



Vážení a milí čtenáři

bezpečnost, spolehlivost, dostupnost – to jsou termíny, které jsou v technických oborech dávno domácí. Nově k nim přibývá zabezpečení informací neboli kybernetická bezpečnost se svými novými termíny, jako jsou šifrování, autentizace nebo integrity dat. V tomto vydání je také několik článků věnovaných řízení dopravy: a zde se objevují další nové termíny, jako např. provozní pohotovost. Kdo se v tom má vyznat? Doufám, že předkládané vydání vám pomůže alespoň trochu se v tomto světě zorientovat.

Zvláště zabezpečení dat a komunikace neboli kybernetická bezpečnost neboli informační bezpečnost je téma, o kterém se stále více diskutuje. Ne tak na stránkách našeho časopisu: připravovali jsme anketu o zmíněném tématu, oslovili jsme inženýrské firmy z oboru, ale odezva byla mizivá. Že by toto téma zatím do Česka nedorazilo? Ale ano. Zrovna včera jsem mluvil se zástupcem jednoho z českých výrobců řídicí techniky o tom, že získali velkou zakázku ze zahraničí, ale zákazník ji podmínil provedením firemního auditu – a zajištění kybernetické bezpečnosti bylo první na řadě. Zde šlo zejména o zabezpečení podnikového informačního systému, aby si do něj pro informace o zakázce nemohla „sáhnout“ zákaznickova konkurence.

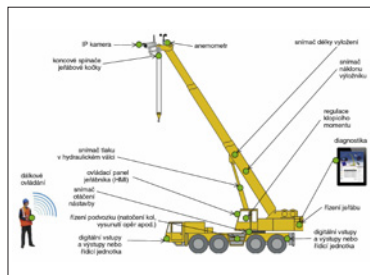
Zabezpečením dat a komunikace se zabývá článek Guido De Bouvera na str. 36 až 37 Kybernetická bezpečnost z pohledu inženýrské firmy. Jen si dovoluji trochu polemizovat s jeho tvrzením v předposlední kapitole, že „udělat alespoň nějaká opatření je lepší než nic“. Tím si nejsem tak jistý, protože „alespoň nějaká opatření“ mohou vyvolat falešný dojem jistoty. Domnívám se, že i v tomto případě je nutné analyzovat riziko a stanovit, jaká jeho míra je přípustná – a potom s tímto zbytkovým rizikem počítat. Neexistuje žádná naprosto bezpečná výroba, zcela zabezpečený systém ani nedobytná pevnost.

Nehoda bývá někdy výsledkem bizarní, až neuvěřitelně nepravděpodobné shody náhod. Takové případy si potom člověk snadno pamatuje. Mnohem častější však bývají příčiny zcela banální. Konstrukční chyba, vada materiálu, omyl obsluhy. Nebo i úmyslné porušení bezpečnostních předpisů a obejití bezpečnostních systémů. Na str. 18 až 20 najdete článek o metodě lockout/tagout. Její spolehlivost vyplývá z její jednoduchosti, ale její slabinou je to, že dohodnutá pravidla musí všichni bezpodmínečně dodržovat. Jenže to zdržuje a oprava musí být dokončena včas...

Nový rok bez neúměrného spěchu a stresu – a bez nehod vám přeje

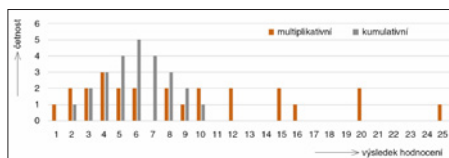
Petr Bartošík, šéfredaktor

Bezdrátové komunikační systémy a bezpečnost mobilních strojů 10



Je možné bezdrátové sítě WLAN podle IEEE 802.11 použít v časově kritických a bezpečnostních úlohách? Koncepte *black channel* a redundance komunikačních kanálů s využitím protokolu *Parallel Redundancy Protocol* (PRP) umožňují na tuto otázku odpovědět kladně.

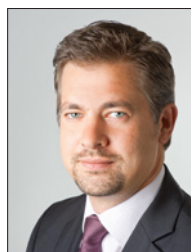
Analýza HAZOP: výběr opatření ke snížení rizik 28



Metoda HAZOP (*Hazard and Operability Study*) se stala standardem pro validaci provozuschopnosti

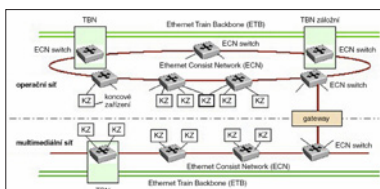
a bezpečnosti projektů složitých technologických zařízení. Při studii realizované touto metodou je obvykle vygenerováno množství opatření pro snížení rizik. Tento článek porovnává přístupy ke stanovení jejich priorit.

Proč je v průmyslu kromě bezpečnosti stále důležitější i zabezpečení dat? 38



V moderní automatizaci se stále častěji používají otevřené systémy. To je užitečné z hlediska jejich vzájemné spolupráce, ale nese to s sebou velká rizika z hlediska zabezpečení dat a komunikace. Kai Strübbe z TÜV SÜD AG upozorňuje na to, že komunikační infrastruktura výrobních podniků a všechny komponenty jejich řídicích systémů by proto měly být certifikovány nezávislou certifikační institucí.

Řídicí systémy vlaku 40



Pro systémy ve vlacích je podstatnou vlastností interoperabilita, neboť vozidla mohou být různých typů a od různých výrobců, a mají-li být provozována jako vlak, musí být jejich palubní

systémy schopny spolupracovat. Článek se zaměřuje na systém nadřazeného řízení, který zajišťuje rozhraní k lokálním systémům, ke strojvedoucímu, k ostatním vozidlům vlaku a na stacionární stranu.

Harmonogram a ediční plán časopisu Automa na rok 2014

č.	uzávěrka	expedice	oborové téma	přehled trhu
2	13. 01. 14	17. 02. 14	automatizace v hutnictví, slévárenství a těžkém průmyslu, automatizace v plastikářském průmyslu	termokamery
3	11. 02. 14	13. 03. 14	chytré továrny a integrovaná výroba (mezinárodní veletrh Amper 2014)	
4	11. 03. 14	14. 04. 14	automatizace při těžbě, dopravě, skladování a zpracování sypkých materiálů	
5	10. 04. 14	14. 05. 14	roboty, manipulátory, výrobní a montážní linky (veletrh Automatica v Mnichově), výrobní logistika, identifikace zboží a osob v průmyslové výrobě	snímače obrazu
6	12. 05. 14	13. 06. 14	technická diagnostika, řízení údržby, <i>asset management</i> , sledování spotřeby energií a surovin	
7	10. 06. 14	14. 07. 14	řízení ve vodohospodářství a v čistírnách odpadních vod, řízení vodárenských a stokových sítí, ochrana proti povodním	hydrostatické hladinoměry
8-9	11. 08. 14	09. 09. 14	automatizace v automobilovém průmyslu a strojírenské výrobě, automatizace obráběcích strojů (MSV v Brně)	
10	11. 09. 14	10. 10. 14	automatizační technika pro elektrárny, teplárny a energetiku (Elosys v Trenčíně)	vírové průtokoměry
11	10. 10. 14	12. 11. 14	řízené elektrické pohony a servopohony (SPS/IPC/Drives)	měníče frekvence
12	11. 11. 14	11. 12. 14	automatizační technika v chemickém a petrochemickém průmyslu a v plynárenství, produktovody	