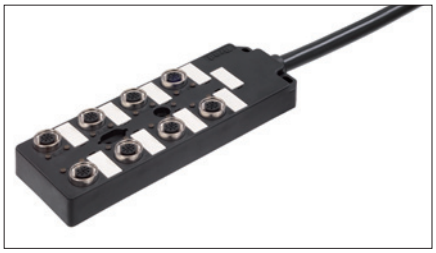
Brad MPIS a HarshIO od firmy Molex – aktivní a pasivní IO moduly

Jedním z dlouhodobých partnerů společnosti OEM Automatic je německá firma Molex, specialista na propojovací techniku a kabeláž. Molex nabízí pasivní i aktivní prvky infrastruktury v robustním provedení do nejnáročnějších prostředí. Tyto prvky se používají v takových oborech průmyslu, jako jsou výroba automobilů, manipulace s materiálem, potravinářství, robotika, solární technika atd.

Produkty Molex, které OEM Automatic nabízí, lze rozdělit do několika skupin:
- pasivní propojovací prvky určené pro přenos signálů ze senzorů a akčních členů nebo pro distribuci energie prostřednictvím standardizovaných konektorů M8, M12, M23, M40 a rozbočovačů MPIS (multiportové propojovací systémy),
- aktivní propojovací prvky určené pro sběrnicové systémy s podporou nejběžnějších komunikačních protokolů,
- „heavy duty“ konektory – robustní typy kovových konektorů,
- konektory DIN pro ovládání solenoidových ventilů.

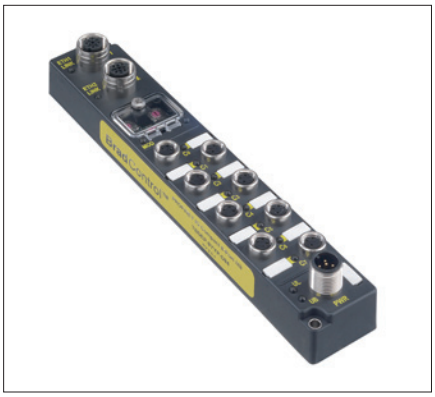
Pasivní I/O moduly

Produktová značka Brad® zahrnuje standardizované prvky pro použití v průmyslu. K jejich atributům patří jednoduchost návrhu instalace i snadnost následné údržby. Patří mezi ně pasivní I/O moduly MPIS (*Multi-Port Interconnection Systems; obr. 1*) s konektory M8 (čtyři, osm nebo deset portů) nebo M12 (čtyři nebo osm portů, čtyřpólové nebo pětipólové konektory) a s kabelem WSOR (*Weld-Slag and Oil-Resistant*). Kabel WSOR je odolný proti olejům i odstřikujícímu kovu při svařování. Tyto rozbočovače umožňují rychlé, snadné a spolehlivé připojení I/O signálů koncentrovaných do jednoho tzv. *home-run* kabelu. Cenově zajímavé řešení zpřehledňuje infrastrukturu na strojích, kde jsou tyto moduly instalovány. Vstupně-výstupní moduly MPIS jsou vhodné i do velmi náročných provozních podmínek (krytí IP67). Jsou vybaveny signalizačními LED, které obsluhu na místě informují o stavu zařízení.



Obr. 1. Pasivní I/O modul MIPS

Moduly MPIS jsou ideální pro malé a střední stroje. U velkých zařízení je již výhodnější použít moduly HarshIO – sběrnicově propojené aktivní I/O moduly.



Obr. 2. Sběrnicový I/O modul HarshIO

HarshIO – aktivní distribuční moduly

Moduly HarshIO (*obr. 2*) sbírají signály ze snímačů a akčních členů a převádějí je na telegramy provozní sběrnice nebo průmyslového Ethernetu.

Pokud jde o průmyslový Ethernet, HarshIO podporují protokoly Modbus TCP, EtherNet/IP a Profinet, které patří v praxi k nejpoužívanějším. Jsou určeny pro efektivní propojení průmyslových zařízení a jejich ovládání či diagnostiku ze vzdálených řídicích pracovišť.

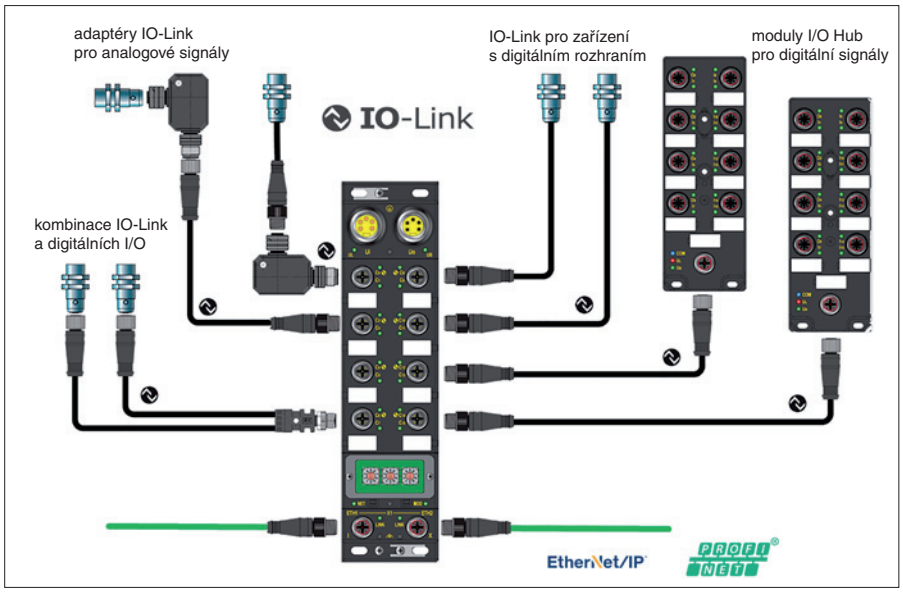
Moduly HarshIO umožňují spolehlivé, rychlé a jednoduché připojení I/O z provozních zařízení díky patentovanému propojovacímu mechanismu Brad® Ultra-Lock® – konektory se upevní na port pouhým nasunutím, bez nutnosti šroubovat matici, a přitom není omezena těsnost spojení – krytí je IP67 nebo IP68.

Indikační LED pro zobrazení stavu modulů a displej pro zobrazení IP adres zpřehledňují diagnostiku na místě. Vestavěný webový server umožňuje dálkové monitorování a konfiguraci rozbočovačů. Vestavěný ethernetový dvouportový switch snižuje množství kabeláže. Vestavěné switche mohou být manažovatelné i nemanažovatelné. Je možné použít přímý i křížený ethernetový kabel.

Moduly HarshIO podporují kromě průmyslového Ethernetu také běžné průmyslové sběrnice, jako jsou Profibus-DP, DeviceNet nebo CANopen.

Moduly IO-Link

IO-Link je relativně nový standard pro komunikaci se snímači a akčními členy. Byl standardizován jako součást normy IEC 61131-2 *Industrial-process measurement and control – Programmable controllers – Part 2: Equipment requirements and tests*. Jde o digitální sériovou komunikační linku typu bod-bod (*point-to-point*), která rozšiřuje možnosti klasické třívodičové (senzorové) infrastruktury využívající konektory M8 nebo



Obr. 3. Využití komunikačního systému IO-Link s moduly IO-Link Master a I/O Hub

M12. IO-Link se vyznačuje jednoduchostí a cenovou úsporností. Nejsou třeba drahé stíněné kabely, které jsou vyžadovány u snímačů s přenosem analogového signálu nebo u standardních sběrnicových systémů, není třeba ani další kabeláž pro samostatně vedené napájení.

Jednoduchost připojení snímačů, možnost jejich dálkové online parametrizace a rychlá diagnostika systému při odhalování poruch, to je jen krátký výčet kladů komunikačního systému IO-Link.

Výrobce Molex nabízí pro IO-Link několik produktů z řady HarshIO, které fungují jako IO-Link Master a umožňují prostřednictvím protokolů Profinet nebo EtherNet/IP propojit IO-Link s nadřazeným řídicím systémem. Modul IO-Link Master má osm univerzálních portů – každý z osmi portů dovolí připojit jedno zařízení IO-Link a jeden standardní vstupní nebo výstupní digitální signál.

Doplňkem pro rozšíření počtu portů modulu IO-Link Master je digitální rozbočovač I/O Hub. Jde o I/O modul s osmi duálními porty M12, který s modulem IO-Link Master komunikuje taktéž prostřednictvím IO-Link (*obr. 3*).

Uvedené produkty na český trh dodává společnost OEM Automatic.

(OEM Automatic, spol. s r. o.)

SCADA Security Conference 2017

Ve dnech 12. a 13. října 2017 uspořádala společnost Progres Partners Advertising v pražském hotelu DAP v rámci projektu Future Forces Forum (FFF) první ročník konference SCADA Security.

V nabídce akcí FFF má konference SCADA Security dlouhodobé ambice řešit aktuální i budoucí hrozby, sledovat trendy a určovat správný směr vývoje v oblasti zabezpečení systémů pro sběr dat a dispečerské řízení (SCADA). V době tzv. hybridních válek se právě úspěšná kybernetická obrana stává významným prvkem celkové bezpečnosti nejen průmyslu.

Na konferenci vystoupilo 29 řečníků ze sedmi zemí a zúčastnilo se jí 166 registrovaných odborníků z deseti zemí.

Témata konference byla rozdělena do osmi okruhů, které řešily:

- aktuální a budoucí kybernetické trendy a hrozby,
- nové technologie v oblasti bezpečnosti průmyslových řídicích systémů,
- bezpečnost řídicích systémů,
- telematiku a bezpečnost moderních dopravních prostředků,
- rozdíly mezi informačními a operačními technologiemi,
- odpovědnost podnikatelských subjektů a státu v ochraně kyberprostoru,
- koncept Industry 4.0,
- lidský faktor ve vztahu ke kybernetické bezpečnosti.

Konference byla dále doplněna několika bilaterálními a multilaterálními jednáními. Jedním z nich byl např. kulatý stůl na téma Bezpečnostní složky a systémy SCADA za účasti zástupců Ministerstva obrany ČR, Národního úřadu pro kybernetickou a informační bezpečnost, akademických a průmyslových organizací, vedený pod organizační záštitou Pracovní skupiny kybernetické bezpečnosti sdružení AFCEA (*Armed Forces Communications and Electronics Association*). Dalším příkladem je Portugalsko-italsko-slovensko-české fórum o vzájemné spolupráci v oblasti kybernetické bezpečnosti, pořádané portugalskou pobočkou AFCEA.

Během konference si zájemci mohli prohlédnout doprovodnou výstavu produktů a řešení jednotlivých partnerů konference, kde byla prezentována konkrétní řešení dopadů kybernetických hrozeb a také postupů, jak takovým hrozbám čelit a předcházet. Příkladem je prezentace Tobiase Schroedela, který v několika praktických ukázkách názorně předvedl dopady těchto hrozeb a možná rizika v oblasti informačních systémů (IT) a provozních zařízení (OT). Zúčastnilo se rovněž množství právních expertů, kteří se zapojili do diskuse nejen ohledně odpovědnosti za škody způsobené kybernetickými útoky, ale i v oblasti ochrany osobních údajů či bezpečnosti průmyslových řídicích systémů. Kybernetická bezpečnost se tak ukázala jako multidisciplinární obor, ve kterém IT a bezpečnostní odborníci zastupují jen jednu komunitu moderní společnosti.

Atraktivní program, který doprovázel intenzivní networking během konferenčních přestávek a večerního společenského setkání, spolu s početnou účastí zástupců z oblasti informatiky i průmyslu, státních institucí, vědy a výzkumu poskytly všem účastníkům mnoho zajímavých informací, novinek, nových kontaktů a přístupů včetně obchodních příležitostí pro partnery a vystavovatele.

K převládajícím myšlenkám, o kterých se diskutovalo, patřilo, že kritická informační infrastruktura tvoří páteř moderní společnosti. Průmyslové řídicí systémy jsou důležitou součástí této kritické infrastruktury, avšak zatím na ně není kladen patřičný důraz, a to i přesto, že v posledních několika letech bylo mnoho kybernetických útoků vedeno právě proti nim.

Konstruktéři průmyslových zařízení se inspirují prvky běžnými ve světě ICT a využívají je, aby dosáhli lepší propojitelnosti a nižší ceny. Propojení IT a OT nebo koncept IoT vedou k vyšší produktivitě, avšak zároveň se průmyslové řídicí systémy stávají výrazně zranitelnějšími kybernetickými útoky.

S realizací procesů podle metodiky průmyslu 4.0 nebezpečí v průmyslu skokově roste. Bylo konstatováno, že se již nyní smazala obrana hranice, tzv. perimetru, která ještě donedávna platila jako cesta k obraně řídicích systémů před útoky zvenčí. Jednou z možností snížení rizik je přístup k řídicí síti jako k jednomu z technologických uzlů celé řídicí infrastruktury. Znamená to průběžně sít monitorovat, diagnostikovat, analyzovat nestandardní situace a tak odhalovat možné cílené útoky již v počátku a zmenšit rozsah škod, popř. zcela zabránit poruchám, haváriím a produkci mimo tolerance. Představa cíleného útoku na software robotu není nereálná. Na jednoznačných faktech bylo dokladováno, jak snadno lze z internetu získat konfigurační programy řídicích jednotek a na základě substitučních hesel se připojit na jejich programové vybavení.

Cestou bezpečné digitalizace se jeví standardizace všech procesů, snižování operativy a vytváření simulačních modelů.

Velkým tématem jsou lidé. Od konstatování, že přes 90 % cílených útoků je vedeno prostřednictvím personálu, po vztah provozních a vedoucích zaměstnanců ke kyberbezpečnosti. Za nedostatečnou je považována situace, kdy se v této oblasti vzdělávají jednotlivci, ale ne týmy. Nicméně nabídka školení existuje.

Tématu vztahů personálu k bezpečnosti se dotklo několik přednášek z různých oblastí bezpečnosti při řízení procesů v průmyslovém podniku. Od nebezpečí práce v *home office* po stále se objevující bariéry mezi podnikovými informatiky a automatizací. Metodika průmyslu 4.0 by měla tyto mentální bariéry odstraňovat, avšak i přednášející na této konferenci konstatovali, že informatici mají své podnikové sítě dobře zabezpečené, ale riziko představují pracovníci odpovědní za realizaci a provoz automatizace: doslova byli nazváni „šmudlové v koutku“. Tento názor dokumentuje nekompetentní přístup informatiků k bezpečnosti provozu všech informačních systémů v průmyslu. Věřme ve změnu myšlení všech zainteresovaných dříve, než některá z cílených kyberhrozeb dojde naplnění.

Konference Scada Security 2017 byla jednoznačně přínosem k důležitému tématu bezpečnosti řízení nejen v průmyslu, ale všude tam, kde se prvky automatizace a řízení využívají – v zemědělství, v zásobování energiemi, dopravě, městech a domech. Výměna i protichůdných názorů je důležitá. Velký dík patří organizátorům i partnerům akce.

Radim Adam