Pod lupou
- odborné združenia, organizácie, úrady

Cieľom tejto pravidelnej rubriky je informovať vás o dianí v oblasti elektrotechniky a automatizácie z pohľadu rôznych záujmových združení, medzinárodných organizácií či orgánov štátnej správy. Budeme sa snažiť informovať vás o významnejších projektoch a aktivitách, ktoré majú priamy vplyv na dianie na slovenskom trhu alebo by mohli byť aspoň inšpiráciou pre celú odbornú komunitu.

International Society of Automation (ISA)

Norma ISA99 Kybernetická bezpečnosť a správa o inovovaných technológiách je k dispozícii

Nová americká národná norma a inovovaná, široko používaná technická správa, ktoré sa týkajú kybernetickej bezpečnosti, boli publikované združením ISA.

Nová norma ANSI/ISA-99.00.01-2007 Bezpečnosť priemyselných automatizačných a riadiacich systémov, časť 1: Terminológia, koncepcie a modely je prvou zo série noriem ISA, ktoré rozoberajú kybernetickú bezpečnosť pre priemyselné automatizačné a riadiace systémy. Prvá časť sa venuje kľúčovým koncepciám, terminológii a modelom a bude slúžiť ako základ pre ďalšie normy, ktoré sa aktuálne v rámci série noriem ISA99 pripravujú. Inovovaná technická správa ANSI/ISA-TR99.00.01-2007 Bezpečnostné technológie pre priemyselné automatizačné a riadiace systémy poskytuje prehľad a posúdenie v súčasnosti dostupných nástrojov kybernetickej bezpečnosti, technológie a prostriedky obrany pre zmiernenie kybernetických útokov. Pravidlá uverejnené v technickej správe sú určené pre existujúce aj nové priemyselné automatizačné a riadiace systémy, ktoré sa používajú na reguláciu a monitorovanie mnohých priemyselných aplikácií a kritických procesov.

Technická správa opisuje kľúčové kategórie technológií kybernetickej bezpečnosti, typy produktov dostupných v týchto kategóriách a výhody a obmedzenia používania týchto produktov v prostredí priemyselných automatizačných a riadiacich systémov, ktoré je náchylné na útoky a známu kybernetickú zraniteľnosť. Navyše správa poskytuje odporúčania a návody použitia týchto produktov kybernetickej bezpečnosti. ISA Inštitút pre dodržiavanie kybernetickej bezpečnosti bude mať za úlohu identifikovať a propagovať štandardizované produkty a systémy kybernetickej bezpečnosti v aplikáciách priemyselných automatizačných a riadiacich systémov. Produkty alebo systémy vyhovujúce spomínanej norme a technickým predpisom budú mať oprávnenie prezentovať sa označením ISASecure, čo bude pre vlastníkov podnikov, systémových integrátorov a nákupcov úplne jasným odlíšením bezpečnostných vlastností od ostatných systémov.

HART Communication Foundation (HCF)

HCF pripravilo nové vývojové a testovacie nástroje

HART® Communication Foundation (HCF) oznámilo koncom minulého roku vydanie verzie 3. 1. Integrovaného vývojového prostredia na opis HART zariadení (HART Device Description Integrated Development Environment DD-IDE). Táto nová veria podporuje HART-om rozšírenú špecifikáciu jazyka na opis zariadení (DDL), ako aj zariadení pre normu WirelessHART. Skupina nástrojov HCF DD-IDE je komplexným súborom programovacích nástrojov pre efektívny vývoj, testovanie a údržbu opisov HART zariadení. „Nová skupina nástrojov DD-IDE je súčasťou trvalého procesu zlepšovania technológie Foundation a zároveň snahou zlepšiť vytváranie a testovanie opisov HART zariadení pre nové zariadenia alebo vylepšené prevádzkové zariadenia," skonštatoval Ed Ladd, riaditeľ technologických programov v HART. „Navyše nová technológia pre vývoj a testovanie opisov zariadení bola široko prijatá vývojármi zariadení a prístrojov, ako aj dodávateľmi zariadení na celom svete."

Klúcovými prvkami novej DD-IDE verzia 3.1. sú:
- ? aktualizovaný konfigurátor inteligentných prístrojov SDC-625 na validáciu a testovanie opisu zariadení,
- ? aktualizovaný simulátor zariadení XM TR-DD,
- ? vylepšený DDL Tokenizer,
- ? nový editor opisu zariadení,
- ? vylepšený pomocník (wizards) pre vývoj opisu zariadení.

Nový DD-IDE zlepšuje produktivitu vývojárov vďaka zjednodušeniu vývoja opisu zariadení, a to vďaka pridaniu štandardných „C" nástrojov a podpore predchádzajúcich vývojových etáp. Jazyk na opis zariadení (IEC 61804-2, EDDL) je od roku 1990 kľúčovým prvkom technológie HART a je HART normou a zároveň jedinou technológiou schválenou HCF na konfigurovanie HART zariadení. Vylepšený jazyk na opis zariadení (DDL) zjednodušuje a zjednocuje prezentáciu informácií o inteligentných zariadeniach pre dodávateľov aj používateľov automatizácie na celom svete.

IEC

Funkčná bezpečnosť: výpočet rizika, záchrana životov

Elektrické, elektronické alebo programovateľné elektronické systémy vykonávajú čoraz častejšie bezpečnostné funkcie. Tieto systémy sú zvyčajne zložité, čo v praxi neumožňuje kompletne určiť každý chybový stav alebo otestovať všetky možné režimy práce. Je náročné predpovedať bezpečné správanie, hoci testovanie je jednou so základných vecí. Výzvou je navrhovať systémy takým spôsobom, aby sme sa v prevádzkach vyvarovali nebezpečných zlyhaní alebo aby sme ich dokázali riadiť už na začiatku ich vzniku. IEC61508 zahŕňa funkčnú bezpečnosť bezpečnostných systémov, ktoré využívajú elektrické a/alebo elektronické a/alebo programovateľné elektronické technológie. IEC publikovalo interview s guru v oblasti funkčnej bezpečnosti Ronom Bellom o jeho osobných názoroch, čo to funkčná bezpečnosť je a ktorým smerom sa bude do roku 2010 vyvíjať séria populárnych noriem IEC 61508.

11. decembra 2005, v sklade paliva v anglickom Buncefielde, sa spínač preplnenia, ktorý mal monitorovať výšku hladiny paliva, pokazil práve vtedy, keď zamestnanci plnili palivo do zásobníka. Palivo sa vylievalo do okolia, vyparovalo sa, dosiahlo k zdroju iniciácie a vybuchlo. Výsledkom bolo, že oheň sa podarilo uhasiť až po štyroch dňoch. Dvadsať bielych valcových palivových zásobníkov prasklo ako vajíčka. Aj keď nedošlo k iným nešťastiam, boli zničené domy a obyvatelia museli byť evakuovaní. O niekoľko mesiacov skôr, 23. marca 2005 explodovalo v americkom meste Texas potrubie petrochemickej spoločnosti BP, pričom o život prišlo 14 ľudí.

Nie všetky udalosti môžu byť také dramatické alebo medializované ako Bouncefield či Texas, avšak tie len podčiarkujú skutočnosť, že systémy zlyhávajú. Po takýchto udalostiach začnú experti na bezpečnosť študovať

reťaz udalostí a vykonávajú analýzu danej náhodnej poruchy. Expert IEC Ron Bell konštatuje, že analýza poruchy pomáha identifikovať, čo sa urobilo zle. Oveľa podstatnejšie však je, že odhalenie zlomového bodu pomáha navrhovať riadiace systémy tak, aby sa riziko nebezpečných situácií znížilo na minimum. Systémy funkčnej bezpečnosti sú skôr aktívne ako pasívne. Bezpečnostné pásy nemôžu byť systémom funkčnej bezpečnosti, ale napr. airbag takýmto systémom je. Nakoľko sa celosvetový trh čoraz viac globalizuje, ázijský trh expanduje, ceny súdnych žalôb rastú a environmentálne povedomie trvalo rastie, čoraz viac narastá aj požiadavka noriem na správne postupy navrhovania či už airbagov v autách, kolotočov, vlakov či detských inkubátorov. To viedlo k prijatiu noriem bezpečnosti v mnohých krajinách. Trh funkčnej bezpečnosti, ktorý v roku 2007 dosiahol úroveň 850 mil. USD, by mal v tomto roku narásť o ďalších 50 mil. USD.

Spoločenské a ekonomické súvislosti

Slovné spojenie „správne postupy" majú vo svete noriem pre bezpečnosť, ako je aj IEC 61508 Funkčná bezpečnosť elektrických, elektronických a programovateľných elektronických bezpečnostných systémov, špecifický význam. Hlavnou myšlienkou je dosiahnuť funkčnú bezpečnosť bezpečnostných systémov. Aby to bolo možné, treba vziať do úvahy každú fázu od začiatočného konceptu cez vypracovanie bezpečnostných požiadaviek až po schémy bezpečnosti, konštrukcie, inštalácie, údržby a modifikácie. R. Bell toto nazýva „životným cyklom bezpečnosti". Tento životný cyklus umožňuje vytvoriť bezpečnostné systémy s definovanou úrovňou bezpečnostných vlastností a zníženým rizikom poruchy. Každý bezpečnostný systém vyžaduje vykonávanie bezpečnostných funkcií a tie sa realizujú prostredníctvom postupnosti krokov vykonávaných elektronicky alebo niekedy prostredníctvom zásahu človeka. Prvým krokom je identifikácia, čo musí bezpečnostný systém nevyhnutne vykonať. Táto časť normy IEC 61508 sa zaoberá funkciou bezpečnosti. Identifikuje začiatočné riziko bez existujúcej ochrany a to, čo treba vykonať na dosiahnutie cieľového prijateľného rizika. Zo spoločenského pohľadu je výraz „prijateľný" práve tým ošemetným, skonštatoval R. Bell, pretože sa potvrdilo, že takéto systémy sa pokazia. Náročnou úlohou je schopnosť maximalizovať prínosy a možnosti počítačových technológií pri dosiahnutí prijateľných rizík v riadených technológiách a prevádzkach. „Bezpečnostné systémy v chemických podnikoch sú čoraz viac postavené na báze počítačov a chybové stavy sú zložité. Len prijatím systematického prístupu k všetkým aspektom návrhu a aplikácie takýchto bezpečnostných systémov možno získať istotu, že sa podarí dosiahnuť cieľovú hranicu prijateľného rizika," skonštatoval R. Bell.

V Buncefielde sa pokazil snímač výšky hladiny; v Texase vybuchlo staré potrubie. „Dôležitou stránkou je určenie prijateľného rizika spojeného s konkrétnymi nebezpečnými udalosťami v riadení prevádzok a technológií. Prijateľné riziko je vytvorené z postupnosti udalostí zlyhaní a frekvencie výskytu týchto postupností. V kontexte návrhu bezpečnostných systémov sa to môže pretlmočiť do otázky, akú najnižšiu frekvenciu porúch ste pripravený akceptovať pre bezpečnostný systém, aby ste dosiahli konkrétne úroveň prijateľného rizika?" uviedol R. Bell. Odpoveď na túto otázku determinuje, aké spoľahlivé majú byť bezpečnostné systémy. Akú cenu sú občania ochotní zaplatiť za bezpečnosť? Vyzerá to tak, že iróniou je, že ochrana životov, samozrejme teoreticky, determinuje, koľko úmrtí ste ochotní prijať.

Bezpečnostné kruhy

Len čo sú tieto hranice bezpečnosti dohodnuté, fáza návrhu určí úrovne bezpečnosti jednotlivých funkcií. Keďže tieto systémy sú stavané na presne danú chybovosť, odborníci na funkčnú bezpečnosť, napr. R. Bell, charakterizujú bezpečnosť skôr ako integritu než ako spoľahlivosť. Tak vznikli úrovne bezpečnostnej integrity (safety integrity levels, SIL) od 1 po 4, pričom 1 je najnižšia a 4 najvyššia úroveň bezpečnostnej integrity. A tu je priestor práve pre IEC 61508. Táto norma uvádza parametre návrhu pre každú úroveň. Najjednoduchšie je predstaviť si tieto systémy ako kruhy obkľučujúce konkrétny cieľ, napr. petrochemickú prevádzku. Pridanie každého jedného kruhu prináša ďalšiu úroveň bezpečnosti. Jeden kruh môže predstavovať elektronický alarm; ďalší kruh môže predstavovať systém na zníženie tlaku. Práve vďaka viacúrovňovému modelu nemusia byť všetky bezpečnostné systémy prísne stavané na úroveň SIL 3 alebo 4. Čím viac systémov máte, tým môže byť každá SIL nižšia. Zahrnutie spomínaných kruhov od začiatku je z hľadiska bezpečnostnej integrity tou najlepšou cestou, ako predísť haváriám. Predtým, ako sa stal R. Bell riaditeľom Electrical and Control System Group v anglickej inštitúcii HSE (Health&Safety Executive), analyzoval spolu so svojimi kolegami 37 havárií zapríčinených chybou riadiacich systémov vo fáze ich životného cyklu. Výsledky publikované v knihe s názvom „Bez kontroly: prečo systémy zlyhávajú a ako predchádzať zlyhaniam" (HSE Books, 2003) uviedol, že viac ako 60 % zlyhaní sa stalo pre nevhodné technické podmienky, čo znamená, že chyby boli do systému vnesené skôr, ako bola daná aplikácia spustená. „Identifikácia, aké sú riziká, je skutočne veľmi náročná úloha, pretože potrebujete identifikovať, čo zlé sa môže stať predtým, ako budete môcť povedať „tak takto tomu môžeme predísť". Takže ak v zložitom obrábacom stroji alebo nejakej prevádzke nedokážete identifikovať, čo by sa mohlo pokaziť, tak potom, keď sa to naozaj pokazí, nemáte nič po ruke, čím by ste to zastavili," uviedol R. Bell. To je teda oblasť, ktorú rieši IEC 61508.

Dnešné a budúce výzvy

Pri návrhu bezpečnostných systémov existuje veľa nesprávnych možností, ktoré by mohli znamenať vznik rizika. Ak neidentifikujete kľúčové kroky v reťazci, potom ani nemôžete nasadiť niečo, čo by takémuto riziku predchádzalo. Ak nebudete vedieť, čo má bezpečnostný systém robiť, tak potom nebudete vedieť robiť nič, keď sa skutočne niečo stane. Podobne môžete chybne navrhnúť bezpečnostný systém na úroveň SIL 1, keď mal byť navrhnutý aspoň na úroveň SIL 3, čo zvyšuje možnosť vzniku nehody. Rovnaké výzvy a úlohy sa však kladú aj na ekonomiku návrhu. Nedá sa navrhnúť hneď všetko najlepšie, pretože je to extrémne nákladné. Treba si uvedomiť zákonné požiadavky krajiny, v ktorej bude zariadenie nasadené, a uistiť sa, že prijateľné riziko možno dosiahnuť vďaka týmto predpisom," skonštatoval R. Bell. Mnohé podniky a prevádzky boli postavené pred desiatkami rokov. Tieto „zastarané systémy" čakajú jedinečné výzvy, obzvlášť z pohľadu odborného personálu. Dlhoročný pracovníci poznajú každé jedno zariadenie tak dobre, že sa nepotrebujú pozerať do dokumentácie na ich bežnú prevádzku a údržbu. IEC 61508 umožňuje vykonať diferenčnú analýzu zastaraných systémov. Zjednodušene povedané, umožní vám to skontrolovať, aké zastarané sú pôvodné systémy vzhľadom na aktuálne najlepšie riešenia špecifikované v IEC 61508. Potom nasleduje rozhodnutie, aké opatrenia bude potrebné prijať. V mnohých prípadoch sa totiž staré bezpečnostné systémy dosť odlišujú od tých, ktoré by sme navrhli v súčasnosti. „Kľúčovou vecou je zabezpečiť, že po vykonaní diferenčnej analýzy bude vykonaný zodpovedný plán ďalšieho postupu," uviedol R. Bell. Normy IEC prechádzajú v súčasnosti revíziou, ktorá by sa mala zavŕšiť začiatkom roku 2010.

-tog-

www.atpjournal.sk

Norma ISA99 Kybernetická bezpečnosť a správa o inovovaných technológiách sú k dispozícii na adresách www.isa.org/isa9900012007 a www.isa.org/isatr9900012007.

Viac informácií o ISASecure možno nájsť na adrese www.isa.org/ISASecure.

Viac informácií o sérii IEC noriem 61508 nájdete na adrese http://www.iec.ch/zone/fsafety/.