Riadiaci systém TELEPERM-XS použitý pre bezpečnostné systémy JE V-1

Pavol Karaba

Úvod

Realizovaním Postupnej rekonštrukcie JE V-1, ktorá prebehla v rokoch 1996 až 2000, bol v systéme ochrany reaktora inštalovaný nový programovateľný riadiaci systém TELEPERM-XS (TXS) od firmy SIEMENS. Systém ochrany reaktora je aktívny systém, ktorý zabezpečuje v havarijných situáciách tieto bezpečnostné ciele:
- odstavenie reaktora a udržanie jeho podkritickosti,
- núdzové chladenie aktívnej zóny a odvod zvyškového tepla,
- zabránenie zvýšeniu rádioaktivity a úniku rádioaktívnych látok do okolia.

Opis funkcie riadiaceho systému

Riadiaci systém ochrany reaktora je systém, ktorý nepretržite sleduje jadrovo-fyzikálne parametre reaktora a fyzikálne parametre hlavného technologického zariadenia primárneho a sekundárneho okruhu. Spracováva a vyhodnocuje signály prislúchajúce projektovaným aj neprojektovaným haváriám. Po ich vyhodnotení a logickom spracovaní vydáva akčné signály, ktoré aktivujú technologické bezpečnostné systémy. Tieto bezpečnostné systémy riadia prevádzku tak, aby sa pri havarijných udalostiach stav reaktora a hlavného technologického zariadenia udržal v bezpečných medziach.

1. Štruktúra a členenie riadiaceho systému ochrany reaktora

Riadiaci systém ochrany reaktora sa člení na:
- systém automatického odstavenia reaktora (RTS) vrátane systému obmedzenia výkonu reaktora (ROM),
- systém ovládania bezpečnostných zariadení (ESFAS) vrátane zabezpečenia núdzového napájania z dieselgenerátora (DG).

Riadiaci systém je vybudovaný ako dvojnásobne redundantný (2 x 100 %) trojkanálový systém v každej redundancii, pričom obidve redundancie sú úplne nezávislé a priestorovo oddelené. Stupeň redundantnosti zodpovedá strojno-technologickému deleniu bezpečnostných systémov.

V hrubých rysoch môžeme riadiaci systém rozčleniť na tri časti:
- hlavná automatická cesta,
- informačná časť,
- testovacia časť.

Hlavná automatická cesta

Hlavná automatická cesta zabezpečuje:
- snímanie hodnôt meraných veličín (MU),
- napájanie snímačov a úpravu analógových signálov (GA),
- zber a vyhodnotenie údajov počítačmi na zber údajov (ER),
- logické spracovanie údajov počítačmi na spracovanie údajov (VR),
- výberové hodnotenie výstupných signálov (ST).

Snímanie hodnôt meraných veličín v každej redundancii sa realizuje pre každé iniciačné kritérium v troch meracích kanáloch. Napájanie meracích prevodníkov a úprava analógových signálov je riešená v analógovej časti riadiaceho systému. Následne sa analógové signály modulmi prevodníkov A/D digitalizujú a vstupujú do počítačov na zber údajov ER. Digitalizované signály sú modulmi SW prekročenia medze preformované na dvojhodnotové iniciačné signály, ktoré sa ďalej posielajú na spracovanie do počítačov na spracovanie údajov VR. Pre trojkanálové usporiadanie hlavnej automatickej cesty sa telegramy z kanálového počítača ER posielajú k trom počítačom VR. V každom počítači VR sa z iniciačných signálov logickým výberom dva z troch vytvorí aktívny signál, ktorý sa ďalej spracúva navrhnutým algoritmom ochrany.

Každý kanálový počítač ER, VR má dva procesory funkcií, ktoré spracovávajú iniciačné kritériá z diverzných premenných sledovanej havarijnej udalosti. Preto jednotlivé procesory funkcií pracujú s rôznym užívateľským SW. Týmto zapojením sa dosahuje vysoká odolnosť zariadenia voči poruche so spoločnou príčinou a vysoká disponibilita celého riadiaceho systému.

Výstupné signály z troch kanálových počítačov VR sa vyhodnocujú výberovými prvkami (výber dva z troch) vo výstupnej časti riadiaceho systému. Týmto výberom je generovaný akčný signál, ktorý vstupuje do ovládacej časti bezpečnostných systémov.

Informačná časť

K systému ochrany reaktora patrí zber signálov a hlásení, ktorý registruje stav zariadenia na dôležitých miestach hlavnej automatickej cesty, čiastočne na HW moduloch a čiastočne na SW funkčných stavebných prvkoch.

Zbieranie signálov zabezpečuje príslušný interfejs hlásení (MI) v každej redundancii riadiaceho systému a po ich spracovaní ich posiela do informačného zariadenia blokovej dozorne (BD) a núdzovej dozorne (ND), kde sa uskutočňuje ukazovanie, prípadne protokolovanie signálov:
- meracími prístrojmi,
- konvenčným signalizačným zariadením,
- cez interfejs hlásení (MI) na dvoch operátorských staniciach,
- cez interfejs hlásení a služieb (MSI) na dvoch operátorských staniciach (OS) a na stanici služieb,
- prostredníctvom gateway (GW) v technologickom informačnom systéme (TIS).

Koncepcia hlásení sa delí na:
- výstražné hlásenia,
- zobrazenie stavu.

Na úrovni hlásení na BD a ND sa jednotlivé signály zlučujú do sumárnych hlásení.

Testovacia časť

Úlohou testovania je odhaliť skryté poruchy HW a SW hlavnej automatickej cesty. Koncepcia testovania je založená na troch vzájomne sa doplňujúcich metódach skúšania:
- kontrola (sledovanie) identickosti chodu,
- autotestovanie,
- opakované skúšky.

Kontrola identickosti chodu je cyklicky bežiaca skúška s časom cyklu 50 ms. Na odhalenie porúch má stanovené odchýlky medzi redundantne získanými signálmi. Táto skúška je špecifikovaná

vo funkčných schémach a prebieha v interfejse hlásení (MI). Autotestovanie je do modulov procesora implementovaná, spojito prebiehajúca skúška s cyklickým skúšaním HW komponentov procesora s časom cyklu 50 ms. Pozostáva z jedného alebo z viacerých modulov, ktoré využívajú operačný čas. Na testovanie využívajú voľný čas medzi cyklami spracovania programov funkčných schém. Typickými skúškami sú:

- skúška procesora,
- skúška pamäte RAM,
- skúška pamäte ROM,
- kontrola zbernice.

Chyby zistené cyklicky prebiehajúcimi skúškami sú hlásené operatívnemu personálu BD. Všetky potrebné informácie pre diagnostiku a opravu zariadenia sú k dispozícii na stanici služieb. Opakované skúšky zahŕňajú funkčné skúšky SW a HW hlavnej automatickej cesty a skúšky aktívnych bezpečnostných zariadení.

Funkčné skúšky zariadenia

Funkčné skúšky sú aktivované ručne zo stanice služieb. Vykonávanie skúšok a ich protokolovanie prebieha automaticky. Signály skúšok a spätných hlásení sa vytvárajú a spracúvajú v interfejse služieb a hlásení (MSI). Ako rozhranie medzi stanicou služieb a počítačmi ER, VR slúži interfejs hlásení (MI). Aby bolo možné skúšky vykonať, musí sa skúšané zariadenie prepnúť do režimu „skúška“. Blokády zabezpečujú, že v režime „skúška“ môže byť iba jedna redundancia zariadenia systému ochrany reaktora. Skúška sa preruší, ak sa vyskytnú neprípustné podmienky v bloku alebo v skúšanom zariadení. Zvolenie skúšky sa musí zrušiť ručne.

Skúšanie aktívnych bezpečnostných zariadení

Z panelu ochrany reaktora na BD sa zvolí skúšaná redundancia. Na zvolenie je potrebný povoľovací signál zvolenia skúšky, ktorý sa vytvorí zadaním číselného kódu z panela ochrany reaktora. Pre celkovú úspešnosť skúšky musí byť technologické zariadenie pripravené na výkon skúšky tak, aby akčné členy pri skúške reagovali na akčné signály. Skúšky akčných signálov sú iniciované obslužnými prvkami z panela ochrany reaktora. Úspešnosť skúšky je signalizovaná a dokumentovaná zariadeniami hlásení v paneloch ochrany reaktora. Počas tejto skúšky zostávajú strojná ochrana a ochranné signály bezpečnostných systémov účinné.

2. Štruktúra vybavenia HW

Programovateľný riadiaci systém ochrany reaktora je zostavený z komponentov, ktoré sú kvalifikované na základe typovej skúšky:

- v časti na snímanie hodnôt meraných veličín sú použité prevodníky tlaku, teploty, tlak diferencie, napätia výkonu s výstupným unifikovaným analógovým signálom 4 až 20 mA,
- v časti na úpravu analógových signálov sú použité jednotky napájania snímačov a spracovania analógových signálov a jednotky galvanického oddelenia zo zariadenia TELEPERM-C,
- v časti digitálnej techniky sú použité:
  a) moduly na vstup a výstup analógových a dvojhodnotových signálov zo systému SIMATIC S5,
  b) počítačové moduly na spracovanie signálov a komunikácie multiprocesorového systému AS 990, ktoré sú vybavené procesormi INTEL i80468; tieto moduly sú zariadením TELEPERM-XS,
  c) na sériový prenos údajov medzi počítačmi sú použité zbernice SINEC L2, SINEC H1. Zbernica SINEC L2 (elektrické skrúcané dvojvodičové vedenie s prenosom typu RS–485) je použitá na systémový prenos údajov medzi počítačmi ER, VR v rámci redundancie. Zbernica SINEC H1 (vedenie z optických vlákien zodpovedajúce štandardu Ethernet) je použitá na prenos hlásení medzi ER, VR a MI, MSI, OS a stanicou služieb,
- v časti na výberové hodnotenie výstupných signálov sú použité relé fy Siemens a logické prvky výberu dva z troch zo systému ISKAMATIC B.

3. Štruktúra vybavenia SW

SW implementovaný do bezpečnostného riadiaceho systému sa rozdeľuje na systémový a užívateľský.

Systémový SW

Systémový SW tvorí integrálnu súčasť nasadeného HW. Pre TXS je použitý operačný systém reálneho času MICROS. Veľkú časť operačného systému tvorí komunikačný SW, ktorý beží v komunikačných procesoroch. Tým je jednoznačne oddelený od operačných systémov procesorov funkcií. Komunikačné úlohy operačného systému v počítačoch funkcií sa obmedzujú iba na inicializáciu komunikačných procesorov a na sprístupnené čítanie a zápis do pamäte RAM komunikačného procesora.

Užívateľský SW

Užívateľský SW vychádza z technologického nasadenia. Vo všeobecnosti pozostáva zo slovného opisu, matematických vzťahov a vysvetľujúcej grafiky. Aby bola štruktúra zrozumiteľná, je zobrazená vo forme funkčných schém.

Užívateľský SW pozostáva z:

- modulu funkcie,
- modulov funkčnej schémy,
- modulov skupín funkčných schém,
- vykonávacieho prostredia,
- ošetrenia poruchových a výnimočných situácií,
- modulov inerfejsov.

Tieto programy boli vytvorené pri projektovaní nástrojom SPACE a následne nahrané do počítačov funkcií.

Programovací nástroj SPACE pozostáva z programových nástrojov, ktoré na báze grafických funkčných schém umožňujú automatické generovanie strojového kódu. Zhotovením funkčných schém pomocou editora funkčných schém a príslušných nástrojov je zabezpečená skúška konzistencie.

Programy, ktoré priamo vyvolávajú automatický zásah, tvoria hlavnú automatickú cestu. Programy hlavnej automatickej cesty sa vykonávajú v 50 ms cykloch. Užívateľský SW bol vyvinutý podľa požiadaviek IEC 880.

4. Elektrické napájanie systému ochrany reaktora

Aby bola zabezpečená nepretržitá prevádzka systému ochrany reaktora, sú všetky elektronické skrine ochrany reaktora (skrine RS) vybavené dvojitým napájaním 24 V DC. To sa privádza zo skríň elektrického napájania systému ochrany reaktora, ktoré sú vybavené meničmi jednosmerného napätia 220 V DC/24 V DC. Tieto meniče sú napájané napätím 220 V DC z dvoch nezávislých elektrických rozvádzačov ZN 1. kategórie. Počítačové skrine MI, MSI v dozorniach sú napájané z priestorovo priradených skríň napájania systému ochrany reaktora v blokovej a núdzovej dozorni.

5. Riadenie prevádzky

Riadenie prevádzky sa uskutočňuje z centrálnej blokovej dozorne (BD) alebo obmedzene z núdzovej dozorne (ND). Pri haváriách aktivuje riadiaci systém ochrany reaktora automaticky všetky potrebné bezpečnostné zariadenia. Na zvládnutie havárie však môžu byť potrebné aj ručné opatrenia. Na základe priority signálov ochrany reaktora pred prevádzkovými signálmi môže byť ručné ovládanie vykonané až vtedy, keď nepôsobia akčné signály systému ochrany reaktora. Keďže niektoré akčné signály sú uložené do pamäte, treba pred realizáciou ručného zásahu vykonať nulovanie

pamätí. Nulovanie pamätí akčných signálov je plánované vtedy, keď sa má ručnými opatreniami zlepšiť priebeh havárie v čase od jej vzniku dlhšom ako 30 minút.

6. Vykonávanie prevádzkovej kontroly

V priebehu prevádzky sa vykonávajú tieto činnosti, ktoré priamo vplývajú na kvalitu a spoľahlivosť zariadenia systému ochrany reaktora:

a) Pravidelné kontroly pri prevádzke zariadenia

Cieľom týchto kontrol je zisťovanie a odstraňovanie dôsledkov postupného opotrebovania zariadenia a predchádzanie vzniku náhodných porúch.

Tieto kontroly pozostávajú z:
– kontroly skríň zariadenia,
– kalibrácie meracích obvodov,
– funkčných skúšok algoritmu ochrany,
– opakovaných skúšok akčných členov.

Skúšky sa vykonávajú v definovanom čase alebo vo funkčných cykloch podľa typových kontrolných a kalibračných postupov. Opakované skúšky akčných členov sa vykonávajú podľa SURVEILLANCE programov.

Pravidelné kontroly sa v celom rozsahu vykonávajú minimálne raz za rok počas plánovanej odstávky na výmenu paliva. Vtedy sa zabezpečuje nepriechodnosť akčných signálov na skúšanej redundancii vytiahnutím konektorov z výstupnej časti riadiaceho systému. Toto zaistenie je potrebné, aby pri vykonávaných kontrolách neboli aktivované akčné členy bezpečnostných systémov. Po odistení akčných signálov sa vykonáva preverenie priechodnosti akčných signálov podľa typových SURVEILLANCE programov. Vykonanie každej pravidelnej kontroly je vyhodnotené a zaprotokolované.

b) Nepravidelné kontroly pri prevádzke zariadenia

Cieľom týchto kontrol je zisťovanie a odstránenie náhodných porúch vzniknutých za prevádzky zariadenia. Pre nepravidelné kontroly sa vypracovávajú individuálne programy špecifické pre danú poruchu. Po odstránení poruchy zariadenia sa vykoná odskúšanie príslušného zariadenia podľa typových postupov a SURVEILLANCE programov na pravidelné kontroly.

c) Oprava zariadenia

Oprava zariadenia sa vykonáva na základe vystaveného hlásenia o poruche. Na zaistenie opravy analógovej časti zariadenia počas prevádzky sa využíva simulácia analógového signálu, ktorá zabezpečí vykonanie opravy analógovej časti bez ovplyvnenia činnosti riadiaceho systému. Pri oprave zariadenia počítačovej časti ER, VR musí byť vypnuté napájanie procesorových kariet, na ktorých je zistená porucha. Potom je možná oprava chybného komponentu (vstupnej alebo výstupnej karty, prevodník A/D, prípadne procesorovej karty) výmenným spôsobom. Pri výmene chybných procesorových modulov treba nahrať príslušný SW, skontrolovať hodnotu premenných parametrov a obsah permanentnej (EPROM) pamäte. Po ukončení opravy sa zariadenie uvedie do prevádzky reštartovaním počítača. Následne sa vykoná vyskúšanie tej časti algoritmu ochrany, ktorý zasiahla oprava zariadenia podľa typových kontrolných postupov.

7. Vyhodnotenie prevádzky riadiaceho systému

Veľký dôraz sa kladie na sledovanie a vyhodnotenie poruchovosti zariadenia, ktoré sa vykonáva priebežne počas celej prevádzky zariadenia. Poruchovosť zariadenia TXS z dvoch blokov za obdobie troch rokov je zaznamenaná v tab. 1.

zariadenie TXS	rok 2001 poruchy SW	rok 2001 poruchy HW	rok 2002 poruchy SW	rok 2002 poruchy HW	rok 2003 poruchy SW	rok 2003 poruchy HW
hlavná automat. cesta	5	10	1	4	–	4
testovacia časť	–	1	–	–	1	1
informačná časť	34	7	13	3	6	1

Tab.1

a) Najväčšiu poruchovosť spôsobila informačná časť, hlavne počítačové zariadenie operátorských staníc a prepojovacích staníc gateway. Tieto poruchy zahŕňajú zamrznutie počítačov, neoprávnenú signalizáciu fragmentu a nemožnosť jej kvitovania, prípadne poruchy spojené s nefunkčnosťou monitora alebo hard disku. Na poruchách informačnej časti sa v jednom prípade podpísal výpadok komunikačného procesora a komunikačnej linky. Ostatné poruchy boli v signalizačných prvkoch (chybná žiarovka príp. LED dióda).

b) Poruchy testovacej časti boli spôsobené poruchou tlačidlového ovládača, alebo nefunkčnosťou kódovacieho zariadenia.

c) Poruchy hlavnej automatickej cesty v prevažnej miere boli spojené s poruchou snímača technologickej veličiny, modulu napájacieho zdroja ±24 V a poruchou napájacích kariet v analógovom module. Jednu poruchu, pri neodôvodnenom zapôsobení akčného signálu, zapríčinila počítačová karta.

Prevádzku riadiaceho systému charakterizuje jeho stále klesajúca poruchovosť. Z hľadiska spoľahlivosti sú poruchy hlavnej automatickej cesty považované za relevantné, pretože obmedzili funkčnosť zariadenia riadiaceho systému v jednom kanáli hlavnej automatickej cesty. Nakoľko táto časť je trojkanálová s výberom 2 z 3-och, činnosť riadiaceho systému zostala zachovaná. Vzniknuté poruchy v testovacej, alebo informačnej časti sú irelevantné, lebo nespôsobili obmedzenie činnosti hlavnej automatickej časti. Porovnaním počtu vyskytnutých porúch s počtom nasadených prvkov, zariadenie TXS v súčasnosti vykazuje veľmi nízku poruchovosť. Na znížení jeho poruchovosti sa odzrkadlili aj prijaté opatrenia, medzi ktoré patrila výmena pôvodných počítačov operátorských staníc za nové s väčšou kapacitou operačnej pamäte, ako i všetkých napájacích kariet dotknutých analógových modulov za napájacie karty inej výrobnej série.

Záver

Vyhodnotenie poruchovosti zariadenia riadiaceho systému TXS jednoznačne potvrdilo, že počítačový riadiaci systém TXS s dvojredundantnou a trojkanálovou štruktúrou je vysoko spoľahlivý a vykazuje veľkú odolnosť voči jednoduchej poruche. Poruchy, ktoré sa vyskytli na zariadení, neovplyvnili prevádzku systému ochrany reaktora a tým ani jadrovú bezpečnosť prevádzkovaných blokov JE V1.

Literatúra

[1] GRUNBECKEN, Siemens,1996: Koncepcia skúšok systému ochrany reaktora.

[2] HERMANN, Siemens, 1996: Systém ochrany reaktora, koncepcia hlásení.

[3] WERNER, Siemens, 1996: Štruktúra systému ochrany reaktora.

Ing. Pavol Karaba

ved. odd. bezpečnostných a riadiacich systémov
Slovenské elektrárne, a. s.
závod Atómové elektrárne Bohunice
919 31 Jaslovské Bohunice
e-mail: karaba.pavol@ebo.seas.sk