

Simulace a testování programu

Pro instalaci systému TwinCAT jako takovou není nutná žádná zvláštní licence, součástí volně dostupné instalace je vývojové prostředí (které je zdarma) a runtime, který může běžet v režimu zkušebních licencí (jež jsou také zdarma, ale je nutné je každých sedm dní obnovit z vývojového prostředí). Simulace a testování programu v prostředí TwinCAT tedy mohou být vykonány v podstatě na jakémkoliv počítači a není třeba ani

kupě žádných licencí. Licenci je tudíž nutné zakoupit až při reálném použití hotového a odladěného programu.

Závěr

Software pro řízení od společnosti Beckhoff je používán už od roku 1988. První software měl název S1000 a běžel pod operačním systémem DOS. Dalším krokem byl velmi známý a stále hojně používaný TwinCAT 2, který byl uveden na trh v roce 1996. Od roku

2010 se začala používat nejnovější verze řídicího softwaru TwinCAT 3. V průběhu času doznal TwinCAT značných změn a od doby jeho vzniku přibýlo množství nových funkcí (nedávno např. počítačové vidění nebo komunikace s cloudem), ale základní funkce, a to rozšíření operačního systému Windows o možnost práce v reálném čase a PLC řízení, zůstává.

(BECKHOFF Česká republika, s. r. o.)

Konference Kaspersky Lab v Soči

Ve dnech 19. až 21. září uspořádala společnost Kaspersky Lab v ruském městě Soči mezinárodní konferenci na téma Kybernetická bezpečnost v průmyslu: příležitosti a výzvy v době digitální transformace.

Podobnou konferenci pořádala Kaspersky Lab již poště a účastníci se jí přední odborníci na digitální zabezpečení průmyslových řídicích systémů, specialisté a manažeři z přibližně dvaceti zemí: více než 250 účastníků přijelo kromě domácího Ruska také z Číny, USA, zemí EU, Saudské Arábie, Spojených arabských emirátů, Íránu, Egypta nebo Japonska. Byli mezi nimi zástupci významných firem v oboru (Honeywell, Schneider Electric, Omron Corporation, Siemens), výzkumníci a profesori z mezinárodních univerzit a výzkumných institucí (Clemsonova univerzita v Jižní Karolině v USA, Singapurská univerzita techniky a designu, německý Fraunhoferův institut optroniky, systémové techniky a zpracování obrazu nebo Ruské národní koordináční středisko pro počítačové incidenty). Mezi pozvanými hosty a řečníky byli také zástupci americké asociace pro automatizaci ISA, která se problematice kybernetické bezpečnosti v průmyslu dlouhodobě věnuje (soubor standardů ANSI/ISA 62443, dříve ISA S99, je jejich dílem), nebo prestižní konzultantské společnosti ARC Advisory Group, která nedávno otevřela svou pobočku v Rusku.

Hlavním tématem všech přednášek, diskusí a sdílení informací bylo, jak bezpečně propojit informační techniku a systémy s průmyslovou řídicí technikou, ať jde o řízení strojů, robotů, celých závodů, nebo distribučních sítí. Diskutovalo se rovněž o využití

umělé inteligence při zajišťování kybernetické bezpečnosti, aktuálních principech hodnocení zabezpečení průmyslových řídicích systémů nebo o možnostech využití penetračních testů v průmyslu. Mnohé zcela nové problé-

nických sekcí. Celkem polovina z padesáti přednášek byla prezentována řečníky ze zemí mimo Rusko.

V podnikatelské sekci se diskutovalo mj. o regulatorních požadavcích v oblasti kybernetické bezpečnosti, jako je např. nový ruský zákon o kybernetické bezpečnosti kritické infrastruktury, dále o tom, jak vybrat efektivní nástroje k zajištění kybernetické bezpečnosti, a o praktických aspektech zajištění kybernetické bezpečnosti v průmyslu.

V technické sekci si účastníci vyměňovali zkušenosti s implementací opatření na zabezpečení průmyslových řídicích systémů v praxi, s detekcí kyber-fyzických hrozeb a hledáním slabých míst v průmyslových řídicích systémech.

Během přestávek mohli účastníci zavítat též na výstavku, kde měli možnost seznámit se s produkty Kaspersky Lab, ICL System Technologies, Avantech a USSC. Ve stánku firmy Kaspersky Lab mohli účastníci poprvé vidět také nový KICS for Networks: specializovaný software pro sledování průmyslových komunikačních sítí, který detekuje všechny anomálie v provozu a registruje důležité události z hlediska zabezpečení informací bez toho, že by jakkoliv ovlivňoval vlastní řízení průmyslových procesů.

Během konference jsem natočil dva rozhovory, na jejichž základě vzniknou články, které budou zveřejněny v následujících vydáních časopisu *Automa*: o mýtech v oblasti zabezpečení průmyslových řídicích systémů a o chytré výrobě a průmyslu 4.0 v Rusku.

Petr Bartošík



Obr. 1. Pohled do přednáškového sálu



Obr. 2. Doprovodná výstavka představila mj. řešení KICS for Networks od Kaspersky Lab

my s sebou přinášíjí koncepce průmyslového internetu věcí, průmyslu 4.0, *smart grids* a *smart cities*.

Konference se skládala z plenárních přednášek a paralelních podnikatelských a tech-