### Aplikace pro mobilní zařízení

Aplikace DRM Mobile (dostupná v Google Play i App Store) nabízí další funkce: kromě mobilního dohledu mohou uživatelé registrovat svá zařízení pomocí QR kódu. Dostupná je potom jejich adresa MAC, Device ID, instalační software nebo defaultní heslo. Jakmile je zařízení registrováno do zákaznického účtu, je možné do něj prostřednictvím funkce správy profilu automaticky nahrávat zákaznické konfigurace.

### *Edge computing*

Nejnovější generace routerů Digi umožňuje zabezpečený běh zákaznických aplikací „na hraně“ sítě IoT, tedy ve vrstvě *edge*. Protože logické funkce i počáteční zpracování dat jsou realizovány v blízkosti provozovaných zařízení, snižuje se zatížení mobilní sítě a náklady na přenos dat. Pro vytváření zákaznických aplikací je k dispozici knihovna skriptů v jazyce Python.

### Zabezpečení dat a komunikace

Pro správu podnikových sítí IIoT a poskytovatele služeb je zvláště důležité zabezpečení připojení. Produkty i služby společnosti Digi International proto pravidelně procházejí přísnými interními i externími audity. Odpovědní pracovníci firmy mají certifikace CISSP (*Certified Information Systems Security Professional*), RHCE (*Red Hat Certified Engineer*), CCNP (*Cisco Certified Network Professional*), MCSE (*Microsoft Certified Solutions Expert*), CSA (*Certified Security Analyst*), CEH (*Certified Ethical Hacker*) a *Certified Lead Implementer* podle ISO 27002. DRM pomáhá splňovat požadavky na zabezpečení centralizací distribuce bezpečnostních záplat, plánováním přenosové kapacity, centralizovaným logováním, skenováním shody s pravidly a upozorněním na neshodná zařízení, řízením změn, zálohováním a obnovou ze zálohy i detekcí pokusů o napadení. Komunikace prostřednictvím DRM dokonce vyhovuje podmínkám na šifrování lékařských záznamů (v USA) HIPAA (*Health Insurance Portability and Accountability Act*).

### Shrnutí

„Internet věcí nejsou jen propojená zařízení, ale bez propojení nelze IoT realizovat,“ řekl Scott Nelson, Chief Product Officer společnosti Digi International. „DRM pomáhá našim zákazníkům zajistit, aby jejich zařízení nejen byla online, ale aby byla připojena bezpečně a pracovala efektivně.“

Nezáleží na tom, kde ve světě je zařízení umístěno – třeba i na místech, kde by člověk ani být nechtěl, jako jsou vrtné plošiny v moři nebo kompresorové stanice v poušti –, ani na tom, jaký analytický software zákazník používá, DRM vždy zprostředkuje spolehlivý a bezpečný přenos dat důležitých pro optimalizaci podnikových procesů.

Více informací zájemci najdou na adrese www.digi.com/pr/digi-remote-manager.

*Petr Bartošík*

krátké zprávy

## ▶ Společnosti Siemens a Kazanorgsintez podepsaly kontrakt na výstavbu elektrárny v Tatarstánu

Společnosti Siemens a Kazanorgsintez (součást TAIF Group) potvrdily kontrakt na výstavbu elektrárny s kombinovaným cyklem o výkonu 250 MW v Tatarstánu v Ruské federaci. Smlouvu podepsali v průběhu fóra Russian Energy Week generální ředitel firmy Kazanorgsintez Farid Minigulov a prezident firmy Siemens v Rusku Alexander Liberov. Podle kontraktu se firma Siemens stala generálním dodavatelem projektu elektrárny, kterou bude využívat sama firma Kazanorgsintez. Součástí elektrárny budou plynová turbína SGT5-2000E a parní turbína SST-600, která využívá vysokotlakou páru vyráběnou chlazením plynové turbíny, obě se svým generátorem. Dodán bude také distribuovaný řídicí systém elektrárny a zařízení pro distribuci elektřiny. Uvedení do provozu je plánováno na rok 2023. Celkový objem kontraktu je přibližně 290 milionů eur. Součástí kontraktu jsou rovněž dvě servisní smlouvy: Siemens se zavazuje udržovat po dobu třinácti let nejen novou 250 MW elektrárnu pro Kazanorgsintez, ale také 495 MW elektrárnu Nizhnekamskneftekhim. Ta byla prvním velkým společným projektem firmy Siemens s firmou ze skupiny TAIF.

Jedním z důvodů výstavby nových zdrojů elektřiny je omezení dopadů na životní prostředí. Palivem pro plynovou turbínu elektrárny s kombinovaným cyklem totiž bude generátorový plyn (syngas), vznikající jako vedlejší produkt v pyrolytických pecích závodu na výrobu etylenu, jenž dosud neměl jiné využití. Firma tím vyřeší dva problémy najednou: bude mít palivo pro novou elektrárnu a smysluplně využije vedlejší produkt závodu na výrobu etylenu. *(Bk)*

## ▶ Národní centrum Průmyslu 4.0 má nové představenstvo

Předsedou představenstva Národního centra Průmyslu 4.0 (NCP 4.0) je Jiří Kabelka z DEL, a. s., a místopředsedou Petr Šimoník z Vysoké školy báňské – Technické univerzity Ostrava. „V Národním centru Průmyslu 4.0 se angažuji již od jeho počátku,“ říká Jiří Kabelka ke svému zvolení a dodává: „Své předsednictví vnímám jako závazek a zároveň ocenění naší společnosti DEL. Věřím, že adopce technických inovací může Českou republiku posunout opět na špičku Evropy, a svou činností v rámci NCP 4.0 k tomu chci dále přispívat.“

Členy představenstva NCP 4.0 jsou zástupci dalších partnerů, a to prof. Vladimír Mařík za ČVUT v Praze, prof. Pavel Václavek za VUT v Brně, Eduard Palíšek za Siemens, Jana Polášek Filová za Škoda Auto, Jaroslav Řasa za ABRA Software a Jiří Holoubek za Svaz průmyslu a dopravy. „V představenstvu NCP 4.0 se nám podařilo koncentrovat vůdčí osobnosti českého průmyslu, což ještě více posílí a znásobí dopad aktivit, které realizujeme,“ komentuje složení představenstva ředitel NCP 4.0 Jaroslav Lískovec.

Národní centrum Průmyslu 4.0 je otevřená akademicko-průmyslová platforma, která v současné době sdružuje téměř 50 partnerů z oblasti akademické a průmyslové sféry včetně technických univerzit ČVUT, VUT, VŠB-TUO, TUL a ZČU. Hlavními průmyslovými partnery jsou Siemens a Škoda Auto. NCP 4.0 se zaměřuje také na start-upy a malé a střední firmy. Důležitou součástí NCP 4.0 je experimentální pracoviště Testbed pro Průmysl 4.0, které demonstruje výrobu podle konceptu průmyslu 4.0. *(ev)*

## ▶ Mezinárodní konference SCADA Security

Ve dnech 4. a 5. listopadu 2019 se bude v Praze konat mezinárodní konference SCADA Security, na které vystoupí čeští i zahraniční odborníci s praktickými ukázkami útoků na kritické informační a komunikační systémy a představí nejefektivnější metody obrany. Na konferenci se rovněž bude diskutovat o aktuálních otázkách ohledně zavádění moderních komunikačních sítí (5G) ve vztahu k digitalizaci průmyslu (Industry 4.0 – Connected World, mobilita a internet věcí) a kybernetické bezpečnosti. Paralelní workshopy se budou věnovat nejen kyberneticko-bezpečnostní osvětě, ale i takovým tématům, jako je využívání moderních ICT při ochraně obyvatelstva.

Účast na konferenci potvrdil např. Martin Fabry (Accura), Serhii Halahan (NPC UKenergo), Dettmer Hendrik (TÜV Trust IT), Jiří Kasner (Colsys-Automatik), Vladimír Rohel (Národní agentura pro komunikační a informační technologie) a Tobias Schroeder.

Součástí konference je i výstava produktů a řešení renomovaných tuzemských i zahraničních firem, které budou prezentovat nejmodernější technologie a řešení z oblasti SCADA/ICT a kybernetické bezpečnosti.

Další informace, program a online registrace jsou k dispozici na webových stránkách konference: http://bit.ly/35nRJgn. *(ed)*