Softvér ako súèas´ riešenia bezpeènosti

Ve¾kos´ nákladov a zlo´itos´ spojená s dosiahnutím všetkých po´iadaviek kladených na bezpeènos´ stále rastie. Zoznam bezpeènostných a vládnych nariadení a noriem rastie a výsledkom je väèší tlak na u´ aj tak napnuté termíny a rozpoèty výdavkov, stále vzdelávanie a preško¾ovanie in´inierov èi kratší èas na pridávanie nových funkcií do zariadení.

Nadradenos´ bezpeènosti v riadení a automatizácii procesov sa zo zrejmých dôvodov nebude zmenšova´. Okrem etických a morálnych imperatívov sú tu ešte právne, finanèné a obchodné dôvody. Nedostatoèné vyhovenie týmto po´iadavkám znamená potenciálny problém zákonnej zodpovednosti, finanèné pokuty a stratu trhov. V mnohých, presne zdokumentovaných prípadoch viedlo nedodr´anie po´iadaviek k zásahu regulaèných orgánov a previerkam bezpeènosti, èo vytvorilo nie dobrý obraz danej spoloènosti a prepad zisku.

Keï´e sa prostredníctvom zabudovaných softvérových aplikácií dostáva do riadiacich a automatizaèných systémov èoraz viac funkcií súvisiacich s bezpeènos´ou, je jednoduché predstavi´si proces vývoja softvéru ako súèas´ celého problému bezpeènosti. Tento poh¾ad je však krátkozraký. Dobrá softvérová platforma a správne vývojové nástroje a technológie pou´ívané správnym spôsobom umo´òujú v súèasnosti vytvori´pevný základ na splnenie naj´iadanejších noriem týkajúcich sa certifikácie bezpeènosti – na èas a v rozsahu plánovaných investièných prostriedkov.

V tomto èlánku opisujeme tri kroky, ako mô´u výrobcovia procesných riadiacich a automatizaèných systémov vyu´i´mo´nosti a silu nových zabudovaných softvérových riešení na zní´enie nákladov pri zachovaní zhody s po´iadavkami bezpeènosti a získaní novej formy konkurenènej výhody.

Krok 1: Unifikácia vyu´ívania viacjadrových technológií a virtualizácie

Unifikácia je tradènou cestou k úspore nákladov. Avšak pre dodávate¾ov riadiacich a automatizaèných systémov na trhu vyvstáva nieko¾ko komplikácií. Aby mohli produkty preukáza´zhodu s normou IEC61508, musia by´ich ´a´iskové technológie podrobené certifikácii. To následne zvyšuje náklady a èas umiestnenia skúšaného produktu na trhu. Po´iadavky na väèšiu prepojite¾nos´ – drôtovú (ethernet) aj bezdrôtovú (Bluetooth, WLAN) – vytvárajú ïalšie výzvy v oblasti schopnosti vzájomnej spolupracovate¾nosti z h¾adiska rôznorodých komunikaèných protokolov. Mnohí dodávatelia majú ve¾kú bázu inštalácií postavenú na starších systémoch, ktoré vy´adujú údr´bu, a musia nájs´nové spôsoby, ako ich inovova´bez straty investícií. Pre tých, ktorí chcú zo´a´úrodu z unifikácie bez ohrozenia zhody s normami ochrany a bezpeènosti, sú tu dva nové smery na trhu zabudovaných systémov, prinášajúce reálne riešenie tejto situácie: viacjadrové procesory a technológia virtualizácie (hypervízor).

Najnovšie viacjadrové procesy sa z h¾adiska výkonu výrazne zlepšili a vzrástol aj výkon na watt pri jednojadrových procesoroch. Zlepšila sa aj ich aplikaèná rozširovate¾nos´ a vïaka nahradite¾nosti procesorov s viacerými jadrami sú ochránené aj investície do softvéru. Trendy smerujúce k viacjadrovým procesorom sú u´ jednoznaène a k dispozícii sú na to optimalizované operaèné systémy, middleware a rôzne podpor-

né nástroje. Vyu´ itím najnovších viacjadrových technológií a virtualizaèných koncepcií sú dodávatelia v súèasnosti schopní kombinova´ rôznorodé operaèné systémy na jednej zdru´ ujúcej platforme, èo vytvára pevný základ na zni´ ovanie nákladov za rôzne materiálové vstupy a rastúcu funkcionalitu.

Druhým z prístupov je virtualizácia, ktorá umo´ òuje spúš´ anie viacerých operaèných prostredí nezávisle jedného od druhého na jednom fyzickom zariadení. Napr. na jednom zariadení tak mo´ no ma´ spustený operaèný systém reálneho èasu, napr. VxWorks, a univerzálny operaèný systém, napr. Linux. Takéto oddelenie alebo segmentovanie disku dovo¾uje ove¾a flexibilnejšie priraïovanie (alokáciu) zdrojov. Napríklad jadrá na výpoèty mô´ u by´ výluène priradené jednej virtuálnej doske alebo ich mô´ u sploène vyu´ íva´ viaceré virtuálne dosky. Pamä´ mô´ e by´ segmentovaná tak, ´ e ka´ dá doska má svoj jedineèný, pevne stanovený pamä´ ový priestor, do ktorého nemô´ e zasiahnu´ ´ iadna iná virtuálna doska. Virtualizácia tie´ umo´ òuje oddeli´ funkcie súvisiace s bezpeènos´ ou (napr. softPLC) od ostatných funkcií. Do úvahy treba vzia´ aj skutoènos´ , ´ e unifikované platformy budú tlaèi´ na potrebu mno´ stva rôznorodých platforiem operaèných systémov. Operaèné systémy sa budú èoraz viac vyu´ íva´ metódami najlepších skúseností. Operaèné systémy reálneho èasu majú v porovnaní s univerzálnymi operaènými systémami, ako je napr. Linux, ve¾kú výhodu z h¾adiska po´ iadaviek na determinizmus èi menšiu zlo´ itos´ , èo z nich robí vhodných kandidátov na proces certifikácie èo do bezpeènosti. Linux má na druhej strane ve¾ké výhody pri implementácii rýchlo sa rozvíjajúcich komunikaèných štandardov alebo GUI (grafických pou´ ívate¾ských rozhraní). Je teda zmysluplné vyu´ i´ prínosy obidvoch systémov pri návrhu nových systémov a vy´ a´ i´ to najlepšie z obidvoch svetov. Vyu´ ívaním unifikovaných technológií, ako je hypervízor, sa to stáva skutoènos´ ou.

Viacjadrové procesory a virtualizácia sú sploène presvedèivou kombináciou, ktorá výrazne zvyšuje výkon a spo¾ahlivos´ priemyselných systémov. Výsledkom je, ´ e výrobcovia prevádzkových riadiacich a automatizaèných systémov mô´ u spoji´ viac funkcionality do menších fyzických zariadení, zní´ i´ ich cenu a zlo´ itos´ a upriami´ pozornos´ na splnenie po´ iadaviek spojených s certifikaèným procesom týkajúcim sa bezpeènosti.

Mnohé firmy sa u´ vrhli do nasadzovania viacjadrových a hypervízorových technológií a sú uvelièené z toho, èo všetko doká´ u vo svojich zariadeniach ponúkny´ , a to bez narastania zlo´ itosti èi skrytých „náš¾apných mín“.

Krok 2: Štandardizácia na otvorených platformách

Vzh¾adom na vzrastajúcu pozornos´ rozlišovania na softvérovej vrstve sa zmenila aj úloha zabudovaných softvérových aplikácií. Mo´ nos´ prida´ funkcie ochrany a bezpeènosti prostredníctvom softvéru do štandardizovanej hardvérovej platformy sa stala k¾úèovou témou. V súèasnosti je u´ be´ né, ´ e programovate¾né logické automaty pou´ ívajú jadrá (kernels) s reálnym èasom. Avšak konvergencia a unifikácia prináša výsledky v celom hodnotovom re´ azci. Výrobcovia strojných zariadení sa v súèasnosti spoliehajú na softvér, v ktorom vytvárajú celé prostredie na bezpeènos´ , ochranu a prepojite¾nos´ . Práve oni sa nachádzajú v pozícii unifikácie funkcií, ale zároveò potrebujú výraznú podporu zo softvérovej vrstvy. Súèasne sa problematika bezpeènosti a ochrany posúva v rámci celého hodnotového re´ azca, èo vy´ aduje potrebu u´ ších partnerstiev s dodávate¾mi vývojových nástrojov na zabudovaný softvér, operaèné systémy a middleware. Nako¾ko systémy sa stávajú èoraz otvorenejšie a štandardizovanejšie, majú výrobcovia strojných zariadení ve¾ké mo´ nosti zdru´ ovania a hladkej integrácie rôznorodých subsystémov pri súèasnom zní´ ení nákladov a zlo´ itosti. Uvedené trendy prinášajú výrobcom potenciál na riešenie problémov z h¾adiska celého ´ ivotného cyklu zariadení. Vývojový cyklus býva zvyèajne od dvoch do troch rokov, cyklus dodávania zariadenia býva zvyèajne do osem rokov s po´ iadavkou na podporu poèas desiatich rokov. ´ ivotný cyklus zariadenia, ktorý býva v niektorých prípadoch aj viac ako 20 rokov, je pod tlakom ïalšieho predl´ ovania, a to prostredníctvom èastejších programov aktualizácie, èo však z poh¾adu dodávate¾ov vytvára po´ iadavku na rozsiahlejšiu podporu.

Dodávatelia softvérových zariadení mô´ u zákazníkom pomôc´ prekona´ tieto aj ïalšie výzvy, ako napr. ochráni´ podiel na trhu, duševné vlastníctvo a èas uvedenia zariadenia na trh a zároveò zní´ i´ celkové náklady na vlastníctvo. Vïaka modulárnemu softvéru mo´ no napríklad zní´ i´ èas uvedenia zariadenia na trh, avšak prvky, ako zásobník UDP (User Datagram Protocol), treba certifikova´ opakovane. Prostredníctvom modulárnej certifikácie mô´ u by´ štandardné softvérové prvky dodané ako súèas´ certifikovaného balíka, èím sa z nich stávajú dôveryhodné prvky. Zákazníci sa tak mô´ u spolieha´ na tento zdokladovaný softvérový balík certifikovaný pod¾a normy IEC 61508, ktorý umo´ òuje urýchli´ proces preukazovania zhody, ale aj väèšiu prispôsobite¾nos´ u´ vo fáze vývoja.

Pre mnohých výrobcoch strojov, ktorí pošku¾ujú po vyu´ ívaní Linuxu, problematika podpory naberá na váhe. Aj v tomto prípade existuje urèitá unifikácia technológií, spojená s lepšími vývojovými nástrojmi, ale aj s ve¾kým roztrieštením na trhu s riešeniami postavenými na Linuxe. Výrobcovia sa namiesto vyu´ ívania podporovaných a preverených komerèných riešení èasto pokúšajú dáva´ dokopy bezplatné linuxové riešenia. Úplne sa podceòuje komplexnos´ Linuxu a obchodné výzvy. Zameranie na Linux, stabilita aplikácií, zhoda s otvorenými štandardmi, poistenie proti škodám, dokumentácia a škálovate¾nos´ sú len nieko¾kými benefitmi profesionálne spravovaných aplikácií a tak by sa malo na to prihliada´ u´ vo fáze výberu.

Otvorené technológie skombinované s virtualizáciou a konceptom viacjadrových procesorov, ktoré sme u´ opísali, prinášajú nové vysokovýkonné mo´ nosti. Dôle´ itou skutoènos´ ou pre pou´ ívate¾ov prevádzkových riadiacich a automatizaèných systémov vyu´ ívajúcich Linux ako operaèný systém je, ´ e v tej istej aplikácii na jednej hardvérovej platforme doká´ u oddeli´ prvky týkajúce sa bezpeènosti od tých, ktoré s bezpeènos´ ou nesúvisia. Linux ako otvorený operaèný systém prináša vysoký potenciál pre nové vlastnosti a inovatívny middleware, ktoré pri po´ iadavkách na bezpeènos´ zvyèajne zvyšujú zlo´ itos´ . Technológia hypervízora umo´ òuje na softvérovej úrovni zjednoti´ Linux a operaèný systém reálneho èasu a umo´ ni´ chod s bezpeènos´ ou súvisiacich aj nesúvisiacich aplikácií na tej istej hardvérovej platforme. Viacjadrové technológie v spojení s hypervízorovou technológiou umo´ òujú spúš´ anie a súèasný chod rôznorodých operaèných systémov na tej istej hardvérovej platforme, avšak v oddelených, chránených priestoroch.

Krok 3: Stava´ na základe, ktorý podporuje zmeny

Jedným z hlavných dôvodov, preèo sa softvérové procesy skôr chápu ako èas´ problému a nie ako súèas´ riešenia, je, ´ e sú zabudované z ad hoc nástrojov a technológií, èoho výsledkom je enormná zlo´ itos´ . Štandardizácia postavená na otvorených platformách pomô´ e viac prispôsobi´ proces vývoja softvéru a pripravi´ ho lepšie na budúce po´ ia-

davky. A èo je dôle´itejšie, aplikácia sa vytvára na štruktúre podporujúcej súhrnné po´iadavky, ktorá dr´í krok s rýchlo sa meniacimi po´iadavkami na bezpeènos´. Napríklad riešenie od spoloènosti WindRiver s oznaèením VxWorks 61508 Platform umo´òuje vývojárom vytvára´ aplikácie, ktoré musia by´ certifikované pod¾a po´iadaviek normy IEC 61508 a ïalších súvisiacich noriem, napr. IEC 62304 pre oblas´ lekárstva èi CENELEC 50126 pre oblas´ dopravy. Vývojári mô´u vïaka tejto platforme získa´ všetky výhody viacjadrových procesorov s uistením, ´e majú pevný základ z h¾adiska operaèného systému spåòajúceho prísnejšie po´iadavky èo do certifikácie bezpeènosti. Pridaním hypervízorovej technológie mo´no pod platformou VxWorks spúš´a´ kritické bezpeènostné úlohy, prièom komunikaèné protokoly mô´u be´a´ pod Linuxom (príp. iným operaèným systémom), èím sa na jednom stroji zabezpeèia všetky riadiace funkcie. Koncept hypervízorovej technológie zjednodušuje aj správu predošlých, zdedených aplikácií. Integrované slu´by pomáhajú pou´ívate¾om odstráni´ riziko spojené s projektmi bezpeènosti a unifikácie, a to prostredníctvom garantovania hladkého a predvídate¾ného umiestòovania produktov na trh s dokladovate¾nou návratnos´ou investícií a ziskovos´ou. Unifikovaný vývojový re´azec navyše podporuje trend smerom k vyu´ívaniu viacerých operaèných systémov, èo umo´òuje, aby sa aplikácie obracajúce sa na rôznorodé operaèné systémy vyvíjali naraz a v rovnakom prostredí. To je výnimoèný prínos pre vývojárske tímy. Otvorenos´ štruktúry rámcov Eclipse, ktorá umo´òuje integráciu aj iných nástrojov, sa stáva pre vývojárov a výrobcov strojných zariadení kritická.

Záver

Oblas´ riadenia procesov aj výrobcovia strojných zariadení stoja na prahu revolúcie. Ak funkcionalita niekedy poháòala inovácie, efektivitu nákladov a èas umiestòovania produktov na trh, tak v súèasnosti sú najdôle´itejšími po´iadavkami bezpeènos´ a ochrana. Do èoraz viac cenovo prístupných hardvérových platforiem sa bude vklada´ ove¾a viac funkcionality a èoraz viac sa bude oèakáva´ aj od softvéru.

Zdroj textu: *Wiegand, J.: Safety: Make Software Pert of the Solution, Three Steps That Control and Process Automation Developers Can Take to Achieve Safety Compliance While Cutting Cost and Complexity, White Paper, Wind River Systems, Inc. 2010.*

Zdroj obrázkov: *InSources Solutions, www.insourcess.com, FANUC Robotics, www.fanucrobotics.co.uk, MAG Cincinnati.*

www.windriver.com