„Podporujeme výskumné aktivity na Slovensku/Projekt je spolufinancovaný zo zdrojov EÚ

PREHĽAD DIZAJNOV MANAŽMENTU VEĽKÝCH DÁTOVÝCH TOKOV, PRE VÝVOJ MODELOV PREDIKCIE A OPTIMALIZÁCIE V ENERGETIKE

ZOSTAVENÉ NA AKTUÁLNE PRÍSTUPNÝCH DÁTACH, V KONTEXTE SMARTGRID

Predmetom siedmej analýzy v rámci projektu bolo zhrnúť možnosti najefektívnejších prístupov strategického manažmentu dát jeho analytických, distribučných a komunikačných subsystémov, na základe request-system design, zaručujúcich bezpečnosť dát. Táto správa je len formálnym výstupom širšej analýzy vhodnosti rôznych prístupov, v ktorej sme ako kritérium zohľadnili najmä aktuálny stav manažmentu dát o spotrebe a výrobe elektrickej energie na Slovensku a funkčný SmartGrid ako pomyselný cieľ očakávanej transformácie Slovenskej energetiky.

1. Plánovanie stratégie manažmentu dát v kontexte SmartGrid

SmartGrid používa obojsmernú digitálnu komunikáciu s pokročilými senzormi pre zber a analýzu dát. Tým transformuje existujúcu rozvodnú sieť na dynamickú, inteligentnú, prenosová a distribučná sieť, ktorá má mať do veľkej miery samo-korekčnú a samo-optimalizačnú schopnosť. SmartGrid má mať funkcie simulácie a extrapolácie dát v reálnom čase a funkciu analýz anomálií. Jeho užívateľské prostredie má podporovať komplexnejšie

vizualizácie a on-line monitorovania zariadení (napr. reakcia na dopyt, dynamické nastavovanie cien elektrickej energie a participácia na trhu s elektrickou energiou). Prakticky všetky zložky SmartGrid môžu generovať dáta, ktoré sú zaujímavé. Preto je potrebné manažovať objem zbieraných a spracovávaných dát. Tento objem je generovaný s očakávanou frekvenciou, ktorá je spolu s kvalitou dát, ich rôznorodosťou a možnosťou ich verifikácie ďalšou premennou, ktorú treba ustrážiť pri nastavovaní systémov manažmentu dát v SmartGrid. Bez korektne navrhnutého a kvalitne implementovaného systému pre manažment dát, sú systémy zberu, prenosu, zabezpečenia a analýzy dát len neefektívnymi funkciami bez strategickej koordinácie.

Nižšie sú, ako príklad, uvedené zariadenia, ktoré môžu byť súčasťou siete SmartGrid a odhady objemov dát, ktoré sú schopné generovať.

- Synchrónne **fázory** sa používajú na monitorovanie elektrického prúdu vo vedení a zabezpečujú, že elektrina je vždy vo fáze. V závislosti na charaktere siete a tom, ako sú nasadené, môže ich byť značný počet. Každý z nich vytvára medzi 50 - 200 bajtov na jedno čítanie a číta šesťdesiat krát za sekundu.

- **Merače ovisu** (sagometers) sa používajú na meranie ovisu vedenia na meranie teploty na prenosovej sústave. Pri frekvencii približne dvanásť čítaní za hodinu zozbierajú 50 bajtov dát na čítanie.

- **Detektory porúch** sa používajú na kontrolu a identifik0áciu porúch v prenosových alebo distribučných linkách. Generujú veľmi malé množstvo dát, menej ako 10 bytov na čítanie. Zároveň, dáta posielajú len ak identifikujú problém.

- **Skladovacie zariadenia** sú používané na ukladanie elektriny pri lokálnych distribučných staniciach, ako aj na poliach väčších zberov obnoviteľných zdrojov energie, ako sú solárne a veterné farmy. Za hodinu zrealizujú približne štyri 100 bajtové čítania (tento odhad je pre batérie pri lokálnych distribučných miestach).

- **SmartMetre** hrajú vo všeobecnosti väčšiu úlohu v SmartGrid implementáciách. V priemere generujú okolo 50 bajtov dát pri jednom čítaní. Frekvencia čítania variuje od typu zariadenia a typu OOM. Typicky, sa dáta čítajú raz za hodinu pre rezidenčných klientov (napr. domácnosti) a každých pätnásť minút pre komerčných zákazníkov.

Okrem potreby manažmentu zberu dát z týchto zariadení je potrebné, aby tieto zariadenia v inteligentnej sieti navzájom komunikovali. Cieľom tejto komunikácie je diagnostikovať a koordinovať reakciu siete na rôzne udalosti. Jednotlivé inštitúcie, využívajúce informácie (agregáty dát) zo SmartGrid musia spoločne identifikovať svoje potreby a naplánovať strategický manažment zdrojov na vytvorenie systému koordinovaného prenosu dát. Systém teda bude musieť zvládať zber a úpravu dát, vzájomnú komunikáciu medzi zariadeniami a medzi dátovým úložiskom a inštitúciami, ktoré využívajú dáta zo SmartGrid. To znamená, že inštitúcie musia plánovať aj frekvenciu zberu a tvorby agregátov dát zo sústavy, nakoľko to má obchodné dôsledky. Ak napr. SmartMeter posiela dáta trikrát za deň, tejto frekvencii sa musia prispôsobiť aj všetky obchodné procesy. Obchodník/distribútor nemôže sľúbiť svojim zákazníkom, že budú mať svoje dáta na webových stránkach spoločnosti na úrovni hodín

a v reálnom čase, v prípade, že SmartMeter odosiela dáta do systému trikrát denne. Otázka potom je, aké sú požiadavky koncového užívateľa. Aj preferencie koncových užívateľov preto ovplyvňujú akú stratégiu manažmentu dát zvolíme.

2. Manažment zabezpečenia inteligentných sietí

Často podceňovaný aspekt riadenia SmartGrid je manažment bezpečnosti. Inštitúcie venujú veľa úsilia zabezpečeniu jednotlivých zariadení v SmartGrid, ale často neberú do úvahy bezpečnosť dát a dátového prenosu medzi subsystémom zberu - analytickým subsystémom a inštitúciami. Popísané zariadenia ukladajú významné množstvo citlivých dát, vrátane behaviorálnych profilov zákazníkov. Tieto zariadenia musia byť zaistené proti rôznym formám nepovolenej manipulácie, vrátane fyzického odcudzenia, ale aj proti kybernetickým útokom. Teroristický útok na takýto systém by mohol spôsobiť značné škody. Testy ukazujú, že štandardný spôsob umiestnenia zariadení za firewallom nebude stačiť a bude potrebný bezpečnostný systém špecificky vytvorený na mieru požiadavkám systému SmartGrid.

Ako sme uviedli v prvom reporte na tému bezpečnosti, telekomunikačný priemysel v minulosti čelil niektorým z týchto problémov a z jeho skúseností je nutné vychádzať pri manažmente bezpečnostných systémov v SmartGrid. Na rozdiel od dôsledkov kybernetických útokov na telekomunikačné inštitúcie, zlyhanie zabezpečenia v SmartGrid by potenciálne mohlo mať ďalekosiahlejší dopad na spoločnosť. Dáta a agregáty v podobe informácií musia byť chránené pri prenose medzi nástrojmi, pretože odoslanie falošných dát do autonómnych systémov môže spôsobiť ich vypnutie alebo abnormálne správanie nástrojov (teda priame poškodenie siete). Bude potrebné vytvoriť nové metódy overovania identity zariadení a inštitúcií a request-based systém komunikácie informácií.

Mnoho distribučných a IT spoločností uvažuje o implementácií takýchto bezpečnostných systémov na teoretickej úrovni, ale v súčasnosti je len málo riešení špecializovaných na tento problém. Problematike ochrany osobných údajov a IT bezpečnosti elektrických sietí sa venovalo viacero inštitúcií. Jedna z tých, ktoré doniesli najpokrokovejšie implementácie je North American Electric Reliability Corporation's (NERC), ktorej norma Critical Infrastructure Protection (CIP) je predpisovou normou pre verejné služby v USA. NERC CIP štandardizuje riadenie kybernetických systémov, ktoré podporujú prevádzku hromadného elektrického systému. Pretože v USA veľká časť infraštruktúry na podporu SmartGrid sústavy pracuje na báze IP identifikácie, NERC CIP poskytuje štandardy a pokyny pre zisťovanie identity a riadenie kritických kybernetických systémov, čím uľahčuje situáciu manažmentu bezpečnosti systému, tak fyzickej a kybernetickej.

K manažmentu bezpečnosti odporúčame pristúpiť obdobne a systém vytvoriť na mieru. Viac informácií je uvedené v reporte č. 4, ktorý bol venovaný ochrane citlivých údajov, anonymizácii a automatizácii bezpečnostných procesov.

3. Manažment veľkosti objemu dát, ktorý majú právo držať jednotlivé inštitúcie

V súčasnosti, väčšina inštitúcií berúcich dáta z prenosovej siete (za rôznymi účelmi) ukladá tieto dáta i historické dáta interne. Držať celý objem dát nemusí byť praktické a zároveň, takéto narábanie s dátami radikálne zvyšuje šancu zneužitia či už citlivých údajov o výkone siete, alebo osobných údajov, ktoré sú generované nástrojmi v SmartGrid. V kontexte nastavenia stratégie manažmentu dát, musia inštitúcie definovať aké zdroje dát a analýzy potrebujú. Zároveň, je veľmi dôležité, aby nebolo identifikované len množstvo a kvalita dát, ktoré potrebujú na výkon svojej činnosti, ale aj presný časový úsek, na ktorý tieto dáta potrebujú. Nemá zmysel držať dáta len pre istotu, špeciálne, ak takáto archivácia znižuje bezpečnosť systému. Každý dátový sklad musí mať zásady, ktoré umožnia historické a neužitočné dáta odstrániť. Či už tento systém bude fungovať prostredníctvom zdieľaných databáz, archivácie alebo inou metódou, manažment životného cyklu dát je kritickou premennou.

4. Tri alternatívy strategického manažmentu dát v kontexte SmartGrid

Návrh stratégie manažmentu zberu, ukladania, analýzy, komunikácie a bezpečnosti dát bude od inštitúcií vyžadovať, aby vypracovali vlastný plán alebo sa integrovali do spoločného plánu, ktorý maximálne využíva nové analytické a komunikačné možnosti SmartGrid-u, a zároveň čo najefektívnejšie znižuje s transformáciou spojené náklady a riziká. Nižšie uvádzame tri alternatívne prístupy k manažmentu dát v SmartGrid.

5. Operátor distribučných systémov (ODS) ako facilitátor systému

Tento model je založený na vytvorení dátových hubov. Hub je štandardizovaný, centralizovaný alebo decentralizovaný bod pre interakciu so systémom, v ktorom sú k dispozícii všetky prevádzkové údaje a údaje potrebné na komunikáciu so systémom, jeho subsystémami alebo užívateľmi (štátne a súkromné inštitúcie, právnické a fyzické osoby). ODS poskytujú tieto dáta užívateľom prostredníctvom dátových hubov, nediskriminujúcim spôsobom, ako regulovaní facilitátori trhu. Je na užívateľoch, aby ich dáta obohatili ďalšími informáciami (napr. o cenové signály, tarify, predikcie). Táto spätná väzba im umožní vytvárať nové typy služieb. Z dôvodov zabezpečenia dát a ochrany súkromia, koncoví zákazníci budú majiteľmi ich osobných údajov (viď report č. 4 o ochrane osobných údajov pre informáciu čo je a čo nie je osobný údaj užívateľa). Komunikácia takýchto dát tretím stranám musí byť schválená.

V tomto modele manažmentu sú ODS vnímaní ako operátori technickej infraštruktúry, vrátane fungovania hubov a tvorby nových služieb. Sú zodpovední za spoľahlivosť prevádzky informačnej sústavy a pôsobia ako neutrálni sprostredkovatelia informácií v systéme medzi nástrojmi generujúcimi dáta a užívateľmi. ODS by mali mať prostriedky a možnosti, plánovať a manažovať zmeny v SmartGrid a tým prinášať inováciu. Taktiež kontrolujú riziká v sústave. ODS spolupracujú so všetkými ostatnými účastníkmi trhu. Je možné, aby slúžili ako informačný kanál smerom od prevádzkovateľov prenosových sústav k výrobe a spotrebe, pripojenej ich sieti. Nastavenie tejto stratégie sa líši podľa toho, či uprednostníme facilitáciu prostredníctvom decentralizovaných dátových hubov, alebo existenciu centrálneho dátového hubu.

Táto stratégia manažmentu dát umožňuje ODS poskytovať platformu, na ktorej zainteresované strany v SmartGrid môžu stavať inovačné služby, zdokonaľovať pridanú hodnotu SmadGrid. Popísaný model ponúka jasnú štruktúru vlastníctva dát a kontroly procesov a zodpovedností prevádzkovateľov a užívateľov. Model je v súlade s moderným prístupom ku kybernetickej bezpečnosti, ktorú moderuje na základe distribúcie ukladaných dát cez huby a kontrolované sprostredkovanie informácií. Takéto nastavenie integruje čiastkové procesy a informačné toky, aktuálne spravované inštitúciami, ktoré dnes nekomunikujú. Optimalizácia procesov a komunikácie má potenciál ušetriť značné zdroje. Manažment SmartGridu pomocou ODS facilitátorov má značné výhody pre užívateľov. Súhrnné údaje vyžiadané užívateľom sú centralizovane a/alebo decentralizovane uložené. To umožňuje verifikáciu a validáciu bezpečnosti zákazníckych dát v regulovanom prostredí.

Z pohľadu obchodu, je výhodou neutralita spracovania a distribúcie dát, ktorú zaručuje ODS. Sú tak zabezpečené štandardizované procesy prístupu k informáciám, čo podporuje hospodársku súťaž. Model zabezpečuje transparentnosť a jasnú distribúciu zodpovednosti v sprostredkovaní dát verejnému a súkromnému sektoru. ODS budú ako facilitátori sytému neustále k dispozícii, a budú disponovať potrebnými informáciami pre užívateľov systému. Údaje pochádzajúce z aktivít ODS (napr. zmien a aktualizácií systému manažmentu dát) sú priamo kontrolované a komunikované, preto ODS môžu plniť aj pomocnú informatívnu úlohu. Ide o nákladovo dlhodobo efektívny prístup.

Nevýhodou je, že si táto stratégia vyžaduje značné zmeny v regulácii, v súčasných kontrolných mechanizmoch a má veľké prvotné implementačné náklady. Pre jej zavedenie by bolo potrebné nadizajnovať a nasadiť sériu nových analytických a bezpečnostných subsystémov, exekučných procesov a priniesť nové rozhranie pre komunikáciu. Je treba poznamenať, že trend výmeny informácií prostredníctvom hubov už možno pozorovať aj v rámci krajín EÚ. Krajiny ako Holandsko, Belgicko takýmito (de)centralizovanými hubmi disponujú. Iné sa rozhodli vytvoriť huby len pre niektoré procesy. Napríklad, Portugalsko má centralizovaný hub pre zber dát potrebných na estimáciu odchýlky a jej komunikáciu.

6. Tretia strana ako facilitátor systému – nezávislý centrálny dátový hub.

Druhá alternatívna na realizovateľnú stratégiu manažmentu dát v SmartGrid pozostáva z nezávislej komunikačnej platformy riadenej jedným hubom. Táto centrála bude mať za úlohu realizovať tri základné funkcie: spolupráca so zainteresovanými užívateľmi SmartGrid, zber a ukladanie dát a ich spracovanie. Hlavné aktivity centrály preto budú: manažment prijímania čerstvých dát a ich štandardizácia (agregácia), manažment historických dát a odovzdávanie kustomizovaných informácií konečným spotrebiteľom alebo ich povereným zástupcom (predajcovia elektriny, spoločnosti poskytujúce energetické služby a.i.). Fakt, že tretia strana, je ako riadiaci orgán komunikačnej platformy nezávislá, umožní neutrálnu facilitáciu systému smerom k všetkým zúčastneným stranám.

Nezávislá komunikačná platforma zaistí, že iba autorizované a oprávnené strany budú schopné prijímať a odosielať dáta do centrálneho systému. Centrála je regulovaným agentom, ktorej kontrolórom (nie riadiacim orgánom) by mala byť vládna agentúra alebo inštitúcia. Jej povinnosti a práva musia byť jasne zadefinované. Mali by medzi ne patriť: zodpovednosť za manažment procesov pri zmene dodávateľa, komerčná a nekomerčná distribúcia informácií užívateľom systému (tretím stranám), zhromažďovanie dát, optimalizácia distribúcie dát a komunikácie informácií medzi zainteresovanými článkami systému (eliminácia redundantných výmen dát medzi subjektmi). Centrálny hub bude dáta spracovávať do agregátov s informačnou hodnotou a synchronizovať potreby užívateľov systému s možnosťami zberu a analýzy dát. Centrálny hub facilitujúci systém ako tretia strana nevystupuje ako poskytovateľ meteringových služieb. Za zber dát, ich kvalitu a časovú prístupnosť by mal v tomto prípade byť zodpovedný ich dodávateľ alebo administrátori distribučných sietí.

Táto stratégia predstavuje odľahčenú verziu prvej alternatívy a prináša viaceré výhody pre zainteresované strany systému. Prvou je nezávislosť tretej strany, čím je možné vyhnúť sa korupčnému správaniu (napr. preferencia užívateľov pri komunikácii informácií). Druhou sú relatívne nízke časové, finančné a technické náklady na nasadenie platformy na SmartGrid. Treťou, je potenciál ušetriť značné náklady pomocou centralizácie systému a optimalizácie komunikácie (transferu) informácií a dát medzi užívateľmi systému. Táto stratégia podporuje komunikáciu a zefektívňuje potenciálnu spoluprácu zúčastnených strán, pričom ich aktivity dokáže regulovať prostredníctvom otvárania a zatvárania komunikačných kanálov.

Napríklad nový dodávateľ by musel nadviazať komunikáciu s Centrálnym hubom a preukázať vôľu konečných užívateľov zmeniť svojho pôvodného dodávateľa v jeho prospech. Po splnení podmienok, by Centrálny hub komunikoval prítomnosť nového dodávateľa relevantným stranám, zastavil by odosielanie dát o danom koncovom užívateľovi (zákazníkovi) pôvodnému dodávateľovi a začal ich sprostredkovávať vo vyžiadanej podobe novému dodávateľovi, ktorého si koncový užívateľ (zákazník) zvolil. Koncovému zákazníkovi to umožní byť agilnejší vo výbere služieb, čo zvýši konkurenčný boj a tým kvalitu služieb, čím sa celý systém zefektívni. Obdobne by sa platforma správala aj pri dodávateľoch riešení pre

subsystémy dátovej bezpečnosti alebo predikčných modelov estimácie odchýlky. Takýto prístup k manažmentu systému zberu a dátovej analýzy má potenciál priniesť dobré výsledky v posilnení postavenia koncových spotrebiteľov. Dodávatelia a inštitúcie ako užívatelia systému budú motivovaní zefektívniť svoje procesy, cez reakciu na dopyt. Centrála má pritom primárnu rolu poskytovateľa neutrálneho a efektívneho prístupu k informáciám.

Medzi európske krajiny využívajúce túto stratégiu manažmentu dát v energetike patrí Veľká Británia, Dánsko, Poľsko, Taliansko a najnovšie aj Estónsko. Vo svete je to hlavne Austrália, Ekvádor a štát Texas, USA. Írsko je príkladom krajiny, ktorá kombinuje túto stratégiu s prvou popísanou tak, že disponuje samostatnou komunikačnou platformou a ODS hubmi pre zber a analýzu dát po vzore prvej alternatívy.

7. Správcovia brán dôveryhodného prístupu k dátam ako facilitátori systému

Tretí efektívny prístup k manažmentu dátových štruktúr v SmartGrid vychádza z vytvorenia bezpečných dátových brán do zdieľaných databáz. Tieto brány by mali byť manažované špecializovanými oddeleniami certifikovaných spoločností, ktoré budú vystupovať ako operátori-správcovia bezpečného prístupu k relevantným dátam. Svoje služby budú poskytovať všetkým autorizovaným účastníkom a zainteresovaným stranám. Sieť správcov a brán bezpečného prístupu bude navrhnutá tak, aby zlepšila aktuálne existujúce štruktúry systému, role a zodpovednosti sa im budú meniť postupne, s implementáciou nových subsystémov v SmartGrid. Správca má za úlohu manažovať prístup k dátam a vzdialený prístup k funkciám (napr. analytickým, vizualizačným a bezpečnostným), ktoré umožňujú tvorbu výstupov z dát zbieraných v SmartGrid (dáta zo SmartMetrov, meteorológia, socio-demografia, dáta o trhu a obchode atď.). Správca dátovej brány má za úlohu dlhodobo spravovať prístupové práva regulovaných a neregulovaných užívateľov systému (na úrovni poskytovateľov služieb aj koncových spotrebiteľov) a vykonávať akcie smerom k nim v kontexte ich požiadaviek a im udelených práv prístupu k informáciám. Na to, aby správcovia mohli agilne komunikovať, je potrebné vytvoriť na pozadí vhodný automatický, inteligentný, seba optimalizujúci systém pre spracovanie informácií zo širokej škály nových a existujúcich zariadení pripojených do SmartGrid. Tento systém by mal správcovi brány prístupu k informáciám uľahčiť jeho aktivitu predspracovaním dát do podoby, z ktorej žiadateľ dát vie vychádzať, alebo pre neho majú rovno informačnú hodnotu (nemusia sa posielať dáta ale informujúce deskriptívne reporty). Systém postavený na dátových bránach a ich certifikovaných správcoch vytvára veľkú flexibilitu, pokiaľ ide o prístup a spracovanie dát. Sympatické je, že pri svojej implementácii umožňuje zachovať pôvodné úlohy a zodpovednosti štátnych a polo-štátnych inštitúcií. V súčasnom systéme vyžaduje len minimálne zmeny v aktuálnej štruktúre.

Tento model, poskytuje spravodlivý, agilný, bezpečný a regulovateľný prístup k dátam a analytickým funkciám na všetkých úrovniach služieb a komunikácie medzi aktérmi v systéme a spotrebiteľmi. Certifikovaní správcovia majú za úlohu poskytovať služby autorizovaným užívateľom. Konajú v konkurenčnom prostredí. Systém zaisťuje bezpečnosť

spotrebiteľov a práva občanov na ochranu súkromia a investícií už svojou štruktúrou – autorizovaným prístupom, priznávanou úrovňou regulácie prístupu k dátam a certifikáciou správcov. Predpokladáme, že takýto prístup uľahčí integráciu nových zariadení, procesov a funkcií do SmartGrid. Umožňuje postupne inovovať technológie a služby. Ak využijeme túto stratégiu manažmentu dát v SmartGrid, nebude nutné vytvárať nové regulačné štruktúry zakaždým, keď bude do SmartGrid nutné implementovať nový nástroj alebo proces (napr. nový obchodný zámer). Tento systém, je vo svojej podstate distribuovaný a preto nevytvára monopol sprostredkovateľa dát, informácií a služieb (v porovnaní s Centralizovaným hubom ktorého operátor je ODS v prvom prípade). Správca nedisponuje dátami a neuchováva ich, manažuje len prístup k nim. Táto stratégia si vyžaduje striktnejší prístup k systémom dátovej bezpečnosti, nakoľko decentralizácia dátových brán zvyšuje riziko kybernetického útoku. Certifikovaní správcovia brán musia spolu aktívne komunikovať.

Spotrebitelia by mohli ťažiť z faktu, že majú slobodu voľby pri zúčastnení sa na interakcii so systémom na strane dopytu. V dlhodobom horizonte, systém brán a ich správcov by mohol uľahčiť procesy ako zmenu dodávateľov či integráciu nových bezpečnostných služieb a inteligentných aplikácií pre dodávateľov do SmartGrid. Predpokladom pre efektívne zavedenie tejto stratégie manažmentu je vytvorenie štandardného postupu a pravidiel získania prístupu k dátam, teda zadefinovanie podmienok, ktoré užívateľ musí splniť, informačných úrovní, ku ktorým môže dostať prístup a mechanizmov regulácie prístupu zainteresovaných strán k dátam.

Tento prístup by síce mohol uľahčiť proces premeny aktuálnej siete na inteligentný, reaktívny, systém, ale vyžadoval by si rozsiahle legislatívne zmeny a zavedenie nových postupov pri výmene dát v energetike s čím sú spojené aj zvýšené náklady pre účastníkov trhu s elektrinou. Prvky systému správcov a brán sú už v prevádzke napríklad vo Veľkej Británii a Nemecku. Rada štátov takýto systém vyvíja (alebo aspoň jeho časti). Systémy tohto typu sú využívané v manažmente telekomunikačných dátových systémov.

8. Záver

Našim cieľom v tomto reporte bolo urobiť prehľad prístupov k manažmentu dát a distribúcie dát v SmartGrid. V našich návrhoch sme zohľadňovali súčasný stav zberu dát a požiadavky subsystémov (bezpečnostného, analytického, vizualizačné a systémov zberu dát) potrebných pre efektívne fungovanie SmartGrid. Veľkou premennou bola aj potreba aktívnej a pasívnej komunikácie zainteresovaných strán, či existencia spätnej dátovej väzby, dôležitej pre auto-korektívne a auto-optimalizačné procesy subsystémov v SmartGrid. Popísali sme tri možné prístupy k manažmentu dát v SmartGrid aj s príkladmi krajín, v ktorých sú implementované. Prístup prostredníctvom nezávislého centrálneho hubu sa z pohľadu súčasného legislatívneho prostredia a zaužívaných postupov pri výmene dát javí ako najvhodnejší v kontexte Slovenskej Republiky. Záverom by sme chceli upozorniť, že vhodnosť prístupov k manažmentu dát a ich aplikácie do značnej miery závisí aj na rozpočte, ktorým budú SmartGrid projekty v budúcnosti disponovať.