Sjednocení řízení a bezpečnosti: přínosy versus rizika

Jakkoliv se praxe v průmyslu přiklání jako k osvědčenému postupu ke vzájemné izolaci řídicích a bezpečnostních funkcí, současné iniciativy v oblasti integrace dat v podnicích a řízení nákladů jsou podnětem k úvahám o tom, jak tyto funkce a systémy, které je zajišťují, do určité míry sjednotit. V současnosti existují tři základní přístupy k integraci, a to přístup „s použitím rozhraní“, při němž oddělené systémy, řídicí a bezpečnostní, spolu komunikují prostřednictvím softwarového mostu vytvořeného na zakázku, přístup „sjednocené, ale oddělené“, při kterém tyto navzájem rozdílné systémy využívají vyhrazené fyzicky izolované síťové kanály, mezi nimiž se informace předává v rámci nadřazené řídicí sítě, a přístup „společný“, kdy řídicí a bezpečnostní systémy sdílejí společný operační systém. V článku jsou tyto tři základní modely stručně charakterizovány a porovnány z hledisek shody se standardy bezpečnosti a cenové efektivity.

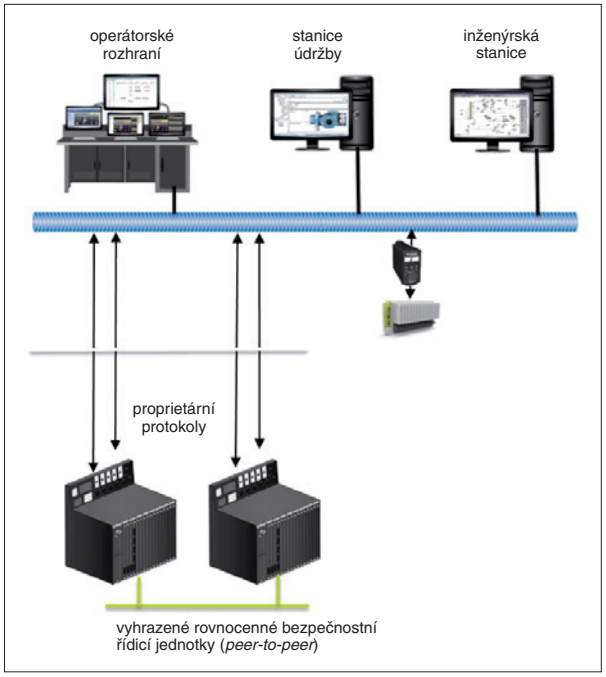
Bezpečnostní přístrojové systémy (*Safety Instrumented System* – SIS) jsou průmyslové bezpečnostní sítě zajišťující funkční bezpečnost technologických zařízení a procesů. Jako záloha pro případy, kdy se automatizační systém stane z nějakého důvodu neschopným řídit potenciálně nebezpečný technologický proces, musí být nepřetržitě k dispozici. K ochraně systémů SIS před poruchami vlivem téže příčiny, která způsobila selhání systému řídícího technologický proces, se jako tradiční osvědčená metoda používá vzájemné striktní fyzické i funkční oddělení obou systémů, řídícího a bezpečnostního. S rostoucí složitostí podnikání v podmínkách globální ekonomiky ovšem přicházejí často navzájem protichůdné požadavky na těsnější integraci podniku, vyšší úroveň bezpečnosti a menší náklady. Vedoucí pracovníci v mnoha firmách vidí východisko z tohoto dilematu ve sjednocení a fúzi bezpečnostních a řídicích funkcí.

Pro manažery v oboru provozní bezpečnosti a správy rizik může bezpečnostní systém představovat zlatý důl cenných údajů, které, stanou-li se dostupnějšími, mohou být nápomocné při identifikaci prvotních známek budoucích problémů. Vedoucí v inženýrských útvarech vidí nadbytečnou práci, která by mohla odpadnout, a provozní vedoucí vidí ostrovy aktivit, které by mohly snáze komunikovat jak navzájem, tak i s okolím v podniku. Vedoucí v úseku údržby vidí množství údajů o stavu strojů a zařízení, které mohou přispět ke zkvalitnění a zlevnění údržby, a ekonomové nadbytečné investice a náklady na školení zralé k úspoře sloučením obou systémů v jeden.

Dodavatelé automatizační techniky, ve snaze vyjít vstříc uvedeným potřebám, nabízejí různé modely sjednocených řídicích a bezpečnostních systémů (*Integrated Control and Safety System* – ICSS) s různou úrovní integrace. V dalším textu jsou postupně charakterizovány a porovnány co do přínosů a rizika tyto čtyři principiální modely: úplné fyzické oddělení systémů, sjednocení systémů s použitím softwarového rozhraní vytvořeného na zakázku, sjednocení s využitím izolovaných subsystémů v řídicí síti typu klient-server a sjednocení na společné řídicí platformě.

Rozdíl mezi PAS a SIS

Přestože jak systém pro řízení technologických procesů (*Process Automation System* – PAS), tak i bezpečnostní přístrojový systém (SIS) jsou v podstatě řídicí systémy, jejich určení je principiálně odlišné.



Obr. 1. Kombinovaná struktura Foxboro Evo: řídicí a bezpečnostní systém tvoří společně ICSS podle modelu „sjednocené, ale oddělené“(integrated but separate)

Systém PAS, známý také pod označením distribuovaný řídicí systém (*Distributed Control System* – DCS) nebo základní systém pro řízení procesu (*Basic Process Control System* – BPCS), řídí chod technologického procesu. Řídí ho podle hodnot provozních (technologických) veličin poskytovaných provozními přístroji, např. snímači tlaku, teploty atd., přes I/O karty do řídicího počítače, popř. počítačů. K systému PAS také patří vývojové prostředí a inženýrské nástroje používané při jeho konfigurování a údržbě. Uživatelé komunikují se systémem prostřednictvím operátorského rozhraní (*Human Machine Interface* – HMI).

Bezpečnostní přístrojové systémy také zajišťují řídicí funkce na základě signálů z provozních přístrojů. Na rozdíl od systémů PAS, optimalizovaných pro komplexní zpracování velkých množství technologických proměnných, je však jejich úkolem v případě potřeby bezpečně a spořádaně ukončit určité stanovené provozní činnosti, které jinak mohou spadat do oblasti působnosti systému PAS. S ohledem na jejich určení jsou systémy SIS označovány rovněž jako systémy nouzového vypnutí (*Emergency Shutdown* – ESD). Systémy SIS zajišťující kritické funkce ESD jsou optimalizovány co do rychlosti a spolehlivosti. Řídicími jednotkami v systémech SIS jsou obvykle redundantně provedené rychlé programovatelné automaty (*Programmable Logic Controller* – PLC), které jsou důkladně ověřené a certifikované z hlediska spolehlivosti.

Téměř žádná větší či velká firma zpracovávající nebezpečné materiály či provozující jinak potenciálně nebezpečné činnosti se neobejde bez systému SIS jako zálohy příslušného základního řídicího systému. Systémy SIS zajišťují nezávislé řízení technologických operací, zpravidla při použití vyhrazených provozních přístrojů, modulů I/O, sítí, inženýrských stanic, konfiguračních nástrojů a operátorských rozhraní. Takovéto uspořádání dominuje po celém světě, přičemž častější jsou případy, kdy souběžně použité systémy PAS a SIS pocházejí od různých dodavatelů, než naopak.

Jako výsledek úsilí vynaloženého za účelem umožnit strategičtější využití informací o funkční bezpečnosti zařízení či ušetřit peníze sjednocením bezpečnostních a řídicích funkcí v současnosti existují čtyři principiální modely sjednocení řídicích a bezpečnostních systémů (ICSS). Poradenská firma ARC ve své analýze *Process Safety Systems Global Market Research Study* (Průzkum světového trhu s bezpečnostními systémy pro spojité technologické

procesy) z roku 2013 zavádí pro tyto čtyři modely a jim odpovídající struktury ICSS označení „oddělené“ (*separated*), „s propojovacím rozhraním“ (*interfaced*), „sjednocené, ale oddělené“ (*integrated but separated*) a „se společnou řídicí základnou“ (*common*).

Údržba v prostředí oddělených systémů PAS a SIS

V odpovědi techniků odpovědných za funkční bezpečnost zařízení na dotaz na jimi preferovanou úroveň integrace řídicích a bezpečnostních funkcí se jich většina postaví proti integraci vůbec, jako takové. Ukázal to průzkum uskutečněný společností Schneider Electric (tehdy Invensys) v roce 2010 u více než 200 zákazníků včetně 23 z vedoucích 25 naftařských firem a 45 z vedoucích 50 chemických firem na světě. Z respondentů jich 78 % trvalo na zajištění funkční bezpečnosti cestou striktního oddělení bezpečnostního systému od řídicího a 74 % respondentů označilo za kriticky důležitou existenci nezávislých ochranných vrstev (*Independent Protection Layer* – IPL).

Hlavní normy týkající se funkční bezpečnosti technologických zařízení, IEC 61508 a IEC 61511, jsou v otázce integrace řídicích a bezpečnostních funkcí poněkud nejednoznačné. Ale není pochyb o tom, že použití navzájem oddělených systémů uspokojuje požadavky na přítomnost nezávislých ochranných vrstev, které zabrání vzniku potenciálně nebezpečných situací; za podmínky, že současně neselžou oba systémy, řídicí i bezpečnostní.

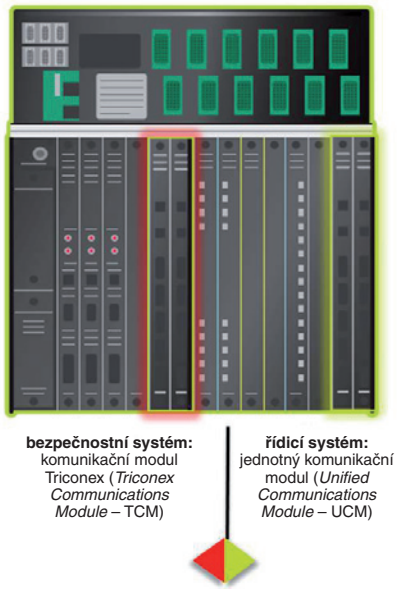
Uspořádání s oddělenými systémy také nejdokonaleji odpovídá normě IEC 61511-1, část 11.2.4, kde je vyžadováno, aby základní řídicí systém (PAS) byl realizován jako oddělený a nezávislý natolik, že „není ohrožena funkční integrita bezpečnostního systému“, a klauzuli 9.5 téže normy, věnované potřebě předcházet poruchám společného původu, poruchám v důsledku soufázovosti a závislým poruchám s doporučením zaměřit se na:

– vzájemnou nezávislost ochranných vrstev,
– vzájemnou různorodost ochranných vrstev,
– fyzické oddělení ochranných vrstev navzájem,
– ochranu před poruchami společného původu mezi ochrannými vrstvami a základním řídicím systémem.

Při oddělených řídicích a bezpečnostních funkcích je ovšem třeba realizovat, obsluhovat a udržovat dva různé systémy, takže to také může být cesta nejnákladnější. Rovněž mohou být, jako následek takto striktní izolace provozních a bezpečnostních údajů, ztraceny mnohé příležitosti ke zdokonalením v oblasti údržby, odstraňování závad a analýzy trendů.

Struktury ICSS s propojovacím rozhraním

Struktury využívající propojovací rozhraní stále ještě zachovávají vysoký stupeň separace. Řídicí a bezpečnostní systém si v nich již navzájem vyměňují informace, a to prostřednictvím softwarových rozhraní vytvořených na zakázku při využití standardních komunikačních protokolů, jako jsou např. OPC, Modbus, Profibus, Profinet, TCP a HART. Rozhraní se nejčastěji používá tehdy, když řídicí a bezpečnostní systémy pocházejí od různých dodavatelů a konečný uživatel potřebuje, aby tyto systémy za určitým specifickým účelem sdílely určité vybrané údaje.



Obr. 2. V kombinované struktuře Foxboro Evo od společnosti Schneider Electric jsou dílčí kanály řídicí sítě fyzicky izolovány při jednosměrném sdílení údajů přes příslušný komunikační modul; uživatelé mohou zvolit úroveň integrace řídicího a bezpečnostní systému podle své potřeby – od úplného sjednocení (se společnou základnou, model common) po naprosté oddělení (model separated)

Za předpokladu, že integrátoři systémů realizující taková rozhraní mají dostatek zkušeností v oboru bezpečnostních systémů, může být tato metoda velmi bezpečná. Avšak informace, kterou poskytuje, bude vždy omezena zadávací specifikací a následná průběžná údržba a dodatečné změny mohou být velmi nákladné. Mimoto integrita takové brány nejspíše nebude prověřena validací provedenou třetí stranou.

Struktury ICSS sjednocené, ale oddělené (kombinované)

Na třetí úrovni integrace, tedy ve strukturách nazvaných ARC jako „sjednocené, ale oddělené“ (*integrated but separate*; dále v textu pro jednoduchost jako „kombinované“ – pozn. red.), používají jednak bezpečnostní a jednak řídicí logické jednotky jim vyhrazené nezávislé síťové kanály v rámci řídicí sítě. Izolované dílčí sítě klientských zařízení mohou navzájem sdílet údaje, avšak nesdílejí řídicí funkce. Například ve struktuře systému pro řízení spojitých technologických procesů Foxboro Evo™ od společnosti Schneider Electric jsou bezpečnostní řídicí jednotky navzájem rovnocennými uzly řídicí sítě s volnou strukturou Foxboro Evo Mesh (*obr. 1*).

V kombinované struktuře jsou veškeré údaje zformátovány tak, aby proudily bez dalších úprav mezi fyzicky izolovanými dílčími kanály nadřazené řídicí sítě, a to jednosměrně, což zajišťuje příslušný komunikační modul (*obr. 2*). V kombinovaném případě jde o strukturu *informačně/datově sjednocenou*, umožňující firmám bez rizika sjednotit řídicí a bezpečnostní údaje a dále těžit z odpovídajícího zvýšení produktivity a snížení nákladů. Avšak současně také *fyzicky rozdělenou*, ve které jsou všechny funkce realizovány při použití samostatných zařízení a kterou lze v krajním případě zkonfigurovat do podoby zcela oddělených systémů (model *separated*).

Na tyto kombinované struktury je všeobecně nahlíženo jako na uspořádání kompatibilní s normami IEC požadujícími nezávislé ochranné vrstvy. Důvodem je, že dílčí kanály řídicí sítě jsou u nich nezávislé a poruchy v jednom systému nemají vliv na ten druhý.

Bezpečný přístup ke všem údajům uživateli umožňuje získat jednotný vhled do kombinované řídicí struktury, který výrazně přispívá k větší bezpečnosti a produktivitě provozu zařízení a snižuje náklady. Základním principem je přitom *jednotný přístup* – ať jde o proběhlé události a jejich sekvenci, správu systému, inženýrink, údržbu či prokazování shody s předpisy.

Jednotné úložiště a správa událostí

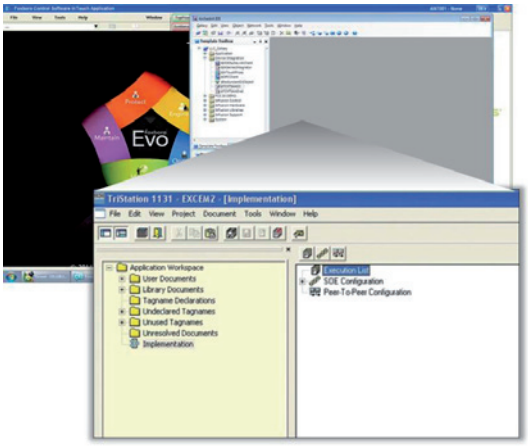
Bezešvé spojení řídicího a bezpečnostního systému uživateli umožňuje použít sdílené úložiště údajů o událostech včetně jejich sekvence. V kombinované struktuře Foxboro Evo např. jsou údaje o událostech a diagnostická hlášení ze systému a jejich sekvence ukládány do jednoho a téhož úložiště spravovaného programem pro integraci řídicího softwaru v podniku, který je součástí Foxboro Evo. Při uchovávání všech událostí a jejich sekvence ve společném úložišti mohou koneční uživatelé snáze následně analyzovat jakoukoliv poruchu v chování zařízení včetně např. chybného (neodůvodněného) vypnutí apod., s použitím běžných nástrojů ji zpětně přezkoumat a s větší efektivitou zjistit její základní příčinu.

Jednotná správa a údržba systémů

V kombinované struktuře (*obr. 3*) lze velmi efektivně využít všechny nabízené možnosti diagnostiky a správy provozního zařízení, jako např. ověření funkce ventilu částečným zdvihem, čímž se zjednodušuje ověřování akčních členů a klesá pravděpodobnost chybného zásahu bezpečnostního systému. Při snadné dostupnosti rozsáhlých funkcí diagnostiky a správy systémů mohou koneční uživatelé jednoduše vytvořit jediné rozhraní, jehož prostřednictvím lze sledovat stav celé struktury a, je-li to třeba, potvrzo-

vat systémová výstražná hlášení. Tím se také minimalizuje počet kroků potřebných k doručení informace z bezpečnostního systému operátorovi – a čím méně kroků, tím menší pravděpodobnost, že vznikne chyba. Jednodušší je také školení operátorů.

Skutečnost, že diagnostické údaje lze zaslat ze snímačů přímo do akčních členů apod., může zjednodušit správu bezpečnostních funkcí a ve svých důsledcích také zefektivnit údržbu. Například výstrahy z přístrojů připojených pomocí rozhraní HART je možné adresovat přímo operátorům a pracovníkům údržby jako včasné upozornění na problémy s přístrojem nebo okolními zařízeními. Prediktivní ověření poté mohu ochránit zařízení před falešnými zásahy bezpečnostního systému.



Obr. 3. Kombinovaná struktura Foxboro Evo nabízí k současnému sledování stavu řídicího i bezpečnostního systému jednotné společné rozhraní

Jednotný inženýrink

Sjednocený inženýrink vlastní kombinované struktuře umožňuje dosáhnout toho, že jakákoliv schválená změna provedená v bezpečnostním systému je okamžitě k dispozici také v řídicím systému k použití ve spojení se zobrazovacími nebo archivačními funkcemi či k ustanovení blokovacích podmínek, které řídicí systém může použít v širším řídicím schématu.

Projektanti také ocení jediné rozhraní pro přístup do struktury a unifikované vývojové prostředí společné pro oba systémy, bezpečnostní i řídicí. Produktivitu jejich práce dále zvyšují společné programovací procedury a jazyky i požadavky na instalaci. Systémoví inženýři ocení zlepšení v oblastech správy výstražných hlášení, časové synchronizace, správy přístupových práv a autorizace uživatelů a také to, že odpadá dosavadní nutnost mapovat data. To vše dohromady dovoluje výrazně zkrátit dobu potřebnou k uvedení do provozu nových instalací.

Jednotné prokazování shody

Jednotné úložiště, správa systémů a pracovní postupy vlastní kombinovaným strukturám mohou být nápomocné také při zajišťování shody s normami a předpisy. Kombinovaná struktura může poskytovat dokonalejší revizní záznamy o zařízeních včetně historie kalibrací, konfigurací řídicího a bezpečnostního systému, změn v pracovních postupech a nejrůznějších událostí. Správa dokumentů i změnové řízení jsou zde snazší.

Protože však zavést kombinovanou strukturu podle modelu „sjednocené, ale oddělené“ (*integrated but separate*) vlastně znamená nainstalovat dva v podstatě separátní systémy, lze očekávat jen minimální snížení nákladů na samotnou techniku, i když i zde je možné dosáhnout určitých úspor v oblasti komunikace. Největší finanční přínos zde vzniká v důsledku zvýšení efektivity při sběru údajů, konfigurování kombinované struktury, správě výrobního zařízení a činnosti operátorů, a to bez ohrožení funkční bezpečnosti.

Všeobecně je přijímán názor, že kombinované struktury ICSS podle modelu „sjednocené, ale oddělené“ jsou schopny plnit požadavky na ochranné vrstvy zakotvené v normách IEC 61508 a IEC 61511. Tyto normy, a především jejich doporučení týkající se údržby nezávislých ochranných vrstev, jsou v současnosti revidovány.

Struktura ICSS se společnou základnou

Ve sjednocené struktuře ICSS se společnou základnou (model *common*) jsou řídicí jednotky bezpečnostních přístrojových systémů (*SIS logic solvers*) vestavěny v řídicí platformě. Z hlediska sjednocení údajů a informací lze při tomto uspořádání dosáhnout v podstatě všech přínosů nabízených na předchozím stupni integrace, tj. kombinovanými strukturami podle modelu „sjednocené, ale oddělené“. A protože stačí instalovat pouze jednu řídicí platformu a spravovat jedno uživatelské prostředí, lze v porovnání s předchozími modely s velkou pravděpodobností očekávat nejnižší pořizovací i provozní náklady. Současně ovšem, protože zde je menší počet ochranných vrstev, jde o volbu přinášející nejvyšší úroveň rizika.

Protože řídicí jednotky SIS jsou součástí téže platformy jako základní řídicí systém a jsou uloženy na téže základní desce, událost, která negativně ovlivní platformu řídicího systému, odstaví z činnosti i SIS. Což je zcela v rozporu s účelem SIS jako nezávislé ochranné vrstvy. A je tudíž zcela na místě otázka, zdali přístup založený na použití společné platformy vůbec může splňovat shora uvedená kritéria IEC, vyžadující eliminaci poruch společného původu, poruch v důsledku soufázovosti a závislých poruch.

Některé struktury ICSS se společnou platformou získaly od třetích stran certifikáty bezpečnosti na úrovni SIL 3, které potvrzují, že příslušná řídicí jednotka SIS na požádání spolehlivě zareaguje. Úroveň SIL je ovšem ověřována nezávisle na způsobu použití zařízení, přičemž není brána v úvahu eventualita chyby se společnou příčinou. Nejsou uvažovány ani problémy související se systematickými chybami neodmyslitelně provázejícími použití téže hardwarové základny.

Souhrn a závěry

Poradenská firma ARC ve své analýze z roku 2013 uvádí, že nepolevující tlaky na snížení průvodních rizik a celkových nákladů na automatizační projekty vedou mnoho konečných uživatelů k hledání způsobů, jak navzájem těsněji propojit řídicí a bezpečnostní systémy a moci tak u nových projektů zvolit pro oba dva systémy téhož dodavatele. Ochránit v potřebné míře a za přijatelnou cenu své závody a pracovníky při změnách úrovně rizika, ať už na základě vnitřní podnikatelské potřeby nebo vlivem vnějších událostí, dokážou v budoucnu jen prozíraví uživatelé, kteří se rozhodnou pro dodavatele nabízející produkty s co největší flexibilitou při sjednocování obou systémů. Při rozhodování, zda použít sjednocenou strukturu využívající rozhraní, kombinovanou strukturu podle modelu „sjednocené, ale oddělené“, nebo strukturu se společnou platformou, bude záležet především na podnikatelské strategii té které uživatelské firmy a její toleranci k riziku. Firmy vyžadující bezpečnost bez ohledu na cenu budou pravděpodobně nadále využívat oddělené systémy. A naopak, odvážné firmy ochotné riskovat s vidinou maximální úspory nákladů, se mohou rozhodnout pro bezpečnostní systém běžící společně s řídicím systémem na jediné platformě. Ti, kdo dbají na rovnováhu mezi úsporou nákladů a úrovní rizika, pravděpodobně sáhnou po kombinované struktuře (informačně sjednocené, ale fyzicky oddělené), která je podle analytiků z ARC stále oblíbenější a stává se preferovaným řešením.

Samotná volba uspořádání je ovšem jenom částí příběhu. Úspěch jakékoliv řídicí a bezpečnostní struktury závisí také na konstrukci a kvalitě provedení hardwaru a na kvalifikaci pracovníků, kteří ji realizují, obsluhují, udržují a spravují.

Grant Le Sueur,
Director, Product Management,
Schneider Electric,
Phil Knobel,
Director, Product Management,
Schneider Electric

Z anglického originálu *Integrated Control and Safety – Assessing the Benefits; Weighing the Risks*, Invensys Systems, Inc., white paper, 2014; překlad a úprava redakce; publikováno se souhlasem Invensys Systems s. r. o.