Analýza komunikácie meničov frekvencie na zbernici Profibus

Peter Drahoš, Igor Bélai

Článok analyzuje komunikáciu na zbernici Profibus-DP po pripojení meniča frekvencie na zbernicu ako zariadenia slave. Pomocou špecializovaného diagnostického nástroja boli vykonané experimenty na pracovisku typu multimaster s dvanástimi typickými prevádzkovými zariadeniami. Pozornosť je sústredená na meniče frekvencie pri inicializácii komunikácie s využitím príkazov aplikačnej vrstvy ISO/OSI a v prevádzke, kde sa riadia vnútorným stavovým diagramom, ktorý je vymedzený v aplikačnom komunikačnom profile Profidrive.

1. Úvod

Tento článok voľne nadväzuje na príspevok publikovaný v predošlom čísle časopisu [6], v ktorom bola opísaná cyklická komunikácia s typickými prevádzkovými zariadeniami, vrátane segmentu s inteligentnými senzormi. Veľmi často používanými zariadeniami na Profibus-DP sú inteligentné akčné členy typu menič frekvencie, ktorých komunikácia a správanie sú opísané v nasledujúcich kapitolách.

Usporiadanie a komunikačné vzťahy zariadení na experimentálnom pracovisku boli vyobrazené v [6]. Zariadeniami *slave* sú dva moduly vzdialených vstupov a výstupov (RIOS1, RIOS2), dva meniče frekvencie (Drive1, Drive2) a komunikačné prevodníky: DP/DP coupler a Intelligent Linker DP/PA.

Menič frekvencie Drive1 je typu Micromaster 420 so skalárnym frekvenčne-napäťovým riadením asynchrónneho motora, na ktorom je nainštalovaný rotačný inkrementálny snímač polohy typu IRC. Signál zo snímača IRC je privedený na počítadlo impulzov v module RIOS2. Menič frekvencie Drive2 je typu Sinamics G120 s vektorovým riadením a implementovaným obvodom regulácie rýchlosti.

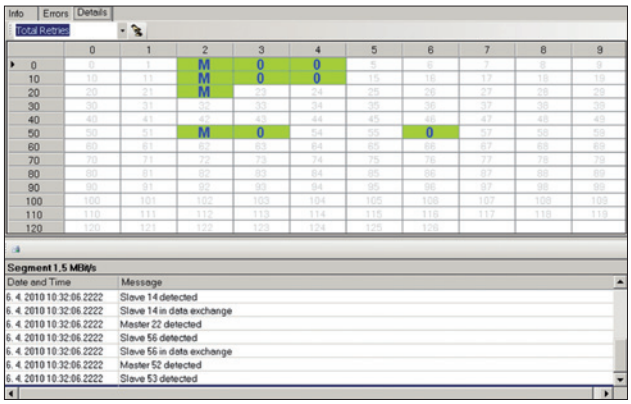
Z hľadiska toku riadiacich informácií master PLC2 komunikuje so zariadeniami RIOS2 a Drive1. Master PLC5 riadi menič frekvencie Drive2.

2. Diagnostický nástroj na analýzu komunikácie

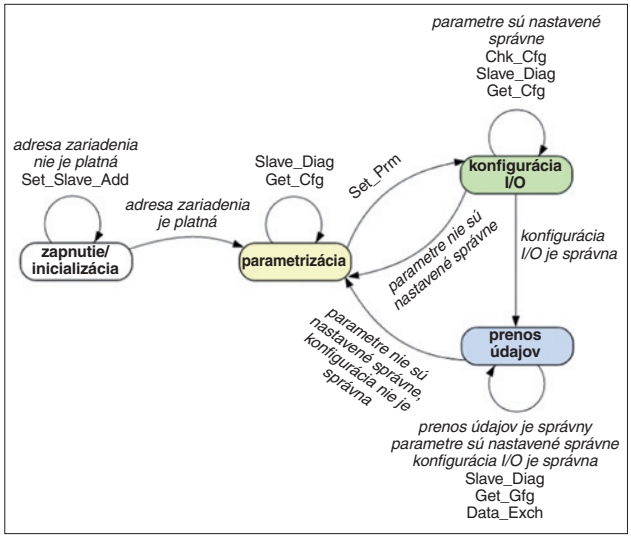
Na kontrolu a analýzu komunikácie bol použitý analyzátor protokolu Softing BC450 [5]. BC450 vykonáva dôkladnú analýzu komunikácie na zbernici, deteguje zariadenia na zbernici a ich komunikačné vzťahy. Vyhodnocuje časovanie zbernice, analyzuje prenášané telegramy a počíta chyby komunikácie a diagnostické správy. Svojou činnosťou neovplyvňuje úrovne signálov ani komunikáciu. Zaznamenané a vypočítané hodnoty vizualizuje aplikácia bežiaca na osobnom počítači, s ktorou je BC450 prepojený pomocou USB. Na *obr. 1* je príklad bezporuchového stavu komunikácie na testovacej sieti Profibus uvedenej na *obr. 1* ([6]). Nástroj názorne zobrazuje počet diagnostických udalostí jednotlivých zariadení pri ich výskyte. Na základe nich môže používateľ predvídať možné výpadky komunikácie. Hlavným indikátorom problémov na zbernici je počet opakovaní vysielaných správ.

Hlavné komunikačné časové intervaly, ktoré nástroj zaznamenáva, sú:

1. *dĺžka ostatného komunikačného cyklu* – doba obehu poverenia (*tokenu*) všetkými zariadeniami *master*,
2. *dĺžka cyklu výzvy* – časový interval, ktorý začína vysla ním rámca výzvy daného zariadenia *master* určeného prvému zariadeniu *slave* (ktoré je zariadeniu *master* priradené) a končí prijatím rámca odozvy od posledného zariadenia *slave* priradeného danému zariadeniu *master*,
3. *doba nečinnosti zbernice* – čas, ktorý pre dané zariadenie *master* uplynie medzi prijatím rámca odozvy a vyslaním nasledujúceho rámca výzvy (minimálne 33 bitových intervalov),
4. *doba oneskorenia stanice slave* – čas, ktorý uplynie medzi prijatím výzvy a následnou odozvou zariadenia *slave*.



Obr. 1. Prehľad zariadení na zbernici Profibus s uvedeným počtom porúch komunikácie a diagnostických hlásení (zariadenia master sú označené písmenom M)



Obr. 2. Stavový automat zariadenia Profibus-DP slave

3. Pripojenie zariadenia *slave* na zbernicu

Správanie zariadenia *slave* na zbernici Profibus je opísané stavovým automatom uvedeným na *obr. 2*, ktorý má štyri stavy: zapnutie/inicializácia, parametrizácia, konfigurácia I/O a prenos údajov [3]. Prechody medzi týmito stavmi sa realizujú v postupnosti komunikačných cyklov zbernice a sú iniciované príkazmi zo zariadenia *master*. *Master* vysiela jednotlivé príkazy až po prijatí odozvy na predchádzajúci príkaz.

V *tab. 1* je príklad komunikácie medzi zariadením *master* a jemu priradeným zariadením *slave* s adresou 14, po pripojení napájania na zariadenie *slave*. Počas experimentu bola zaznamenaná komunikácia na zbernici pred zapnutím napájania a po ňom.

V prípade, že zariadenie *slave* nekomunikuje, zariadenie *master* mu na základe nastavenej konfigurácie siete vysiela

v každom komunikačnom cykle výzvu o zaslanie diagnostických informácií (telegramy 4924 a 4945, služba Slave_Diag). Typ príkazu je špecifikovaný číslom bodu prístupu ku službe (SAP – *Service Access Point*). Čísla a funkcie bodov prístupu ku službám pre cyklickú komunikáciu sú sumarizované v *tab. 2*. V *tab. 1* sú čísla SAP uvedené súčasne s adresou zariadenia. Napríklad adresa 14.60 predstavuje SAP 60 nachádzajúci sa v zariadení s adresou 14.

Po pripojení napájania a vnútornej inicializácii vstupuje menič frekvencie Drive1 (zariadenie *slave* s adresou 14) do stavu parametrizácia. Po prijatí príkazu na načítanie diagnostických údajov (SAP 60, telegram č. 4945) odpovedá telegramom 4946, v údajovej časti ktorého oznamuje nepripravenosť na cyklický prenos údajov a taktiež to, že ho neparametrizovalo žiadne zariadenie *master*.

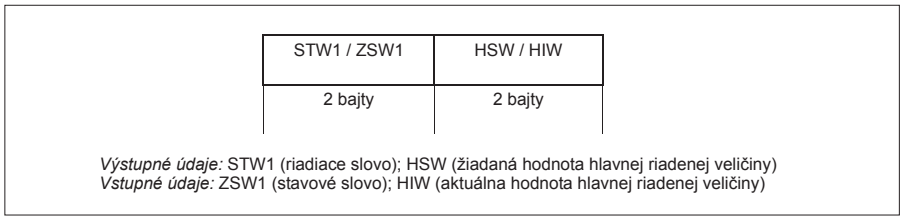
V komunikačnom cykle č. 3 *master* vysiela príkaz Set_Prm (SAP 61, telegram 4964), ktorý spôsobí prechod zariadenia *slave* do stavu konfigurácia I/O. V údajovej časti príkazu sa nachádzajú nové hodnoty pre parametrizáciu. Význam hodnôt pre parametrizáciu: prevzatie zariadenia *slave* zariadením *master* (v popisovanom prípade ide o zariadenie *master* s adresou 12), nastavenie časovania zbernice a špecifických parametrov zariadenia *slave*. *Slave* potvrdzuje prijatie parametrov telegramom č. 4965 bez údajovej časti (služba SC – *Short Acknowledge*).

V komunikačnom cykle č. 4 vysiela *master* príkaz Chk_Cfg (SAP 62, telegram 4989). Zariadenie *slave* kontroluje vlastnú konfiguráciu a v telegrame č. 4990 odpovedá kladným potvrdením príkazu (SC).

V nasledujúcich komunikačných cykloch vysiela *master* výzvy o zaslanie diagnostických informácií (SAP 60, služba Slave_Diag), až pokým nie je zariadenie *slave* pripravené na cyklický prenos údajov. Zariadenie *slave* o tom informuje zariadenie *master* telegramom č. 5061 a počínajúc komunikačným cyklom č. 8 začína cyklická komunikácia *master-slave*.

Tab. 1. Príklad komunikácie medzi zariadeniami master a slave po pripojení napájania zariadenia slave a prenos údajov medzi meničom frekvencie a PLC

Číslo	Kom. cyklus	Adresa	Primitíva	Služba	Údaje
4924	1	12.62 → 14.60	výzva	Slave_Diag	
4945	2	12.62 → 14.60	výzva	Slave_Diag	
4946	2	14.60 → 12.62	odozva	Slave_Diag	02 05 00 FF 80 B5
4964	3	12.62 → 14.61	výzva	Set_Prm	B8 02 03 0B 80 B5 00 E0 00 00
4965	3	14.61 → 12.62	odozva	SC	
4989	4	12.62 → 14.62	výzva	Chk_Cfg	00 F1
4990	4	14.62 → 12.62	odozva	SC	
5012	5	12.62 → 14.60	výzva	Slave_Diag	
5013	5	14.60 → 12.62	odozva	Slave_Diag	02 0C 00 0C 80 B5
5036	6	12.62 → 14.60	výzva	Slave_Diag	
5037	6	14.60 → 12.62	odozva	Slave_Diag	02 0C 00 0C 80 B5
5060	7	12.62 → 14.60	výzva	Slave_Diag	
5061	7	14.60 → 12.62	odozva	Slave_Diag	00 0C 00 0C 80 B5
5082	8	12 → 14	výzva	Data_Exch	00 00_ 00 00
5083	8	14 → 12	odozva	Data_Exch	FB 41_ 00 00
5549	29	12 → 14	výzva	Data_Exch	04 76_ 00 00
5550	29	14 → 12	odozva	Data_Exch	FB 41_ 00 00
5831	41	12 → 14	výzva	Data_Exch	04 76_ 00 00
5832	41	14 → 12	odozva	Data_Exch	FB 31_ 00 00
5853	42	12 → 14	výzva	Data_Exch	04 77_ 00 00
5854	42	14 → 12	odozva	Data_Exch	FB 31_ 00 00
6001	48	12 → 14	výzva	Data_Exch	04 77_ 00 00
6002	48	14 → 12	odozva	Data_Exch	FB 32_ 00 00
6024	49	12 → 14	výzva	Data_Exch	04 7F_ 00 00
6025	49	14 → 12	odozva	Data_Exch	FB 32_ 00 00
6167	54	12 → 14	výzva	Data_Exch	04 7F_ 00 00
6168	54	14 → 12	odozva	Data_Exch	FB 34_ 00 00
6178	54	52 → 53	výzva	Data_Exch	04 7F_ 19 9A riadiace slovo_žiadaná hodnota
6179	54	53 → 52	odozva	Data_Exch	6B 37_ 19 9A stavové slovo_skutočná hodnota



Obr. 3. Štruktúra vstupných a výstupných údajov meničov frekvencie [2]

4. Riadenie meniča frekvencie na základe profilu Profidrive

Štruktúra údajov prenášaných medzi zariadením *master* a meničom frekvencie obsahuje riadiace (stavové) slovo a žiadanú (aktuálnu) hodnotu hlavnej riadenej veličiny. Štruktúra prenášaných údajov je na *obr. 3*.

Hodnota hlavnej žiadanej veličiny (HSW na *obr. 3*) je vyjadrená celým číslom z rozsahu ±16 378. Hodnota 16 378 predstavuje 100 %. Hlavnou riadenou veličinou pre menič frekvencie Drive1 je frekvencia statorového napätia motora a pre Drive2 je ňou žiadaná uhlová rýchlosť rotora. Oba meniče frekvencie patria v rámci Profidrive do triedy „AK 1 – štandardný pohon“. Meniče frekvencie uvedené v úvode sú z hľadiska konštrukcie a algoritmu riadenia asynchrónneho motora rozdielne, ale napriek tomu sú zjednotené z hľadiska štruktúry údajov a spôsobu komunikácie v zmysle profilu Profidrive.

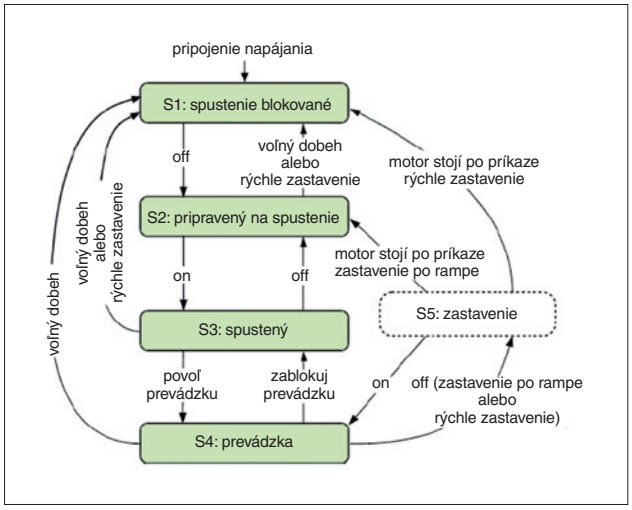
Činnosť meniča frekvencie pri spúšťaní a vypínaní je opísaná všeobecným stavovým automatom uvedeným na *obr. 4*. Stavy S1 až S5 sú signalizované hodnotou bitov stavového slova (ZSW1). Prechody medzi stavmi sú iniciované riadiacimi slovami (STW1) vysielanými do meniča frekvencie zo zaria-

Tab. 2. Body prístupu ku službám (SAP) pre cyklickú komunikáciu [3]

SAP	Služba
SAP 0	Data_Exch (cyklický prenos údajov)
SAP 54	komunikácia *master-master*
SAP 55	Set_Slave_Add (nastavenie adresy zariadenia *slave*)
SAP 56	Rd_Inp (načítanie vstupnej hodnoty)
SAP 57	Rd_Outp (načítanie výstupnej hodnoty)
SAP 58	Global Control (príkazy pre zariadenia *slave*)
SAP 59	Get_Cfg (načítanie konfiguračných údajov)
SAP 60	Slave_Diag (diagnostika zariadenia *slave*)
SAP 61	Set_Prm (odoslanie parametrizačných údajov)
SAP 62	Chk_Cfg (kontrola údajov o konfigurácii)

denia *master*. Znamená to, že riadiaci program bežiaci na zariadení *master* musí generovať vhodnú postupnosť riadiacich slov, ktoré umožnia prechod do cieľového stavu. Význam bitov riadiacich a stavových slov špecifikuje komunikačný profil Profidrive [2].

V *tab. 1* je uvedená postupnosť prechodov medzi stavmi S1 až S4 po zapnutí napájania meniča frekvencie Micromaster 420. V stave S1 má stavové slovo meniča hodnotu FB41 H. V tomto stave sa menič frekvencie nachádza v komunikačných cykloch 8 až 40. Prechod do stavu S2 spôsobuje riadiace slovo 0476 H vysielané v komunikačných cykloch 29 až 41. Stavové slovo meniča v stave S2 má hodnotu FB31 H. Na prechod do stavov S3 (FB32 H) a S4 (FB34 H) sú použité riadiace slová 0477 H a 047F H. Potrebné riadiace slová sú generované v používateľskom programe PLC2 na základe vyhodnotenia aktuálneho stavu meniča frekvencie.



Obr. 4. Všeobecný stavový automat pohonného objektu Profidrive

9. Záver

V experimente je analyzovaný štart komunikácie inteligentného meniča frekvencie. Toto zariadenie *slave* je monitorované od okamihu jeho pripojenia na zbernicu až po dosiahnutie prevádzkového stavu špecializovaným diagnostickým nástrojom. Komunikácia má dve fázy: naštartovanie cyklickej komunikácie Profibus a ovládanie prechodov v stavovom automate meniča frekvencie. V prvej fáze komunikácie, po zapnutí, prechádza *slave* stavmi parametrizácie a konfigurácie do cyklického prenosu údajov. V druhej fáze komunikácie sa podľa požiadaviek riadiaceho systému a v zmysle aplikačného profilu Profidrive uvedie do plného prevádzkového stavu.

Poďakovanie:
Článok vznikol s podporou združenia Profibus SK.

Literatúra:
[1] BÉLAI, I. – DRAHOŠ, P.: *Komunikačné systémy pre automatizáciu*. STU Bratislava, 2012.
[2] *PROFIdrive Drive Technology, V 3.1.2*. PROFIBUS Nutzerorganisation e. V., Germany, 2004.
[3] POPP, M.: *The New Rapid Way to PROFIBUS DP*. PROFIBUS Nutzerorganisation e. V., Germany, 2003.
[4] *MICROMASTER, PROFIBUS Optional Board – Operating Instructions, User Documentation*. Siemens, 2002.
[5] *PROFIBUS protocol analyser BC-400-PB, BC-450-PB, User Manual*. Softing AG, Germany, 2008.
[6] DRAHOŠ, P. – BÉLAI, I.: *Analýza komunikácie inteligentných senzorov na zbernici Profibus*. Automa, 2012, č. 8-9, s. 52–54.

Ing. Peter Drahoš, PhD.,
Ing. Igor Bélai, PhD.,
ÚRPI, FEI STU, Bratislava

Ing. Igor Bélai, PhD., je absolventom Elektrotechnickej fakulty SVŠT Bratislava v odbore elektronické počítače. Po dokončení doktorského štúdia v odbore automatizácia a riadenie pôsobí ako odborný asistent na ústave riadenia a priemyselnej informatiky FEI STU Bratislava. Zaoberá sa problematikou priemyselných komunikačných systémov a číslicových servosystémov.
Ing. Peter Drahoš, PhD., je absolventom Elektrotechnickej fakulty SVŠT Bratislava v odbore technická kybernetika. Po dokončení doktorského štúdia v odbore automatizácia a riadenie pôsobí ako odborný asistent na ústave riadenia a priemyselnej informatiky FEI STU Bratislava. Zaoberá sa problematikou priemyselných komunikačných systémov, senzormi a netradičnými pohonmi.

Konference o zabezpečení informačních systémů

Ve dnech 30. ledna až 1. února 2013 se v Berlíně na konferenci IT-Defense sejdou nejvýznamnější odborníci na počítačovou bezpečnost, hackeři a autoři odborných publikací, aby diskutovali o aktuálních otázkách počítačové bezpečnosti. Konference se bude konat už pojedenácté. V programu jsou každoročně „namíchány“ strategické prezentace, technicky detailní přednášky i poutavé referáty informující o tématu odlehčenou, zábavnou a interaktivní formou. Důležitou součástí je také večerní setkání a kulaté stoly s příležitostí k osobním diskusím mezi odborníky.

O tom, jak funguje moderní špionáž a jak pracovníci špionážních agentur získávají tajné a citlivé informace z počítačových dat, bude hovořit Ira Winkler, bývalý spolupracovník americké Národní bezpečnostní agentury NSA a jeden z nejvýznamnějších odborníků v oblasti počítačové špionáže. Charlie Miller, také bývalý spolupracovník NSA, publicista a hacker specializující se zejména na produkty Apple, předvede, jak získat přístup k inteligentnímu telefonu iPhone prostřednictvím NFC. Dawn Cappelliová, technická ředitelka společnosti CERT, uvede seznam deseti nejdůležitějších pravidel pro zabezpečení informačních systémů proti útokům zevnitř firmy. Jayson E. Street bude hovořit o metodách sociálního inženýrství k získávání citlivých informací a o jejich až překvapivě snadném a účinném využití v hackerské praxi. Podplukovník Volker Kozok z německého spolkového ministerstva obrany bude přednášet o vlivu aktivistů zapojených do sociálních sítí na politiku a hospodářství. A nakonec se mohou účastníci těšit na přednášku bezpečnostního experta Shreeraje Shaha o zranitelnosti HTML5.

Tito a ještě mnozí další odborníci vystoupí ve dvoudenním programu konference a třetí den s nimi budou moci návštěvníci v rámci setkání u kulatých stolů diskutovat na vybraná témata.

Konferenci pořádá společnost Cirosec GmbH. Další informace a přihlášku zájemci najdou na www.it-defense.de. Kapacita je omezena na 200 osob a lze očekávat, že i přes vysoké účastnické poplatky bude brzy naplněna.

(Bk)