Kybernetická bezpečnost řídicích a informačních systémů v základních službách

Zákon o kybernetické bezpečnosti přinesl řadu opatření a změn u projektů zaměřených na komunikační a informační technologie. Týká se nejenom státních zakázek, spadají do něj i provozovatelé základních služeb, tedy z oblasti energetiky, plynárenství či dopravy. Jak se na tyto změny připravili vývojáři a výrobci řídicích systémů, kteří zde informační systémy a služby dodávají? Na to jsme se ptali Pavla Kulíka, ředitele útvaru Technický rozvoj společnosti ZAT, která dodává řídicí systémy a know-how pro energetiku a průmysl takřka do 70 států světa.

Pavel Kulík

Vaše společnost nasazuje řídicí systémy ve strategických segmentech z oblasti základních služeb. Jaká opatření jste museli v souvislosti se zákonem přijmout?

Jako dodavatel řídicích systémů do klasické i jaderné energetiky, plynárenství i drážní dopravy jsme tyto požadavky samozřejmě intenzivně řešili. Dodáváme systémy do oborů s nároky na dlouhou životnost a bezporuchovost řídicího systému. S příchodem tohoto zákona k nim přibyly další na zabezpečení proti úmyslnému kybernetickému napadení. Implementovali jsme řadu technických opatření pro zvýšení odolnosti řídicích stanic SandRA proti kybernetickým útokům, zároveň neustále pracujeme na zlepšování interních procesů. Z jaderné energetiky máme mnohaleté zkušenosti s naplňováním specifických požadavků regulačních úřadů v různých zemích. Náš řídicí systém SandRA proto splňuje všechny legislativní požadavky na bezpečnost a spolehlivost. Nicméně pro upřesnění, nejde jen o jedno řešení, které by bylo možné použít u všech projektů. Konkrétní způsob zajištění kybernetické bezpečnosti je vždy závislý na podmínkách provozu řídicího systému. Zákazníci si často specifikují své konkrétní požadavky, které musí řídicí systémy splňovat. Například jaderná elektrárna má jiné požadavky než klasická nebo zákazník z oblasti distribuce plynu.

Které obory jsou na tom z pohledu bezpečnosti nejlépe?

Logicky nejdále v oblasti zabezpečení byla jaderná energetika, kde se požadavky na kybernetickou bezpečnost do značné míry potkávají s již dříve aplikovanými nároky na jadernou bezpečnost. Řídicí systémy jsou zde velmi strukturované. Často se využívají pouze jednosměrné komunikace speciálními protokoly. Rovněž fyzická ochrana – zamezení neoprávněné manipulace se zařízením – je zde na velmi vysoké úrovni. Specifické požadavky včetně těch na kybernetickou bezpečnost v současné době řešíme například na elektrárně Loviisa ve Finsku, kde dodáváme řídicí systém SandRA pro primární část jaderné elektrárny. V klasických elektrárnách byla situace jiná. Systémy řídicí jednotlivé části technologie byly často připojeny do jedné komunikační sítě. Dnes dochází právě z důvodu zvýšení kybernetické bezpečnosti k jejímu rozdělení na „komunikační ostrovy". Komunikace mezi ostrovy je pak striktně omezena a jednoznačně specifikována. Tomu přizpůsobujeme i řešení našich projektů.

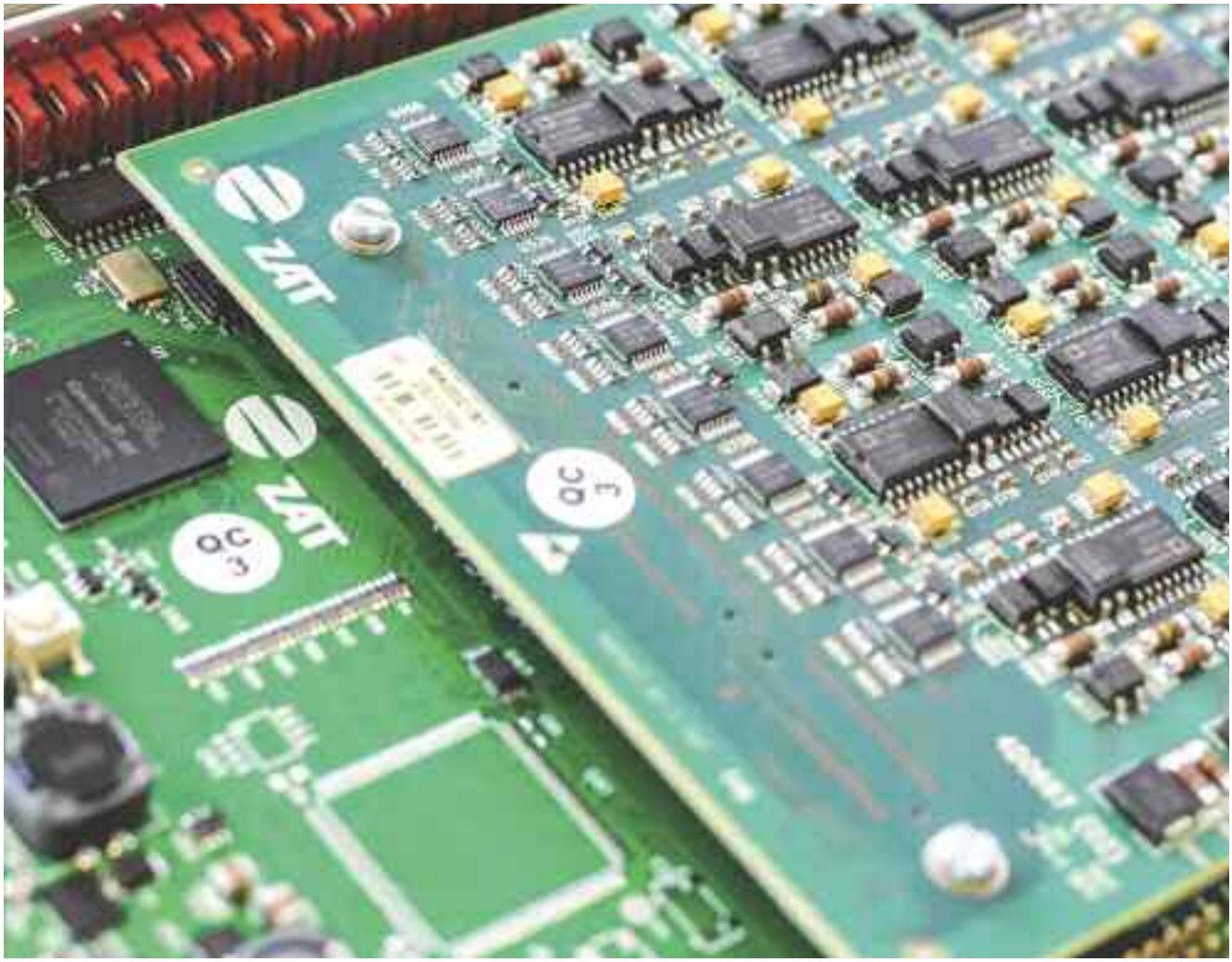
V současné době se často skloňuje kybernetická bezpečnost v distribuci plynů. Jak to vypadá v tomto segmentu?

Ač by se laikovi mohl zdát opak, pro nás, výrobce řídicích systémů pro náročné průmyslové

Budova ZAT v Příbrami

procesy, je realizace kybernetické bezpečnosti v oblasti distribuce zemního plynu velkou technickou výzvou. Na rozdíl od výše zmíněných jaderných a klasických elektráren, kde jsou komunikační sítě i samotné řídicí systémy umístěny uvnitř uzavřeného střeženého objektu, v oblasti přepravy zemního plynu jde o rozsáhlé sítě s velkým množství připojených zařízení, často bezobslužných, navíc na rozlehlém území pokrývajícím celou Českou republiku. Komunikační sítě mohou být realizovány mnoha způsoby. To klade vysoké nároky na zabezpečení nejen komunikačních sítí, ale zejména

Osazovací linky SMT na výrobu elektronických desek ve vysoké průmyslové kvalitě



Řídicí systém Sandra Z200 používaný v klasické energetice

Řídicí systém SandRA Z100 určený pro jadernou energetiku

koncových řídicích stanic. V rámci aktuálně realizovaného projektu například dodáváme řídicí systémy pro velké předávací a regulační stanice i na rozsahem menší kontrolní a měřicí body. Do našich řídicích stanic jsou komunikačně připojena zařízení od různých výrobců, zároveň komunikujeme data na centrální dispečinky dodané jinou firmou. To klade značné nároky na zabezpečení.

Jak zde řešíte kybernetickou bezpečnost?

V rámci kybernetické bezpečnosti implementujeme technologie umožňující šifrování komunikace, autorizaci přístupů pro servisní účely, blokování nepoužívaných služeb, kontrolu integrity softwarového vybavení stanic atd. To platí i pro inženýrské nástroje určené pro tvorbu aplikačního softwaru. Vždy však záleží na charakteru konkrétní aplikace a koncepci zajištění kybernetické bezpečnosti provozovatele, které z opatření je vhodné použít.

U jakých dalších projektů jste v poslední době řešili kybernetickou bezpečnost?

Například vodní elektrárna Lipno I je od loňského roku řízena bezobslužně ze 140 km vzdáleného dispečinku ve Štěchovicích v režimu virtuálního bloku až 120 MWe. Původní systém jsme kompletně nahradili novým řídicím systémem SandRA, který zároveň zajišťuje najetí a nafázování bloků v extrémně krátkých časech. Dalším probíhajícím projektem, kde nasazujeme systémy s požadavky na kybernetickou bezpečnost, je například již zmiňovaná finská jaderná elektrárna Loviisa.

Jaké jsou vaše další cíle v oblasti kybernetické bezpečnosti?

Uznávaný americký odborník na informační bezpečnost Bruce Schneier řekl: bezpečnost není produkt ale proces. Proto i našim cílem není jen zvyšovat technickou odolnost našich řídicích systémů proti kybernetickým útokům, ale zejména rozvíjet spolupráci s našimi zákazníky na poli kybernetické bezpečnosti. Jedině tak lze dosáhnout funkčního výsledku. Naše vývojové oddělení pracuje na zvýšení odolnosti řídicích stanic SandRA proti kybernetickým útokům dlouhodobě, můžeme tak klientovi dlouhodobě garantovat požadovanou bezpečnost a spolehlivost. Ostatně odolnost instalovaných řídicích systémů proti kybernetickým útokům si standardně testují jak samotné firmy, tak i nezávislé auditorské společnosti.

(red)