Aplikácia bezpečnostných systémov v chemickom priemysle

Všeobecne

Chemický priemysel patrí charakterom svojej výroby k veľmi rizikovým z hľadiska ohrozenia zdravia a života pracovníkov a možných materiálnych škôd. V rafinériách sa vo výrobnom procese vyskytujú médiá, ktoré sú horľavé, výbušné a toxické.

V rizikových výrobniach vybavených modernou riadiacou technikou sa z uvedených dôvodov, okrem riadiacich systémov (najčastejšie DCS), aplikujú nezávislé systémy bezpečného odstavenia (ESD), ktorých úlohou je odstaviť výrobný proces v tých prípadoch, keď sa vymkol spod kontroly DCS. Systémy bezpečného odstavenia pracujú úplne automaticky bez toho, aby do ich činnosti musela zasahovať obsluha.

Snahou je, aby odstavenie prebehlo bezpečne pre obsluhu a pokiaľ je to možné bez poškodenia technologického zariadenia. Na ESD systémy sa preto kladú veľké požiadavky na spoľahlivosť. Musia byť konštruované tak, aby spĺňali požiadavky príslušných noriem a boli certifikované príslušnými inštitúciami.

Pri ESD systémoch treba zaručiť to, aby nedochádzalo k neodôvodneným odstaveniam výrobne z dôvodu zlyhania ESD (dostupnosť *(angl. availability)*). Na druhej strane však treba splniť aj zdanlivo protichodnú požiadavku tzv. bezpečného zlyhania *(angl. fail-safe)*. Táto požiadavka znamená, že systém v odôvodnenom prípade odstaví výrobný proces aj vtedy, ak sa na ňom vyskytla technická chyba.

Základné pojmy z oblasti ESD systémov

ESD

ESD – „emegency shut down“, čiže systém bezpečného odstavenia (alebo aj havarijný blokovací systém). Čo to však znamená? Ide o systémy realizované na báze PLC (programmable logic controller) s rýchlym vzorkovaním, ktoré sú postavené na najvyššom stupienku hierarchie riadenia. Úlohou ESD je ochrana ľudí a technologických zariadení pri dosiahnutí kritických hodnôt procesných veličín.

Architektúra systému

Architektúra ESD sa skladá z procesorovej časti a vstupno-výstupnej časti. Podľa požiadaviek dodávateľov technológie alebo zákazníka sa používa zdvojená, niekedy strojnásobená (najmä jadrová energetika) konfigurácia systému. V závislosti od stupňa požiadaviek na bezpečnosť stačí niekedy zdvojiť procesorovú časť, niekedy treba zdvojiť aj vstupno-výstupnú časť. Najčastejšie sa používa redundantná procesorová časť a kombinovaná vstupno-výstupná časť. Pre vybrané kritické obvody sa používa redundantná a pre indikačné obvody neredundantná v/v časť.

Online modifikácia

Zdvojená procesorová časť je aj podmienkou systému s bezvýpadkovým prechodom na novú verziu blokovacej logiky, čo nazývame online modifikácia. Pri modifikácii systému sa odstaví jeden procesor a nová aplikácia sa nahrá do jeho pamäte, zatiaľ čo druhý procesor riadi proces. Po nahratí novej aplikácie, jej validácii a kontrole sa systém prepne na procesor s novou aplikáciou bez toho, aby čo len na okamih stratil kontrolu nad procesom. Potom sa nová aplikácia nahrá aj do druhého procesora a po reštarte už opäť beží proces v redundantnom móde.

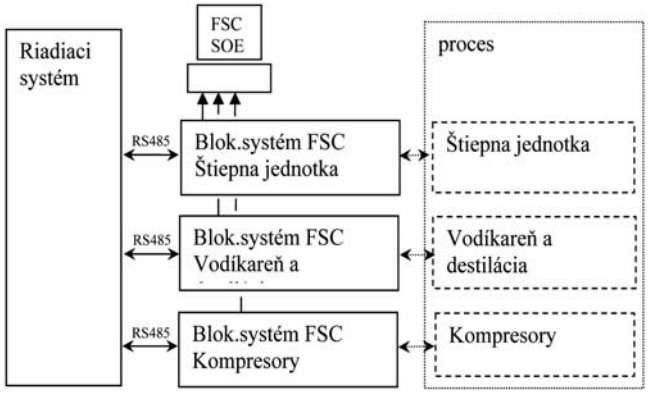
Fault tolerant systémy

Systémy PLC s redundantnou procesorovou a V/V časťou vyrába už väčšina dodávateľov PLC, ale len veľmi málo výrobcov dodáva systémy s tzv. chybovou bezpečnosťou (fault tolerant alebo systémy fail safe). Ide o systém s prepracovaným matematickým modelom identifikácie porúch v reálnom čase.

Aplikácia ESD vo výrobniach komplexu Hydrokrak

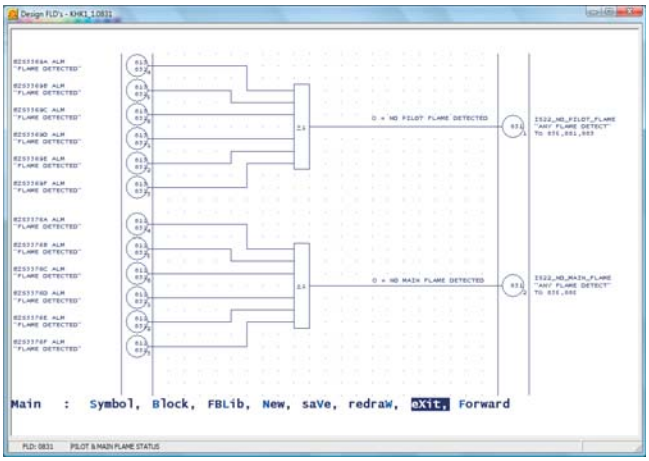
V komplexe výrobní Hydrokrak bol ešte v roku 1999 vymenený existujúci systém za „fault tolerant“ systém FSC od firmy Honeywell. Systém Honeywell FSC je certifikovaný TÜV Bayern pre triedy AK1-AK6 a s klasifikáciou SIL3 podľa IEC61508. Súčasná verzia je založená na konfigurácii dvoch zo štyroch procesorov, čiže každá procesorová

karta obsahuje dva samostatné procesory. Pri intenzifikácii výrobnej jednotky začiatkom tohto roku bol pôvodný FSC systém rozšírený o ďalšiu skriňu elektroniky a doplnený o riadiaci systém najväčších kompresorov výrobnej jednotky, taktiež FSC od firmy Honeywell. Doplnenie nahrádza doteraz používaný, morálne zastaraný systém riadenia. Všetky FSC systémy na VJ KHK sú realizované s redundantnou procesorovou časťou a kombinovanou V/V časťou. Zobrazovanie informácií je realizované na operátorských konzolách riadiaceho systému (DCS), ktorý tak prebral funkciu používateľského rozhrania pre celý bezpečnostný a blokovací systém.



Bloková schéma riadenia VJ

Blokovacia logika štiepnej jednotky bola kompletne nahradená novou, dôkladne prepracovanou logikou, ktorá významným spôsobom zlepšila nielen bezpečnosť, ale aj informovanosť operátora o procese. Podstatne sa zvýšil aj komfort obsluhy výrobnej jednotky, najmä v časti obsluhy pecí. Pre aplikačných inžinierov je návrh a implementácia bezpečnostných systémov vždy veľká výzva, pri ktorej má programátor po ukončení silný pocit profesionálneho zadosťučinenia. Podklady k projektu spracúval CB&I Brno, Česká republika, na mimoriadne vysokej profesionálnej úrovni. Žiaľ, v poslednom čase sú takto perfektne pripravené podklady vzácnosťou, takže spoluprácu si programátor ESD skutočne vychutnal.

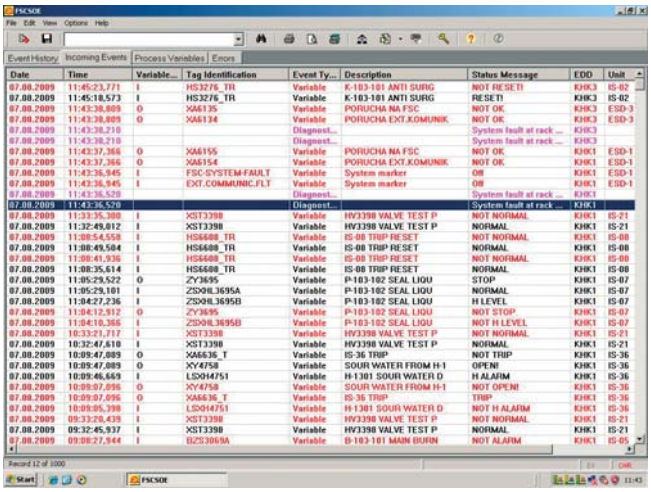


Príklad logických diagramov

Najväčším problémom celého projektu bol nedostatok času na testovanie aplikácie na „živom" systéme, keď sa dajú odhaliť rôzne úskalia logického riadenia. Tie vyplývajú z priebehu a poradia vykonávania logických funkcií počas chodu programu. Aj milisekundový impulz na zaťažovacom ventile niekoľkomegawatového stroja môže mať za následok vibrácie, ktoré spôsobia vyblokovanie stroja a následne celej prevádzky. Keďže väčšia časť aplikácie sa realizovala na rozšírenom systéme, ktorý bol odstavený len presne určený čas a nebol k dispozícii simulátor FSC systému, bolo nutné niečo vymyslieť, aby sa skrátil čas potrebný na testovanie logiky počas odstávky na minimum. Jediným rýchlym riešením bola úprava aplikácie na systém, ktorý bol k dispozícii (FSC na riadenie kompresorov) premapovaním fyzických vstupov a výstupov do pamäťovej oblasti určenej na komunikáciu. Tým sa aplikácia dala preložiť a nahrať do hardvéru. Testovanie bolo už len otázkou hodín strávených projektantom a aplikačným inžinierom pri bežiacej aplikácii.

Veľmi závažnou časťou realizácie býva skompletizovanie komunikačných kanálov. V tejto aplikácii bola požiadavka na komunikáciu s riadiacim systémom, komunikácia so systémom SOE (Sequence of Events) a vzájomná komunikácia medzi systémami štiepnej jednotky a kompresorov. Najdôležitejšia komunikácia s riadiacim systémom sa realizovala ako dva samostatné kanály, ktoré boli v FSC plne redundantné, t. j. boli použité štyri komunikačné porty FSC systému na komunikáciu s riadiacim systémom. Komunikácia prebieha prostredníctvom protokolu MODBUS RTU. Prvotné problémy s občasným vypadávaním komunikácie boli vyriešené po odporúčaní výrobcu riadiaceho systému znížením komunikačnej rýchlosti. Komunikácia so SOE bola pre vzdialený FSC systém na kompresoroch doplnená o optické prevodníky, čím sa vzdialenosť stala len otázkou kvality „optickej časti" komunikačnej cesty. Vzájomná komunikácia medzi vzdialenými FSC systémami bola tiež doplnená o optické prevodníky. V súčasnosti slúži na časovú synchronizáciu vzdialeného FSC systému, aby bol zaistený súlad a správnosť časových značiek v SOE. Zároveň však slúži aj ako rezerva na rozšírenie systému na štiepnej jednotke v prípade potreby, keďže FSC-FSC komunikácia je certifikovaná ako „safety" komunikácia.

Systém na riadenie kompresorov bol navrhnutý ako tzv. „one touch" systém, čím sa myslí minimalizácia zásahov operátorov do celého procesu nábehu a riadenia kompresorov. Nad celým bezpečnostným blokovacím systémom bdie kolektor SOE (sequence of events), čiže systém na záznam udalostí. Táto tzv. „žalobaba" slúži na prehľadnú analýzu toho, čo sa dialo v systéme ESD na celej VJ a v prípade výpadku VJ na rekonštrukciu udalostí a príčin výpadku.



Príklad výpisu SOE

Záver

Rekonštrukcia bezpečnostného systému komplexu výrobní spojená s rozšírením aplikačnej oblasti bola pripravená po veľmi dobrej a dôslednej spolupráci s projektantom a zrealizovaná vo veľmi krátkom čase odstávky komplexu výrobní vďaka rozsiahlym simuláciám, ktoré tvorili významnú časť realizácie projektu.

AXESS

AXESS, spol. s r. o.

Ing. Peter Kováčik
Námestie hraničiarov 31 – 33
851 03 Bratislava
Tel.: 02/62 24 75 70
Fax: 02/62 24 75 38
e-mail: axess@axess.sk
http://www.axess.sk