

# Bezpečný a spolehlivý systém řízení energobloku

Kotelna i celý energoblok v Moravskoslezských cukrovarech a. s., závod Hrušovany nad Jevišovkou (dále MSC), jsou nově řízena řídicím systémem Simatic PCS7 a bezpečnými řídicími jednotkami (PLC) typu Simatic S7-400 H/F. Následující článek předkládá důvody, které vedly k použití uvedené konfigurace, stručně popisuje vlastnosti PLC S7-400 H/F a informuje o technologickém zařízení energobloku a způsobu jeho řízení prostřednictvím navrženého systému. Závěrem jsou shrnuty zkušenosti z uvádění použitých řídicích prostředků do provozu.

## Požadavky

K technologickému zařízení energobloku patří vlastní zařízení na výrobu technologické páry s akčními členy vyžadujícími speciální, zcela bezpečné ovládání (olejové hořáky, přívody paliva apod.), akční členy vlastního zařízení kotelny i pomocných provozů a agregátů a potřební rozvody technologické páry potřebné pro výrobu cukru.

Prvořadým požadavkem je zajistit bezpečný provoz tlakových celků energobloku. Vzhledem ke kontinuálnímu charakteru výroby cukru je dalším důležitým aspektem spolehlivost řídicího systému, neboť přerušení chodu kotlů v průběhu zpracovatelské kampaně může znamenat velké finanční ztráty. Velmi důležitá je také dostatečně velká kvalita regulačních pochodů jak uvnitř systému kotelny, minimalizující pravděpodobnost vzniku poruch, tak na výstupech z kotelny, kde je podmínkou zajištění požadovaných hodnot parametrů technologické páry. Kvalita páry má vliv na celý proces výroby, a tudíž i na kvalitu cukru a hospodárnost jeho výroby. Provozní požadavky na energoblok logicky vedou na potřebu velmi spolehlivého řídicího systému, v určitých speciálních oblastech kombinovaného s tzv. bezpečnými (odolnými proti poruše) řídicími prvky.

## Výběr řídicího systému

Zmíněným požadavkům vycházejí přední výrobci průmyslové automatizační techniky vstříc nabídkou systémů s velkou spolehlivostí a systémů odolných při poruše.

Systémy s velkou spolehlivostí (*high availability systems*) jsou uspořádány tak, že i při poruše uvnitř systému dále vykonávají požadované řídicí funkce. Většinou využívají tzv. redundanci (tj. nadbytečné technické prostředky), nejčastěji v podobě zdvojení buď všech, nebo alespoň některých vybraných hardwarových komponent. Zdvojují se (popř. v některých případech ztrojují apod.) např. technické prostředky od vlastních sni-

mačů, přes vstupní moduly řídicího systému až po procesory, komunikační linky či operátorská rozhraní. U systémů tohoto typu je pak deklarován beznárazový a především automatický přechod na záložní prvky systému v případě chyby nebo přerušení činnosti některé ze zálohovaných komponent.

Systémy odolné proti vnitřní poruše (označované také jako *Emergency Safe Devices* – ESD, *fail safe* systémy, systémy odolné při poruše, systémy se zaručenou bezpečností apod., dále *bezpečné systémy*) mají svůj jednoduchý ekvivalent v řešení bezpečnostních obvodů v podobě bezpečnostních modulů. Jako plnohodnotné řídicí systémy nabízejí ovšem, v porovnání s bezpečnostními moduly, propracovanější modularitu, pružnější provedení a především možnost algoritmizace chování podle

boru zvolil řešení na bázi řídicího systému Simatic PCS7 s řídicími jednotkami (PLC) typu Simatic S7-400 F/H navržené firmou Compas automatizace, spol. s r. o. Použitá řídicí technika od firmy Siemens umožňuje současně distribuovat moduly I/O, a to při použití redundantní komunikační sítě Profibus. Moduly I/O tak lze umístit v blízkosti technologických zařízení tím se významně redukuje požadavky na kabelové trasy (*obr. 1*).

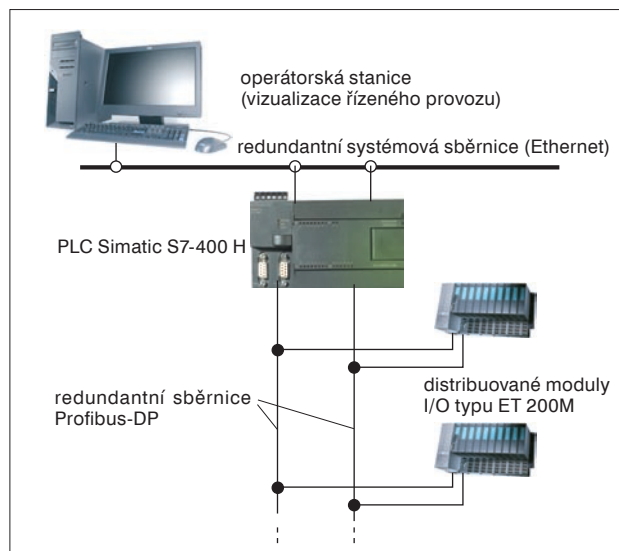
## Koncepce systému Simatic S7-400 H/F

Řídicí jednotky Simatic S7-400 H/F jsou určeny pro řešení úloh vyžadujících od řídicího systému bezpečnou a velmi spolehlivou funkci. Hardware celého systému je navržen tak, aby bylo možné všechny komponenty

v případě potřeby zdvojit a tím dosáhnout výrazného nárůstu spolehlivosti řídicího systému. Při poruše na úrovni procesorové jednotky se systém během jednotek milisekund zcela spolehlivě beznárazově přepne na záložní procesor. Stane se tak při použití komponent, které redundanci podporují, ať už jde o procesory, centrální vany, napájecí zdroje, komunikační moduly pro síť Profibus či odpovídající moduly I/O. Synchronizaci chodu redundantních procesorů zajišťují speciální moduly, umístěné na procesorových kartách a spojené optickým kabe-

lem. Procesory pracují tak, že jeden je po spuštění startu řídicího systému aktivní, tj. zpracovává program a aktivuje akční členy. Druhý procesor, záložní, sleduje stav aktivního procesoru a synchronizuje svá interní data podle aktuálních hodnot na svém aktivního procesoru. Je-li přerušena činnost aktivního procesoru či se ztratí spojení prostřednictvím synchronizačního kanálu, aktivní procesor se přepne do stavu zálohy a záložní procesor se stane aktivním a okamžitě přebere řízení.

Z pohledu programového vybavení je pro vytvoření aplikačního programu a splnění požadavků na bezpečnost třeba instalovat knihovní bezpečnostní funkce (*Failsafe Functions*), které jsou potřebné k vytvoření tzv. bezpečnostní (*failsafe*) části programu. Pro vývoj softwaru je podstatné, že programátor používá stejné prostředí jako pro běžné úlohy, tedy Step 7, popř. vývojové prostředí



Obr. 1. Příklad struktury řídicího systému s PLC Simatic S7-400 H/F

potřeb řízeného zařízení. Důležité je, že součástí dodávky bezpečného systému je prohlášení, které formou certifikátu zaručuje kvalitu použitého softwaru, umožňující jeho využití pro úlohy bezpečnostní povahy.

Předním světovým výrobcem systémů s velkou spolehlivostí i bezpečných systémů je firma Siemens. Jako první výrobce na světě dodává již několik let řídicí jednotky vyzačující se současně oběma skupinami vlastností. Sloučení vlastností charakteristických pro systémy s velkou spolehlivostí a bezpečné systémy v jednom řídicím systému značně zjednodušuje jeho propojení s vlastním sekvenčními i kontinuálními řídicími prvky technologických zařízení, neboť řídicí jednotky většinou buď využívají tentýž typ procesoru, nebo v rámci sekvenčního řídicího programu mají sdílenou paměť pro výměnu dat.

Provozovatel energobloku na základě svých potřeb a technicko-ekonomického roz-

Simatic PCS7. Pouze při tvorbě bezpečnostní části programu musí vytvořit několik funkcí a respektovat určitá omezení.

### Struktura aplikačního programového vybavení

Projekt realizovaný v MSC řeší řídicí systém, jeho měřicí část a regulaci dvou olejových kotlů o parním výkonu 55 t/h a 65 t/h, zapalovací automatiku hořáků a bezpečné odstavování těchto kotlů (obr. 2). Projekt zahrnuje také měřicí a regulační smyčky instalované na pomocných zařízeních souvisejících s provozem kotlů (olejové hospodářství, okruhy pro napájení kotlů vodou, stanice pro redukci tlaku páry a vzduchový kompresor).

Aplikační programové vybavení bylo vytvořeno ve vývojovém prostředí Simatic PCS7 s přidáním bezpečnostními funkcemi S7-F-Systems. Jeho základní struktura byla zvolena s ohledem na požadavky na bezpečnost při poruše, tj. funkce související se zapalováním hořáků a blokací chodu kotlů byly umístěny v bezpečnostní části a ostatní funkce ve standardní části programu Simatic PCS7. Dále je program členěn podle technologických úseků energobloku.

Při tvorbě bezpečnostní části programu je nutné dodržet určitá pravidla (např. podle EN 954-1), která systém vyžaduje a která není možné obejít či změnit. Základním pravidlem je neměnné pořadí volání bezpečnostních funkcí. Jako první se volají funkce pro zpracování vstupů a v následujících krocích funkce převádějící data ze standardní části programu, logické a matematické funkce, funkce převádějící data do standardní části programu a nakonec funkce pro zpracování výstupů. Dalším pravidlem je, že se data mezi bezpečnostní a standardní částí aplikačního programu přesouvají s využitím převodních (konverzních) funkcí. Příslušné funkce pro převody dat bylo třeba použít také mezi skupinami uvnitř bezpečnostní části programu. S ohledem na uvedená pravidla byly funkce bezpečnostní části aplikačního programu rozděleny do těchto čtyř skupin:

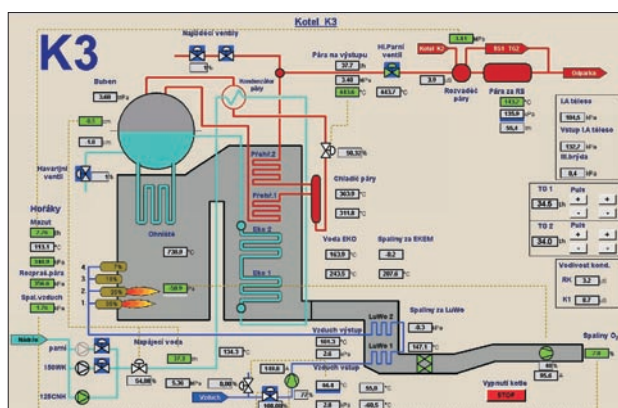
- *vstupy*: zpracování vstupních signálů s návazností na hardwarovou konfiguraci PLC,
- *blokady*: vyhodnocení podmínek blokujících chod kotle,
- *zapalování*: sekvence automatického zapálení hořáku,
- *výstupy*: přenos řídicích signálů na výstupy PLC.

Bezpečnostní část aplikačního programu se programuje v grafickém prostředí stejným

způsobem jako standardní část systému Simatic PCS7. Jednotlivé funkce jsou graficky konfigurovatelné a data jsou přenášena prostřednictvím spojnic mezi bloky (obr. 3). Programátor pracuje s komfortními a přehlednými nástroji, jejichž úspěšné použití vyžaduje znalost principů realizace bezpečných řídicích systémů.

### Napojení na operátorské rozhraní a řešení úplné redundance

K vizualizaci provozu energobloku a za operátorské rozhraní v dané konfiguraci systému Simatic PCS7 slouží dvě navzájem nehy



Obr. 2. Ukázka vizualizace kotle K3 se všemi měřicími okruhy

závislé operátorské stanice (viz také obr. 2). Obě obsahují ethernetové rozhraní (karty CP1613) napojené na samostatné síť (obr. 1). Přepínání komunikace po redundantní síti Ethernet je zajištěno příslušným nastavením a aktivací softwarového modulu (S7RedConnect).

### Uvádění do provozu

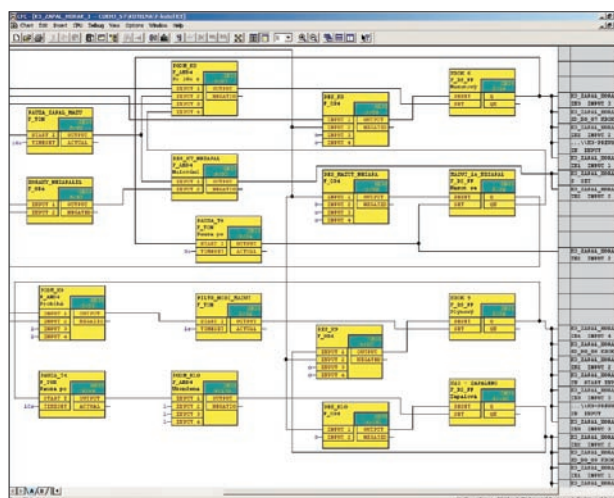
Všechny měřicí a řídicí obvody byly oživeny při zkušebním provozu během asi jednoho měsíce za přítomnosti odborné obsluhy kotlů a specialistů firmy Compas automatizace zodpovědných za zavedení všech požadovaných funkcí řídicího systému. Zvláštní pozornost vyžadovalo nastavení bezpečných modulů I/O, a to zejména správné nastavení úrovně bezpečnosti podle navržené třídy bezpečnosti a z toho vyplývající zapojení snímačů a akčních členů. Po několika zkušebních zapalovacích sekvencích, fungování blokačních podmínek a všech zabezpečovacích funkcí byl zahájen zkušební provoz jednoho kotle. Postupně byly nastaveny regulační obvody a prověřeny ty funkce, které lze vyzkoušet pouze při provozu s výrobou

páry. Při větším odběru páry byl do provozu uveden i druhý kotel. Zkušební provoz byl ukončen po nastavení všech projektovaných regulačních obvodů. Jako součást celkového řešení bylo oživeno také datové propojení řídicího systému energobloku s řídicím systémem na bázi Simatic PCS7 Osx (pod operačním systémem Unix), realizovaném také firmou Compas automatizace, který řídí vlastní proces výroby cukru.

### Závěr

Lze konstatovat, že zavedení jednoho z nejmodernějších současných prostředků určených k realizaci systémů vyznačujících se velkou spolehlivostí a odolností proti vnitřní poruše – PLC z rodiny Simatic třídy H/F od firmy Siemens – bylo úspěšné a z pohledu aplikačních techniků, specialistů s rozsáhlými zkušenostmi s řídicími systémy Siemens, bezproblémové. Dlouhodobým přínosem pro uživatele je mj. vysoká míra integrace celého řešení automatizovaného systému řízení (ASŘ) založeného na distribuovaném řídicím systému Simatic PCS7, zajištěná řešitelem ASŘ, firmou Compas automatizace, takže zaškolení pracovníci zákazníka nemají při údržbě systému Simatic S7-400 H/F problémy s provozem dodaného řešení ASŘ a péči o ně.

Pro uživatele je vždy přínosné takové řešení, které je založeno na certifikovaných a vy-



Obr. 3. Způsob konfigurování bezpečnostní (failsafe) části aplikačního programu

zkoušených systémech od světového výrobce. Naplněny byly i další důležité předpoklady úspěchu komplexní modernizace energobloku – kooperativní přístup techniků a specialistů MSC a zkušenosti pracovníků řešitele – firmy Compas automatizace, certifikovaného dodavatele řešení na bázi automatizační techniky od firmy Siemens (tzv. Siemens Solution Provider).

Ing. Jiří Petr,  
Ing. Zbyněk Bezchleba,  
Compas automatizace spol. s r. o.