Průmyslový Ethernet V: Bezpečná komunikace po Ethernetu

František Zezulka, Ondřej Hynčica

Problematika funkční bezpečnosti (*safety*) je jedním z nejaktuálnějších témat současné etapy vývoje automatizační techniky ve vyspělých průmyslových zemích. Týká se i přenosů dat v průmyslových řídicích systémech. Nelze se jí tedy vyhnout ani v seriálu o průmyslovém Ethernetu, jehož dále předkládaná, pátá část se zabývá metodami umožňujícími zvýšit bezpečnost komunikace v sítích Ethernet.

1. Definice pojmů z oblasti bezpečnosti podle normy ČSN EN 61508

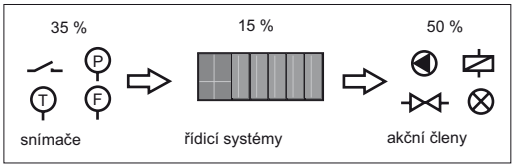
V důsledku obtíží s překladem pojmů *safety* a *security* do některých jazyků (např. v češtině, ale i v němčině se pro oba uvedené anglické pojmy používá jedno slovo – *bezpečnost*) je v této terminologii mnoho nejasného i mezi technickou veřejností. Uveďme proto nejprve, co bude v tomto textu pod pojmem bezpečná komunikace myšleno. Vyjde se přitom z normy IEC 61508 pro oblast funkční bezpečnosti elektrických, elektronických a elektronických programovatelných systémů (E/E/EP systémy), resp. jejího českého překladu ČSN EN 61508 ([2], [3], [4], [5], [8]).

Podle uvedených norem lze rozlišit a posuzovat tři základní druhy bezpečnosti, a to bezpečnost primární, nepřímou a funkční. Význam těchto a dalších vybraných základních pojmů, na nichž staví ČSN EN 61508, je uveden v *tab. 1*.

Velmi důležitý je v uvedených normách pojem *integrita bezpečnosti* a související pojmy, definované v *tab. 2*.

Protože komunikační podsystém je součástí E/E/EP systémů souvisejících primárně s řízením a sběrem dat z řízených strojů, výrobních linek i technologických systémů (EUC) a sekundárně i s E/E/EP spojenými s bezpečností, je zřejmé, že na průmyslový Ethernet jsou kladeny požadavky z hlediska funkční bezpečnosti. Je tedy třeba důsledně vycházet ze standardu IEC 61508, který staví na těchto pěti základních předpokladech:

1. Žádný systém nemůže být absolutně spolehlivý, tedy nelze vyloučit jeho možné selhání ani *n*-násobnou redundancí. Růst spolehlivosti systémů (např. redundancí – zálohováním dalším identickým systémem) zvyšuje stupeň pohotovosti, resp. funkceschopnost celku, obecně však nemusí vést k větší funkční bezpečnosti.
2. Přináležitost systému do určité SIL znamená, že je akceptováno zmenšení rizika na určitou mez danou odpovídající třídě SIL (odpovídající pravděpodobnosti bezporuchové funkce bezpečného systému).
3. Funkční bezpečnost zařízení jako celku musí být zaručena i při selhání bezpečnostních funkcí řídicího (nebo komunikačního) systému; jak toho bude dosaženo, není předmětem normy.
4. Bezpečné systémy odpovídající určité SIL musejí být konstruovány podle daných pravidel (pro hardware i software) tak, aby měly požadovanou spolehlivost odpovídající dané třídě SIL.
5. Funkční bezpečnost se vztahuje na celý řetězec podle *obr. 1* (na něm je současně uvedeno rozdělení poruch podle jejich přináležitosti jednotlivým kategoriím komponent řetězce zajišťujícího funkční bezpečnost).



Obr. 1. Výskyt chyb v prvcích bezpečnostního řetězce realizovaného programovatelným elektronickým systémem (PES)

Celková pravděpodobnost výskytu chyby ve fungování programovatelného elektronického systému (*Programmable Electronic System* – PES) je sumou pravděpodobností chybné funkce jednotlivých komponent v celém PES.

Z *obr. 1* je patrné, že největší pravděpodobnost poruchy v celém řetěz-

Tab. 1. Vybrané základní pojmy z oblasti funkční bezpečnosti podle ČSN EN 61518

Bezpečnost	odstranění nepřijatelného rizika
Primární bezpečnost	zahrnuje primární rizika, jako jsou např. úrazy elektrickým proudem, šoky, nebo popálení způsobená zařízením
Nepřímá bezpečnost	zahrnuje vedlejší důsledky nesprávné funkce zařízení, které přímo neohrožují zdraví osob
Funkční bezpečnost	část celkové bezpečnosti týkající se řízeného procesu nebo stroje (*Equipment under Control* – EUC) a systému řízení EUC, která je závislá na správném fungování E/E/EP systémů souvisejících s bezpečností, anebo na systémech souvisejících s bezpečností založených na jiných technických principech a konečně na vnějších prostředcích pro snížení rizika
Riziko	kombinace pravděpodobnosti výskytu poškození a závažnosti tohoto poškození
Přípustné riziko	riziko, které je přijatelné v daných souvislostech založených na běžných hodnotách společnosti
Zbytkové riziko	riziko zbývající po přijetí ochranných opatření
Nebezpečí	potenciální zdroj poškození, újmy
Chyba	ukončení schopnosti zařízení vykonávat požadovanou funkci
Bezpečná chyba	chyba, která není natolik závažná, aby narušila funkci systému nebo způsobila nebezpečný stav systému
Nebezpečná chyba	chyba, která může uvést bezpečnostní systém do nebezpečného stavu nebo stavu, kdy není schopen plnit svou funkci

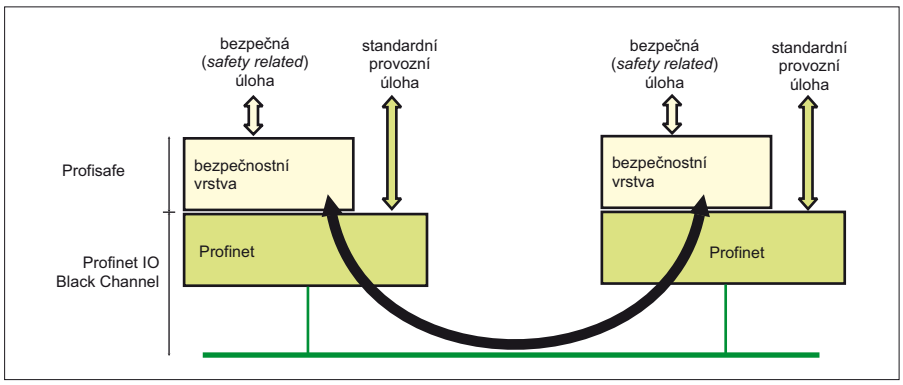
Tab. 2. Pojem integrita bezpečnosti a pojmy s ním související podle ČSN EN 61508

Integrita bezpečnosti (*safety integrity*)	pravděpodobnost, s jakou systém související s bezpečností bude uspokojivě plnit požadované bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu
Integrita bezpečnosti softwaru (*software safety integrity*)	míra vyjadřující pravděpodobnost, že software bude v E/E/EP systému souvisejícím s bezpečností plnit své bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu
Integrita bezpečnosti hardwaru (*hardware safety integrity*)	část integrity bezpečnosti systémů souvisejících s bezpečností týkající náhodných poruch hardwaru charakteru nebezpečné poruchy
Úrovně integrity bezpečnosti (*Safety Integrity Level* – SIL)	diskrétní úroveň (jedna ze čtyř úrovní, definovaných normou) pro stanovení požadavků integrity bezpečnosti bezpečnostních funkcí přiřazených E/E/EP systémům souvisejícím s bezpečností, kde úroveň integrity bezpečnosti 4 má nejvyšší úroveň integrity bezpečnosti a úroveň 1 nejnižší (zkratkou SIL 1 až SIL 4)

ci vykazují čidla, akční členy a jejich kabeláž jen celkem 15 % chyb vzniká ve vlastním řídicím a komunikačním systému. Ethernet jako dosti robustní komunikační systém by pravděpodobností bezporuchového stavu (*Average Probability of Failure on Demand* – PFD, tj. pro případ, že bezpečnostní systém působí jen velmi zřídka – *on demand*), kte-

Tab. 3. Možné chyby při přenosu dat a metody jejich eliminace

Možné chyby dat při přenosu	Metody eliminace chyb						
	sekvenční číslování dat	časová značka dat	potvrzení příjmu dat	identifikace odesílatele a příjemce	zálohování dat	redundance dat	kontrola platnosti dat
opakování	x	x				x	
ztráta	x		x			x	
vkládání	x		x	x		x	
špatné pořadí	x	x				x	
nekonzistence			x		x		x
zpoždění		x					
propojení safe a non-safe			x	x			x
přetečení paměti směrovače		x					



Obr. 2. Princip „black channel“

přenosu, které mohou být způsobeny náhodným elektromagnetickým rušením působícím na přenosový kanál, poruchami a chybami komunikačního hardwaru i systematickými chybami některých komponent standardního provozního hardwaru a softwaru.

Jak na principu *black channel* realizovat bezpečný komunikační kanál, lze ukázat

prvky komunikujících entit (např. zajištění bezpečného stavu zařízení). Z *obr. 2* je dále patrné, že standardní provozní data i bezpečná data (související s bezpečností, *safety relevant*) jsou přenášena současně jedním společným komunikačním kanálem, přičemž data související s bezpečností jsou použita pro bezpečné úlohy a data bez vazby na bezpečnost (standardní provozní data) se používají pro standardní provozní úlohy.

Na *obr. 3* je princip z *obr. 2* blíže specifikován pro celý bezpečnostní řetězec z *obr. 1*. Je zde patrný současný přenos provozních a bezpečných dat jedním komunikačním kanálem (např. Profinet) i to, že přenosy bezpečných a provozních dat jsou navzájem nezávislé. K zajištění přenosu bezpečných dat (bezpečnou komunikaci) by tedy měl postačovat jednoduchý komunikační kanál. Jeho případné zdvojení nesouvisí s bezpečností, ale s provozní dostupností (pohotovostí, *availability*) zařízení.

V [9], jsou specifikovány tyto možné typy poruch a chyb při přenosu dat:

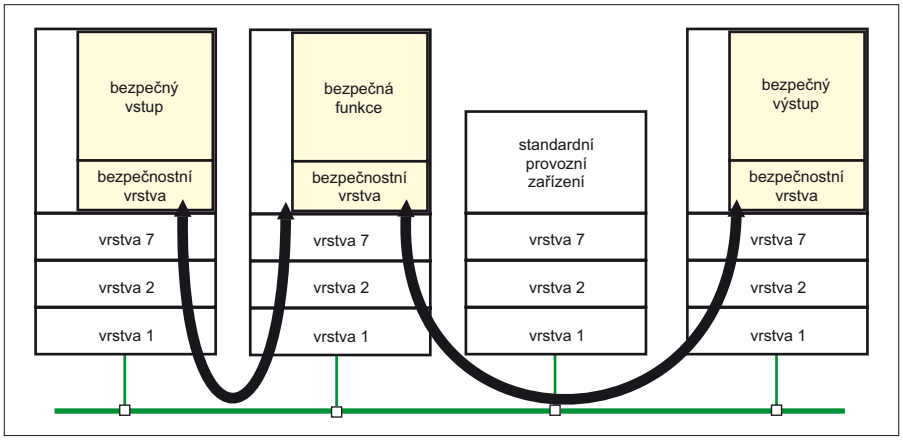
- *opakování*: opakovaný příjem stejných dat,
- *ztráta*: nedoručení dat,
- *vkládání*: příjem dat od jiného než předpokládaného (určeného) odesílatele,
- *špatné pořadí*: data jsou přijata v jiném pořadí, než v jakém byla odeslána,
- *nekonzistence*: data jsou poškozena,
- *zpoždění*: větší než přípustný interval mezi odesláním a příjmem dat,
- *propojení „safe“ a „non-safe“*: nepřípustná komunikace mezi bezpečnostním (*safe*) a obyčejným (*non-safe*) odesílatelem či příjemcem.

Tamtéž jsou také definovány odpovídající bezpečnostní mechanismy, které lze zavést do

rá je 10^{-8} až 10^{-7} pro třídu SIL 3, měl stačit již ve svém standardním provedení. Přesto je však třeba se mechanismy bezpečné komunikace v průmyslové síti, a tudíž i v síti Ethernet zabývat.

2. Princip „black channel“

Předpoklad uvedený v kap. 1 ad 3 je splněn při použití principu tzv. černého komunikačního kanálu (*black channel*). Tento princip vychází ze zcela utilitárního a ekonomického požadavku neměnit nic na hardwaru ani softwaru standardních komunikačních systémů (např. CAN, Profibus, Ethernet, Ethernet Powerlink, Profinet apod.), které jsou již z principu své provozní funkce dobře nebo velmi dobře zabezpečeny před vznikem poruchy. Potřebné a požadované třídy SIL těchto komunikačních systémů nechť se tedy dosahuje nikoliv zvětšováním spolehlivosti (zmenšování pravděpodobnosti vzniku poruchy) v dolních vrstvách protokolu, nýbrž vřazením bezpečné vrstvy do sedmé vrstvy komunikačního modelu nebo nad ni. V principu by protokol sedmé vrstvy (s vnořenou bezpečnostní vrstvou) měl eliminovat všechny možné chyby



Obr. 3. Současná provozní a bezpečná (safety related) komunikace v síti Profibus

např. na systému Profisafe (*Profibus Safety*), viz [7], [10] a internetové odkazy.

Na *obr. 2* je na vlastní komunikační kanál (Profibus, Profinet) nahlíženo jako na „černý kanál“, který může, ale nemusí fungovat spolehlivě.

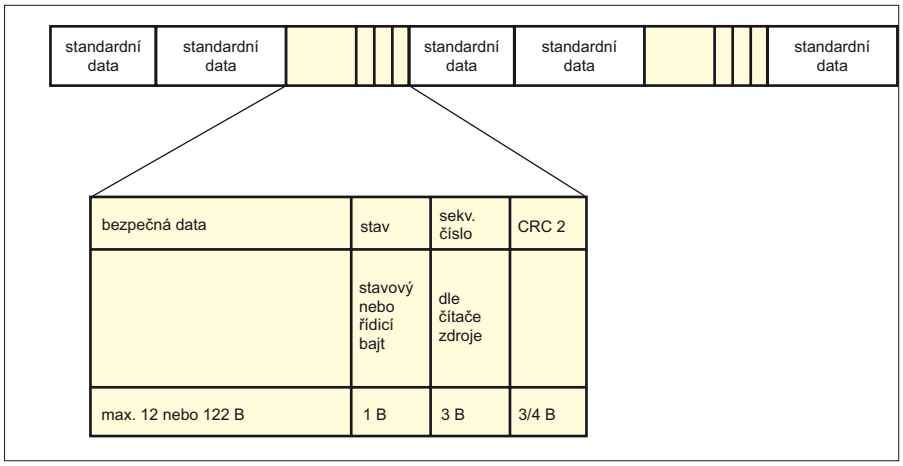
Funkce bezpečnostní vrstvy (*safety layer*) spočívá v detekování poruch a realizaci opatření eliminujících vliv poruchy v komunikačním kanálu v součinnosti s bezpečnostními

vnořené bezpečnostní vrstvy komunikačního protokolu pro eliminaci již uvedených chyb [9]. Těmito mechanismy jsou:

- *sekvenční číslování dat*: odesílatel disponuje čítačem, jehož hodnota s odesláním každého údaje (skupiny údajů) vzroste o jedničku, a ke každému odeslanému údaji je připojena aktuální hodnota čítače,
- *časová značka*: odesílatel doplňuje každý odeslaný údaj informací o čase, v ně-

mž byl údaj odeslán (časová značka, *time stamp*),
- *potvrzení příjmu dat*: příjemce informuje odesílatele, že data úspěšně přijal,
- *identifikace odesílatele a příjemce*: data obsahují identifikaci odesílatele a příjemce,
- *zálohování dat*: odesílaná data se zálohují na straně odesílatele,
- *redundance dat*: data se odesílají redundantně (několikanásobné odeslání dat, kódování dat),
- *kontrola platnosti dat*: přidání kontrolních dat (např. použitím CRC).

V *tab. 3* je uvedeno, jak jednotlivé bezpečnostní mechanismy eliminují ty které jednotlivé typ chyby při přenosu dat [9].



Obr. 4. Pakety protokolu Profisafe jednoduše vnořené do toku standardních datových rámců

Minimem požadovaným od bezpečného komunikačního protokolu je schopnost eliminovat všechny již zmíněné chyby. Protože každá síť má své zvláštnosti a speciální chybové módy, je při tvorbě bezpečného protokolu důležité mít důkladné znalosti o použitém typu sítě.

Nejběžnější případ vnoření bezpečných dat do komunikačního protokolu je ukázán na *obr. 4* na příkladu protokolu Profisafe ([7], [10] a internetové odkazy). Podobně jako jsou standardní data doplněna doplňujícími bajty paketu, jsou bezpečná data doplněna bajty použitých bezpečných mechanismů z *tab. 3* a vnořena do toku dat mezi standardní rámce.

3. Řešení bezpečné komunikace v síti Ethernet

Třebaže Ethernet má jinak vesměs vynikající vlastnosti, není v současné podobě, tj. jako síť typu LAN, schopen vyhovět požadavkům na bezpečnou komunikaci. Bezpečné úlohy obecně vyžadují bezpečnou práci s daty, to např. znamená, že i komunikační parametry musejí být nastavovány bezpečným způsobem. V tom případě by se ale adresa IP musela nastavovat jiným protokolem než protokolem DHCP, který je k tomu účelu v sítích typu LAN používán. Protokol DHCP však není bezpečný protokol ve smyslu IEC 61508. Rovněž server poskytující adresy IP není bezpečným serverem (*safety relevant)*. V tom momentě výhoda protokolu TCP ztrácí na významu, neboť řídicí mechanismus spojovací služby (*connection oriented*) také není bezpečný. Má-li být Ethernet schopen realizovat bezpečnou komunikaci, musí být bezpečnostní mechanismy použity v sedmé vrstvě.

Z uvedeného je jistě zřejmé, že konstatovaná nedostatečná bezpečnost komunikace nepadá na vrub vlastního Ethernetu (první a druhá vrstva referenčního modelu ISO/OSI), ale až nadstavbě – konkrétně protokolu DHCP aplikační vrstvy.

Měření na Ethernetu v praxi potvrzují jeho vysoký stupeň robustnosti (odolnosti proti vnitřním i vnějším poruchám včetně elektromagnetické kompatibility) i v průmyslovém prostředí (viz [1], str. 64, *Robustness*). Navíc díky velké šířce přenášeného frekvenčního pásma je reálné předpokládat, že bude možné přenášet v jedné síti jak provozní, tak bezpečná data (*safety relevant*). To značně zjednoduší instalaci sítě, její uvádění do chodu a sníží cenu instalace. Při použití průmyslových sběrnic typu fieldbus je mnohdy nutné vést standardní provozní data po jedné síti a bezpečná data ve zvláštní síti (*safety fieldbus*) nebo zvláštními bezpečnými spoji vedenými mezi dvěma body, tj. od havarijních tlačítek k bezpečným akčním členům.

Téměř všechny významnější průmyslové sítě (*fieldbus*) mají v současné době svoji bezpečnou variantu (AS-I Safety at Work, Interbus Safety, CAN safety, Profisafe, SafetyBus atd.). Všechny mechanismy pro bezpečnou komunikaci, uvedené v přehledu v *tab. 3*, nejsou ovšem použity u každé z uvedených průmyslových sběrnic. U metod podporujících provoz v reálném čase s tvrdými požadavky (*hard real-time*) na dobu odezvy (*deadline*) a synchronizaci (*jitter*), jako jsou např. EtherCat, Ethernet Powerlink, Profinet a SERCOS III, nejsou použity zejména ty mechanismy, které v bezpečném režimu jsou časově náročné. Například Ethernet Powerlink nepoužívá z uvedených mechanismů (*tab. 3*) potvrzování příjmu, redundanci dat. Podobně Profinet IO nepoužívá potvrzování příjmu a časovou značku (tu nahrazuje mechanismem *watchdog*).

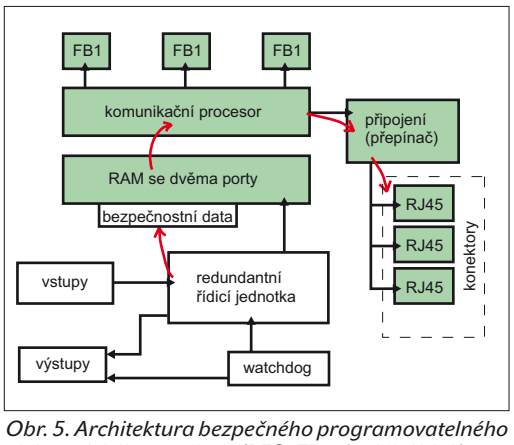
4. Příklad PES souvisejícího s bezpečností

Na *obr. 5* je zobrazena obecná struktura programovatelného elektronického systému (PES) s vlastnostmi bezpečného řídicího a komunikačního systému [1].

Jeho redundantní (zdvojený) procesorový systém generuje data se vztahem k bezpečnosti systému (*safety related data)*. Tato data jsou přenášena do jiné jednotky typu PES, která rovněž podporuje bezpečnou komunikaci, prostřednictvím paměti RAM se dvěma porty a komunikačního procesoru. Jestliže komunikační procesory komunikujících entit nejsou schopny do stanoveného času přenést data, uplatní se princip černého komunikačního kanálu a procesor PES uvede řízený proces např. do bezpečného stavu. Je zřejmé, že takový mechanismus jednak zmenšuje rychlost přenosu, současně zvyšuje bezpečnost systému, avšak zmenšuje pohotovost (*avaliability*) toho systému.

Závěr

Pátá část seriálu o průmyslovém Ethernetu pojednává o bezpečnosti automatizovaných řídicích systémů. Je v ní stručně připomenuta norma IEC 61508, definující funkční bezpečnost systémů, řízených a zabezpečených elektrickými, elektronickými a programovatelnými elektronickými systémy. Jsou zde uvedeny a stručně charakterizovány principy umožňující zvýšit úroveň funkční bezpečnosti průmyslových sítí a způsoby, kterými je toho dosaženo.



Obr. 5. Architektura bezpečného programovatelného elektronického systému (PES; FB – funkční blok)

Literatura:
[1] LÜDER, A. – LORENTZ, K.: *IAONA Handbook – Industrial Ethernet*. IAONA e. V., 2nd edition, Magdeburg, 2005.
[2] ČSN EN 61508-1 *Funkční bezpečnost E/E/EP systémů souvisejících s bezpečností. Část 1: Úvod*. ČNI, Praha, 2002.
[3] ČSN EN 61508-4 *Funkční bezpečnost E/E/EP systémů souvisejících s bezpečností. Část 4: Definice a zkratky*. ČNI, Praha, 2002.
[4] ČSN EN 61508-5 *Funkční bezpečnost E/E/EP systémů souvisejících s bezpečností. Část 5: Příklady metod určování úrovní integrity bezpečnosti*. ČNI, Praha, 2002.
[5] ČSN EN 61508-7 *Funkční bezpečnost E/E/EP systémů souvisejících s bezpečností. Část 7: Přehled technik a opatření*. ČNI, Praha, 2002.
[6] TANGERMANN, M.– LÜDER, A.: *The IAONA Handbook for Network Security, Version 1.3*. IAONA e. V., Magdeburg, October 2005.
[7] *Safety Communication – Safety Integrated – System overview*. Siemens AG, 2005.
[8] UHER, J.: *Úvod do funkční bezpečnosti I: norma ČSN EN 61508*. Automa, 2004, roč. 10, č. 8-9, s. 66–71.
[9] WRATIL P.: *Sichere Netzwerke – Technik und Anwendung*. Elektrotechnik, 21/2005, s. 72–77.
[10] *State of the Art and Trends in Safety, Security, Wireless Technologies and Real-time Properties*. D01.1-1-V1, EU – FP6/2004/IST/NMP/2 – 016696 VAN, 2006.
[11] ZEZULKA, F. – HYNČICA, O.: *Průmyslový Ethernet I: Historický úvod*. Automa, 2007, roč. 13, č. 1, s. 41–43.
[12] ZEZULKA, F. – HYNČICA, O.: *Průmyslový Ethernet II: Referenční model ISO/OSI*. Automa, 2007, roč. 13, č. 3, s. 86–90.
[13] ZEZULKA, F. – HYNČICA, O.: *Průmyslový Ethernet III: Fyzické provedení sítě Ethernet*. Automa, 2007, roč. 13, č. 6, s. 40–44.
[14] ZEZULKA, F. – HYNČICA, O.: *Průmyslový Ethernet IV: Principy průmyslového Ethernetu*. Automa, 2007, roč. 13, č. 10, s. 57–60.

Odkazy na internet:
http://support.automation.siemens.com/WW/view/en/21978204
http://www2.automation.siemens.com/cd/safety/html_76/produkte/feldbus?systarchi.hlm

prof. Ing. František Zezulka, CSc. (zezulka@feec.vutbr.cz),
Ing. Ondřej Hynčica (hyncica@feec.vutbr.cz),
UAMT FEKT VUT v Brně

Recenze: Výpočty a simulace v programech Matlab a Simulink

Karban, P.: *Výpočty a simulace v programech Matlab a Simulink*. Computer Press, Brno, 2006, ISBN 978-80-251-1448-3, 224 stran formátu 167 × 225 mm, náklad neuveden, cena 249 Kč.

Publikací o programové sadě Matlab, spolehlivém a stabilním pomocníkovi široké řady uživatelů od středoškolských studentů po akademické a výzkumné pracovníky, není nikdy dost, ale nejsou ani výjimkou. Proto jsem se zájmem otevřel knihu Pavla Karbana, abych zjistil, v čem je jiná než publikace, které znám. Jde o knihu svým způsobem originální, protože nevznikla prostým překladem zahraniční literatury či uživatelských příruček dodávaných výrobcem, ale na základě zkušeností z běžného používání. Podle autora je kniha určena studentům technických vysokých škol, kteří potřebují výpočetní nástroj, dokonalou vědeckotechnickou kalkulačku pro numerické ověřování teoretických partií přednášené látky, a zároveň prostředek pro řešení samostatných studentských prací. Jak velké popularitě se Matlab těší, je zřejmé z počtu účastníků tradičního každoročního setkání příznivců programu Matlab, konference *Technical Computing Prague*, pořádané každoročně firmou Humusoft, s. r. o., autorizovaným prodejcem produktů firmy The MathWorks pro ČR, ve spolupráci s akademickými institucemi. Zdálo by se tedy, že Matlab žádnou osvětu nepotřebuje. Není to však pravda. Jednak se Matlab stále vyvíjí a jednak je to nástroj tak rozsáhlý, že i zkušený uživatel méně používané, a přesto užitečné funkce či konstrukce časem zapomene.

Kniha je psána formou srozumitelnou i naprostému laikovi. Na konkrétních příkladech vede čtenáře k získání základních dovedností.

Nejprve se čtenář seznámí s grafickým prostředím, aby následně rychle získal první zkušenosti s používáním programu Matlab jako výkonné kalkulačky s numerickým i grafickým výstupem výsledků. Pro složitější výpočty a programové konstrukce je třeba proniknout do tajů různých typů dat, od reálných čísel, přes komplexní čísla, řetězce, pole až po struktury. Samostatné kapitoly jsou věnovány operacím s maticemi, práci s polynomy, složitějším sekvencím operací a psaní uživatelských funkcí, práci se soubory a prostředkům pro grafickou vizualizaci. Uvedená témata zaujímají polovinu rozsahu knihy.

Další část knihy, tentokrát čtvrtina rozsahu, je věnována použití programu Matlab k řešení úloh z matematické analýzy (výpočet určitého integrálu a derivace funkce, řešení diferenciálních rovnic), dynamiky mechanických soustav a elektrotechniky (analýza elektrického obvodu včetně dynamiky přechodových dějů, výpočty v oblasti elektrostatických a elektromagnetických polí).

Zbývající část knihy je věnována programu Simulink, nadstavbovému nástroji programového prostředí Matlab, který je určen k modelování a simulačním výpočtům dynamických systémů popsaných blokovým schématem sestaveným z prvků vestavěných knihoven či bloků definovaných uživatelem. Nechybí popis často používaných základních prvků knihoven a jednoduché příklady simulace dynamicky elektrických a elektromechanických obvodů.

V příloze jsou stručně uvedeny možnosti rozšíření prostředí Matlab o tematicky zaměřené knihovny funkcí, tzv. toolboxy. Připomeňme, že seznam obsažený v knize není a ani nemůže být vyčerpávající, a že je dobré se podívat na http://www.matlab.com, popř. na http://www.humusoft.cz/matlab, s aktuálními informacemi o možných rozšířeních programu Matlab.

Čtenáři doporučuji přeskočit odstavec *Alternativa zdarma – GNU Octave* na stranách 13 a 14, který je zařazen podle mého názoru nevhodně. Čtenář nabude dojmu, že když se naučí Matlab, nemusí si jej opatřit, protože k Matlabu existuje něco zcela ekvivalentního, a navíc zdarma. Není to tak, úplná kompatibilita není zaručena.

V knize najde poučení, inspiraci a chuť pracovat s programem Matlab každý, kdo tohoto výkonného pomocníka zná jen z doslechu. Autor nepředpokládá, že je čtenář vzdělán v programování, elektrotechnice, mechanice či matematické analýze. Jednoduchost, s jakou je úvod do Matlabu koncipován, je hlavní předností knihy, která tak může posloužit nejen jako příručka pro studenty vysokých škol, jak je psáno v předmluvě, ale i jako průvodce programem Matlab pro středoškoláky.

Petr Horáček,
FEL ČVUT v Praze,
ProTyS, a. s.