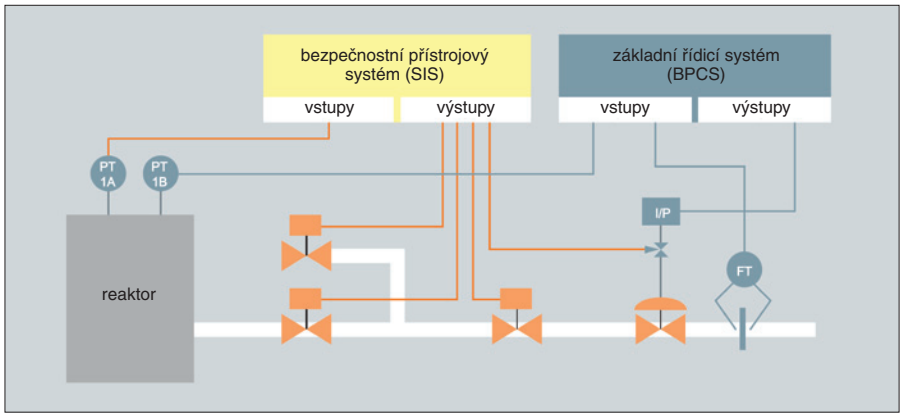
Správa životního cyklu bezpečnostního přístrojového systému

K efektivnímu zajištění funkční bezpečnosti technických zařízení jsou vedle bezpečných, tj. proti poruše odolných automatizačních prostředků nezbytné také nástroje pro jejich správu. Společnost Siemens nabízí provozovatelům spojitých technologických procesů pro tyto účely vyspělé produkty Simatic S7 F Systems a Simatic Safety Matrix.

Požadavky v oblasti funkční bezpečnosti zařízení a provozů se spojitými technologickými procesy stanovuje norma ČSN EN 61511 *Funkční bezpečnost – Bezpečnostní přístrojové systémy pro sektor průmyslových procesů*. Základní pojmy a principy, na nichž tato norma staví, připomíná úvodem k dalšímu výkladu *obr. 1*. Norma ČSN EN 61511 dále rozlišuje tři fáze životního cyklu bezpečnostního přístrojového systému (dále stručně *životního cyklu bezpečnosti*). Jsou jimi analýza, realizace a provoz s údržbou.



Obr. 1. Bezpečnostní přístrojová funkce (Safety Instrumented Function – SIF) realizovaná ve společném prostředí bezpečnostního přístrojového systému (Safety Instrumented System – SIS) a základního řídicího systému (Basic Process Control System – BPCS)

Fáze analýzy

Procedura správy životního cyklu bezpečnosti vždy začíná podrobným prozkoumáním koncepce příslušného technologického procesu a zařízení, představ o způsobu zajištění jeho funkční bezpečnosti a historických záznamů, a to za účelem určit známá i potenciální bezpečnostní rizika související s provozem zařízení.

V dalším kroku se zjištěná rizika posuzují z hlediska přijatelnosti. Cílem je vyloučit nepřípustná rizika, a určit pravděpodobnost výskytu a odhadnout možné důsledky podstatných nebezpečných událostí. Z mnoha používaných metod patří k nejznámějším např.:

- analýza ohrožení a provozuschopnosti (*Hazard and Operability Analysis* – HAZOP),
- analýza stromu událostí (*Event Tree Analysis* – ETA),
- analýza s použitím kontrolních seznamů (*Check List Analysis* – CLA),
- analýza poruch a jejich dopadů (*Failure Modes and Effects Analysis* – FMEA).

K podpoře uvedených i ostatních metod analýzy rizik jsou na trhu dostupné rozličné nástroje umožňující tyto metody do jisté míry automatizovat. Výsledek analýzy rizika je zaznamenán jako součást specifikace požadavků na bezpečnost zařízení. Tato specifikace je základem následného projektu zařízení či závodu a lze ji zobrazit v podobě matice příčin a účinků (*cause-and-effect matrix*).

Pravděpodobnost vzniku událostí ovlivňujících bezpečnost zařízení a jejich dopady lze zmenšit přijetím vhodných ochranných opatření (*Layers of Protection Analysis* – LOPA).

Jedním z možných ochranných opatření je použití bezpečnostního přístrojového systému (*Safety Instrumented System* – SIS). Jde o nezávislý bezpečnostní systém tvořený množinou bezpečnostních obvodů, které se skládají ze základních automatizačních komponent od snímače, přes logický rozhodovací modul až po akční člen a realizují příslušné bezpečnostní funkce (SIF). Použít SIS je účelné z těchto důvodů:

- *přerušení provozu*: technologický proces či zařízení jsou při zjištění jakéhokoliv abnormálního provozního stavu automaticky převedeny do bezpečného stavu,
- *tolerance*: dokud jsou dodrženy stanovené podmínky, je provoz zařízení bezpečný,
- *redukce*: možné následky nebezpečné události jsou minimalizovány, a její účinek je tudíž omezený.

Čím vyšší je úroveň integrity bezpečnosti (SIL) bezpečnostního přístrojového systému, tím většího snížení rizika lze dosáhnout (*tab. 1*).

Fáze realizace

Ve fázi realizace se volí technické a programové prostředky a struktura budoucího bezpečnostního přístrojového systému, určují se časové intervaly mezi průkaznými zkouškami jeho komponent a SIS se sestavuje, instaluje a uvádí do provozu.

Ke konfigurování a programování bezpečnostní řídicí jednotky S7-400FH společnost Siemens dodává knihovnu bezpečnostních funkčních bloků (*F-block library*), obsaženou ve vývojovém prostředí Simatic S7 F Systems, a programový nástroj Simatic Safety Matrix.

Prostředí S7 F Systems s knihovnou *F-block* a nástroj Safety Matrix

Vývojové prostředí S7 F Systems umožňuje parametrizovat jednotku S7-400FH a bezpečnostní moduly I/O (*F-module*) typové řady ET 200.

K podpoře činnosti projektanta jsou k dispozici funkce umožňující:

- porovnat bezpečnostní programy (*F-program*),
- zjistit změny provedené v bezpečnostním programu (s použitím kontrolních součtů),
- oddělit navzájem bezpečnostní a standardní funkce.

Tab. 1. Úroveň integrity bezpečnosti ve vztahu k faktoru snížení rizika a pravděpodobnosti selhání bezpečnostního obvodu (bezpečnostní přístrojové funkce)

Úroveň integrity bezpečnosti (SIL)	Pravděpodobnost selhání při vyžádání funkce (PFD) za rok[1)]	Činitel snížení rizika (RRF)
SIL 4	$\geq 10^{-5}$ až $<10^{-4}$	10 000 až 100 000
SIL 3	$\geq 10^{-4}$ až $<10^{-3}$	1 000 až 10 000
SIL 2	$\geq 10^{-3}$ až $<10^{-2}$	100 až 1 000
SIL 1	$\geq 10^{-2}$ až $<10^{-1}$	10 až 100

[1)] V režimu s malou četností zásahů, tj. pouze na vyžádání v důsledku výskytu nebezpečné poruchy.

Přístup k bezpečnostním funkcím (*F-function*) může být chráněn heslem. Knihovna bezpečnostních bloků v prostředí S7 F Systems obsahuje předem specifikované funkční bloky pro tvorbu aplikačních bezpečnostních programů v editoru vývojových diagramů CFC (*Continuous Function Chart*) nebo při použití nástroje Safety Matrix, který je na tomto editoru založen (*obr. 2*). Certifikované bezpečnostní funkční bloky jsou mimořádně robustní a zachytí chyby v programu typu např. dělení nulou nebo přetečení. Není třeba k nim vytvářet rozličné doplňkové podprogramy pro detekování chyb a reakci na ně.

Simatic Safety Matrix

Software Simatic Safety Matrix od společnosti Siemens, který lze použít namísto tvorby programů v editoru CFC, je moderní prostředek pro správu životního cyklu bezpečnosti umožňující přístrojové bezpečnostní systémy snadno nejen konfigurovat, ale také provozovat a udržovat. Nástroj využívá osvědčený princip matice příčin a účinků a uplatní se výhodně všude tam, kde určité stavy zařízení či procesu vyžadují specifické reakce s ohledem na bezpečnost.

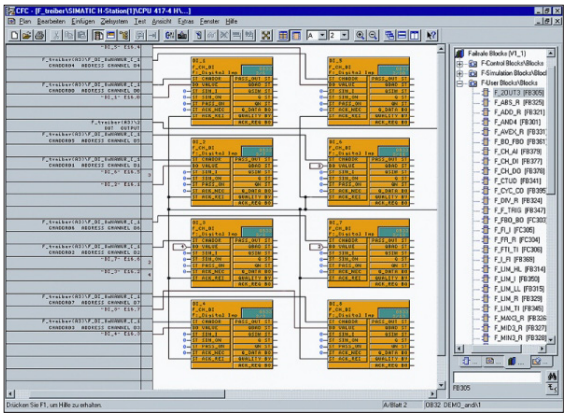
Bezpečnostní algoritmy lze v prostředí Simatic Safety Matrix programovat nejen snáze, ale také mnohem rychleji než tradičním způsobem. Na základě analýzy bezpečnostních rizik může projektant k jednotlivým událostem (příčinám), které mohou nastat při provozu zařízení, snadno přiřadit určité reakce bezpečnostního přístrojového systému (účinky).

Nejprve se do jednotlivých řádků tabulky ve tvaru matice, podobné pracovní ploše tabulkového procesoru, zapíšou možné události (vstupy) a určí se jejich typ a počet, logické vazby, možná zpoždění a případné blokace i veškeré přípustné závady. Poté se ve sloupcích tabulky specifikují reakce na každou jednotlivou událost (výstupy).

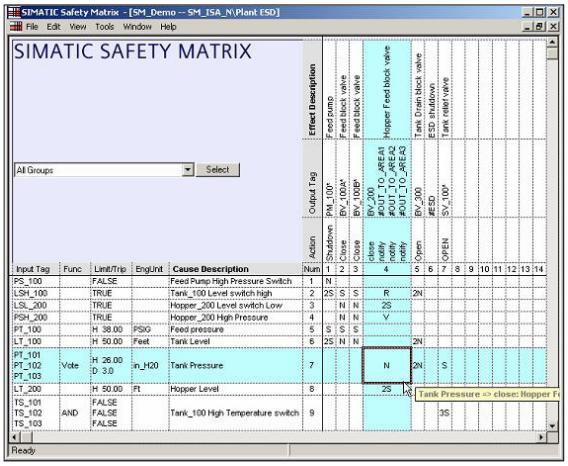
Události a reakce se spolu jednoduše propojí kliknutím na buňky tabulky nacházející se v průsečících příslušných řádků s odpovídajícími sloupci (*obr. 3*). Nástroj Safety Matrix z tohoto zadání automaticky generuje úplné bezpečnostní programy v podobě CFC. Projektanti nemusí mít žádné zvláštní znalosti techniky programování a mohou se zcela soustředit na problematiku funkční bezpečnosti svých provozů.

Každému vstupnímu signálu lze v případě potřeby přiřadit funkci zajišťující jeho předzpracování, a to při zachování možnosti simulace. Algoritmus předzpracování lze snadno konfigurovat.

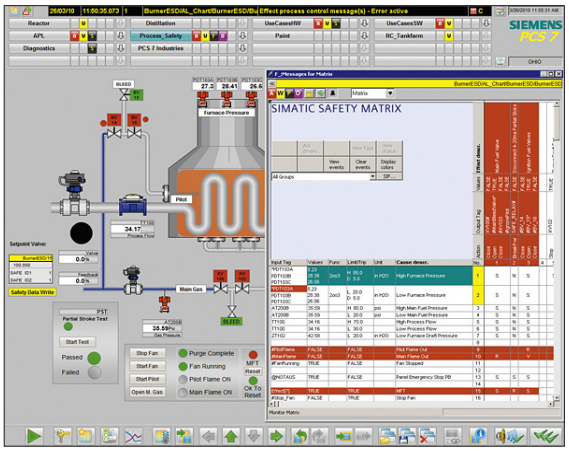
Vedle výstražných hlášení odvozených z chování provozní veličiny lze také generovat výstrahy odvozené z každé jednotlivé příčiny i jednotlivého účinku a poskytovat diagnostické informace. Lze stanovit různé profily priorit a kvitací. Barevná schémata výstražných hlášení a zpráv lze přizpůsobit specifickým požadavkům zákazníka nebo podmínkám v regionu. Pro správu výstražných hlášení je možné nastavovat souhrnné výstrahy a prioritu jednotlivých výstrah i individuálně volit způsob jejich kvitace.



Obr. 2. Tvorba aplikačního bezpečnostního programu v editoru CFC



Obr. 3. Safety Matrix: přiřazení specifických reakcí (účinků) možným provozním událostem (příčinám)



Obr. 4. Okno prohlížeče Safety Matrix Viewer na displeji operátorské stanice základního řídicího systému Simatic PCS 7

Přínosy pro uživatele

Přínosy z použití nástroje Safety Matrix během fáze realizace jsou zejména:

- snadné programování s využitím metody příčin a účinků,
- není nutná znalost programovacích technik,
- konfigurovatelná funkce předzpracování vstupního signály,
- funkce generování výstrah a dostupnost diagnostické informace u každé jednotlivé příčiny i účinku včetně symbolického označení veličiny,
- předběžné výstrahy u analogových signálů,
- volitelné barevné schéma zobrazení zpráv a výstražných hlášení,
- automatické generování bezpečnostních programů ve tvaru CFC včetně ovladačů,
- automatické sledování verzí,
- vestavěné sledování změn,
- tisk úplné matice příčin a účinků.

Fáze provozu a údržby

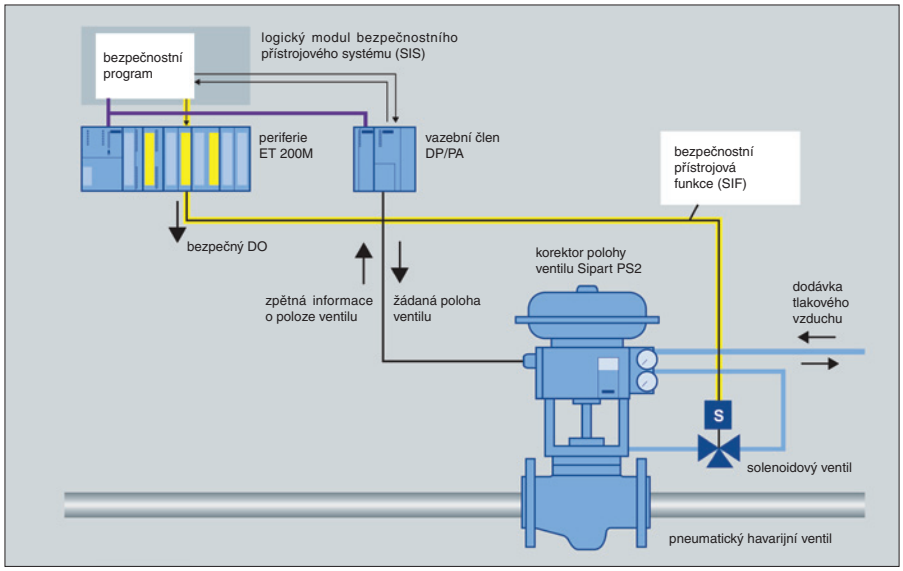
Třetí fáze životního cyklu bezpečnosti zahrnuje používání, údržbu a úpravy bezpečnostního přístrojového systému včetně etapy ukončení provozu a popř. i likvidace zařízení či závodu.

Simatic Safety Matrix Viewer

Ke snadnému a intuitivnímu sledování a ovládání SIS v prostředí Simatic PCS 7 Operator Station během provozu technologického zařízení se používá prohlížeč Simatic Safety Matrix Viewer, zajišťující operátorovi přímý přístup ke všem důležitým údajům (*obr. 4*). Stavy signálů se zobrazují *on-line* v matici příčin a účinků. Vedle úplného zobrazení úplné matice lze vytvářet i zvláštní dílčí zobrazení vybraných příčin a účinků, z nichž se operátor může snadno vrátit zpět k zobrazení úplné matice nebo přejít k zobrazení výstrah.

Prohlížeč umožňuje operátorovi bez prodlení přijímat a ukládat výstražné zprávy, zaznamenávat události související s bezpečností, měnit hodnoty parametrů apod. Spolu se symbolickým označením veličiny se vždy zobrazují její mezní provozní hodnota, aktuální provozní hodnota a simulovaná hodnota.

Funkce pro konfigurování, obsluhu a údržbu bezpečnostních systémů dostupné v prostředí Simatic Safety Matrix jsou navíc účelně doplněny funkcemi pro správu verzí a pro dokumentování zásahů operátorů a změn v programech.



Obr. 5. Uspořádání bezpečnostního obvodu umožňující provádět zkoušku částečným zdvihem (Partial Stroke Test – PST)

Přínosy pro uživatele

Ve fázi provozu zařízení jsou přínosy nástroje Safety Matrix zejména:
- dokonalá integrace do řídicího systému Simatic PCS 7,
- zobrazení konfigurace SIS i výstrah s použitím matice příčin a účinků,
- zobrazení symbolického označení veličiny ve výstražném hlášení,
- zobrazení a ukládání sekvence událostí,
- okamžité zobrazení a ukládání výstrah,
- vestavěné obslužné funkce typu přemostění, nastavení počáteční hodnoty, vložení přednostní hodnoty a změny hodnoty parametru,
- automatické ukládání a dokumentování všech zásahů operátora,
- automatické sledování verzí,
- automatické dokumentování změn.

Příklad použití: jak udržet SIL bez vynucených odstávek

Jako akční členy realizující přístrojové funkce a zajišťující havarijní přerušení procesu a bezpečné odstavení zařízení (*Emergency Shutdown Device* – ESD) se často používají dálkově ovládané havarijní ventily. Aby bylo jisté, že tyto ventily v případě potřeby skutečně zasáhnou, musí být pravidelně průkazně ověřována jejich provozuschopnost.

Při odstávce zařízení lze provozuschopnost ventilu průkazně ověřit jeho zkouškou v celém rozsahu zdvihu kuželky (*Full Stroke Test*). Protože však přitom dochází k úplnému uzavření ventilu, při zařízení v chodu je tato metoda zpravidla nepoužitelná.

Zkouška ventilu částečným zdvihem (PST)

Vynikající alternativou je v uvedené situaci zkouška jen částečným zdvihem kuželky ventilu (*Partial Stroke Test* – PST), při níž se pohyblivost kuželky ověří jen částečným pootevřením nebo přivřením ventilu bez přerušení chodu procesu (*obr. 5*). Obvyklý je částečný zdvih o velikosti asi 10 až 15 % celkového zdvihu. Záleží na provozních podmínkách a na požadovaném stupni diagnostického pokrytí.

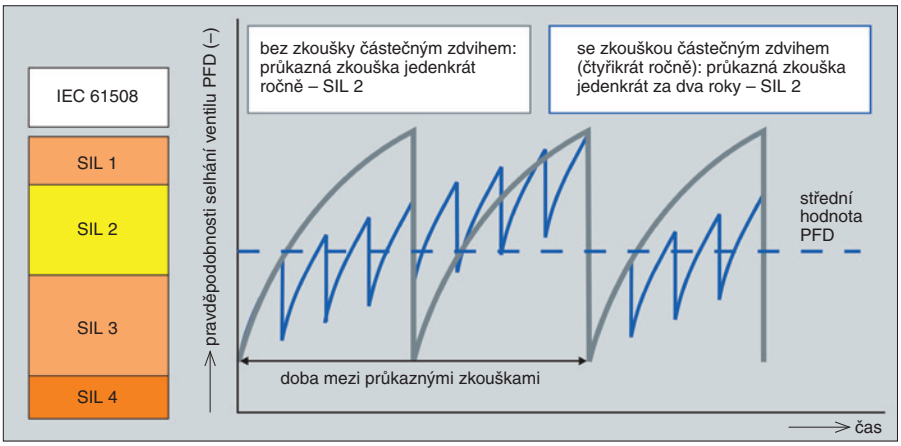
Při použití zkoušek částečným zdvihem lze prodloužit časový interval mezi požadovanými průkaznými zkouškami, prováděnými v celém jmenovitém rozsahu činnosti ventilu, aniž by se změnila (klesla) úroveň integrity bezpečnosti (SIL). Při pravidelném ověřování metodou PST např. čtyřikrát za rok lze dobu mezi dvěma průkaznými zkouškami prodloužit z jednoho na dva roky (*obr. 6*).

Bezpečnostní přístrojový systém od společnosti Siemens obsahuje předem zkonfigurované funkční bloky pro pravidelné automatické ověřování ventilů metodou PST v určených časových intervalech. Tyto bloky poskytují operátorovi zpětnovazební informaci a popř. výstrahu, pokud jde o provozuschopnost ventilu, a na základě výpočtu pravděpodobnosti selhání ventilu při požadavku na jeho činnost (*Probability of Failure on Demand* – PFD) stanovují dobu do další průkazné zkoušky ventilu.

K zobrazení v rámci operátorského rozhraní jsou k dispozici šablony umožňující rychle zkontrolovat stav každého jednotlivého ventilu. Zobrazují se zadané hodnoty parametrů zkoušky částečným zdvihem i naposled zjištěný stav ventilu a informace o dalších plánovaných zkouškách.

Přínosy pro uživatele metody PST v podání společnosti Siemens

Přínosy metody PST v podání společnosti Siemens jsou zejména:
- ověření ventilu kdykoliv *on-line* bez ovlivnění výroby,
- odhalení rozličných typů závad zkouškou,
- preventivní diagnostika,
- variabilita parametrů zkoušek a delší doby mezi průkaznými zkouškami,



Obr. 6. Pravidelné zkoušky ventilu částečným zdvihem umožňují prodloužit přípustnou dobu mezi předepsanými průkaznými zkouškami z jednoho na dva roky

- minimalizace doby přemostění havarijního ventilu nebo přerušení procesu,
- pokles pravděpodobnosti selhání ventilu při vyžádání jeho funkce,
- poskytnutí zpětných informací o průkazných zkouškách požadovaných k udržení potřebné úrovně bezpečnosti.

Závěr

Simatic S7 F Systems a Simatic Safety Matrix představují ucelený systém umožňující uživatelům automatizačních prostředků značky Siemens v závodech se spojitými technologickými procesy velmi efektivně spravovat bezpečnostní přístrojové systémy během celého jejich životního cyklu. Nacházejí uplatnění nejen v uvedeném příkladu péče o havarijní ventily, ale i v mnoha dalších úlohách ochrany technických zařízení či produktů před poškozením nadměrným tlakem či teplotou, zabraňují únikům médií atd. Další informace jsou na www.automation.siemens.com v sekci *Safety Integrated*.

(Siemens, s. r. o.)