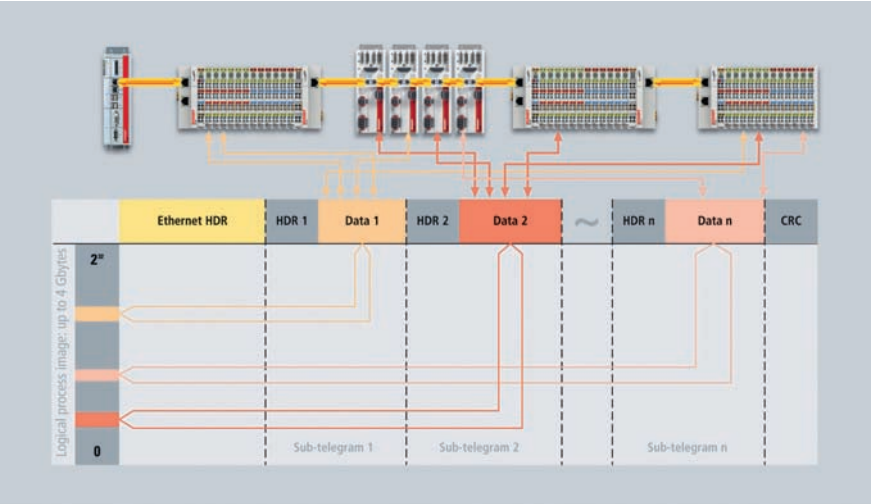
Obr. 7 Protokoly EtherCAT: ukážka integrácie protokolu FSoE

Start-Up List

Už bolo uvedené, že protokol CoE slúži aj na parametrizáciu zariadenia EtherCAT. Parametre sa ukladajú do pamäti EEPROM napojenej na EtherCAT Slave Controller každého zariadenia (obr. 6). Parametre zariadenia sú teda naviazané na dané fyzické zariadenie a možno ich meniť pomocou mailbox komunikácie a opakovane prepisovať. Pri výmene zariadenia je žiaduce, aby nové fungovalo ako to predchádzajúce. Práve vďaka parametrizácii cez protokol CoE je to možné. V riadiacom systéme možno nastaviť všetky parametre tak, aby pri prípadnej výmene zariadenia EtherCAT systém pomocou CoE prepísal všetky parametre na požadované hodnoty. Zoznamu s takými parametrami môžeme hovoriť napr. Start-Up List a bez problémov ho môžeme aplikovať aj vo veľmi komplexných zariadeniach, ako sú napr. servomeniče, kde sú oproti východiskovému stavu prednastavené desiatky parametrov.

Synchronizační skupiny (Sync Units)

V úvodnom diele tohto seriálu sme opísali zloženie EtherCAT Frame. Takže už vieme, že dátovú časť EtherCAT-u delíme na tzv. datagramy, a tiež to, že jednotlivé datagramy sú riadené EtherCAT COMMAND, ktorých je viac typov. Aby sme pochopili význam synchronizačných skupín, sú pre nás dôležité Command, ktoré obsluhujú procesné dáta. (Pre úplnosť sú to Command: LRD – Logical Read, LWR – Logical Write, LRW – Logical ReadWrite.) Z uvedeného zoznamu vyplýva, že tieto základné dátové jednotky obsluhujú buď skupiny čisto vstupných dát, čisto výstupných procesných dát, prípadne môžu obslúžiť zariadenia, ktoré dáta čítajú aj zapisujú. Dátová skladba každého datagramu je nasledujúca. Obsahuje samozrejme hlavičku, ďalej dátovú časť, ktorú reprezentujú práve procesné dáta vstupov a výstupov. Poslednú časť datagramu tvoria 2 Byte pre kontrolný mechanizmus, ktorému hovoríme Working Counter. Opis detailného fungovania tohto mechanizmu nechajme na záverečný diel nášho seriálu, kde opíšeme pravidlá fungovania na úrovni zariadení EtherCAT Slave a samozrejme vyhodnotíme tento mechanizmus zo strany EtherCAT Master. Ruka v ruke s diagnostikou ide aj to, že celá topológia EtherCAT môže byť rozdelená na viac skupín, čo má dôležitý funkčný význam. Záleží na tom, či toto rozdelenie vytvorí EtherCAT Master alebo sa do vytvorenia logických celkov vloží sám používateľ. Praktický význam vytvorenia synchronizačných skupín spočíva v tom, že vzniknú uzavreté, spravidla používateľom vytvorené funkčné a logické celky, ktoré nebudú funkčne ovplyvnené problémom týkajúcim sa inej synchronizačnej skupiny.



Obr. 8 Ukážka rozdelenia procesných dát medzi viacerými datagramami EtherCAT

Aby sme to pochopili správne, uveďme príklad: používateľ rozdelí vstupy aj výstupy z hlavného rozvádzača, zároveň definuje synchronizačnú skupinu pre safety prvky a do samostatných synchronizačných skupín zahrnie aj jednotlivé funkčné skupiny stroja. Ak dôjde k poruche komunikácie v jednej z funkčných častí (napr. k odpojeniu alebo poškodeniu kábla EtherCAT alebo k výpadku ovládacieho napájania), bude sa tento výpadok týkať len dotknutej časti a všetky ostatné skupiny zachovajú plnú funkčnosť a budú všetky dáta správne komunikovať, vyhodnocovať aj diagnostikovať.

Dôležité je pripomenúť informáciu z minulého dielu, že každý EtherCAT Frame vždy prechádza celou topológiou, ktorá je definovaná v rámci daného EtherCAT Master. To, že je jedna časť neprístupná alebo že v tejto časti topológie dochádza k problému, neznamená, že dôjde k výpadku celku. EtherCAT Frame má možnosť vrátiť sa k EtherCAT Master a tým obslúžiť dostupnú časť topológie EtherCAT. V takom prípade nedochádza k strate EtherCAT Frame, ako sa niekedy mylne uvádza.

Možné logické celky na tvorbu synchronizačných skupín:

- oddelenie logických celkov, ako sú hlavné rozvádzače a pridružené menšie rozvádzače stroja,
- oddelenie operátorských pultov,
- oddelenie funkčných celkov stroja,
- oddelenie riadenia motion častí,
- oddelenie bezpečnostných komponentov,
- oddelenie vložených komunikačných rozhraní (Profibus, PROFINET, CANopen, EtherNet/IP…),
- oddelenie častí definovaných ako Hot Connect Group.

Zdroje

[1] https://www.ethercat.org/default.htm

[2] https://www.ethercat.org/download/documents/EtherCAT_Device_Protocol_Poster.pdf

[3] https://www.beckhoff.com/

[4] https://www.youtube.com/user/EtherCATGroup/featured

Text článku bol preložený z pôvodného českého originálu.

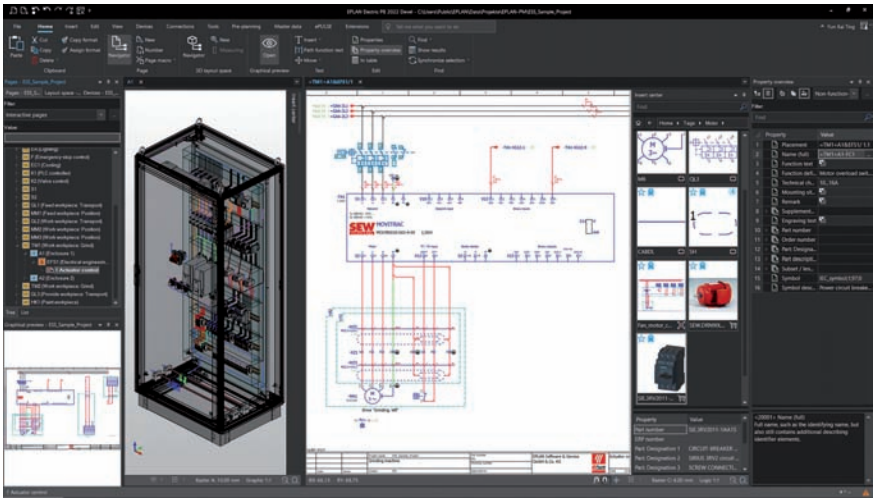
Pokračovanie v ATP Journal 7/2021.

David Smělík

Beckhoff Automation s.r.o.

EPLAN Platforma 2022 v predpremiére!

„Slávnostný výkop" prebehol na tohtoročnom veľtrhu Hannover Messe Digital Edition. Práve tu EPLAN predstavil prvý letmý pohľad na nadchádzajúcu verziu svojej platformy – EPLAN Platforma 2022 – ktorá má byť uvedená na trh v lete. Tí, ktorí očakávali jednoduchú aktualizáciu, boli prekvapení! Za novou platformou EPLAN sa skrýva nová a dôkladne prepracovaná verzia: jedná sa o kompletný balíček, ktorý sa vďaka novému používateľskému rozhraním prekvapivo ľahko používa a súčasne umožňuje plánovanie projektov na báze pracovného toku, a to na nebývalej úrovni efektivity.

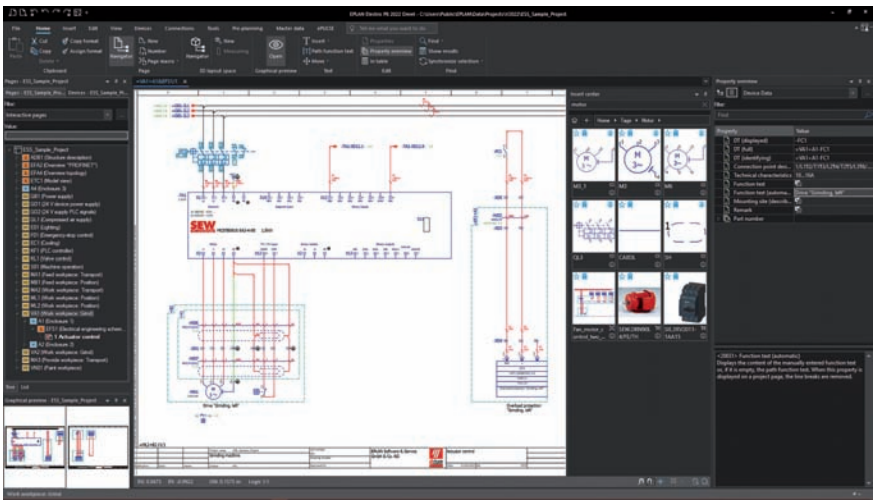


Nová EPLAN Platforma 2022 má úplne nové používateľské rozhranie. Praktický multifunkčný panel nástrojov s moderným pásom kariet sa flexibilne prispôsobuje aplikácii.

Hlavnou novinkou platformy EPLAN je úplne nové používateľské rozhranie, ktoré výrazne uľahčuje jej použitie. Dôraz sa kládol na jednoduchosť a zrozumiteľnosť, pričom vzhľad a funkcie sú založené na najmodernejších aplikáciách pre mobilné zariadenia a medzinárodne uznávaných desktopových aplikáciách. Variabilné karty umožňujú používateľom priamy prístup k dôležitým a často používaným funkciám. Praktický multifunkčný panel nástrojov s moderným pásom kariet (ribbon) sa prispôsobuje aplikácii, napr. pri prepnutí z 2D na 3D. Kombinuje tiež rôzne menu a panely nástrojov do jediného, čo uľahčuje každodennú prácu skúseným používateľom a súčasne umožňuje efektívne (opätovné) zoznámenie sa so softvérom. Okrem toho sme úplne prepracovali používateľské rozhranie na prácu v 2D aj 3D. Výsledkom je moderná aplikácia s optimalizovaným vzhľadom a ovládaním, v neposlednom rade aj vďaka podpore tmavého a svetlého režimu.

Silný výkon aj v rozsiahlych projektoch

Úplne nový grafický nástroj pre 2D zaisťuje optimálny výkon aj v rozsiahlych projektoch. Spracovanie dát je výrazne rýchlejšie, zvlášť import súborov DXF a DWG. Nová centrálna správa komponentov (artiklov) prispieva k vyššiemu výkonu, navyše ponúka flexibilitu pri prispôsobovaní údajov jednotlivých komponentov s využitím objektovo orientovanej správy údajov. Integrovaná správa variantov dovoľuje používateľom ukladať všetky vlastnosti a parametre komponentov s jednotlivými variantmi. Teraz možno komponentom ľahko a rýchlo priradiť rôzne makrá – na ľahké spracovanie externých dát, dokonca aj v kombinácii s Excelom.



Podpora svetlého a tmavého režimu typická pre moderné aplikácie optimalizuje vzhľad aj ovládanie.

Skvelý prehľad o celom projekte

Nové zobrazenie Backstage View umožňuje editovať všetky súčasti projektu EPLAN z jedného centrálneho miesta, napríklad otvárať a vytvárať projekty, importovať súbory DWG a exportovať PLC či výrobné údaje. Zoznam naposledy použitých projektov poskytuje vynikajúci prehľad o vykonanej práci – rovnako ako logické usporiadanie všetkých akcií súvisiacich s projektmi. Nové centrum zjednocuje všetky funkcie vkladania symbolov, makier a komponentov vrátane grafického náhľadu – všetko, čo je potrebné na efektívne vytváranie schém. Často používané komponenty môžete označiť ako obľúbené a priradiť ich k jednotlivým pracovným postupom.

EPLAN eMANAGE prepája platformu s cloudom

Nová EPLAN Platforma 2022, ktorá bude uvedená v priebehu tohto leta pod mottom It´s in your hands, teda Máte to vo svojich rukách, sa vyznačuje mnohými inováciami. Jednou z nich je priame prepojenie softvéru on-premise a v cloude. Aplikácia EPLAN eMANAGE teraz umožňuje nahrávať projekty z platformy EPLAN priamo do cloudového prostredia a tu ich zdieľať a spravovať. Bezplatná verzia aplikácie je dostupná od polovice marca.

Viac informácií nájdete na: https://www.eplan-sk.sk/inyourhands.

EPLAN Software & Services

www.eplan-sk.sk

Najpopulárnejšie typy programovacích jazykov PLC

Výrobné závody po celom svete sa do veľkej miery spoliehajú na riadiace systémy a programovateľné logické automaty (PLC). Tieto technológie sa neustále vyvíjajú a ruka v ruke s tým ide čoraz väčšia potreba odborníkov schopných tieto systémy programovať, podporovať a spravovať. Príležitosť naučiť sa programovať PLC posunula mnohých smerom k lepšie plateným pracovným miestam, istému pracovnému miestu a vynikajúcemu kariérnemu rastu. V nasledujúcom príspevku si predstavíme programovacie jazyky PLC, ich výhody a obmedzenia.

Medzi najpopulárnejšie jazyky na programovanie PLC patria:
- štruktúrovaný text (Structured Text – ST),
- sekvenčný funkčný (vývojový) diagram (Sequentional Function Charts – SFC),
- rebríkový logický diagram alebo jazyk kontaktných/reléových schém (Ladder Logic Diagram – LD),
- funkčný blokový diagram (Function Block Diagram – FBD),
- postupnosť inštrukcií (Instruction List – IL).

Medzinárodná elektrotechnická komisia IEC vo svoje norme 61131-3 načrtáva päť rôznych programovacích jazykov PLC: jazyk kontaktných/reléových schém, štruktúrovaný text, funkčné blokové diagramy, sekvenčné funkčné (vývojové) diagramy a postupnosť inštrukcií. Každý z týchto jazykov má výhody, slabé stránky a prípady najlepšieho použitia. Každý kompetentný programátor PLC si musí uvedomiť tieto možnosti pri riešení programovania konkrétnej aplikácie, využívať správny nástroj pre danú úlohu a mať vlastný pohľad na riešenie problémov. V závislosti od zvolenej platformy PLC môžu byť niektoré jazyky odporúčané alebo nemusia byť k dispozícii vôbec.

Pozrime sa podrobnejšie na každý z týchto jazykov, prejdime si ich aplikácie, všeobecnú štruktúru a prípady použitia.

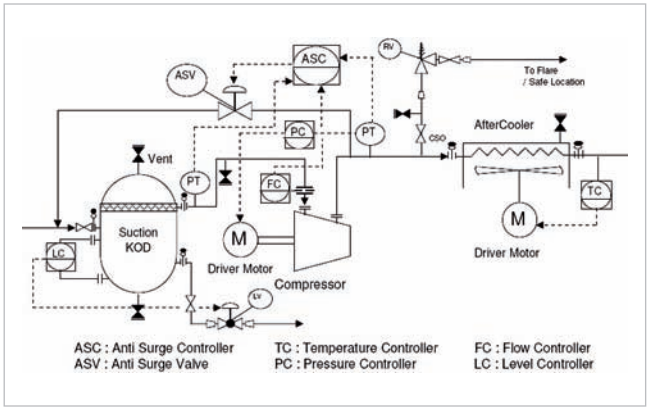
Aký je najobľúbenejší programovací jazyk pre PLC?

Táto otázka je predmetom diskusií medzi programátormi PLC po celom svete. Konsenzus je taký, že najpoužívanejším jazykom na programovanie PLC je jazyk kontaktných/reléových schém, nazývaný aj rebríková logika. Je totiž vysoko flexibilný, ľahko sa učí a veľmi dobre rozumie elektrikárom, ktorí pracovali so schémami modelujúcimi rovnakú architektúru.

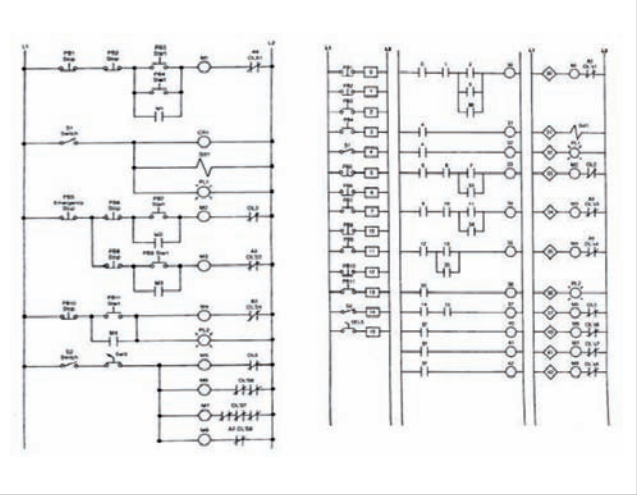
Za posledné desaťročie však do výroby vstúpila mladšia pracovná sila. Títo inžinieri a technici sa primárne učili moderné jazyky, ako sú Java, Python a Javascript keďže tieto jazyky sa viac podobajú na štruktúrovaný text. Treba však zohľadniť aj to, pre ktoré priemyselné odvetvie bude aplikácia programovaná. Vývoj aplikácií pre chemický priemysel sa zvyčajne realizuje použitím schém potrubí a prístrojového vybavenia (Piping and Instrumentation Diagrams – P&ID). Tieto schémy však možno ľahko replikovať pomocou funkčných blokových diagramov (FBD).

Kontaktné/reléové schémy

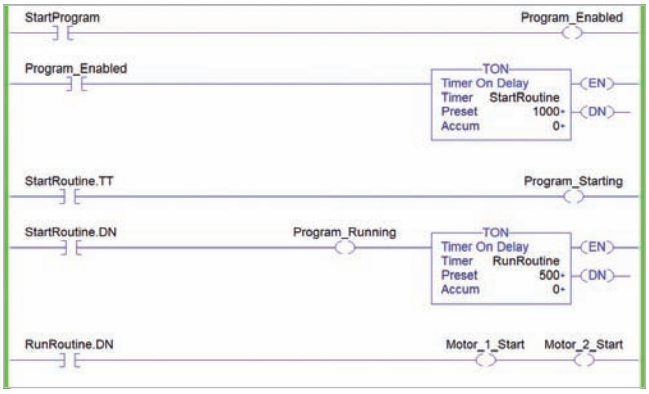
Predtým, ako sa PLC stali populárnymi, bolo riadenie vo väčšine výrobných závodov založené na štandardných relé. Relé zapínali a vypínali zariadenia na základe jednoduchej logiky, ktorá sa realizovala prostredníctvom ich fyzického spínania. Prepojenie týchto zariadení bolo špecifikované na elektrotechnických výkresoch, ktoré predpokladali usporiadanie pripomínajúce rebrík. Po zavedení prvých PLC do prevádzok sa objavilo aj ich programovanie cez



Obr. 1 Príklad chemického procesu, ktorý by sa dal ľahšie implementovať do PLC naprogramovaním funkčných blokov (FBD).



Obr. 2 Schémy vedúce k programovaniu PLC prostredníctvom kontaktných schém



Obr. 3 Programovacie jazyky PLC – príklad programovania PLC v LD v rámci riadiaceho systému RSLogix 5000

kontaktné schémy, ktoré napodobňovalo rozloženie obvodov založených na relé. Inými slovami, logika kontaktných schém (rebríka) bola jedným z prvých programovacích jazykov PLC, ktorý sa dnes kvôli jednoduchosti stále používa.

Od svojho vzniku sa programovanie cez kontaktné/reléové schémy výrazne vyvinulo. Základné princípy fungovania však zostávajú rovnaké. Programovanie PLC cez LD vyhodnocuje každú „priečku rebríka“ v postupnom poradí a hodnotí podmienkové inštrukcie. Ak je výsledok vyhodnotený ako „TRUE“, vykonajú sa výstupné inštrukcie.

Výhody programovania PLC v LD

- Jednoduché na implementáciu a riešenie problémov – LD je vizuálny jazyk, ktorý poskytuje potvrdenie stavu pre väčšinu inštrukcií. Inými slovami, aj ten, kto má málo znalostí o konkrétnom procese, môže ľahko prejsť programom a pochopiť logiku.
- Modulárny dizajn – LD možno ľahko upraviť pridaním alebo odstránením logiky. Každá „priečka“ je samostatnou podmienkou a možno ju podľa potreby odstrániť alebo pridať.
- Odolnosť a konzistentnosť – LD umožňuje programátorovi implementovať mnoho funkcií. Jazyk je však veľmi „zošnurovaný“ štandardmi a neposkytuje úplnú flexibilitu, čím na druhej strane udržuje konzistenciu programu naprieč rôznymi implementáciami.

Nevýhody LD

- Nie je jednoduchý pre všetkých – LD je síce jednoduchý jazyk, ale nie je príliš intuitívny pre tých, ktorí vyrástli na jazykoch ako C, C++, Java alebo Python. Môže byť teda jednoduchší na pochopenie pre elektrotechnikov a pre tých, ktorí majú základné znalosti programovania zostáv.
- Pomalé nasadenie – kvôli vizuálnej povahe logiky v LD trvá programátorovi dlhšie, kým vytvorí logiku, ktorú potrebuje. V porovnaní s inými modernými programovacími jazykmi treba presúvať prvky, čím sa vývojový proces spomaľuje.
- Neintuitívne pre zložité aplikácie – LD je skvelým nástrojom, pokiaľ ide o sekvenčné logické úlohy. Pokiaľ však ide o modernú teóriu riadenia, ktorá zahŕňa PID, riadenie prietoku, analógové snímače a spätnoväzbové slučky, implementácia a dešifrovanie nie sú vždy ľahké.

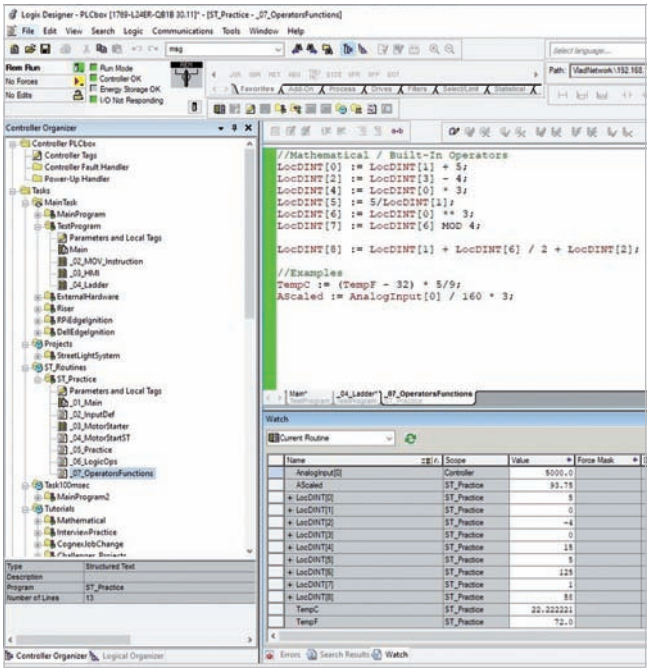
LD je najpoužívanejší programovací jazyk PLC na svete. Je ľahké s ním pracovať a udržiavať programy v ňom vytvorené pre tých, ktorí neprogramujú PLC tak často. Odporúčame vám preto začať s programovaním PLC práve pomocou LD.

Štruktúrovaný text

Štruktúrovaný text je programovací jazyk PLC, ktorý sa veľmi podobá na C alebo assembler. Programátor vytvára riadky programu, ktoré sa spúšťajú postupne, vyhodnocuje konkrétne funkcie, booleovskú logiku a napája príslušné výstupy PLC. Štruktúrovaný text poskytuje jednoduchý prechod do sveta PLC pre tých, ktorí postavili svoje základy na tradičných programovacích jazykoch, ako je C, C++, Java alebo Python. S programom vytvoreným pomocou štruktúrovaného textu možno ľahko narábať aj v textových procesoroch, čo umožňuje jeho rýchlu implementáciu bez potreby hardvéru.

Výhody programovania PLC so štruktúrovaným textom

- Intuitívne pre iné programovacie jazyky – ako sme už spomenuli, štruktúrovaný text sa ľahko naučia tí, ktorí prichádzajú z prostredia softvérového inžinierstva. Obsahuje rovnaké štruktúry, programovacie paradigmy a funkcie, aké by človek očakával v prostredí C alebo Java.



Obr. 4 Programovanie PLC so štruktúrovaným textom – príklad z prostredia Studio 5000 pre PLC systém CompactLogix

- Vysoká komplexnosť – štruktúrovaný text umožňuje väčšiu flexibilitu ako iné jazyky a tým uľahčuje implementáciu pokročilých funkcií pre tých, ktorí tento jazyk ovládajú.
- Prenositeľnosť – štruktúrovaný text je štandardizovaný medzi väčšinou systémov PLC, čo uľahčuje migráciu medzi platformami. Medzi inými platformami nájdete značné rozdiely v iných jazykoch, štruktúrovaný text však možno implementovať do takmer všetkých hardvérových a softvérových platforiem.

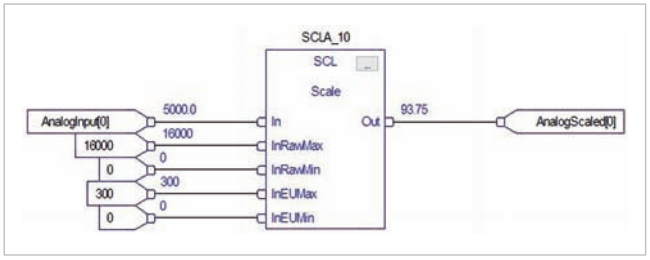
Nevýhody štruktúrovaného textu

- Ťažké riešenie problémov – v porovnaní s programom vytvoreným v LD je štruktúrovaný text z hľadiska riešenia problémov oveľa zložitejší. Neexistujú žiadne vizuálne fronty, menej vizuálnych pomôcok a zvyčajne viac programu na jednom riadku. Tí, ktorí tento jazyk až tak nepoznajú, budú mať problém zistiť priebeh procesu.
- Náchylný na chyby – štruktúrovaný text poskytuje používateľovi väčšiu flexibilitu. Cenou za ňu je však štandardizácia. Programátori musia používať osvedčené postupy v oblasti softvérového inžinierstva na vytvorenie bezpečných riešení a zachytenie potenciálnych chýb softvéru.

Ak nemáte znalosti v inom programovacom jazyku, odporúčame, aby ste sa štruktúrovaný text naučili až po zvládnutí LD. V prostredí výrobných prevádzok sa kvôli uvedeným nevýhodám programovanie prostredníctvom štruktúrovaného textu často nevidí. Je to však vynikajúci spôsob manipulácie s údajmi, implementácie cyklov FOR a ďalších štruktúr, ktoré si v LD vyžadujú viac práce.

Funkčný blokový diagram

Je programovací jazyk vyvinutý s ohľadom na požiadavky aplikácií v chemickom priemysle. Umožňuje používateľovi vytvoriť vizuálne znázornenie a priebeh procesu s príslušnými prechodmi medzi



Obr. 5 Funkčný blokový diagram – príklad škálovania analógového signálu v PLC RSLogix 5000

inštrukciami. Vizuálny editor je používateľsky prívetivý, intuitívny a ponúka prirodzený spôsob implementácie konkrétnych tokov. Najbežnejšou aplikáciou, kde sme využili tento typ programovania PLC, bolo zavedenie PID regulátorov. Vizuálny aspekt FBD umožňuje ľahkú implementáciu PID, ich vizualizáciu, ladenie a riešenie problémov priamo v prevádzke.

Výhody programovania PLC pomocou FBD

- Flexibilný vizuálny editor – editor programovania funkčných blokových diagramov je veľmi používateľsky prívetivý a poskytuje jednoduchý spôsob vytvárania ľubovoľného rozloženia.
- Ideálne pre komplexné programovanie štruktúr – v LD bude musieť používateľ použiť viac priečok na to, čo možno dosiahnuť na jednej stránke FBD. Inštrukcie možno priamo preniesť do zložitejších foriem, ako sú napr. PID slučky, riadenie pohybu a doplnkové inštrukcie (Add-on-Instruction – AOI).
- Používateľsky prívetivý – vizuálny editor FBD je pre väčšinu používateľov prirodzený. Rozloženie procesu možno znovu vytvoriť pomocou metodiky drag-and-drop, kde je malý priestor na chybu.

Nevýhody FBD

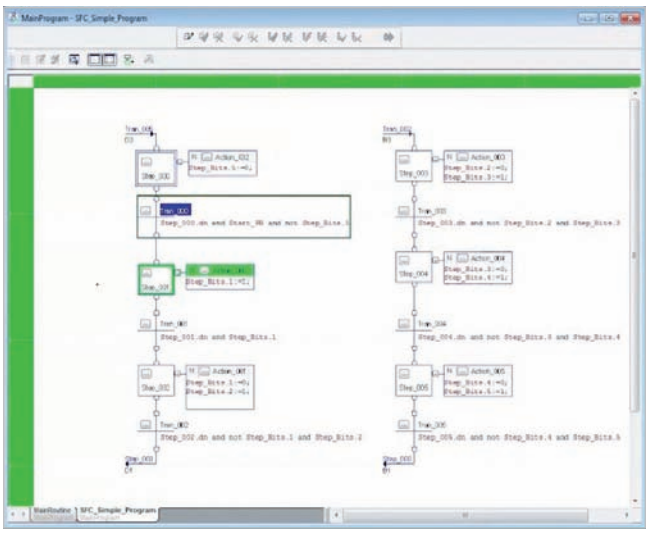
- Ťažko štandardizovateľné – vzhľadom na flexibilitu rozloženia je náročné štandardizovať programy napísané v FBD. Každý programátor PLC bude mať svoj prístup, ktorý sa líši od ostatných. Tí, ktorí prídu už k hotovému programu, budú ťažko chápať tok informácií.
- Problém v mierke – FBD je skvelý vtedy, keď ide o malé implementácie konkrétnych oblastí procesu. Čím je však program zložitejší, tým ľahšie sa v ňom stratíte.

Funkčné blokové diagramy sú veľmi vhodné na programovanie PID slučiek či sekvencií riadenia pohybu. Ak bude potrebné riešiť tieto oblasti, FBD je na to vhodný. Opäť by sme však odporučili osvojiť si programovanie v LD.

Sekvenčné funkčné (vývojové) diagramy

Ako vyplýva už z názvu, sekvenčné funkčné diagramy (SFC) sú vhodné, pokiaľ ide o procesy nasledujúce za sebou. Pre tých, ktorí si to nevedia predstaviť, môže byť príkladom chemická premena zo surovín na hotový výrobok. Vezmime si ako príklad jednoduchý proces varenia. Predstavte si veľké zariadenie na varenie piva s mnohými nádržami, ventilmi, snímačmi tlaku, vykurovacími prvkami a časťou na balenie. Keď operátor začne výrobu novej dávky, proces prejde nasledujúcou postupnosťou krokov (upozorňujeme, že tieto kroky sú zjednodušené):

- Krok 1 – systém je overený na pripravenosť. Sú k dispozícii všetky príslušné prísady? Sú nádrže prázdne? Sú ventily v správnom stave? Ak je odpoveď na všetky otázky kladná, pokračujte. Ak nie, koniec.



Obr. 6 Sekvenčné funkčné diagramy – príklad postupného procesu v PLC RSLogix 5000

- Krok 2 – spustite sekvenciu plnenia nádrže, ktorá môže vyžadovať viac prísad (voda, cukor, soľ, droždie atď.). Overte stav a pokračujte, keď je nádrž plná.
- Krok 3 – spustite proces varenia. Zvyšujte a udržujte teplotu po stanovený čas. Monitorujte tlak v nádrži a podľa toho reagujte. V prípade potreby pridajte prísady. Po dokončení varenia pokračujte ďalším krokom.
- Krok 4 – začnite presun do zadržiavacej nádrže. Naša dávka je pripravená; skontrolujte, či sú všetky príslušné ventily nastavené do správnej polohy, zadržiavacia nádrž je prázdna a začnite proces prepravy.
- Krok 5 – preneste dávku do zariadenia na plnenie do fliaš.

Z uvedeného príkladu je zrejmé, že kroky procesu sa vykonávajú postupne, majú definované začiatočné podmienky a to, ako by proces prebiehal vo výrobnom závode. V LD možno tento proces implementovať prostredníctvom inštrukcie SQI/SQO. Lepším prístupom by však bolo využitie SFC.

Výhody programovania pomocou sekvenčných diagramov

- Napodobovanie procesných tokov väčšiny chemických procesov – dávkovanie je bežný chemický procesný prístup, ktorý vyžaduje stanovené množstvo surovín a transformuje ich na konečný produkt. Pre takéto typy aplikácií je SFC jednotkou.
- Možnosť kombinácie s ST – väčšina editorov SFC umožňuje v špecifických prípadoch použiť štruktúrovaný text na vytvorenie pokročilých logických tokov.

Nevýhody SFC

- Nepoužiteľné vo väčšine aplikácií – je náročné aplikovať sekvenčné funkčné diagramy na proces, ktorý nie je sekvenčný. Inými slovami, SFC má obmedzené možnosti použitia.
- Paralelné toky je ťažké implementovať a odstraňovať v nich problémy – v rámci SFC môžete implementovať neobmedzené množstvo procesných tokov cez SFC. Nakoľko sa procesné cesty delia na viac tokov, je ťažké implementovať samostatné cesty toku, ktoré by viedli k robustnej postupnosti.

Programovanie v SFC je v konkrétnych prípadoch mimoriadne užitočné. No ak chcete zvoliť tento prístup v rámci typu procesu, ktorý nie je postupný – sekvenčný, rýchlo zistíte, že „tadiaľ cesta nevedie“. Ak idete programovať nejakú aplikáciu z reálneho výrobného prostredia, odporúčame, aby ste sa pred samotným programovaním v SFC oboznámili s procesom, porozumeli toku produktu a pokúsili sa zostaviť model na papieri.

Postupnosť inštrukcií

Postupnosť inštrukcií sa často zamieňa so štruktúrovaným textom pre podobné editory. Tieto dva programovacie jazyky možno zvyčajne vidieť na rôznych platformách, pretože ich tok je podobný. Napríklad riadiace systémy a PLC postavené na štandarde Codesys umožňujú používateľom implementovať logiku do postupnosti inštrukcií, zatiaľ čo riadiace systémy postavené na RSLogix 5000 majú prístup iba k štruktúrovanému textu.

Pokiaľ ide o priebeh programu, každý riadok špecifikuje inštrukciu, ako aj podmienky a výsledky konania. V mnohých aspektoch je postupnosť inštrukcií podobnejšia programu vytvorenému v LD ako cez štruktúrovaný text. Každý z týchto jazykov je však schopný vytvoriť rovnaký tok procesu.

Výhody postupnosti inštrukcií

- Vysoko štandardizované – postupnosť inštrukcií je postavená na pevnej štruktúre, ktorá vyžaduje, aby používateľ explicitne vytvoril premenné, špecifikoval podmienky a uviedol zoznam všetkých inštrukcií. Medzi implementáciami programu existujú len malé variácie, čo vedie k ľahkému pochopiteľnému programu.
- Zamerané na inštrukcie – ako už napovedá názov, dôležitosť sa viac prikladá inštrukciám ako dátovému toku. Tento štýl programovania prináša jasný prehľad o spôsobe spracovania údajov v programe.

Nevýhody postupnosti inštrukcií

Programovací jazyk nie je k dispozícii na väčšine platforiem PLC – ako už bolo spomenuté, postupnosť inštrukcií nie je populárnou metódou programovania, pretože pre väčšinu programátorov je neprirodzené. Sú bližšie k tomu, čo môžeme vidieť v assembleri, a nie k inému programovaciemu jazyku na trhu.

Záver

Päť najobľúbenejších programovacích jazykov PLC sú kontaktné/reléové schémy (rebríková logika), štruktúrovaný text, funkčné blokové diagramy, sekvenčné funkčné (vývojové) diagramy a postupnosť inštrukcií. Tieto metódy programovania sú dostupné na väčšine platforiem. Niektoré PLC nemajú všetky typy dostupné v základnej verzii, ale len ako možnosť na dokúpenie.

Odporúčame, aby každý programátor PLC začínal rebríkovou logikou, pretože táto metóda je v priemysle najbežnejšia. Pretože je človek vystavený pokročilým metodikám programovania, je dôležité naučiť sa ďalšie jazyky, ktoré môžu predstavovať ľahší spôsob implementácie konkrétnych procesov.

Zdroj: Romanov, V.: Top 5 Most Popular Types of PLC Programming Languages. [online]. Citované 10. 5. 2021. Dostupné na: https://www.solisplc.com/blog/plc-programming-languages.

-tog-

Agregovaná flexibilita – kde sme a kam kráčame (2)

Agregácia je z hľadiska blížiacej sa aplikácie európskej legislatívy pre dizajn vnútorného trhu s elektrinou jedným z nových fenoménov, ktorý prinesie rozvoj služieb v oblasti riadenia spotreby, flexibility, ako aj ponuky nových produktov pri poskytovaní podporných služieb. Významne vzrastie potenciál aj využiteľnosť flexibility maloodberu vplyvom budovania pokročilej meracej infraštruktúry a systémov riadenia spotreby, nárastu elektromobility a rozvoja konceptu prosumerov. Pri využití tohto potenciálu je potrebná funkčná agregácia malých a distribuovaných zdrojov umožňujúca uplatnenie flexibility na krátkodobom trhu.

Ako sme pripravení na tieto zmeny a akými krokmi je vhodné prispôsobiť sa novej paradigme trhu? V rámci online webinára, ktorý zorganizovala spoločnosť DIGIT, s. r. o., a mediálny portál eFocus.sk pod názvom Agregovaná flexibilita – zmena paradigmy trhu s elektrinou, diskutovali:

- Blahoslav Němeček, partner EY, člen tímu poradenstva pre klientov z odvetvia energetiky v regióne strednej a juhovýchodnej Európy a moderátor podujatia,
- Ivan Trup, obchodno-technický riaditeľ, MicroStep-HDO, s. r. o.,
- Tomáš Rajčan, riaditeľ úseku energetiky a priemyslu, IPESOFT, spol. s r. o.,
- Vladislav Jurík, riaditeľ sekcie Regulácia, Stredoslovenská distribučná, a. s.,
- Richard Kabele, nezávislý konzultant,
- Ján Mišovič, riaditeľ, Nano Energies Slovensko, s. r. o.

V prvej časti seriálu sme priblížili pohľad I. Trupa na predpoklady, ktoré treba splniť, aby sa agregovaná flexibilita na trhu uplatnila, a s T. Rajčanom sme sa pozreli na flexibilitu riadenia portfólia prostredníctvom agregátora. V druhej časti prezentuje pohľad prevádzkovateľa distribučnej sústavy na túto problematiku V. Jurík. Kódexy prenosových sústav v rámci SR a ČR porovnal R. Kabele a skúsenosti z už realizovaného projektu DFLEX a potenciál agregovanej flexibility na Slovensku priblížil J. Mišovič.

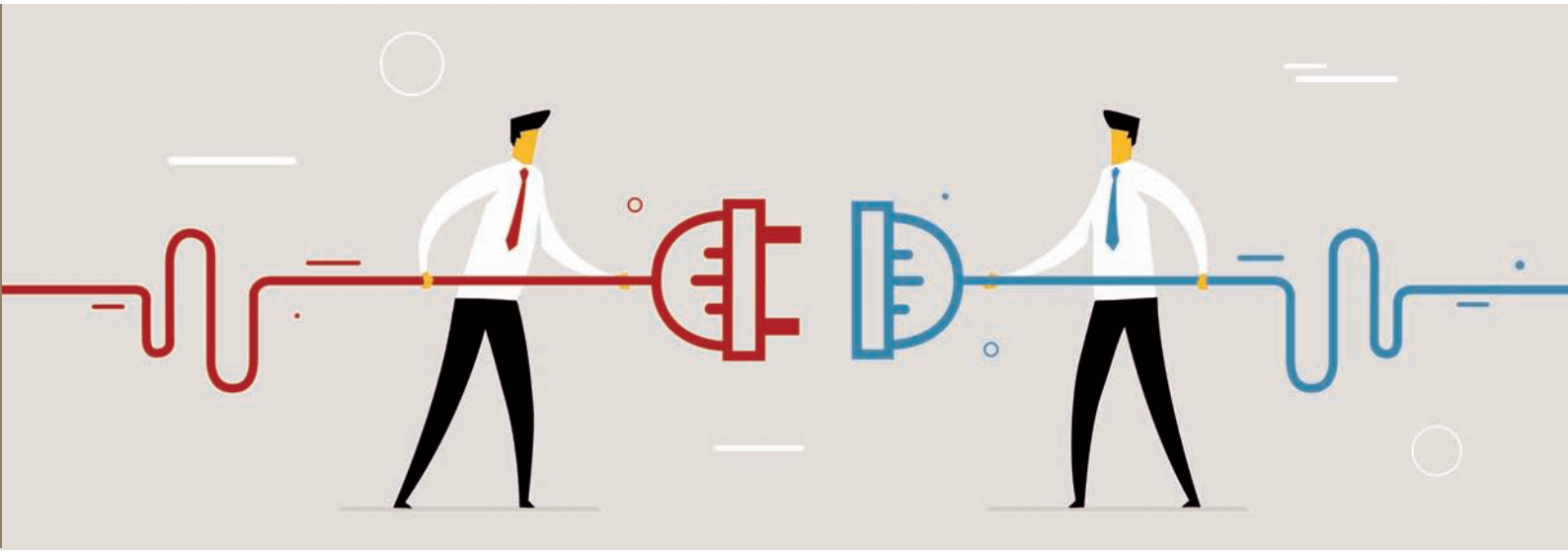
Flexibilita z pohľadu prevádzkovateľa distribučnej siete (PDS)

Vladislav Jurík

Stredoslovenská distribučná, a. s., je z hľadiska počtu odberných miest a objemu distribúcie elektrickej energie druhým najväčším PDS. No to, v čom hrá prím, je rozloha a členitosť územia, ktoré svojimi produktmi a službami pokrýva. V úvode svojho vystúpenia sa V. Jurík zameral na definíciu flexibility tak, ako ju pre PDS definovala legislatíva EÚ. V smernici 2019/944 o vnútornom trhu sa v článku 32 okrem iného uvádza, že flexibilita má slúžiť na riadenie preťaženia sústavy, efektívnosti prevádzky a rozvoja distribučnej sústavy (DS), má byť alternatívou k rozširovaniu sústavy, pričom musí byť obsiahnutá v pláne rozvoja sústavy. „Potešilo nás najmä to, že EÚ vníma flexibilitu ako alternatívu k rozširovaniu DS. Z nášho pohľadu máme vcelku jasnú predstavu o využití flexibility a uvediem k tomu len jeden príklad. Máme lokalitu, kde nie je dostatočná kapacita elektrickej energie. Vybudovanie nového vedenia by trvalo niekoľko rokov. Ak by sme v danej lokalite vedeli využiť nejakého odberateľa alebo výrobcu, ktorý by zníženým odberom alebo naopak zvýšenou výrobou vedel prispieť k riadeniu zaťaženia v tejto lokalite, zrazu by sme vedeli poskytnúť voľnú kapacitu tým, ktorí sa chcú pripojiť. V konečnom dôsledku by nebolo potrebné budovať žiadne nové vedenia a práve vďaka flexibilite by sme zvládli zabezpečiť požadovaný výkon v tejto lokalite. A takýchto príkladov môže byť podstatne viac," vysvetľuje V. Jurík. Tým by sa podarilo generovať úspory v rozvoji a prevádzke DS. Tento prístup by podľa V. Juríka fungoval v určitých lokalitách DS, nedá sa to paušalizovať na celú DS.

Ďalším legislatívnym dokumentom, ktorý sa týka problematiky vnútorného trhu s elektrinou, je nariadenie Európskeho parlamentu a Rady (EÚ) 2019/943, kde sú v článku 18 uvedené poplatky za prístup do sústav, ich používanie a posilnenie. Okrem iného sa tu uvádza, že treba zabezpečiť príslušný legislatívny regulačný rámec, že náklady na obstaranie flexibility aj na IT a infraštruktúru by mali byť kompenzované a tiež to, že náklady musia byť zohľadnené v poplatkoch PDS. „Tieto usmernenia sú dané legislatívou, ale v praxi zatiaľ nevieme povedať, ako to presne bude fungovať. Regulačný rámec je zatiaľ nejasný, nevieme, aká bude skutočná kompenzácia týchto nákladov. Podľa môjho názoru by mali byť tieto náklady zohľadňované každoročne, pričom bolo by asi dobré pozerať sa na náklady na flexibilitu ako na náklady na podporné služby. V tejto súvislosti by som rád zdôraznil jednu vec: flexibilita nie sú podporné služby. Rovnako to asi vníma aj spomínaná európska legislatíva. Sú to určité náklady, ktoré môžu byť každý rok iné. Ak má PDS flexibilitu využívať, musí byť jasne povedané, že ak si ju zabezpečí, bude ju mať aj k dispozícii, pričom náklady s tým spojené budú napr. zohľadnené v priebehu nasledujúceho roka ako oprávnené náklady a budú môcť byť premietnuté do cien," myslí si V Jurík. Využívanie flexibility podľa neho závisí primárne od nastaveného regulačného rámca.

V spomínanej smernici 2019/944, článku 32 sa tiež hovorí, že flexibilita má slúžiť na riadenie preťaženia DS. Čo to znamená z pohľadu PDS a ako to ovplyvňuje rovnováhu v sústave? Stredoslovenská distribučná, a. s., ako jeden z troch PDS pôsobiacich na Slovensku má najviac odberateľov elektrickej energie, ktorí využívajú elektrické vykurovanie. V súčasnosti sú využívané vysoké a nízke tarify za odber elektrickej energie, ktoré sú statické (time-of-use) a aplikované len pri niektorých sadzbách. ÚRSO orientačne stanovuje dobu trvania vysokej a nízkej tarify, kedy sa môže aplikovať a pod. Ceny za dodávku elektrickej energie kopírujú vysokú a nízku tarifu v týchto sadzbách. Je toto však vízia, ktorú môžeme očakávať aj v najbližších rokoch a je to súčasne aj vízia smeru rozvoja energetiky v súlade s európskou legislatívou? „Osobne si viem v budúcnosti predstaviť to, že počas dňa bude k dispozícii viac rôznych taríf a dynamické ceny za dodávku elektrickej energie, pričom vplyv statických taríf za distribúciu sa bude výrazne meniť. A prečo? Ak máme v súčasnosti nízku cenu za dodávku v nízkej tarife, zákazník je motivovaný odoberať elektrickú energiu práve v tejto nízkej tarife. Ak však PDS v budúcnosti stanoví nízku cenu v nízkej tarife za distribúciu, ale budú zavedené dynamické ceny pre dodávku elektrickej energie,



môže sa stať, že v tých hodinách, keď by PDS potreboval, aby sa zvýšil odber, bude dodávateľ poskytovať vyššiu cenu. Naopak v čase, keď sa distribútor bude snažiť obmedziť odber, bude dodávateľ ponúkať veľmi výhodné ceny. Je pravdepodobné, že v budúcnosti budeme často svedkami takýchto javov," konštatuje V. Juríк. Dôsledkom bude aj to, že HDO a prepínanie medzi nízkou a vysokou tarifou už nebude možné v takej miere využiť na riadenie preťaženia DS. Aj preto Stredoslovenská distribučná, a. s., vníma flexibilitu ako riešenie, ktoré by malo postupne nahradiť používanie distribučných taríf pre rôzne časové pásma.

Pomocou flexibility by si PDS vedel presnejšie a adresnejšie naplánovať, aký výkon potrebuje v jednotlivých hodinách, určiť, v ktorej lokalite a akú veľkú flexibilitu potrebuje, ale bude musieť za to aj zaplatiť. Uvedený systém bude teda nákladnejší. „Nevyhýbame sa využitiu flexibility aj na úrovni NN, ani to nelimitujeme. Z nášho pohľadu to má tiež svoj zmysel, a to za predpokladu, že sa to bude realizovať cez agregátora. Z pohľadu PDS si neviem predstaviť, ako by sme obehávali niekoľko stoviek či tisícok malých odberateľov a riešili s nimi flexibilitu. Cez agregátora by sme práve mohli nakúpiť celú flexibilitu z nejakej konkrétnej lokality," vysvetľuje V. Juríк. Podľa jeho názoru to celé môže dobre fungovať len vtedy, ak sa odberateľ bude zaujímať o svoje náklady, ak bude využívať možnosti spojené s flexibilitou a znižovať tak svoje náklady na elektrickú energiu.

Flexibilita využívaná v PDS a flexibilita na obchodovanie, to sú podľa V. Juríka dva hlavné smery využitia flexibility. V prvom prípade možno flexibilitu využívať ako nástroj na riadenie sústavy, či už dohodnutý vopred, alebo riadený v reálnom čase a využívaný podľa potrieb v jednotlivých lokalitách. V druhom prípade sa o flexibilite dá uvažovať ako o obchodnom nástroji na bilancovanie odchýlky dodávateľov, agregátorov či používateľov sústavy. Flexibilita na obchodovanie nereflektuje potreby sústavy a v niektorých prípadoch môže až negovať snahy PDS na bilancovanie sústavy. Navyše obchodovanie s flexibilitou bude zaťažené štandardnými javmi, ktoré sa v rámci DS dejú, ako sú napr. obmedzenia z dôvodu plánovaných odstávok, vznik porúch alebo preťaženia v rámci DS.

„Samozrejme zatiaľ nemám konkrétnu predstavu, ako by spomínané postupy mali v praxi presne fungovať a budú musieť byť predmetom širšej diskusie. No ak by som to mal zhrnúť, ako PDS vnímame flexibilitu naozaj ako jeden z kľúčových nástrojov riadenia zaťaženia sústav. Flexibilita má potenciál znížiť potrebu investícií do posilnenia vedení. Bude nepochybne vyžadovať náklady do IT riešení a na jej obstarávanie. Jej rozvoj bude závislý od nastaveného regulačného rámca. A ešte raz chcem zdôrazniť, že pozitívny dosah na ceny bude mať len pre tých používateľov sústav, ktorí budú optimalizovať svoje požiadavky voči PDS, inak povedané, ak sa budú správať racionálne a hľadať spôsoby, ako znižovať svoje náklady na spotrebu elektrickej energie," konštatuje V. Juríк. Veľkým problémom z hľadiska rozvoja flexibility a uplatnenia jej celého potenciálu na trhu je ešte stále nezáujem zo strany používateľov DS. Väčšina z nich sa podľa V. Juríka nespráva racionálne, nesledujú, v akej distribučnej sadzbe, a to aj na úrovni NN, sa nachádzajú. Pritom by vedeli ušetriť zaujímavú časť svojich nákladov za spotrebu nielen elektrickej energie, ale aj vody či plynu. Tento stav demonštruje aj fakt, že zo 130 000 odberných miest, kde Stredoslovenská distribučná, a. s., nainštalovala inteligentné meracie systémy, sa o svoje náklady na elektrickú energiu zaujíma a rieši ich necelých 3 000 odberateľov. Osveta a aktívny prístup práve v tejto oblasti je veľká výzva pre PDS a dodávateľov energií.

Agregácia z pohľadu prevádzkovateľov prenosových sústav

V čase konania seminára ešte nezávislý konzultant, aktuálne už pracovník ČEPS, a. s., R. Kabele sa vo svojom vystúpení venoval porovnaniu agregácie z pohľadu kódexov prevádzkovateľov prenosových sústav (PPS) v ČR a SR. Agregácia aj flexibilita nie sú podľa neho žiadnou novinkou, ale v nejakej forme sú už prítomné dlhšie obdobie. No sú tam samozrejme aj novinky, na ktoré sa práve R. Kabele zameral.

Richard Kabele

Začlenenie agregácie do kódexu prenosovej sústavy v ČR, resp. technických podmienok prenosovej sústavy v SR, sa datuje do roku 2017, keď vstúpilo do platnosti nariadenie EÚ 2017/2195 s usmernením o zabezpečení rovnováhy v elektrizačnej sústave. Treba však povedať, že napr. agregácia už bola prítomná v energetickej praxi ČR a SR dlhodobo, v rámci Slovenska sa agregácia realizovala napr. cez tzv. virtuálny blok. V obidvoch krajinách sa agregácia týkala napäťovej úrovne VVN a VN. Zimný energetický balíček EÚ však vyžaduje využitie agregácie ešte zásadnejším spôsobom, ako to bolo doteraz. Prevádzkovateľom prenosových sústav dáva explicitne povinnosť povoliť účasť agregátorom na trhu s podpornými službami, pričom z kontextu európskej legislatívy sa dá vyčítať, že agregácia má byť umožnená pre všetky typy podporných služieb. Dôležité je zdôrazniť, že legislatíva požaduje, aby bola agragácia zavedená všeobecne a nielen pri poskytovaní podporných služieb. „Agregácia má byť primárne určená pre trhy s elektrickou energiou, aby vyvažovala volatilitu spôsobenú pripájaním OZE. A to je to, čo je úplne nové – pojem nezávislého agregátora. Je to fenomén, ktorý riešenia všetky členské krajiny EÚ a ktorého zavedenie priamo vyžaduje európska legislatíva," vysvetľuje R. Kabele.

Nezávislý agregátor je revolučný krok z toho hľadiska, že posúva flexibilitu z tradičnej úrovne VVN a VN na úroveň NN a bude umožňovať každej jednej domácnosti zúčastňovať sa na trhu s flexibilitou.

Zároveň explicitne každej domácnosti umožňuje, aby si okrem svojho dodávateľa energie vybrala aj svojho agregátora.

R. Kabele sa následne v časti venovanej rôznym typom flexibility odrazil z hľadiska jej použitia od konceptu známeho pod označením USEF (Universal Smart Energy Framework), ktorý hovorí o tom, aké typy flexibility možno aj so zahrnutím agregácie využívať, a zároveň rieši zmluvné väzby. Okrem využívania flexibility z pohľadu spotrebiteľa je dôležité už aj spomínané hľadisko napäťovej úrovne a práve vďaka vzniku agregátorov sa možnosť využívať flexibilitu bude posúvať z úrovní VVN a VN aj na úroveň NN. Z pohľadu PPS je dôležité aj časové hľadisko využívania flexibility. Flexibilita, ktorá je aktivovaná v podobe podporných služieb, sa aktivuje v reálnom čase. Podľa R. Kabeleho je však dôležitá flexibilita trhu pred reálnou prevádzkou sústav, t. j. aby sa stretla ponuka s dopytom. Ak sa to na dennom trhu neudeje, nastupujú nástroje kapacitných mechanizmov, ktoré sú samy o sebe schopné aktivovať nejaké zdroje (zvyčajne strategické rezervy) a posilniť flexibilitu.

V ďalšej časti porovnal R. Kabele pravidlá uvedené v kódexe (ČEPS) alebo technických podmienkach (SEPS) a to, ako tieto dokumenty pracujú s pojmami agregácia či flexibilita, príp. aké prekážky bránia ich zavádzaniu. PPS totiž potrebuje vyhodnocovať nielen samotnú dodávku regulačnej energie, ale aj disponibilitu; rovnako potrebuje istotu, že výkon je k dispozícii, takže môže garantovať výkon danej podpornej služby, resp. jej aktivácie.

Projekt Dflex – uplatnenie flexibility v rámci podporných služieb PPS

J. Mišovič vo svojom vystúpení predstavil projekt Dflex zameraný na uplatnenie DSR flexibility v rámci podporných služieb ČEPS. Cieľom projektu, ktorý sa začal v roku 2019 a potrvá do konca roka 2022, je identifikovať agregáciu flexibility a odstrániť bariéry v ich fungovaní, nastaviť podmienky fungovania nezávislého agregátora pri poskytovaní podporných služieb a využitia metodiky tzv. Baseline. Do projektu sú zapojené súkromné subjekty, ako aj univerzitné pracoviská.

Ján Mišovič

„Aktuálne sa projekt nachádza vo svojej druhej etape, kde sa už vyhodnocujú reálne údaje, porovnávajú sa jednotlivé metódy Baseline, ktoré sú dôležité pre vzťah medzi agregátorom a dodávateľom a tiež pre to, aby bolo možné vyhodnotiť flexibilitu. V rámci projektu je preferovaný model nezávislého agregátora s centrálnym zúčtovaním, s ktorým sú schopné spolupracovať rôzne subjekty – ČEPS či operátor trhu (OTE). Motivácia vzniku a činnosti nezávislého agregátora vzniká na príslušných trhoch, či už ide o trhy s frekvenčnými a nefrekvenčnými produktmi, s produktmi pre PDS, ako aj trhy na uplatnenie bilančných služieb," vysvetľuje J. Miškovič.

Kde sú v podmienkach slovenskej energetiky zdroje na využitie flexibility? Podľa J. Miškoviča pôjde v prvom rade o jednoduché zariadenia využívané v rámci výroby elektrickej energie, ako sú napr. kogeneračné jednotky a tiež zariadenia využívané priemyselnými podnikmi. V druhom kole už pôjde o akékoľvek výrobné alebo spotrebné zariadenia, kde treba niečo ohrievať, chladiť a pod., čiže kde sa bude premieňať jedna forma energie na inú a kde bude možné využiť na akumuláciu energie nejaké zásobníky. „V tejto súvislosti teda pôjde napr. o mraziarne, teplárne, priemyselné čerpadlá, čističky odpadových vôd, veľké budovy či batériové úložiská," vysvetľuje J. Mišovič.

Koniec seriálu.

Anton Gérer

Ewon Cosy+ s vyššou kybernetickou bezpečnosťou

HMS Networks uviedol na trh novú generáciu smerovačov na vzdialený prístup Ewon Cosy+. Vďaka zabudovanému hardvérovému zabezpečeniu umožňuje používateľom bezpečný prístup k priemyselnému zariadeniu odkiaľkoľvek na uvedenie do prevádzky, odstraňovanie porúch a online programovanie.

Už 20 rokov je Ewon synonymom internetového vzdialeného prístupu v priemyselnej automatizácii. Smerovače Cosy a Flexy sú známe tým, že sú ľahko použiteľné, nákladovo efektívne a bezpečné. Viac ako 300 000 zariadení pripojených prostredníctvom cloudovej VPN služby Talk2M potvrdzuje skutočnosť, že Ewon je lídrom v oblasti vzdialeného priemyselného pripojenia.

Bezpečnostný reťazec Cosy+ od HW až po cloud:

- zabudovaný bezpečnostný čip chráni dôverné informácie a poskytuje Hardware Root Of Trust,
- Birth Certificate na zabránenie klonovaniu a falšovaniu,
- silné šifrovanie komunikácie s cloudovou službou Talk2M,
- bezpečnostný certifikát ISO 27001 a partnerstvo v kybernetickej bezpečnosti s NVISO,
- odchádzajúce spojenia nevyžadujú úpravy v existujúcej sieti,
- segregácia siete LAN na zabezpečenie prístupu výhradne k cieľovému zariadeniu,
- sledovateľnosť všetkých aktivít na diaľku prostredníctvom podrobných protokolov a správ,
- možnosť lokálneho blokovania vzdialeného pripojenia pomocou prepínača,
- zvýšená bezpečnosť pomocou digitálneho výstupu indikujúceho aktívne vzdialené pripojenie.

www.controlsystem.sk

Počítačová kriminalita je tretia najväčšia ekonomika sveta

Kybernetické útoky v prvej polovici roku 2021 globálne eskalovali a zasiahli prakticky každé priemyselné odvetvie. Niektorí odborníci na kybernetickú bezpečnosť súhlasia so správou spoločnosti Cybersecurity Ventures a očakávajú, že finančné škody spôsobené počítačovou kriminalitou dosiahnu do konca tohto roka 6 biliónov dolárov. Keby sa to meralo ako krajina, potom by počítačová kriminalita bola po USA a Číne treťou najväčšou ekonomikou na svete.

Cybersecurity Ventures očakáva, že globálne náklady na počítačovú kriminalitu v nasledujúcich piatich rokoch porastú o 15% ročne a do roku 2025 dosiahnu 10,5 bilióna dolárov ročne, čo predstavuje viac ako trojnásobný nárast oproti roku 2015. Predstavuje to najväčší prevod ekonomického bohatstva v histórii. Množstvo výdavkov súvisiacich s kybernetickou kriminalitou bude väčšie ako celosvetový obchod so všetkými nelegálnymi drogami dohromady.

V júni tohto roku si ransomvér vyžiadal prvý oficiálne potvrdený život. Nemecké úrady informovali, že útok ransomvéru spôsobil zlyhanie informačných systémov vo veľkej nemocnici v Düsseldorfe a žena, ktorá potrebovala urgentný príjem, zomrela po tom, čo musela byť prevezená na ošetrenie do iného mesta. Kybernetické hrozby sa rozšírili od zamerania a poškodenia počítačov, sietí a inteligentných telefónov na automobily, železnice, lietadlá, energetické siete a na všetko, čo sa spolieha na elektroniku a siete.

-tog-

Farnell dodáva nový rad napájacích zdrojov Rohde & Schwarz NGA100

Spoločnosť Farnell, člen skupiny Avnet a globálny distribútor elektronických komponentov, výrobkov a riešení, aktuálne rozšírila svoju ponuku testovacích a meracích zariadení o novú sériu napájacích zdrojov NGA100, ktorá je súčasťou portfólia Essentials od spoločnosti Rohde & Schwarz. S intuitívnym manuálnym ovládaním a jednoduchým ovládaním riadeným počítačom možno tieto zdroje použiť pri výskume a vývoji, testovaní výrobkov, opravách, vzdelávaní alebo pri montáži do zástavby (rack) ako súčasť testovacích systémov vo výrobnej prevádzke.

NGA100 novej generácie je ľahko použiteľný základný zdroj napájania, starostlivo navrhnutý na bežné a cenovo dostupné použitie s bohatými funkciami. Je založený na stabilnom výstupe, nízkej hlučnosti a lineárnej topológii umiestnenej v kompaktnom vyhotovení. Poskytuje vynikajúcu presnosť spätného čítania a má rozsah nízkeho prúdu s niekoľkými režimami spánku na realizáciu meraní vyžadovaných zariadeniami internetu vecí (IoT).

Zdroje napájania, ktoré sú vybavené rôznymi externými ovládacími rozhraniami, umožňujú diaľkové snímanie záťaže, aby sa zlepšila presnosť nastavenia a merania, a možno ich ľahko integrovať do automatizovaného testovania. Séria NGA100 tiež umožňuje zákazníkom bezproblémovú a produktívnu prácu v rámci moderných testovacích pracovísk.

Medzi kľúčové vlastnosti série napájacích zdrojov NGA100 patria:
- 3,5-palcový displej na prednom paneli – farebný displej zaručuje, že používatelia budú jasne vidieť všetky prevádzkové podmienky vrátane stavu akýchkoľvek ochranných funkcií. Hodnoty napätia a prúdu sú ľahko čitateľné, do displeja je integrovaná aj štatistika, kde sa zobrazujú minimálne a maximálne hodnoty napájania, napätia a prúdu.
- Pripojiteľnosť – séria NGA obsahuje rozhranie USB na kontrolu a ukladanie údajov. Ethernet s integrovaným webovým serverom ponúka jednoduché ovládanie prístroja priamo cez webový prehliadač a bezdrôtová sieť LAN (WLAN) automaticky pripája prístroj k sieti.
- Montáž do stojana (rack) – kompatibilná súprava na montáž do stojana a zadné výstupné konektory zaisťujú ľahkú integráciu napájacieho radu NGA100 do testovacích systémov. Do každého rámu na stojan možno umiestniť až dve jednotky NGA100.

Spoločnosť Farnell ponúka celú škálu produktov na podporu návrhu, vývoja a testovania elektronických zariadení vrátane napájacích systémov. Aktuálna novinka NGA100 je k dispozícii bez minimálnej hodnoty objednávky a so vzdelávacím zľavovým programom. Zákazníci majú tiež bezplatný prístup k online zdrojom, údajovým listom, prípadovým štúdiám, videám a webinárom a vynikajúcu zákaznícku a technickú podporu, ktorá je k dispozícii nepretržite v miestnom jazyku.

Séria napájacích zdrojov NGA100 od Rohde & Schwarz je k dispozícii od spoločností Farnell v EMEA, element14 v APAC a Newark v Severnej Amerike.

www.farnell.com

Farnell rozširuje škálu nástrojov zážitkového učenia prostredníctvom InkSmith

Spoločnosť Farnell, člen skupiny Avnet a globálny distribútor elektronických súčiastok, produktov a riešení, podpísala globálnu distribučnú dohodu so spoločnosťou InkSmith s cieľom rozšíriť rozsah svojich vzdelávacích produktov a podporiť medzipredmetové vzdelávanie.

Vzdelávanie založené na Climate Action Kit je určené na to, aby študentov naučilo aplikovať technológiu na riešenie problémov v reálnom svete prostredníctvom cieľov OSN v oblasti trvalo udržateľného rozvoja (SDGs). Každý projekt poskytuje jedinečnú príležitosť na prierezové učenie, v rámci ktorého sú študenti povzbudzovaní k spolupráci v skupinách alebo samostatne, v triede alebo na diaľku. Študenti si osvoja zručnosti v programovaní pomocou rôznych výziev zážitkového učenia pri navrhovaní a prototypových riešeniach pomocou BBC micro:bit.

Súprava InkSmith Climate Action Kit pomáha študentom zaoberať sa problémami klimatických zmien prostredníctvom učenia založeného na výzvach. Súprava zoznamuje študentov s rôznymi problémami zmeny klímy týkajúcimi sa SDG15: Život na zemi. Projekty umožňujú študentom preskúmať témy, ako sú odlesňovanie a hnojenie, a navrhovať svoje vlastné riešenia, ako sú automatizované sádzače stromov alebo automatické zavlažovacie systémy pre vertikálne alebo vnútorné poľnohospodárstvo.

Súprava Climate Action Kit, ktorú teraz ponúka spoločnosť Farnell, obsahuje:
- motory, snímače a príslušenstvo potrebné na zvládnutie rôznych projektov v oblasti ochrany životného prostredia,
- vyučovacie zdroje a učebné osnovy na päť projektových lekcií (odlesňovanie, rastliny a opeľovače, chov hmyzu, bezuhlíkové pestovanie a pokročilé poľnohospodárstvo),
- online balíčky učebných osnov, ktoré navrhli odborníci na interné vzdelávanie InkSmith tak, aby boli kompatibilné so vzdialenými prostrediami v triede a hybridnými vzdelávacími prostrediami,
- jednu dosku na pripojenie k BBC micro:bit k téme klimatické zmeny,
- sprievodnú príručku pre učiteľa s pokynmi.

Súprava Climate Action Kit vyžaduje použitie BBC micro:bit, ktorý je k dispozícii samostatne.

Spoločnosť Farnell spolupracovala s viacerými vzdelávacími organizáciami a vládami na podpore strategického zavádzania riešení do výučby orientovanej na vedu, technológie, matematiku a elektrotechniku a má na sklade širokú škálu vzdelávacích zariadení, ktoré môžu byť dodávané pre jednotlivé triedy či školy. Spoločnosť Farnell môže tiež ponúknuť podporu pri poskytovaní a združovaní vybavenia pre veľké programy na mieru, ako bol napr. Super:bit v Nórsku.

Súprava Climate Action Kit je k dispozícii od spoločnosti Farnell v EMEA a element14 v APAC.

www.farnell.com

Technical Computing Camp 2021

Spoločnosť HUMUSOFT, s. r. o., výhradný zástupca spoločností MathWorks, COMSOL AB a dSPACE GmbH pre Českú republiku a Slovensko, organizuje začiatkom septembra na Brnianskej priehrade 8. ročník neformálneho stretnutia priaznivcov technických výpočtov a počítačových simulácií.

Cieľom akcie Technical Computing Campu 2021 (TCC21) je prezentácia a výmena informácií medzi účastníkmi z praxe a škôl. Dvojdenný formát TCC21 dovolil pripraviť bohatý program:

- prednášky o využití prostredí MATLAB, COMSOL Multiphysics a dSPACE v rôznych oblastiach,
- pozvané prednášky používateľov,
- showcase – praktické ukážky využitia nástrojov formou minivýstavy,
- súťaž o najlepší používateľský projekt,
- tvorivá dielňa – príležitosť pracovať v tíme na jednoduchých úlohách,
- expozícia partnerov.

Počas TCC21 sa dozviete o novinkách v základných moduloch MATLAB a Simulink, ďalších nadstavbách a o nových produktoch. V nadstavbe Simscape budú predstavené aktuálne možnosti modelovania multifyzikálnych sústav. Prezentované budú aj možnosti vývoja autonómnych a bezdrôtových komunikačných systémov. Nebude chýbať ani ukážka využitia metód umelej inteligencie pre signály a časové rady. Moderné trendy vo výpočtoch FEM budú predstavené pomocou nástrojov COMSOL Multiphysics. V oblasti dSPACE predstavíme, čo zahŕňa vývoj elektromobilov, smart sietí alebo inteligentných nabíjacích systémov.

mediálny partner atp journal

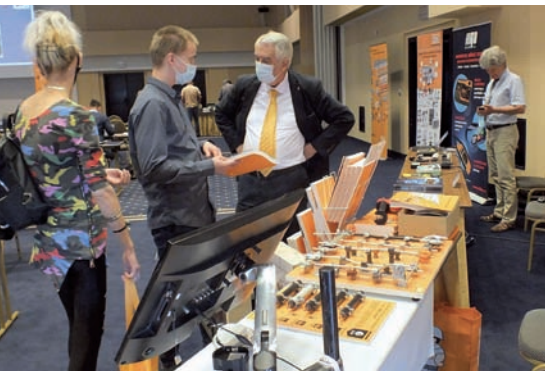
Viac informácií sa dozviete na webovej stránke venujúcej sa TCC21: **https://www.humusoft.cz/event/technical-camp-2021/**

ELTECH SK bol už naživo!

Po ročnej prestávke vynútenej pandémiou sa vo veľkorysých priestoroch hotela Bellevue v Hornom Smokovci uskutočnil už jedenásty ročník celoslovenského stretnutia elektrotechnikov, revíznych technikov elektrických zariadení, projektantov a dodávateľov. Organizátorovi podujatia, spoločnosti Elektro Management, s. r. o., pod vedením Mgr. Petry Bartoškovej sa to za dodržania všetkých protipandemických opatrení podarilo zorganizovať naživo!

O obľube tohto podujatia medzi odbornou verejnosťou svedčí aj to, že napriek stále nie celkom uvoľneným opatreniam sa na podujatí zúčastnilo 75 registrovaných odborníkov a 23 vystavujúcich spoločností. Navyše viac ako polovica zúčastnených prišla na konferenciu prvýkrát. Najväčšie zastúpenie mali už tradične odborníci z oblasti elektrotechniky a projektanti.

Prvý deň podujatia bol na programe praktický workshop zameraný na revízie elektrických spotrebičov, ktoré pre účastníkov zorganizovala spoločnosť ILLKO, s.r.o. Hlavný program druhého dňa sa začal úvodným privítaním P. Bartoškovej, po ktorej sa k slovu dostal Ing. Edmund Pantůček, súdny znalec v odbore elektrotechnika a elektronika, konateľ spoločnosti ANTIRISK – EMC, s.r.o. Vo svojej prednáške sa venoval elektrickým inštaláciám v priestoroch s nebezpečenstvom výbuchu.



Počas dvoch dní konferencie odzneli napríklad aj tieto prednášky:

- Bezpečnosť práce a ochrana elektronických zariadení pred poškodením pri vykonávaní revízií a OPaOS (Ing. Leoš Koupý, konateľ ILLKO, s.r.o.),
- Posudzovanie a OPaOS systému ochrany pred bleskom podľa STN EN 62305-1 až 4 (Jiří Kroupa, spracovateľ slovenského znenia STN EN 62305-3 a 4, riaditeľ kancelárie DEHN + SE pre Slovensko, člen klubu ILPC),
- Montážne chyby pri vyhotovovaní bleskozvodov (Ing. Rudolf Štober, elektroprojektant),
- Komplexný návrh ochrany pred prepätím pre inteligentné stavby (Ing. Jozef Daňo, obchodno-technický manažér OBO Bettermann, s.r.o.),
- Elektromobily – nabíjacie stanice a ich revízie (prof. Ing. Viktor Ferencey, PhD., Ústav automobilovej mechatroniky FEI STU BA, doc. Ing. Ján Vlnka, PhD., Ústav automatizácie, merania a aplikovanej informatiky SjF STU BA).

Z prednášajúcich si najvyššie hodnotenie odniesli Jiří Kroupa a Rudolf Štober, z vystavujúcich spoločností najviac zaujali DEHN a OBO Bettermann, s.r.o.

Druhý deň podujatia doplnil aj praktický workshop spoločnosti EPLAN pod názvom Štyri jednoduché kroky od plánovania po revíznu dokumentáciu pod vedením Ing. Radovana Ovcarčíka. Výstava historických meracích prístrojov či diskusia s Petrom Petrasom, chatárom z Rainerovej chaty, boli pre účastníkov spestrením tohto vydareného podujatia.

Budúci ročník ELTECH SK sa uskutoční od 7. do 9. 6. 2022. Bližšie informácie nájdete na www.elektromanagement.sk.

mediálny partner atp journal

-tog-

Elektrotechnické STN

Prehľad vydaných elektrotechnických STN a ich zmien (triedy 33, 34, 36, 92).

STN P CLC/TS 50136-9: 2021-06 (33 4596) Poplachové systémy. Poplachové prenosové systémy a zariadenia. Časť 9: Požiadavky na spoločný protokol na prenos poplachu používajúci Internet Protocol (IP).*)

STN EN 50397-1: 2021-06 (34 7412) Vodiče s ochranným obalom na vonkajšie vedenia a súvisiace príslušenstvo pre striedavé menovité napätia od 1kV do 36 kV vrátane. Časť 1: Vodiče s ochranným obalom.*)

STN EN 60332-1-2/A12: 2021-06 (34 7101) Skúšky elektrických a optických káblov v podmienkach požiaru. Časť 1-2: Skúška samostatného izolovaného vodiča alebo kábla proti vertikálnemu šíreniu plameňa. Postup pre 1 kW zmiešaný plameň.*)

STN EN 60825-1/A11: 2021-06 (34 1701) Bezpečnosť laserových zariadení. Časť 1: Klasifikácia zariadení a požiadavky.*)

STN EN IEC 60112: 2021-06 (34 6468) Metóda určovania porovnávacieho indexu a indexu odolnosti tuhých izolačných materiálov proti tvorbe plazivých stôp.*)

STN EN IEC 60172: 2021-06 (34 7304) Skúšobný postup na určenie teplotného indexu lakovaných a páskou ovinutých vodičov na vinutia.*)

STN EN IEC 60305: 2021-06 (34 8118) Izolátory pre vonkajšie elektrické vedenia s menovitým napätím nad 1 000 V. Keramické alebo sklené závesné izolátory pre siete so striedavým napätím. Charakteristiky tanierových izolátorov.*)

STN EN IEC 60433: 2021-06 (34 8055) Izolátory pre vonkajšie elektrické vedenia s menovitým napätím nad 1 000 V. Keramické izolátory pre siete so striedavým napätím. Charakteristiky tyčových závesných izolátorov.*)

STN EN IEC 60799: 2021-06 (34 7502) Elektrické príslušenstvá. Prívodné šnúry a prepájacie šnúry.*)

STN EN IEC 62474/A1: 2021-06 (34 5904) Uvádzanie materiálov pri výrobkoch elektrotechnického priemyslu a pre elektrotechnický priemysel.*)

STN P CLC/TS 50459-1: 2021-06 (34 2660) Dráhové aplikácie. Komunikačné a signalizačné systémy a systémy na spracovanie údajov. Európsky systém riadenia železničnej dopravy. Rozhranie rušňovodič – zariadenie. Časť 1: Všeobecné princípy pre zobrazovanie informácií ERTMS/ETCS/GSM-R.*)

STN P CLC/TS 50459-2: 2021-06 (34 2660) Dráhové aplikácie. Komunikačné a signalizačné systémy a systémy na spracovanie údajov. Európsky systém riadenia železničnej dopravy. Časť 2: Ergonomické usporiadanie informácií GSM-R.*)

STN P CLC/TS 50459-3: 2021-06 (34 2660) Dráhové aplikácie. Komunikačné a signalizačné systémy a systémy na spracovanie údajov. Európsky systém riadenia železničnej dopravy. Časť 3: Ergonomické usporiadanie informácií iných ako ETCS.*)

STN EN 50342-4: 2021-06 (36 4310) Olovené štartovacie batérie. Časť 4: Rozmery batérií pre ťažké vozidlá.*)

STN EN 60061-1/A61: 2021-06 (36 0340) Pätice a objímky pre zdroje svetla vrátane kalibrov na kontrolu zameniteľnosti a bezpečnosti. Časť 1: Pätice pre zdroje svetla.*)

STN EN 60061-2/A57: 2021-06 (36 0340) Pätice a objímky pre zdroje svetla vrátane kalibrov na kontrolu zameniteľnosti a bezpečnosti. Časť 2: Objímky.*)

STN EN 60601-1-2/A1: 2021-06 (36 4800) Zdravotnícke elektrické prístroje. Časť 1-2: Všeobecné požiadavky na základnú bezpečnosť a nevyhnutné prevádzkové vlastnosti. Pridružená norma: Elektromagnetické rušenia. Požiadavky a skúšky.*)

STN EN 60601-1-3/A2: 2021-06 (36 4800) Zdravotnícke elektrické prístroje. Časť 1-3: Všeobecné požiadavky na základnú bezpečnosť a nevyhnutné prevádzkové vlastnosti. Pridružená norma: Radiačná ochrana pri diagnostických röntgenových prístrojoch.*)

STN EN 61347-1/A1: 2021-06 (36 0511) Ovládacie zariadenia svetelných zdrojov. Časť 1: Všeobecné a bezpečnostné požiadavky.*)

STN EN 62788-1-4/A1: 2021-06 (36 4605) Meracie postupy na materiály používané vo fotovoltických moduloch. Časť 1-4: Materiály na zapuzdrenie. Meranie optickej priepustnosti a výpočet váženej (na slnečné žiarenie) priepustnosti pre fotóny, indexu žltnutia a cut-off frekvencie UV žiarenia.*)

STN EN IEC 60598-2-23: 2021-06 (36 0600) Svietidlá. Časť 2-23: Osobitné požiadavky. Osvetľovacie sústavy pre svetelné zdroje na malé napätie.*)

STN EN IEC 60645-3: 2021-06 (36 8811) Elektroakustika. Audiometrické zariadenia. Časť 3: Skúšobné signály s krátkym trvaním.*)

STN EN IEC 60675-2: 2021-06 (36 1069) Priamo pôsobiace elektrické ohrievače miestností. Metódy merania funkčných vlastností. Časť 2: Dodatočné podmienky pre meranie faktora vyžarovania.*)

STN EN IEC 60675-3: 2021-06 (36 1069) Priamo pôsobiace elektrické ohrievače miestností. Metódy merania funkčných vlastností. Časť 3: Dodatočné podmienky pre meranie efektívnosti vyžarovania.*)

STN EN IEC 60904-1: 2021-06 (36 4604) Fotovoltické súčiastky. Časť 1: Meranie fotovoltických voltampérových charakteristík.*)

STN EN IEC 60904-10: 2021-06 (36 4604) Fotovoltické súčiastky. Časť 10: Metódy merania lineárnej závislosti a linearity.*)

STN EN IEC 60904-9: 2021-06 (36 4604) Fotovoltické súčiastky. Časť 9: Klasifikácia charakteristík slnečných simulátorov.*)

STN EN IEC 61010-2-202: 2021-06 (36 2000) Bezpečnostné požiadavky na elektrické zariadenia na meranie, riadenie a laboratórne použitie. Časť 2-202: Osobitné požiadavky na elektricky ovládané pohony ventilov.*)

STN EN IEC 61228: 2021-06 (36 0035) Ultrafialové žiarivky používané na opaľovanie. Metóda merania a špecifikácie.*)

STN EN IEC 62485-5: 2021-06 (36 4380) Bezpečnostné požiadavky na akumulátorové batérie a inštalácie batérií. Časť 5: Bezpečná prevádzka stacionárnych lítium-iónových batérií.*)

STN EN IEC 62485-6: 2021-06 (36 4380) Bezpečnostné požiadavky na akumulátorové batérie a inštalácie batérií. Časť 6: Bezpečná prevádzka lítium-iónových batérií pri trakčných aplikáciách.*)

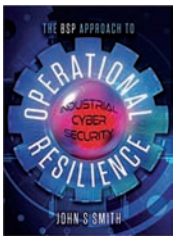
Mesiac vydania STN je uvedený za jej označením v tvare „: 2021-06“.
**) Normy boli vydané v anglickom jazyku.*

Ing. Ľudovít Harnoš
člen SEZ-KES

www.sez-kes.sk

Odborná literatúra, publikácie

Nové knižné tituly v oblasti automatizácie.



The BSP Approach to Operational Resilience: Industrial Cyber Security

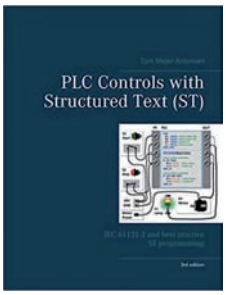
Autor: Smith, J. S., rok vydania: 2020, vydavateľstvo: UK Book Publishing,
ISBN 978-1913179595, publikáciu možno zakúpiť na www.amazon.com

Cieľom uvedenej publikácie je definovať prvotný proces posudzovania rizika kybernetickej bezpečnosti v prostredí priemyselnej výroby. Väčšina výrobných závodov prechádza na vysoko integrovanú digitálnu platformu, v rámci ktorej sú jednotlivé systémy úplne prepojené. IT a OT začínajú byť čoraz užšie prepojené a vďaka tomu dochádza k čoraz užšiemu prepojeniu obchodných systémov s výrobnými systémami. Zámerom tejto knihy je definovať správny „základný" prístup nevyhnutný na vypracovanie odhadu bezpečnostného rizika a na získanie prehľadu na viacerých úrovniach, od predstavenstva až po prevádzku. Predložená publikácia nabáda k uvedomeniu si, že multidisciplinárny prístup od samého začiatku pomôže naplniť dlhodobé ambície v oblasti ochrany prostredia prevádzky a vytvorenia fungujúceho programu bezpečnosti.

Cyber Security: in industrial automation

Autor: Manoj, K. S., rok vydania: 2020, vydavateľstvo: Notion Press,
ISBN 978-1649199768, publikáciu možno zakúpiť www.amazon.com

Predložená publikácia napísaná ľahkým štýlom poskytuje komplexný prehľad o fyzicko-kybernetickej bezpečnosti priemyselných riadiacich systémov. Úžitok z nej budú mať technici v oblasti počítačovej vedy a automatizácie, ako aj študenti a agentúry pre priemyselnú kybernetickú bezpečnosť pri získavaní základných znalostí o kybernetickej bezpečnosti priemyselných riadiacich systémov, a to od konceptu až po realizáciu. Publikácia rozoberá problematiku zberníc vrátane zónovej architektúry a jej nasadenia v dodávke produktov a ďalších priemyselných služieb, diskutuje o sieťach pre systémy SCADA s požadovanou kryptografiou a bezpečnou priemyselnou komunikáciou a poskytuje informácie o priemyselných štandardoch kybernetickej bezpečnosti, ktoré sa v súčasnosti používajú, veľa zdokumentovaných príkladov útokov na priemyselné riadiace systémy, ako aj techník na boj s kyberzločinmi v reálnom svete.

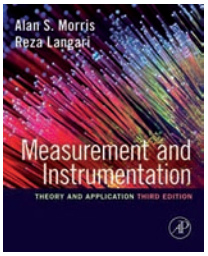


PLC Controls with Structured Text (ST), V3: IEC 61131-3 and best practice ST programming

Autor: Antonsen, T. M., rok vydania: 2020 vydavateľ: Books on Demand,
ISBN 978-8743015543, publikáciu možno zakúpiť na www.amazon.com

Autor má 25-ročné skúsenosti so špecifikáciou, vývojom a dodávkou komplexných priemyselných riadiacich a dozorných systémov. Kniha predstavuje úvod do programovacieho jazyka štruktúrovaného textu (Structured Text, ST), ktorý sa používa v programovateľných logických automatoch (PLC). Tretie vydanie bolo aktualizované a rozšírené o mnoho návrhov a otázok, s ktorými prišli čitatelia a študenti, vrátane požiadavky na ešte viac konkrétnych príkladov programov. Autor sa venuje témam, ako pozadie, výhody a výzvy programovania pomocou ST, syntax, dátové typy, osvedčené postupy a základné programovanie, riešenie problémov, testovanie a štruktúra programu, sekvencer a rozdelenie programu na funkcie a funkčné bloky, riadenie veľkoobjemových zásobníkov a dopravníkových pásov, algoritmus adaptívneho čerpadla a riadenie robota, štruktúra programu PLC pre čerpacie stanice, 3D parkovisko a umývanie automobilov. Kniha obsahuje viac ako 150 príkladov PLC programov so zameraním na napísanie spoľahlivého, čitateľného a štruktúrovaného programu. Systematicky opisuje základné programovanie a ponúka rady a praktické príklady na základe rozsiahlych skúseností autora.

Measurement and Instrumentation: Theory and Application, 3rd Edition



Autori: Morris, A. S. – Langari, R., rok vydania: 2020, vydavateľ: Academic Press,
ISBN 978-0128171417, publikáciu možno zakúpiť na www.amazon.com

Tretie vydanie tejto úspešnej publikácie predstavuje študentom vysokoškolského inžinierskeho štúdia princípy merania a rozsah snímačov a prístrojov používaných na meranie fyzikálnych premenných. Tento jasne a komplexne napísaný text, ktorý poskytuje najvyváženejšie pokrytie teórie/technológií a prístrojového vybavenia, vyzbrojuje študentov a začínajúcich technikov prichádzajúcich do praxe znalosťami a nástrojmi na navrhovanie a budovanie meracích systémov pre prakticky akékoľvek inžinierske aplikácie.

-bch-

Hlavní partneri

AutoCont Control spol. s r.o.
www.autocontcontrol.sk

B+R automatizace, spol. s r.o.
– organizačná zložka
www.br-automation.com

Siemens s.r.o.
www.siemens.sk

V celoročnej súťaži môžete vyhrať tieto ceny

Čistička vzduchu
Philips Dual Scan AC3059/50

Parný čistič
KÄRCHER SC 4 EasyFix Iron

Automatický kávovar
Siemens TI313219RW

ČITATEĽSKÁ SÚŤAŽ ATPJOURNAL 7/2021

Partneri kola súťaže:

Phoenix Contact, s.r.o.

Premier Farnell UK Ltd.

A2B, s.r.o.

V tomto kole súťažíte o tieto vecné ceny:

dáždnik, skrutkovač,
orezávač, pásmo

sada náradia

termotaška, termohrnček
a termoska

Otázky sú veľmi jednoduché. Ak by ste predsa len nepoznali odpovede, pretože vašou parketou je iná oblasť, môžete ich nájsť v tomto čísle ATP Journal, ako aj v článkoch uverejnených na stránke www.atpjournal.sk.

Súťažné otázky:

1. **Aké odolné a vysoko spoľahlivé WLAN komponenty Phoenix Contact použila spoločnosť Zebotec pri výstavbe svojej plávajúcej fotovoltickej elektrárne?**
2. **Ktoré tri kľúčové vlastnosti sú charakteristické pre rad napájacích zdrojov NGA100?**
3. **Aký čas zálohovania možno bežne dosiahnuť pri UPS do 3 kVA pri použití silnejšieho nabíjača bez interných batérií?**
4. **Ako sa nazýva koncept, ktorý spoločnosť Kaspersky považuje za najefektívnejší model na vybudovanie postupov kybernetickej bezpečnosti pre priemyselné podniky?**

Súťažte prostredníctvom **www.atpjournal.sk/sutaz/otazky**

Odpovede posielajte najneskôr do 13. 8. 2021

Pravidlá súťaže sú uverejnené v ATP Journal 1/2021 na str. 55 a na www.atpjournal.sk/sutaz

ATPJOURNAL.SK/SUTAZ

ČITATEĽSKÁ SÚŤAŽ ATP JOURNAL 5/2021
VYHODNOTENIE

Správne odpovede

1. **So súpravou Google AIY Vision Kit si môžete postaviť svoju vlastnú inteligentnú kameru. Koľko bežných objektov dokáže detegovať?**
   1000.
2. **Aké položky obsahujú prispôsobiteľné komponenty RFID štítkov spoločnosti Brady?**
   RFID antény, čipy, voliteľné senzory, lepidlá, materiály štítkov priemyselnej triedy, tvar a farbu štítkov, predtlače štítka a predprogramovanie.
3. **Aký typ robota bol použitý na pracovisku pre zváranie a ohýbanie oceľových potrubných rozvodov pre modulárne zásobníky plynu?**
   Kawasaki RS010L.
4. **Ktorá technológia zvárania sa najčastejšie používa v spojení s robotickým zváraním?**
   Technológia využívajúca elektrický oblúk v ochrannej atmosfére.

Výhercovia

Vladimír Roman, Čadca

Jozef Lackovič, Bučany

Augustín Novák, Báhoň

Srdečne gratulujeme.

ATPJOURNAL.SK/SUTAZ

Zoznam firiem publikujúcich v tomto čísle

Firma • Strana (o – obálka)

atp journal

Redakčná rada

prof. Ing. Alexík Mikuláš, PhD., FRI ŽU, Žilina
Ing. Balogh Richard, PhD., FEI STU, Bratislava
prof. Ing. Belavý Cyril, CSc., SjF STU, Bratislava
prof. Ing. Duchoň František, PhD., FEI STU – NCR, Bratislava
prof. Ing. Fikar Miroslav, DrSc., FCHPT STU, Bratislava
prof. Ing. Hulkó Gabriel, DrSc., SjF STU, Bratislava
prof. Ing. Janíček František, PhD., FEI STU, Bratislava
prof. Ing. Krokavec Dušan, CSc., FEI TU Košice
doc. Ing. Kvasnica Michal, PhD., FCHPT STU, Bratislava
prof. Ing. Malindžák Dušan, CSc., BERG TU, Košice
prof. Ing. Mészáros Alajos, CSc., FCHPT STU, Bratislava
prof. Ing. Murgaš Ján, PhD., FEI STU, Bratislava
prof. Ing. Pavlovičová Jarmila, PhD., FEI STU, Bratislava
prof. Ing. Rástočný Karol, PhD., FEIT ŽU, Žilina
doc. Ing. Schreiber Peter, CSc., MTF STU, Trnava
prof. Ing. Smieško Viktor, PhD., FEI STU, Bratislava
prof. Ing. Taufer Ivan, DrSc., FEI Univerzita Pardubice
prof. Ing. Veselý Vojtech, DrSc., FEI STU, Bratislava
prof. Ing. Zolotová Iveta, CSc., FEI TU, Košice
doc. Ing. Ždánsky Juraj, PhD., FEIT ŽU, Žilina

Babic Branislav,
výkonný riaditeľ ProCS, s.r.o.
Ing. Horváth Tomáš,
riaditeľ HMH, s.r.o.
Ing. Hrica Marián,
riaditeľ divízie A & D, Siemens, s.r.o.
Kroupa Jiří,
riaditeľ kancelárie pre SK, DEHN+SÖHNE
Ing. Lásik Vladimír,
PPA CONTROLL, a.s.
Ing. Mašláni Marek,
riaditeľ B+R automatizace, s.r.o. – o. z.
Mík Pavel,
obchodný riaditeľ ABB, s.r.o.
Ing. Petergáč Štefan,
predseda predstavenstva Datalan, a.s.
Ing. Széplaky Ladislav,
riaditeľ Emerson Process Management, s.r.o.

Redakcia

ATP Journal
Galvaniho 7/D
821 04 Bratislava
tel.: +421 2 32 332 182
fax: +421 2 32 332 109
vydavatelstvo@hmh.sk
www.atpjournal.sk

Ing. Anton Gérer, šéfredaktor
gerer@hmh.sk

Ing. Petra Valiauga, odborná redaktorka
petra.valiauga@hmh.sk

Dagmar Votavová, obchod a marketing
podklady@hmh.sk, mediamarketing@hmh.sk

Zuzana Pettingerová, DTP grafik
dtp@hmh.sk

Mgr. Bronislava Chocholová, PhD.
jazyková redaktorka

Vydavateľstvo

HMH, s.r.o.
Tavarikova osada 39
841 02 Bratislava 42
IČO: 31356273
Vydavateľ periodickej tlače nemá hlasovacie práva alebo podiely na základnom imaní žiadneho vysielateľa.

Spoluzakladateľ

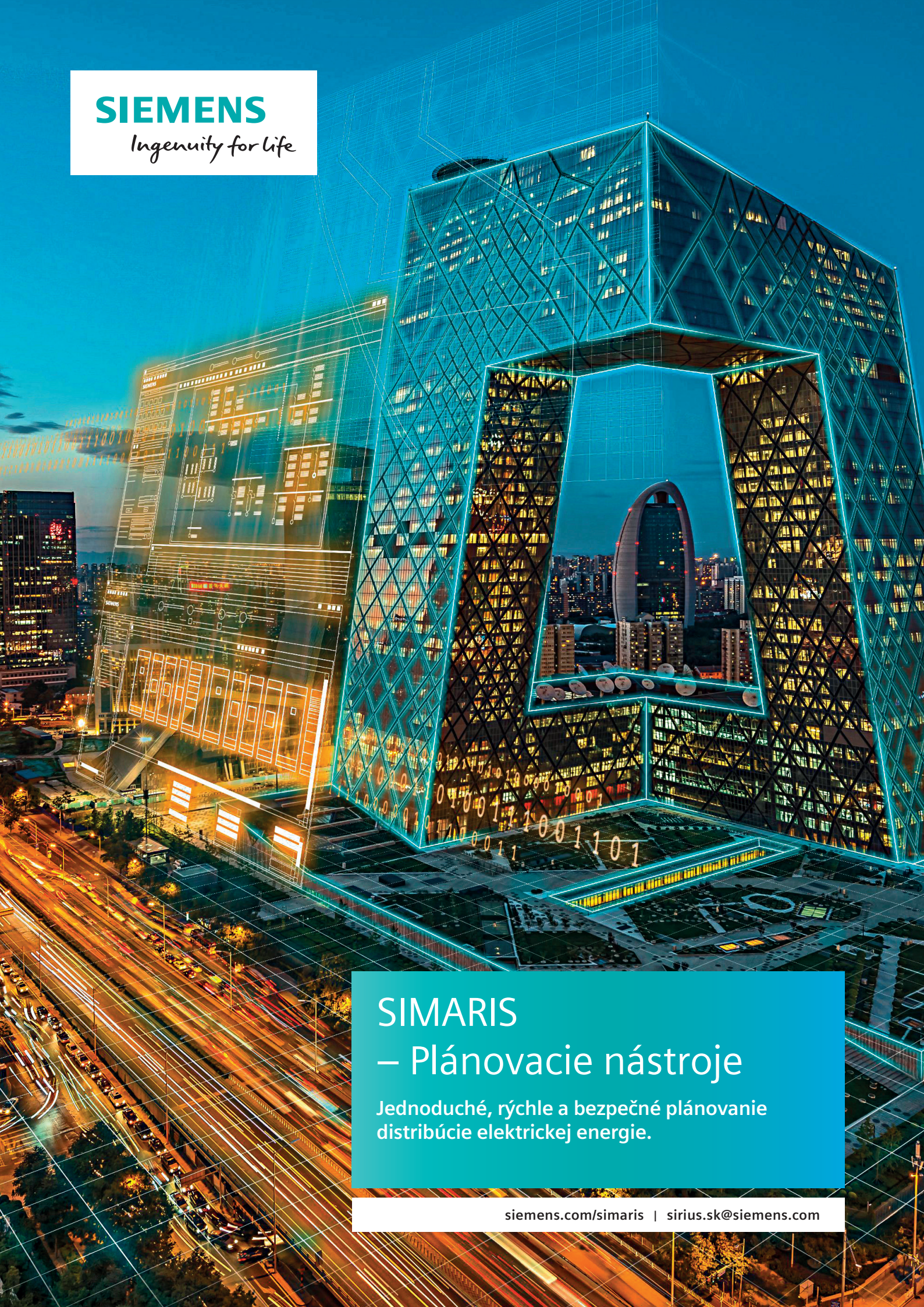
Katedra ASR, EF STU
Katedra automatizácie a regulácie, EF STU
Katedra automatizácie, ChtF STU
PPA CONTROLL, a.s.

Zaregistrované MK SR pod číslom EV 3242/09 **&** Vychádza mesačne **&** Cena pre registrovaných čitateľov 0 € **&** Cena jedného výtlačku vo voľnom predaji: 3,30 € + DPH **&** Objednávky na ATP Journal vybavuje redakcia na svojej adrese **&** Tlač a knihárske spracovanie KASICO a.s. **&** Redakcia nezodpovedá za správnosť inzerátov a inzertných článkov **&** Nevyžiadané materiály nevraciame **&** Dátum vydania: júl 2021

ISSN 1335-2237 (tlačená verzia)
ISSN 1336-233X (on-line verzia)

SIEMENS

Ingenuity for life



SIMARIS
– Plánovacie nástroje

Jednoduché, rýchle a bezpečné plánovanie distribúcie elektrickej energie.

siemens.com/simaris | sirius.sk@siemens.com

Rittal
Wire Station WS 540

Mobilné pracovisko na zapájanie vodičov:

» ergonomická a jednoduchá práca pri príprave vodičov a zapojení rozvádzača,

» variabilné pracovisko s možnosťou úplne ho prispôsobiť aktuálnym potrebám a individuálne ho nakonfigurovať,

» elektricky nastaviteľná výška stola v rozsahu 710 – 1 250 mm s prípravou na montáž monitora,

» súčasťou zostavy je aj prívodný kábel, zásuvková lišta, integrované meradlo a zásuvka na náradie,

» možnosť rozšírenia o odkladacie police na vodiče, držiaky na cievky vodičov, na náradie a drobné diely, police na poloautomaty a mnoho ďalšieho,

» upevnenie príslušenstva k stolu pomocou konzol.