TRENDY V OBLASTI KOMUNIKAČNEJ BEZPEČNOSTI PRIEMYSELNÝCH SIETÍ

TRENDS IN AREA OF SAFETY COMMUNICATIONS WITHIN INDUSTRIAL NETWORKS

Mária Franeková, Aleš Janota, Karol Rástočný

Katedra riadiacich a informačných systémov, Elektrotechnická fakulta, Žilinská univerzita, Univerzitná 1, 010 26 Žilina

Abstrakt Príspevok mapuje trendy v oblasti komunikačnej bezpečnosti priemyselných sietí so zameraním na zabezpečenie funkčnej bezpečnosti. Vychádza z analýzy útokov na priemyselné siete a opisuje odporúčané bezpečnostné ochrany a ich umiestnenie v rámci vrstvového komunikačného protokolu pre siete typu fieldbus, používané pri riadení bezpečnostne kritických procesov.

Summary The paper deals with the problems of safety communication in industrial networks for purpose of assurance of functional safety. It is intents on analysis of treats on industry networks and there is described recommended safety protections and their location into layer communication protocol applicable in fieldbus network, which they are used within safety critical processes control.

1. ÚVOD

S rozšírením moderných informačných a komunikačných technológii do oblasti priemyselnej automatizácie rastie význam riešenia bezpečnosti dát pri ich zbere, prenose, spracovaní a archivácii. Priemyselné komunikačné siete sa stávajú súčasťou rozsiahlych meracích a riadiacich systémov, na báze moderných informačných technológií. Komunikačné cesty v rámci riadiaceho systému predstavujú jedno zo zraniteľných miest, najmä pri používaní otvorených prenosových systémov (mobilná, rádiová sieť...).

Komunikačná bezpečnosť je v štandardoch, ktoré sa aplikujú pre komerčné účely, definovaná zachovaním dôvernosti (k údajom majú prístup len autorizované objekty), integrity (dáta môžu byť modifikované len autorizovanými subjektami a pôvod informácie je overiteľný) a dostupnosti (dáta sú autorizovaným subjektom do určitého času prípustné, nedôjde teda k odmietnutiu služby) [1]. Na dosiahnutie bezpečnostného cieľa v rámci komunikácie sa odporúča aplikovať bezpečnostné funkcie, ktoré presadzujú bezpečnosť a vykonávajú sa pomocou vhodne zvolených bezpečnostných mechanizmov. Bezpečnostné mechanizmy môžu mať softvérovú (riadenie prístupu do systému, používanie hesiel, mechanizmy na báze kryptografie...), hárdverovú (hárdverové šifrovače, autentizačné a identifikačné karty ...), fyzickú (tienenie, trezory, zámky...) alebo administratívnu (právne normy, zákony, vyhlášky, výber dôveryhodnej osoby, certifikačná autorita ...) podobu.

V súčasnosti existuje celý rad bezpečnostných mechanizmov všetkých typov, používajúcich v rôznych aplikáciách. Norma ISO 7498-2 ISO/OSI *Security Architecture* (vyšla aj ako odporúčanie X.800) definuje základné bezpečnostné služby pre komunikačné siete komunikujúce prostredníctvom sedemvrstvového referenčného modelu OSI (*Open System Interconnection*) a odporúča umiestnenie bezpečnostných mechanizmov v rámci jednotlivých vrstiev OSI [2].

V prípade použitia priemyselnej komunikačnej siete pre potreby riadenia bezpečnostne kritických procesov nemožno pri definícií bezpečnostných mechanizmov vychádzať zo všeobecných noriem definovaných pre komerčné účely (internet a pod.). Nedetegovateľné narušenie prenášaných dát (napríklad riadiacich povelov) môže spôsobiť značné materiálne škody alebo škody na ľudskom zdraví. V takomto prípade dostáva bezpečnosť komunikačných ciest odlišné dimenzie. V mnohých prípadoch majú procesy, ktoré treba riadiť v priemyselných aplikáciách, špeciálny prívlastok - kritické procesy súvisiace s bezpečnosťou (*safety - related critical processes*) a riadiaci systém musí garantovať požadovanú úroveň integrity bezpečnosti SIL (*safety integrity level*). Pojem úroveň integrity bezpečnosti definuje základná norma pre technickú bezpečnosť IEC 61508, kde sú určené všeobecné princípy platné pre implementáciu bezpečnostných pravidiel pri použití elektrických, elektronických a programovateľných elektronických systémov súvisiacich s bezpečnosťou [3]. Pre rôzne aplikačné oblasti sú vytvorené vlastné bezpečnostné štandardy, často odvodené zo základných (generických) bezpečnostných štandardov. Z pohľadu komunikačnej bezpečnosti sú podrobne definované bezpečnostné mechanizmy napríklad pre oblasť riadenia železničnej dopravy [4]. V súčasnosti sa začínajú na báze [3] formulovať

princípy bezpečnosti komunikačných subsystémov používaných pri riadení cestnej dopravy [5].
Pre oblasť automatizácie vznikajú nové normy a odporúčania, ktoré tieto princípy aplikujú aj do oblasti riadenia procesov, výrobnej automatizácie a strojových mechanizmov. V oblasti priemyselných sietí je dnes veľmi akceptovateľná technológia fieldbus, ktorá sa stáva štandardom aj v aplikáciách s prívlastkami *safety–related* a *security-related*. Štandardy pre siete fieldbus, IEC 61158 [6] spolu so sériou štandardov IEC 61784-1 [7] a IEC 61784-2 [8], definujú profily komunikačných protokolov pre potreby distribuovaného riadenia spojitých a diskrétnych procesov v aplikáciách pracujúcich v reálnom čase. Návrh štandardu IEC 61784-3 [9], ktorý sa zaoberá funkčnou bezpečnosťou priemyselných sietí, bol v súčasnosti druhýkrát pripomienkovaný národnými komisiami a prerokovávaný na zasadnutí pracovnej skupiny IEC SC65C//WG12 v prvej polovici novembra 2005. Tento štandard definuje bezpečnostné komunikačné vrstvy, ktoré sú implementované do subsystému súvisiaceho s bezpečnosťou podľa [3], ktorý poskytuje nutné bezpečnostné služby medzi dvomi a viacerými účastníkmi v zbernicovej sieti typu fieldbus. Implementácia týchto bezpečnostných služieb umožňuje použiť sieť fieldbus v bezpečnostne kritických aplikáciách.

2. PRINCÍP KOMUNIKÁCIE SÚVISIACEJ S BEZPEČNOSŤOU

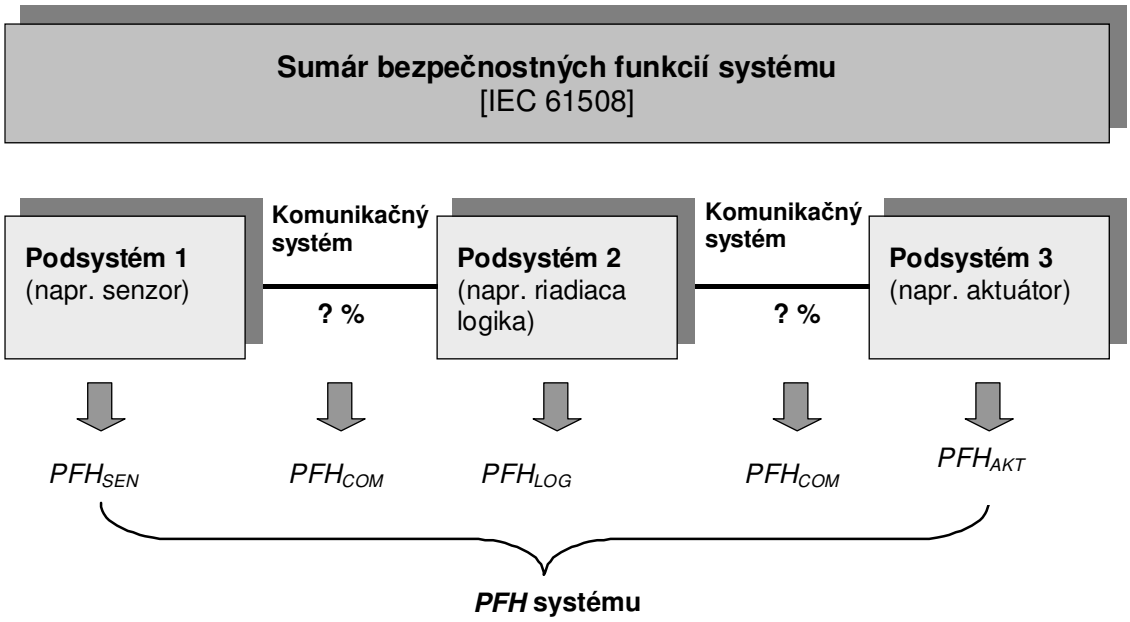
Bezpečnostné funkcie systému, definované v [3], možno rozdeliť na bezpečnostné funkcie zodpovedajúce jednotlivým častiam systému. Na obr. 1. je príklad rozdelenia bezpečnostných funkcií na tri podsystémy. Ak systém súvisiaci s bezpečnosťou používa komunikačný systém na prenos medzi rôznymi miestami, potom sa tento stáva súčasťou systému súvisiaceho s bezpečnosťou a treba dokázať, že prenos „koniec-koniec“ je bezpečný v súlade s normou [3]. Komunikačný systém je tu chápaný ako subsystém, ktorý medzi jednotlivými časťami (senzor, riadiaca logika, aktuátor, ...) dokáže zabezpečiť prenos s garantovanou úrovňou integrity bezpečnosti systému.

Celková intenzita porúch systému za hodinu PFH (*Probability of Failure per Hour*), kvantifikovaná pre jednotlivé triedy integrity bezpečnosti SIL (SIL 1- 4) podľa [3], je potom súčtom čiastkových intenzít od jednotlivých subčastí, včítane komunikačného systému:

$$PFH_{SYS}=PFH_{SEN}+PFH_{COM}+PFH_{LOG}+PFH_{COM}+PFH_{AKT} \quad (1)$$

Akou mierou prispieva komunikačný systém k celkovej bezpečnosti systému závisí od konkrétnej aplikácie, použitého média (metalické, bezdrôtové), triedy prenosového systému a prístupu k systému (s oprávneným prístupom, bez oprávneného prístupu).

Trendom je použitie otvoreného prenosového prostredia, s možnosťou prepojenia komunikácie na verejnú telefónnu a dátovú sieť alebo internet, vrátane služieb intranetu, elektronickej pošty a databáz príslušného informačného systému. Pre drážne aplikácie je podľa [4] definovaných sedem tried otvorených prenosových systémov. Závažnosť útokov pri jednotlivých typoch systémov závisí od technických vlastností systému, včítane bezporuchovosti, pohotovosti systému a realizovaného prístupu do systému cez privátnu



Obr. 1. Miera bezpečnej komunikácie pri výbere bezpečnostných funkcií systému.
Fig. 1. Decomposition of safety communications within safety function of system.

alebo verejnú sieť.
Otvorený prenosový systém je podľa [4] pokladaný za nedôveryhodný systém, pretože používa na komunikáciu prenosové média, ktorých charakteristiky sú pre používateľa neznáme, takisto nie je známy systém smerovania správ v sieti medzi koncami prenosového systému. Takýto systém je vystavený vplyvu iných používateľov systému, ktorí nie sú projektantovi systému známi a môžu sa pokúsiť získať prístup k dátam bez oprávnenia správcu systému.
Pri komunikácii prostredníctvom otvoreného prenosového systému musí byť zaistená primeraná ochrana proti všetkým identifikovaným ohrozeniam bezpečnosti systému. Knižnica ochrán môže byť z časti prebratá z typov ochrán, ktoré používajú systémy prenosu dát nesúvisiace s bezpečnosťou a doplnená o niektoré špeciálne bezpečnostné mechanizmy, vzhľadom na charakter ohrození v otvorenom prenosovom systéme a špecifikum prenosu. Tieto techniky treba do budúcna inovovať, vzhľadom na vývoj metód v danej oblasti.

3. ÚTOKY A OCHRANY V PRIEMYSELNÝCH SIEŤACH

Typy útokov v sieťach závisia v značnej miere od použitého prenosového média a metód prístupu k sieti. Na ich elimináciu sú definované bezpečnostné funkcie, ktoré sa v komunikačnej infraštruktúre implementujú prostredníctvom bezpečnostných mechanizmov. Útok na prenášané dáta možno najčastejšie vykonávať prerušením komunikácie, odpočúvaním komunikácie a modifikáciou správ. Ak sa vykonáva pasívny útok odpočúvaním správ, komunikácia na úrovni dvojbodového spoja predstavuje problém existencie niekoľkých prijímačov, ak sa vykonáva aktívny útok modifikáciou správ, ide o problém existencie viacerých zdrojov.
Aby sa obmedzilo riziko spojené s ohrozeniami je nutné, aby komunikačný systém použitý pri riadení bezpečnostne kritického procesu obsahoval bezpečnostné služby a mechanizmy a poskytoval ich v takej miere, ktorú si vyžaduje daná aplikácia. Použitý sortiment bezpečnostných mechanizmov závisí od konkrétnej aplikácie a špecifikácie komunikačného procesu. Komunikačný subsystém v rámci riadenia bezpečnostne kritických procesov v priemysle má určité špecifiká v porovnaní s komunikačným systémom používaným vo verejných nedôveryhodných sieťach. Medzi jeho odlišnosti patrí to, že platnosť prenášaných dát je časovo závislá (procesy s časovou platnosťou správ), charakter prenosu správ je zväčša cyklický a pri prenose musí byť garantovaná stanovená úroveň integrity bezpečnosti.
Typy útokov na prenášané správy a následné ochrany na ich elimináciu pre priemyselné siete fieldbus sú uvedené v tabuľke 1.
V aplikáciách, kde sú prijaté správy vztiahnuté k času, môže v niektorých prípadoch stará informácia predstavovať pre používateľa potencionálne nebezpečenstvo. Vtedy sa odporúča používať v rámci prídavných dát časovú pečiatku (*time stamp*), ktorá znižuje riziko súvisiace s opakovaním, zmenou poradia a oneskorením správ tým, že správy, ktoré príjme prijímač po časovom limite sa stávajú neplatnými. Pri

Tab. 1. Útoky a ochrany v priemyselných sieťach fieldbus.
Tab. 1. Attacks and measures in fieldbus industry networks.

ÚTOKY	OCHRANY							
	Poradové číslo	Časová pečiatka	Uplynutie času	Autentizácia	Spätná správa	Integritné techniky	Bezpečnostný kód	Kryptografické metódy
Narušenie					✓	✓		✓
Opakovanie							✓	✓
Zmena poradia							✓	✓
Strata	✓				✓		✓	✓
Oneskorenie		✓	✓					
Vloženie	✓			✓	✓		✓	✓
Maskovanie				✓	✓		✓	✓

cyklickom charaktere prenosu môže prijímač kontrolovať oneskorenie medzi dvomi správami. Ak oneskorenie prekračuje definovaný dovolený maximálny čas, musí sa predpokladať chybový stav. Tento mechanizmus sa nazýva časové oneskorenie (*time delay*).

Pre skupinové komunikačné procesy sa odporúčaj použiť prostriedky na kontrolu zdroja všetkých prijatých informácií pred tým, ako sú použité, tzv. identifikátory zdroja a miesta určenia (*identifiers of source and destination*). Správy môžu obsahovať jednoznačný identifikátor zdroja alebo jednoznačný identifikátor miesta určenia alebo obidva identifikátory súčasne. Voľba sa vykoná podľa aplikácie súvisiacej s bezpečnosťou. Pridaním identifikátora zdroja do správ môže používateľ bez nutnosti komunikácie s odosielateľom verifikovať, že správy sú od určeného zdroja.

Ak je k dispozícii vhodný prenosový kanál, možno od príjemcu poslať odosielateľovi spätnú správu (*feedback message*). Použitie spätnej správy môže prispieť k bezpečnosti procesu rôznymi spôsobmi: poskytnutím kladného potvrdenia o prijatí platných a aktuálnych správ, poskytnutím kladného potvrdenia o prijatí poškodených správ, aby sa umožnilo prijatie vhodného opatrenia, potvrdením identity prijímajúceho zariadenia, umožnením synchronizácie hodín vo vysielajúcom a prijímajúcom zariadení, umožnením dynamických kontrolných postupov medzi účastníkmi.

Ak sa v rámci procesu súvisiaceho s bezpečnosťou predpokladá neautorizovaný prístup do systému (ohrozenie typu maskovanie správ) je nutné použiť vhodne navrhnuté autentizačné a identifikačné procedúry (*identification procedures*), napr. otlačok (*digest*) správy. Medzi silné autentizačné mechanizmy patrí použitie digitálneho podpisu (*digital signature*) správy v kombinácii s hašovacími kódmi.

V otvorených prenosových systémoch sú často používané prenosové kódy na detekciu bitových alebo zhlukových chybových stavov. Z pohľadu bezpečnosti proces súvisiaci s bezpečnosťou nesmie dôverovať týmto prenosovým kódom. Na detekciu poškodenia správy sa preto vyžaduje prídavný bezpečnostný kód (*safety code*), riadený procesom súvisiacim s bezpečnosťou. V prípade použitia bezpečnostného kódu sa musí preukázať primeranosť: schopnosti detekcie všetkých očakávaných typov chýb a hodnoty pravdepodobnosti nedetegovaných chýb.

V poslednom období sa v rámci bezpečných priemyselných komunikačných protokolov presadzuje použitie kryptografických techník, ktoré sa v komerčnej sfére používajú už niekoľko desiatok rokov. Kryptografický kód (*cryptographic code*) sa v rámci bezpečnostne kritických procesov odporúča použiť, keď nie je možné alebo je ťažko realizovateľné zvládnutie zlomyseľných útokov v rámci otvoreného prenosového systému. Kryptografické techniky zväčša využívajú prenosové systémy súvisiace s bezpečnosťou pri použití rádiového prenosového systému alebo prenosových systémov pripojených na verejné siete. Tieto techniky možno kombinovať s bezpečným mechanizmom kódovania alebo sa môžu používať samostatne. Kryptografické techniky zahŕňajú použitie algoritmov a metód správy kľúčov (generovanie, prenos, archivácia kľúčov). Ich kvalita a účinnosť závisí od sily algoritmu a utajenia kľúčov [10].

4. MODEL KOMUNIKAČNÉHO PROTOKOLU

Definované ochrany možno implementovať v rámci komunikačného protokolu súvisiceho s bezpečnosťou, pričom typ ochrán sa volí podľa charakteru aplikácie a bezpečnostných požiadaviek na ňu kladených. Vrstvový princíp riešenia bezpečnosti komunikácie v rámci vyčlenenej vrstvy alebo podvrstvy sa stáva trendom nielen v bezpečných protokoloch siete internet a pri zabezpečení komunikácie súvisiacej s bezpečnosťou (*safety-related communication*) v rámci železničných zabezpečovacích systémov [4] ale najnovšie aj v priemyselných sieťach typu fieldbus [9]. Vytvorená bezpečnostne – relevantná vrstva v rámci komunikácie, tzv. fail-safe vrstva (ide najčastejšie o vyššie vrstvy v rámci sedemvrstvového modelu) nenarúša protokoly používané v nižších vrstvách a všetky bezpečnostné mechanizmy sú sústredené len v rámci zvolenej vrstvy. Na obr. 2 je znázornené umiestnenie fail-safe vrstvy v rámci komunikačného protokolu súvisiaceho s bezpečnosťou pre sieť fieldbus do SCL (*Safety Communication Layer*) vrstvy, ktorá je nadstavbou (profilom) siedmej vrstvy z definovaného modelu OSI. Model komunikačného protokolu súvisiaceho s bezpečnosťou pre priemyselné siete typu fieldbus podľa [9] je znázornený na obr. 3. Na implementáciu bezpečnostných mechanizmov má model definované tri vrstvy:

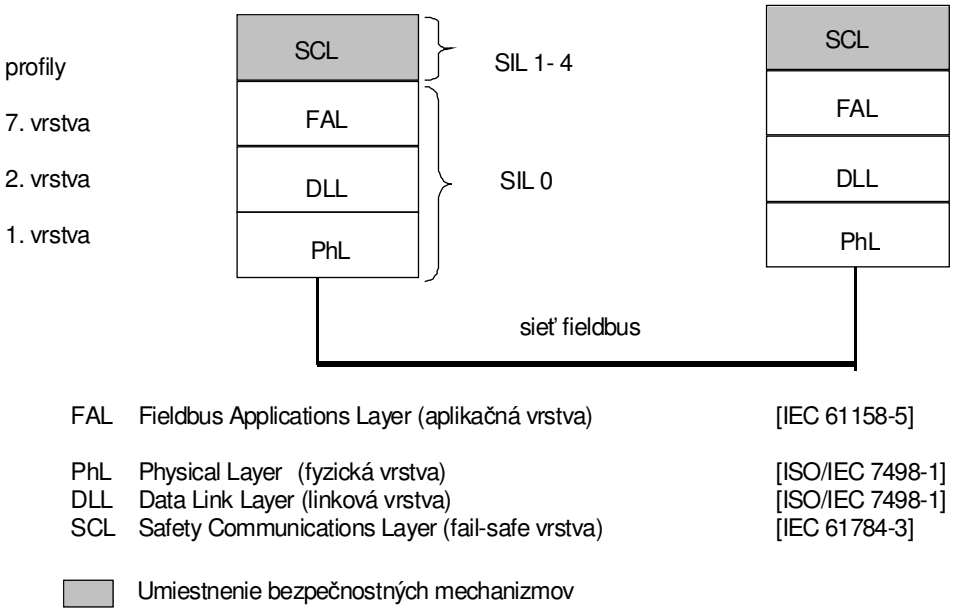
safety layer (vrstva, v ktorej sú implementované autentizačné a integritné algoritmy v rámci uzatvoreného systému, kde sa nepredpokladá neoprávnený prístup do systému),

security layer (vrstva, v ktorej sú implementované silnejšie bezpečnostné mechanizmy na báze kryptografických techník v rámci otvoreného prenosového systému, pričom sa predpokladá neoprávnený prístup do systému),

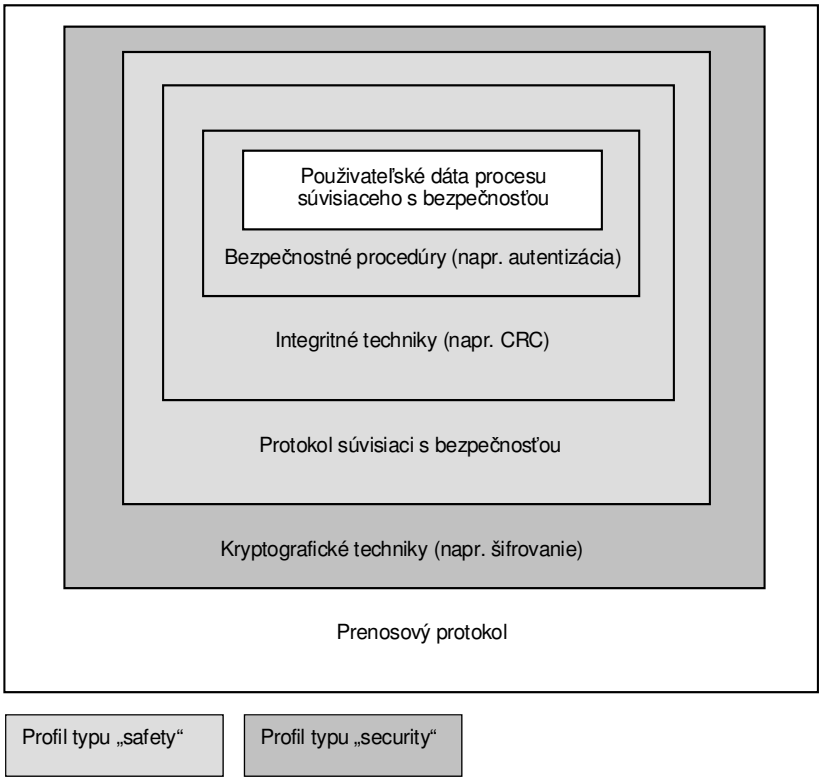
transmission layer (vrstva, v ktorej sú implementované bezpečnostné mechanizmy nedôveryhodného prenosového systému).

Trendom, hlavne pri prenose cez otvorené prenosové systémy, je použitie silných ochrán na báze kryptografie do tzv. vrstvy *security layer*. Pri tvorbe takéhoto typu bezpečného protokolu sa odporúča protokol rozdeliť na tri subprotokoly: protokol pre

službu typu autentizácia, protokol pre službu typu dôvernosť a protokol pre prácu so správou kľúčov (*key management*).



Obr. 2. Umiestnenie bezpečnostnej vrstvy v komunikačnom protokole siete fieldbus.
Fig. 2. Location of safety layer within communication protocol of fieldbus network.



Obr. 3. Model komunikačného protokolu súvisiaceho s bezpečnosťou pre siete fieldbus.
Fig. 3. Model of safety – related communications protocol for fieldbus networks.

5. ZÁVER

Informačné a komunikačné systémy sú dnes súčasťou moderných riadiacich systémov, používaných pri riadení bezpečnostne kritických procesov v automatizácii. Komunikačný systém ovplyvňuje celkovú bezpečnosť takéhoto systému rôznou mierou. Závisí to od typu použitého prenosového systému (uzatvorený, otvorený), od použitého komunikačného média (metalické, bezdrôtové), počtu používateľov systému, definovaných prístupových práv do systému a iných atribútov v závislosti na oblasti, v ktorej sa komunikačný systém používa.

Sortiment bezpečnostných mechanizmov použitých v rámci priemyselnej komunikácie je nutné určiť zo stanovenej analýzy útokov na komunikačný systém a v závislosti od požiadaviek na úroveň integrity bezpečnosti systému. Tieto princípy sa realizujú vytváraním bezpečných vrstiev alebo podvrstiev v rámci protokolov, čím nenarušujú komunikačné protokoly nižších vrstiev. Tento trend sa používa nielen v bezpečných protokoloch siete internet, ale možno ho zaznamenať aj v protokoloch v rámci priemyselných riadiacich komunikačných subsystémov na báze sietí fieldbus.

Fail-safe komunikačné protokoly vyvíjané pre prenos správ súvisiacich s bezpečnosťou okrem „klasických“ bezpečnostných mechanizmoch typu CRC (*cyclic redundancy check*), poradových čísel, časových značiek a adries začínajú používať aj moderné prvky na báze kryptografie so zameraním na zabezpečenie služby dôvernosti, integrity a autentizácie prenosu.

Poďakovanie

Tento príspevok bol spracovaný s podporou Slovenskej grantovej agentúry VEGA, grant č. 1/1044/04 „Teoretický aparát pre implementáciu princípov e-Safety do inteligentných dopravných systémov“.

LITERATÚRA

[1] DOBDA, L.: Ochrana dát v informačních systémech, GRADA, Praha 1998, ISBN 80-7169-479-7

[2] ČSN ISO 7498-2 Systémy na spracovanie informácií. Prepojenie otvorených systémov. Základný referenčný model. Časť 2: Bezpečnostná architektúra

[3] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems. 1998

[4] IEC 62280-2 Railway application, Communication, signalling and processing system – Part 2: Safety related communication in open transmission system

[5] SPALEK, J., JANOTA, A., FRANEKOVÁ, M., VESTENICKÝ, P., BUBENÍKOVÁ, E., CIGÁNEK, P., VESTENICKÝ, M.: Princípy eSAFETY a komplexná bezpečnosť IDS, Sborník abstraktů přednášek konference ITS'05 Prague, SDT ČR, Praha 2005, str. 57-58. ISDN 80-239- 4447-9

[6] IEC 61158 Digital data communications for measurement and control – Fieldbus for use in industrial control systems

[7] IEC 61784-1 Digital data communications for measurement and control. Part 1: Profile sets for continuous and discrete manufacturing relative to fieldbus use in industrial control systems

[8] IEC 61784-2 Digital data communications for measurement and control. Part 2: Additional profiles for ISO/IEC 8820-3 based communication networks in real time applications.

[9] IEC 61784-3 Digital data communications for measurement and control. Part 3: Profiles for functional safety communications in industrial networks

[10] STALLINGS, W.: Cryptography and Network Security, Prentice Hall, Ney Yersey, 2003