VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2021 Ivana Fitere

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

BEZPEČNOST CHYTRÝCH ELEKTROMĚRŮ
SMART METER SECURITY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
Ivana Fitere

VEDOUCÍ PRÁCE
SUPERVISOR
doc. Ing. Petr Mlýnek, Ph.D.

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Ivana Fitere ***ID:*** 211785
Ročník: 3 ***Akademický rok:*** 2020/21

NÁZEV TÉMATU:

Bezpečnost chytrých elektroměrů

POKYNY PRO VYPRACOVÁNÍ:

Prostudujte problematiku bezpečnosti chytrých elektroměrů. Proveďte analýzu využívaných kryptografických algoritmů v oblasti Smart Metering se zaměřením na protokol DLMS a uznávané autority. Proveďte zhodnocení dopadů kybernetické bezpečnosti na provozní, ekonomické a uživatelské aspekty (negativní dopady implementace kybernetické bezpečnosti). Proveďte návrh minimálních a maximálních požadavků vzhledem k funkčnosti (provozní, ekonomické a uživatelské aspekty). Získané poznatky aplikujte do metodiky a vhodnou formou vizualizujte. Na modelovém příkladu vypočtěte CAPEX/OPEX náklady pro navržené požadavky a metodiku.

DOPORUČENÁ LITERATURA:

[1] BURDA, K. Kryptografie okolo nás. CZ.NIC. CZ.NIC. Praha: CZ.NIC, 2019. 132 s. ISBN: 978-80-88168-49-2.

[2] BURDA, K. Bezpečnost informačních systémů. Brno: VUT v Brně, 2013. s. 1-152. ISBN: 978-80-214-4890- 2.

Termín zadání: 1.2.2021 ***Termín odevzdání:*** 31.5.2021

Vedoucí práce: doc. Ing. Petr Mlýnek, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

V súčasnosti je elektronizácia, digitalizácia a prenos dát považovaná za bežnú súčasť nášho života. Práve pri prenose a spracovávaní dát je dôraz na bezpečnosť nevyhnutný. Táto bakalárska práca sa venuje problematike inteligentného merania v elektroenergetike. Základom práce sú technické, prevádzkové, bezpečnostné a ekonomické aspekty nasadzovania inteligentných elektromerov. Prvá časť sa venuje rozboru algoritmov, noriem a štandardov pre smart metering. Práca pokračuje popisom súčasného stavu inteligentného merania v Českej a Slovenskej republike. Ďalšie kapitoly sú venované vytvoreniu hodnotiaceho modelu, dvom rôznym scenárom zabezpečenia, ich rozboru a vyhodnotenia na základe čistej súčasnej hodnoty (NPV). V závere sú výsledky reálneho testu komunikácie GSM pri dvoch rôznych úrovniach zabezpečenia. V XLS prílohe sú tieto modely zobrazené vo forme výpočtov a tabuliek.

KĽÚČOVÉ SLOVÁ

DLMS/COSEM, Low Level Security (LLS), High Level Security (HLS), Elektromer, Bezpečnosť, Key Management System (KMS), GSM, PLC, Vyhláška, Norma, Náklady, Prínosy, CAPEX, OPEX, Čistá súčasná hodnota (NPV), Analýza nákladov a výnosov (CBA)

ABSTRACT

Nowadays, electronization, digitization and data transmission are considered as a standard part of our lives. Security is especially important during data transfer and data processing. This bachelor thesis deals with intelligent metering in power engineering. The work is based on technical, operational, safety and economic aspects of smart meters rollout. The first part deals with the analysis of algorithms, norms and standards for smart metering. The work continues with a description of the current state of smart metering in the Czech and Slovak Republics. The next chapters are devoted to the creation of an evaluation model, two different security scenarios, their analysis and evaluation based on net present value (NPV). Finally, the results of a real test of GSM communication at two different security levels. Models are displayed in the attached XLS file.

KEYWORDS

DLMS/COSEM, Low Level Security (LLS), High Level Security (HLS), Electrometer, Security, Key Management System (KMS), GSM, PLC, Regulation, Norm, Costs, Benefits, CAPEX, OPEX, Net Present Value (NPV), Cost Benefit Analysis (CBA)

FITERE, Ivana. *Bezpečnost chytrých elektroměrů*. Brno, 2021, 58 s. Bakalárska práca. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedúci práce: doc. Ing. Petr Mlýnek, Ph.D.

VYHLÁSENIE

Vyhlasujem, že svoju bakalársku prácu na tému „Bezpečnost chytrých elektroměrů“ som vypracovala samostatne pod vedením vedúceho bakalárskej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autora uvedenej bakalárskej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto bakalárskej práce som neporušila autorské práva tretích osôb, najmä som nezasiahla nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomá následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autorky

POĎAKOVANIE

Rada by som sa touto formou poďakovala môjmu vedúcemu bakalárskej práce pánovi doc. Ing. Petrovi Mlýnkovi, Ph.D. za odbornú pomoc, trpezlivosť a rady. Veľká vďaka patrí taktiež zamestnancom spoločnosti Východoslovenská distribučná, a.s. hlavne pánovi Ing. Jozefovi Dudiakovi, Ph.D. a pánovi Ing. Marcelovi Fitere za ich spoluprácu, podporu a rady z praxe.

Obsah

Zoznam obrázkov

Zoznam tabuliek

Úvod

Elektronizácia, digitalizácia a online informácie sa stávajú prirodzenou súčasťou nášho života. Pri platbe kartou v obchode máme okamžitú informáciu o pohybe na našom bankovom účte cez SMS alebo notifikáciu. Pri rozhovore alebo posielaní SMS cez mobilný telefón dochádza k online registrácii našej spotreby a kreditu. Ľudia prirodzene očakávajú podobné online informácie týkajúce sa viac či menej dôležitých činností alebo výdavkov pri spotrebe bežných komodít alebo služieb. Zoberme si napríklad spotrebu vody, tepla, plynu alebo elektriny ako hlavných komodít v bežnom živote. V tomto svete však dosiahnuť online prístup k informáciám nie je technologicky jednoduché. Jednou z najväčších výziev pri online meraní týchto komodít je samotný prenos informácií v mieste kde vznikajú (elektromer, plynomer, vodomer) do miesta, kde sa môžu hromadne spracovať a byť poskytnuté zákazníkovi. Pri samotnom prenose informácii cez súčasne dostupné komunikačné technológie sa stretávame či už s limitami daných technológií, finančnými aspektami a v neposlednom rade požiadavkami na bezpečný prenos údajov. Pri prenose údajov a hlavne bezpečnom prenose údajov je treba preskúmať celú cestu medzi poskytovateľom údajov a zákazníkom. Pri tomto prenose môže dôjsť k narušeniu komunikačnej cesty neoprávneným zásahom, odcudzeniu dát alebo narušenie integrity dát a tým aj k škodám spôsobeným či už zákazníkovi alebo poskytovateľovi služby. Preto je oblasť kybernetickej bezpečnosti v tomto odvetví kľúčová. Táto bakalárska práca sa vo svojich piatich kapitolách venuje problematike inteligentného merania v elektroenergetike.

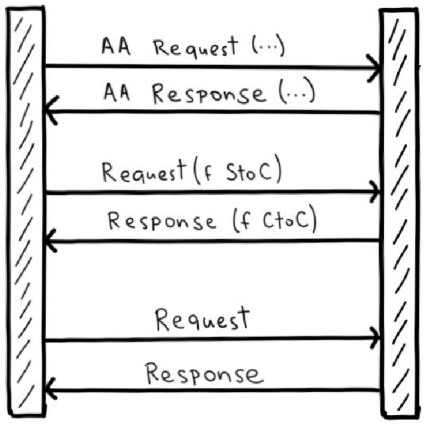
1 Analýza využívaných kryprografických algoritmov v oblasti Smart Metering

Protokol DLMS/COSEM využíva OSI model na modelovanie prenosu informácií medzi dvoma stanicami, v našom prípade medzi elektromerom a zberačom dát. OSI model je založený na koncepte rozdelenia komunikačného systému na 7 abstraktných vrstiev, ktoré sú na sebe uložené. Na úspešné fungovanie tohto systému je nutné jednoznačne identifikovať objekty, ktoré sa v ňom pohybujú.

1.1 Bezpečnosť protokolu DLMS/COSEM

Protokol DLMS/COSEM je postavený na vytváraní spojenia medzi klientom a serverom s obojstrannou autentizáciou. Komunikácia pomocou dátových jednotiek môže byť chránená rôznymi kryptografickými algoritmami a identifikačnými metódami. Správna identifikácia umožňuje serveru znamenite rozlišovať odlišných klientov, ale aj účastníkov tretích strán napríklad operátorov a logovať ich aktivity. Obrázok 1.1 zobrazuje priebeh spojenia. Toto spojenie sa skladá z následujúcich štyroch fáz [2].

1. Prvým krokom je **Application Association (AA)**, proces, v ktorom dochádza k vytvoreniu spojenia medzi klientom a serverom pomocou jednoduchého bezpečnostného konceptu vzájomnej autentizácie 1.1.2.
2. Medzi klientom a serverom sa vymenia a spracujú challenge ($f\,StoC$ a $f\,CtoC$).
3. V prípade úspešného procesu prebehne **výmena správ**.
4. Posledným krokom je **zrušenie AA** a **ukončenie spojenia**.

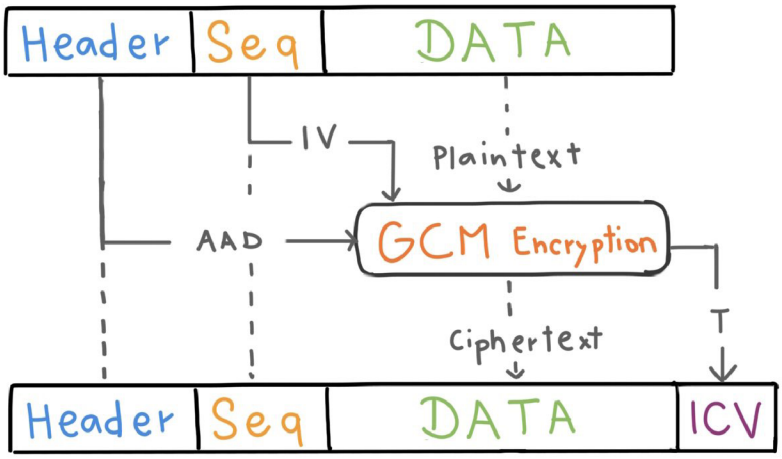


Obr. 1.1: Zostavenie spojenia [2].

1.1.1 Forma zabezpečenia

O šifrovanie datových rámcov sa v protokole DLMS/COSEM stará algoritmus AES-GCM. AES (Advanced Encryption Standard) s režimom Galois/Counter Mode (AES-GCM) poskytuje autentizované šifrovanie čiže dôvernosť i autentizáciu a schopnosť skontrolovať integritu a overenie ďalších údajov (AAD), ktoré sa odosielajú v čistom formáte. Tento algoritmus má 4 hlavné vstupy [2]:

- **tajný kľúč EK** (Encryption Key),
- **inicializačný vektor IV** (Initialization Vector),
- **dáta** vo forme **plaintextu**,
- **dodatočné dáta na autentizáciu ADD** (Additional Authenticated Data), ktoré obsahujú informácie o forme zabezpečenia.



Obr. 1.2: Schéma zabezpečenia dát [4].

Na obrázku 1.2 je vo všeobecnosti znázornená schéma prechodu dát do šifrovanej podoby. Dáta sú vo forme plaintextu spracované algoritmom AES-GCM, do ktorého sú pridané dáta **ADD**, zahrňujúce dodatočné informácie a inicializačný vektor **IV**, obsahujúci nonce a *encryption key*.

Protokol DLMS/COSEM ma niekoľko požiadaviek na zaistenie bezpečnosti. Tie sú autentizácia komunikujúcich partnerov, kontrola prístupových práv v závislosti od roly klienta, komplexná bezpečnosť medzi treťou stranou a serverom, ochrana údajov COSEM a správ xDLMS. Bezpečnosť sa dá rozdeliť na prístupovú a transportnú bezpečnosť.

1.1.2 Prístupová bezpečnosť

Prístupová bezpečnosť je implementovaná pomocou *Association Request* a *Association Response*. Klient aj server sú identifikované adresou a vyjednávajú medzi sebou

kontext autentizácie. *Member Mechanism Name* špecifikuje úroveň zabezpečenia, ktorý klient použije na prístup k serveru. Úrovne zabezpečenia môžu byť:

Lowest Level Security

"Žiadna bezpečnosť". Tento režim neposkytuje žiadne zabezpečenie a neobsahuje potrebné parametre.

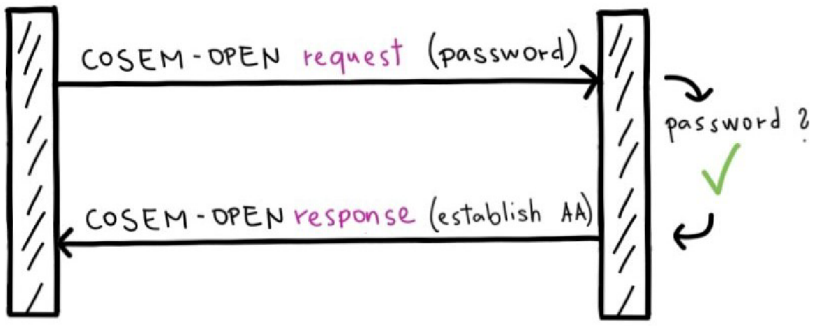
Low Level Security

Zriadenie spojenia pomocou správy *Association Request* je možné autentizovať zvolením identifikátoru objektu OID(Object Identifier) a jeho *Authentication-mechanism Name*. V ďalšom kroku je klientom zaslaný bitový string známy ako *ACSE User Requirement* za účelom vytvorenia autentizovanej relácie. Prvý bit poľa *ACSE User Requirement* označuje požiadavku k autentizácii. Pole *Authenticaton Value* bude verifikované odpovedajúcim autentizačným mechanizmom pokiaľ má prvý prvý bit hodnotu 1. Ak je hodnota *Authentication Value* správna, spojenie je nadviazané. V opačnom prípade je spojenie odmietnuté [2].

LSS umožňuje klientovi prístup na server overením prostého hesla bez šifrovania, ktoré server pozná. Ak je klientovo heslo úspešne prijaté a overené serverom, vytvorí sa spojenie.

K výhodám LLS patrí jej široké používanie v oblasti rôznych zariadení a systémov a taktiež rýchlejšia komunikácia kvôli absencii kryptografických algoritmov. Na druhej strane je však kvôli neprítomnosti šifrovania obyčajné nechránené heslo ľahko upraviteľné použitím jednoduchého man-in-the-middle attacku.
Spojenie LLS sa skladá z týchto krokov zobrazených na obrázku 1.3:

1. Na začiatku spojenia si klient a server vymenia informácie o začiatku a spôsobe komunikácie
2. Klient serveru odošle heslo a dodatočné dáta (identifikátor klienta, identifikátor servera, kontext spojenia, ...).
3. Server si overí, či je heslo správne.
4. Ak je heslo správne, spojenie môže byť zriadené, od tohto momentu sú všetky vyjednané kontexty platné.
5. Ak je heslo nesprávne, spojenie bude odopreté.



Obr. 1.3: Popis úspešnej komunikácie LLS [2].

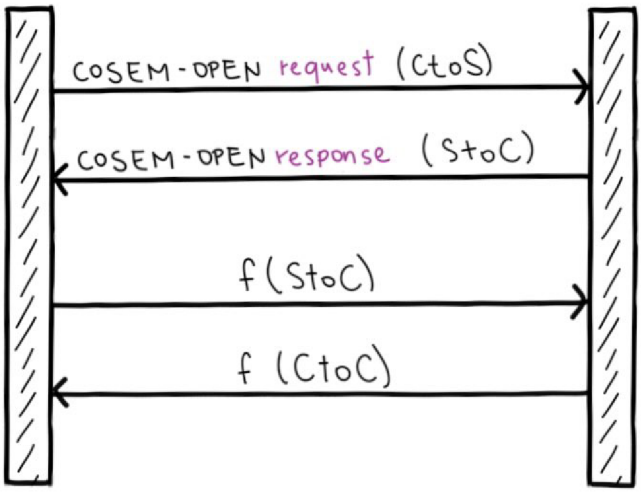
High Level Security

Štruktúra správy *ACSE* sa oproti tej predošlej líši v odpovedi servera pomocou poľa *Authentication Value*, kde namiesto odpovede s výberom autentizácie server odpovedá vyplneným poľom s jednorázovo vygenerovanou hodnotou určenou pre klienta. Po dokončení tohto procesu je serverom pozmenená komunikácia do stavu čiastočnej autentizácie, kde sa zasielané správy *Action Request* a *Action Response* zasielajú s hodnotami odpovedajúcimi výpočtom v závislosti na vybranej autentizačnej metóde. Po úspešnom ukončení preukazovania identity u klienta pomocou *Action Request* serveru a u servera pomocou *Action Response* klientovi, je spojenie povýšené do stavu plno autentizovaného. Štruktúra spojenia má teda tieto kroky podľa *Green Book* [2], znázornené na obrázku 1.4:

1. Klient pošle výzvu *CtoS* a dodatočné dáta (identifikátor klienta, identifikátor servera, kontext spojenia, ...)
2. Server odpovedá na výzvu odpoveďou *StoC* a dodatočné dáta podľa autentifikačného mechanizmu (identifikátor klienta, identifikátor servera, kontext spojenia, ...).
3. V ďalšom kroku klient spracuje *f StoC* v danom autentifikačnom móde a odošle správu serveru.
4. Server skontroluje klientovu odpoveď (*f StoC*) a pri správnom výsledku akceptuje jeho autentifikáciu a odošle *f CtoS* klientovi.
5. Klient skontroluje prijatú správu (*f CtoS*) a pri správnom výsledku autentifikuje server.

Pri používaní HLS sa medzi klientom a serverom vymenia práve štyri správy. Heslo, použité v tejto forme komunikácie už nie je prenášané v jeho prostej podobe. Heslo je zahashované algoritmom ako SHA (Secure Hash Algorithm) alebo RIMPED ako aj osolené na dosiahnutie najvyššej možnej formy bezpečnosti. K výhodám HLS patrí najmä jeho vysoká forma bezpečnosti. K nevýhodám ale možno zaradiť fakt,

že klient je počas komunikácie so serverom verifikovaný iba raz a to na začiatku spojenia.



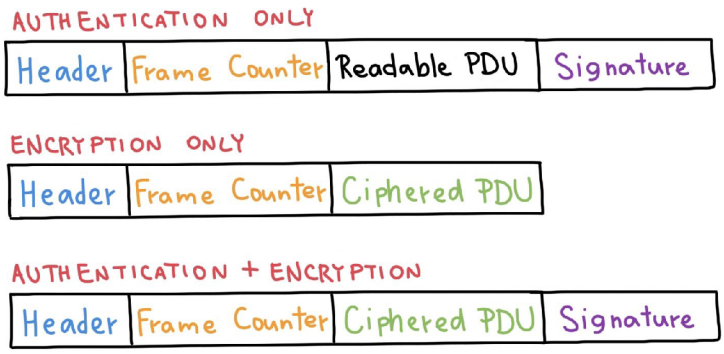
Obr. 1.4: Popis komunikácie HLS [2].

1.1.3 Transportná bezpečnosť

Bezpečnosť dát prenášaných protokolom DLMS je definovaná a zaistená úrovňami *Security suite*. Na zabezpečenie inteligentného elektromera je potrebné zvažovať skutočnosti, ktoré tento *Security suite* udáva, ako vzájomné overenie zariadení, šifrovanie a autentifikácia správ alebo vytvorenie bezpečného dátového komunikačného kanálu. Stupne od 0 do 2 sa líšia aplikovaním odlišných spôsobov zabezpečenia, ako je vidieť v tabuľke 1.1. Úroveň zabezpečenia určuje, ako dobre sú údaje zabezpečené. Údaje je možné zabezpečiť tromi rôznymi spôsobmi podľa obrázku 1.5:

- **Authentication only** – iba overenie totožnosti.
- **Encryption only** – iba šifrovanie.
- **Authentication and Encryption** – kombinácia overenie aj šifrovanie.

Šifrovanie je proces používania algoritmov na presun informácii v takej forme, aby neboli čitateľné nikým iným ako vlastníkom kľúča. Bezpečná komunikácia je nutná na prenos dát medzi zariadeniami. V protokole DLMS/COSEM sa pre zaistenie bezpečnosti využíva hŕstka kľúčov. Ich využitie je definované v tabuľke 1.2.



Obr. 1.5: Rámce APDU v rôznych formách zabezpečenia.

Tab. 1.1: Tabuľka bezpečnostných úrovní Security Suite [2].

Mechanizmy	**Security Suite 0**	**Security Suite 1**	**Security Suite 2**
Šifrovanie	AES-GCM-128	AES-GCM-128	AES-GCM-256
Digitálny podpis	x	ECDSA P-256	ECDSA P-384
Ustanovenie kľúča	x	ECDH P-256	ECDH P-384
Hash	x	SHA-256	SHA-384
Prenos kľúča	AES-256 key wrap	AES-128 key wrap	AES-256 key wrap

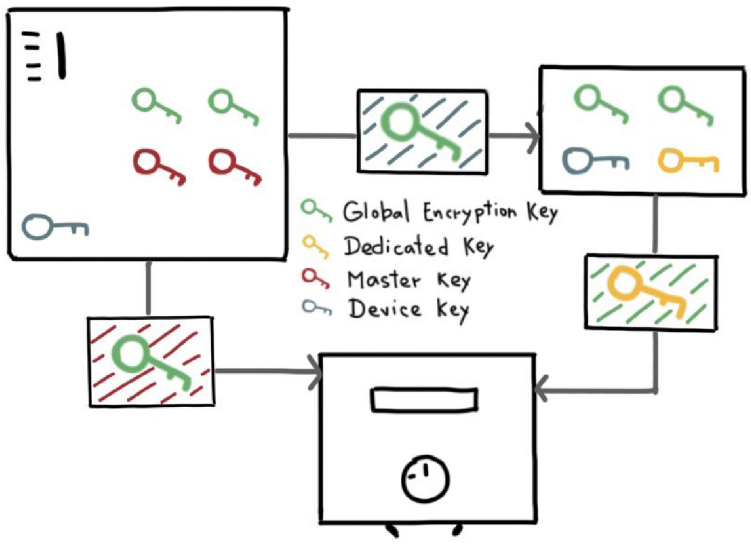
Tab. 1.2: Tabuľka kľúčov využívaných pri komunikácii [2, 4].

Typ kľúča	**Využitie kľúča**
Master Key	Kľúč identifikovaný ako hlavný Key Encryption Key pri šifrovaní správ medzi klientom a serverom, prvotne vložený do zariadenia, ktorý je využívaný aj na aktualizáciu nových kľúčov.
Ciphering Key	Kľúč AES slúžiaci na GCM šifrovanie datových jednotiek.
Authentication Key	Tento kľúč je súčasťou skupiny elementov ADD ktoré sú dôležité pre GCM šifrovanie a v jeho procese je použitý na vytvorenie autentizačného tagu.
Global Unicast Encryption Key	Blokovo šifrovaný kľúč využívaný pre unicast xDLMS APDU alebo COSEM dáta.
Global Broadcast Encryption Key	Kľúč sa používa pre broadcast, kde jeden *Request* je právoplatný pre viac zariadení.
Global Authentication Key	Kľúč sa využíva na autentifikáciu oboch strán, Device Driver aj elektromer.

1.2 Certificate management

Aby sme zaistili zabezpečenie DLMS/COSEM, ktoré boli popísané v predchádzajúcej kapitole musíme definovať autentizačnú schému. Všeobecná schéma môže byť definovaná nasledujúcimi krokmi podľa [2, 4]:

1. V prvom kroku sa použitím bezpečnej správy vygeneruje pár *master key* a *global key* (zelený a červený symbol kľúča na obrázku 1.6). Master key je kľúč, ktorý je do meradla vložený pri výrobe. V niektorých prípadoch je neskôr meniteľný prevádzkovateľom.
2. Druhý krok spočíva v zašifrovaní *global keys master* kľúčom a ich zapísaním do elektromera.
3. V treťom kroku utilita urobí kópiu informácii o kľúčoch pre prevádzkovateľa sústavy (centrálny systém), ktorý ich bezpečne riadi, spracováva a používa prostredníctvom bezpečného hardvér úložiska.
4. Centrálny systém následne bezpečne prenáša materiál s kľúčmi vhodným koncentrátorom a inicializuje spojenie s elektromerom a zároveň obnoví ich *globálne* kľúče, ktoré zašle meradlu aj koncentrátoru.



Obr. 1.6: Príklad prenosu kľúčov.

1.2.1 Key Management System

KMS označuje správu kryptografických kľúčov v kryptosystéme. Patria sem riešenia týkajúce sa generovania, výmeny, ukladania a používania kľúčov. Zahŕňa návrh kryptografického protokolu, kľúčové servery, užívateľské postupy a ďalšie príslušné

protokoly. Key Management System je nevyhnutná štruktúra, ktorá slúži na uzamykanie dôležitých informácií. Je ju možno považovať za chránený priestor, do ktorého je nežiaduce, aby vstupovali neoprávnené osoby – teda osoby bez kľúča. Na zaistenie zabezpečenia DLMS/COSEM musí existovať autentifikačná schéma založená na špecifických kľúčoch 1.2. Kľúče musia byť aktualizovateľné a schopné autentifikácie pomocou ďalších komponent a nových kľúčov, preto je použitie KMS je nevyhnutný a očakáva sa, že kľúče budú prenášané bezpečne a správne. Komunikácia medzi centrálou a elektromerom sa môže realizovať ale aj bez KMS a to pomocou prostej databázy. Bezpečnosť uložených kľúčov potom závisí práve na zabezpečení samotnej databázy, jej koreňového servera a hlavne komunikácie medzi databázou a centrálou.

1.3 Typy komunikácie s meradlami

V súčasnosti sú najrozšírenejšími typmi komunikácie s inteligentnými elektromermi technológie *GSM (Global System for Mobile Communications)* a *PLC (Power Line Communication)*. Použitie tej, ktorej technológie je dané rozsahom nasadenia elektromerov zákazníkovi (rollout). Obe tieto technológie v dnešnej dobe umožňujú implementáciu rôznych foriem zabezpečenia dátovej komunikácie.

1.3.1 Technológia GSM

Technológia GSM využívajúca komerčné dátové služby mobilných operátorov sa spravidla využíva najmä pri **selektívnej inštalácii** (selektívny rollout) meradiel. Selektívne nasadzovanie elektromerov sa volí prevažne vtedy, ak k inštalácii elektromerov nedochádza u každého zákazníka na vývode z trafostanice ale iba u vybraných zákazníkov ktorí spĺňajú kritéria výberu podľa vyhlášky 2.4. Kritériami výberu môžu byť napríklad odberné miesta s ročnou spotrebou vyššou ako 4 alebo 6 MWh (SR: 4 MWh, ČR: 6 MWh), odberné miesta nabíjačiek elektromobilov, odberné miesta s inštalovaným zdrojom elektriny a podobne.

Pri tomto druhu komunikácie je u každého elektromera osadená SIM karta (Subscriber Identification Module) daného operátora komunikujúca s centrálou cez mobilnú sieť ako je zobrazené na obrázku 1.7.

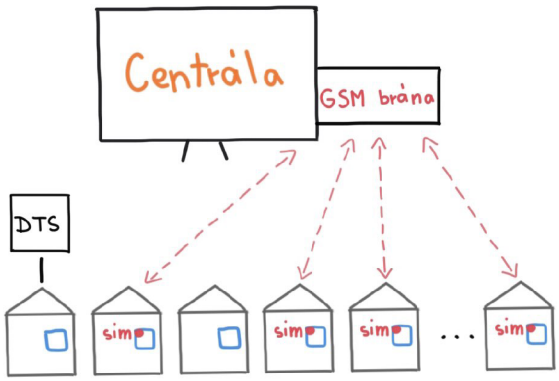
1.3.2 Technológia PLC

Technológia PLC využíva ako prenosové médium silové vodiče distribučnej sústavy. Vhodnými technológiami dokáže namodulovať, vysielať a prijímať signál, ktorý sa šíri od napájacej trafostanice po jednotlivé elektromery u zákazníkov cez distribučnú

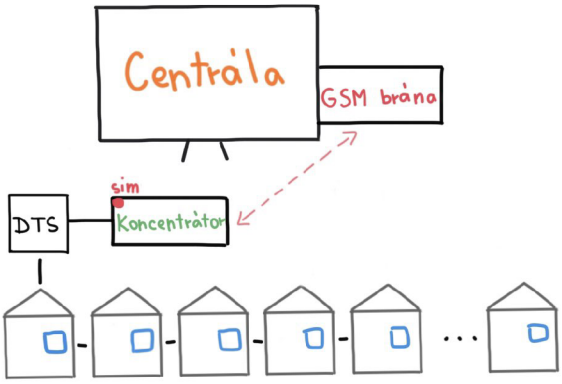
sústavu. Hlavným komunikačným a riadiacim prvkom je koncentrátor inštalovaný spravidla v distribučnej trafostanici. Tento koncentrátor komunikuje s elektromermi u zákazníkov, ktorí sú napájaní z tejto trafostanice. Táto forma komunikácie je vhodná pri **hromadnej inštalácii** (full rollout), kde sú elektromery osadené u všetkých odberných miest napájaných z danej trafostanice. Výhodou tejto formy komunikácie je jej jednoduchosť, ktorá spočíva v prostom využívaní silových vodičov ako prenosového média. Nie sú potrebné žiadne SIM karty u elektromerov. Schéma tejto komunikácie je naznačená na obrázku 1.8.

Údaje z elektromerov sú cyklicky zbierané koncentrátorom a zasielané centrále využitím rôznych iných komunikačných technológií. V prípade že je napájaná sústava geograficky rozsiahla, môžu byť jednotlivé elektromery využívané ako opakovače signálu (repeatre) z koncentrátora. Tým je zaručené, že sa signál z koncentrátora do elektromera a naopak dostane aj do najvzdialenejších miest v systéme.

V súčasnosti sú najrozšírenejšími technológiami PLC technológie G3 a PRIME.



Obr. 1.7: Znázornenie komunikácie pomocou technológie GSM.



Obr. 1.8: Znázornenie komunikácie pomocou technológie PLC.

2 Normy a štandardy pre Smart Metering

2.1 Normy NÚKIB

NÚKIB, teda Národný úrad pre kybernetickú bezpečnosť je správnym úradom, ktorý sa venuje rôznym činnostiam ochrany informácií, vydávaniu opatrení a koordinácii stavu kybernetického nebezpečenstva. Medzi mnohými publikáciami sa nachádza aj *Doporučení v oblasti kryptografických prostředků: Minimální požadavky na kryptografické algoritmy* [5]. Tento dokument sa venuje niekoľkým doporučeniam v oblasti kryptografických prostriedkov. Doporučené kryptografické požiadavky sa delia na dve skupiny. Požiadavky označené ako schválené sú také algoritmy, ktoré sa smú používať v blízkej budúcnosti. Druhá skupina nazvaná ako dostatočná obsahuje algoritmy ktoré sa do roku 2023 odporúčajú prestať používať. Tabuľka 2.1obsahuje prehľad algoritmov rozdelených do skupín podľa Národného úradu pre kybernetickú bezpečnosť.

2.2 Norma ENCS

ENCS – European Network for Cyber Security, v preklade Európska sieť pre kybernetickú bezpečnosť, je nezisková organizácia podporujúca nasadenie bezpečných európskych kritických energetických sietí a infraštruktúry. Ich cieľom je pomôcť prevádzkovateľom sietí pri stanovení požiadaviek na obstarávanie. Použitím týchto požiadaviek v procese výberového konania môžu prevádzkovatelia sietí vychádzať zo zrelej sady predpokladov. Táto rozsiahla norma sa vzťahuje na tri typy sieťovej architektúry a to sieť typu A, kde inteligentný elektromer komunikuje priamo s centrálou pomocou telekomunikačného systému WAN, sieť typu B, v ktorej elektromer komunikuje pomocou lokálnej siete s dátovým koncentrátorom, ktorý následne zozbierané informácie posiela centrále a sieť typu C, ktorá využíva na presun dát rozhranie Gateway. Z textu sú vybrané príklady technických požiadaviek [1].

- **Algoritmy**: Zariadenie by malo používať iba také bezpečnostné požiadavky, ktoré sú definované v jednotlivých reguláciách každej krajiny a nepoužívať vlastné kryptografické algoritmy.
- **Generátor náhodných čísel**: Zariadenie by malo používať algoritmy AIS20 (Apriori Algorithm), AIS 31 alebo FIPS 140-2 (Annex C) (Federal Information Processing Standard).
- **Integrita dát**: Zariadenie musí zabezpečiť integritu všetkých správ prichádzajúcich z nižších vrstiev a ak to nie je možné, správy zahodiť.
- **Validácia vstupných dát**: Zariadenia by mali prejsť viacerými penetračnými testami.

Tab. 2.1: Tabuľka noriem podľa NÚKIBu [5].

Symetrické algoritmy		
Kategória	**Schválené**	**Dostatočné**
Blokové a prúdové šifry	AES keys 128,192,256 b Twofish keys 128 až 256 b Serpent keys 128,192,256 b Camellia keys 128,192,256 b SNOW 2.0 SNOW 3G keys 128 a 256 b ChaCha20 key 256 b	3DES key 112 b Blowfish key $>$ 128 b Kasumi key 128 b
Metódy šifrovania	CCM EAX OCB1 a OCB3 GCM (nonce:69 b, tag:128 b) ChCha20 Poly1305 s kľúčom $<$ 256 GB Schémy typu *Encrypt-then-MAC*	CTR OFB CBC CFB
Metódy šifrovania diskov	XTS EME	
Metódy ochrany identity	HMAC s hašovacou funkciou EMAC CMAC UMAC (tag:64 b)	HMAC-SHA1 CBC-MAC-X9.19
Asymetrické algoritmy		
Algoritmy digitálneho podpisu	DSA key $\geq$ 3072 b EC-DSA key $\geq$ 256 b RSA-PSS key $\geq$ 3072 b EC-Schnorr key $\geq$ 256 b	DSA key 2048 b EC-DSA key 224 b RSA-PSS key 2048 b EC-Schnorr key 224 b
Algoritmy pre procesy s kľúčmi	DH key $\geq$ 3072 b ECDH key $\geq$ 256 b ECIES-KEM key $\geq$ 256 b PSEC-KEM key $\geq$ 256 b ACE-KEM key $\geq$ 256 b RSA-OAEP key $\geq$ 3072 b RSA-KEM key $\geq$ 3072 b	DH key 2048 b ECDH key 224 b ECIES-KEM key 224 b PSEC-KEM key 224 b ACE-KEM key 224 b RSA-OAEP key 2048 b RSA-KEM key 2048 b
Algoritmy hashovacích funkcií		
Funkcie SHA2, SHA3	SHA-256, SHA3-256 SHA-384, SHA3-384 SHA-512, SHA3-512 SHA-512/256, SHA3-512 SHAKE-128, SHAKE-256	SHA-224,SHA-512/224 SHA3-224 RIPEMD-160
Iné funkcie	Whirpool BLAKE2	

- **Firmware**: Zariadenie má povinnosť verifikovať digitálny podpis a odmietnuť triedy ktoré sú podozrivé z modifikácie, podpisy, ktoré sa nedajú verifikovať a taký firmware, ktorý neodpovedá súčasnej verzii.
- **Dôveryhodnosť správ**: Všetky dáta aplikačnej vrstvy musia byť šifrované.

2.3 Vyhláška č. 359/2020 Sb. o měření elektřiny

Vyhláška číslo 359/2020 vydaná dňa 13. augusta 2020 upravuje v súlade so Zákonom o energetike druhy meracích zariadení, umiestnenie meracích zariadení, spôsoby vyhodnocovania a určenia množstva odobratej elektriny. V prechodných ustanoveniach vyhláška definuje okrem iného aj termíny inštalácie inteligentných meradiel a jednotlivé typy meradiel nasledovne [7]:

Termíny

- Meradlo s priebehovým meraním, diaľkovým prenosom údajov a s komunikačným rozhraním pre poskytovanie dát zákazníkovi, ktoré bolo nainštalované do **1. júla 2024**, môže prevádzkovateľ distribučnej sústavy (PDS) ponechať po dobu platnosti jeho overenia.
- V elektrárni alebo na odbernom mieste so zdrojom s inštalovaným výkonom menším ako 10 kW, napätím menším ako 1 kV je možné do **1. júla 2027** merať aspoň typom merania B.
- Meradlo s priebehovým meraním, iným ako denným prenosom údajov, meraním typu B, ktoré bolo inštalované v elektrárni s inštalovaným výkonom menším ako 10 kW, napätím menším ako 1 kV, ktoré bolo nainštalované do **1. júla 2024**, môže PDS ponechať po dobu platnosti jeho overenia.
- Pri napätí menším ako 1 kV, s priamym meraním, s ročnou spotrebou viac ako 6 MWh je termín zavedenia inteligentného meracieho systému do **1.júla 2027**, dovtedy je možné merať typom merania C kategóriou C4.

Typy merania

- **Meranie typu A**:
  - priebehové meranie s diaľkovým denným prenosom údajov,
  - základným meracím intervalom je jedna štvrťhodina.
- **Meranie typu B**:
  - priebehové meranie s iným než denným diaľkovým prenosom údajov,
  - základným meracím intervalom je jedna štvrťhodina,
  - pokiaľ nie je možné vykonať diaľkový prenos údajov z technických dôvodov, je možné prenos údajov vykonať manuálnym spôsobom.

- **Meranie typu C**:
  - Priebehové meranie kategórie **C1**
    - s diaľkovým prenosom údajov,
    - vybavené funkcionalitou diaľkového odpojenia, pripojenia alebo obmedzovačom výkonu, technického blokovania spotrebičov a štandardizovaným komunikačným rozhraním pre poskytovanie dát zákazníkovi,
    - pokiaľ nie je možné vykonať diaľkový prenos údajov z technických dôvodov, je možné prenos údajov vykonať manuálnym spôsobom.
  - Priebehové meranie kategórie **C2**
    - s diaľkovým prenosom údajov,
    - vybavené funkcionalitou technického blokovania spotrebičov a štandardizovaným komunikačným rozhraním pre poskytovanie dát zákazníkovi,
    - pokiaľ nie je možné vykonať diaľkový prenos údajov z technických dôvodov, je možné prenos údajov vykonať manuálnym spôsobom,
    - priebežný záznam strednej hodnoty činného výkonu za merací interval vykonáva priamo meracie zariadenie.
  - Priebehové meranie kategórie **C3**
    - s diaľkovým prenosom údajov,
    - vybavené štandardizovaným komunikačným rozhraním pre poskytovanie dát zákazníkovi,
    - pokiaľ nie je možné vykonať diaľkový prenos údajov z technických dôvodov, je možné prenos údajov vykonať manuálnym spôsobom,
    - priebežný záznam strednej hodnoty činného výkonu za merací interval vykonáva priamo meracie zariadenie.
  - Meranie kategórie **C4**
    - ostatné merania, ktoré môžu byť priebehové a môže byť s diaľkovým prenosom údajov.

Minimálne požiadavky na rozhranie meradiel pre komunikáciu s nadriadenými prvkami infraštruktúry ako napríklad s centrálou alebo koncentrátorom sú zobrazené v tabuľke 2.2.

2.4 Vyhláška č. 358 Ministerstva hospodárstva Slovenskej republiky

Inteligentné elektromery sa podľa Vyhlášku č. 358 Ministerstva hospodárstva Slovenskej republiky delia na 3 skupiny podľa ich rôznych funkcionalít [6].

Tab. 2.2: Tabuľka bezpečnostných požiadavok pre meranie typu C [7].

Zaistenie dôverihodnosti a integrity	Bloková šifra GCM Bloková šifra CCM
Zaistenie dôverihodnosti	Bloková šifra AES-256
Zaistenie integrity	Digitálny podpis DSA 3072 Digitálny podpis EC-DSA-256 Digitálny podpis RSA 3072 Hash SHA2-256 Hash SHA3-256 Mód pre ochranu integrity CMAC Mód pre ochranu integrity HMAC
Management s kľúčami	DH-3072 ECDH-256
Generátor náhodných bitov	HMAC DRBG pre SHA2 a SHA3 Hash DRBG pre SHA2 a SHA3

Termíny

- Prevádzkovateľ regionálnej distribučnej sústavy musí pokryť 80 percent spotreby pomocou inteligentných meracích systémov, ktoré spĺňajú podmienky kategórií 1 až 4 (2.4) do 31. decembra 2021.

Typy merania

- **Meranie typu A**:
  - priebehové meranie s diaľkovým odpočtom.
  - **Kategória 1**
    - Koncový odberateľ elektriny kategórie 1 je taký, ktorý má ročnú spotrebu minimálne 15 MWh, maximálnu rezervovanú kapacitu minimálne 30 kW alebo 45 A.
  - **Kategória 2**
    - Koncový odberateľ elektriny kategórie 2 je taký, ktorý má ročnú spotrebu minimálne 4 MWh, maximálnu rezervovanú kapacitu minimálne 30 kW alebo 45 A.
  - **Kategória 3**
    - Koncový odberateľ elektriny kategórie 2 je taký, ktorý má ročnú spotrebu minimálne 4 MWh, maximálnu rezervovanú kapacitu maximálne 30 kW alebo 45 A.

  - **Kategória 4**
    * Koncový odberateľ elektriny kategórie 4 je taký, ktorý má zariadenie na výrobu elektriny pripojené do distribučnej sústavy.
- **Meranie typu B**:
  - priebehové meranie bez diaľkového odpočtu.
- **Meranie typu C**:
  - bez priebehového merania a bez diaľkového odpočtu.

3 Súčasný stav Smart Meteringu v Slovenskej republike

3.1 Stav na Slovensku

Odporúčania sa od roku 2013 vzťahujú na Vyhlášku č. 358 Ministerstva hospodárstva Slovenskej republiky, ktorou sa ustanovuje postup a podmienky v oblasti zavádzania a prevádzky inteligentných meracích systémov v elektroenergetike.

3.2 Prehľad elektromerov implementovaných na východnom Slovensku

Skupina elektromerov inštalovaných na východnom Slovensku sa podľa rozsahu funkcií delí na tri skupiny, a to na skupinu so základnými funkcionalitami, skupinu s pokročilými funkcionalitami a napokon skupinu špeciálnu, so špeciálnymi funkcionalitami. Tieto funkcionality možno rozdeliť do troch základných skupín podľa popisu typu komunikácie. Skupina funkcionalít zvýraznená sivou, spadá pod úlohu **čítania dát** kedy sa uskutočňuje spojenie medzi centrálou a zariadením. V prípade tohto spojenia sa u väčšiny elektromerov realizuje spojenie pomocou najvyššej bezpečnostnej úrovne, teda úrovňou HLS, pri ktorej sa využíva mechanizmus výzva-/odpoveď. V tomto procese je po dotaze centrály na klienta serveru vrátená odpoveď s jednorázovo vygenerovanou hodnotou, slúžiacou k zahashovaniu hesla. V momente úspešnej autentizácie je proces dokončený a centrála si od elektromera môže pýtať informácie. Druhou skupinou funkcionalít je skupina týkajúca sa **prijímania povelov od centrály**. Funkcionality tohto charakteru sú v tabuľke zvýraznené sivou farbou. Patria sem napríklad možnosti zmeny taríf alebo povelov vedúcim k zmene stavov v elektromeroch. Do tretej skupiny spadajú funkcionality spojené s **riadením elektromera** ako napríklad komunikácia s dispečerským systémom, registrácia odberu a dodávky elektriny vo viacerých sadzbách alebo spínanie taríf podľa aktuálnej situácie. Zabezpečenie jednotlivých skupín sa líši v ich rozdelení do jednotlivých kategórii podľa typu elektromera a jeho schopnosti zabezpečovania.

Čítanie dát

Ako je podľa názvu jasné, do tejto skupiny patrí najmä pravidelný odpočet z jednotlivých meradiel a ich diaľkový prenos. Funkcionality spadajúce do tejto skupiny sú v tabuľke 3.1 zvýraznené sivou farbou. Správne zabezpečenie prenášaných informácii

je v tejto ako aj v inej skupine mimoriadne dôležité. Pri nedostatočnej úrovni šifrovania sú informácie odkryté a vystavené útočníkom. Elektromery v tejto skupine poskytujú zabezpečenie kombináciou oboch úrovní overenia identity aj šifrovania správ (authentication and encryption) spolu s využitím úrovne *security suite*. Tento spôsob umožňuje obojstrannú autentifikáciu zahrňujúcu výmenu náhodných čísel digitálneho podpisu počas vytvorenia komunikačného kanálu. Obsah správ prichádzajúcich z oboch strán je teda zašifrovaný a podpísaný, čo znemožní útočníkovi modifikovať dáta kvôli autentizovanému podpisu a zneužitiu dát kvôli jej šifrovaniu. Niektoré elektromery staršieho typu však do týchto ideálnych pomerov nespadajú a využívajú zabezpečenie iba s autentifikáciou (authentication only) a použitím *security suite*. Toto zariadenie dokáže teda overiť totožnosť strán a zasielať správy s digitálnym podpisom, vďaka ktorým je modifikácia neoprávneného užívateľa znemožnená no útočník ma prístup k otvoreným zaslaným hodnotám.

Ideálnym prípadom zabezpečenia prenášaných dát je použitie vhodných zabezpečovacích funkcií v kombinácii s autentizáciou aj zašifrovaním dát. Šifrovanie blokovou šifrou AES-GCM-128 s použitím vhodného digitálneho podpisu EC-DSA s kvalitným kľúčom väčším ako 256 b či iných algoritmov ako DSA alebo RSA. V algoritme operácií AES-GCM-128 sú postupne číslované bloky kombinované s inicializačným vektorom (IV), pri ktorom je nevyhnutná jeho jedinečnosť pri každom prúde a šifrované blokovou šifrou E, zvyčajne AES. Výsledok tohto šifrovania sa potom XORuje s plaintextom, aby sa vytvoril šifrový text. V prípade hashovacích funkcií by sa mal využívať minimálne štandard SHA-256.

Povelovanie a riadenie elektromera

Táto skupina funkcionalít sa týka prijímania povelov od centrály v kontexte synchronizácie času, zmeny sadzieb ale aj možnosti diaľkového odpojenia. Niektoré z týchto funkcionalít majú vysokú bezpečnostnú hodnotu a jej zneužitie by mohlo spôsobiť škody a finančné straty. Dôkladné zabezpečenie je v tomto prípade kľúčové. Všetky zariadenia teda fungujú v móde autentizácie a šifrovania (authentication and encryption) s použitím *security suite*, ktorou je docielené náležité bezpečnostné minimum, do ktorého útočník zasiahnuť nevie.

Správne zabezpečenie je v tomto prípade zaistené, kryptografické metódy *security suite* by mali zodpovedať minimálne úrovni *Security Suite 1*, ktorá je definovaná v tabuľke 1.1.

3.3 Rozdelenie kategórií podľa ich funkcionalít

1. Funkcionalita s názvom *Obojsmerná komunikácia medzi OM a centrálou IMS*: Takáto dátová komunikácia počíta s obojsmerným tokom dát – k spotrebiteľovi aj od spotrebiteľa.
2. Funkcionalita s názvom *Monitoring OM lokálnym pripojením k IMS*: Sprístupnenie údajov aj zákazníkovi priamo z elektromera.
3. Funkcionalita s názvom *Priebehové meranie odberu a dodávky činnej energie s diaľkovým odpočtom*: Diaľkový odpočet s intervalom 15 minút.
4. Funkcionalita s názvom *Registrácia odberu a dodávky elektriny vo viacerých sadzbách*: Táto funkcionalita umožní uloženie práce vo viacerých tarifách a tým pádom fakturáciu elektriny v rôznych cenách spotrebovanú v rôznych časoch.
5. Funkcionalita s názvom *Pravidelný odpočet určeného meradla a diaľkový prenos nameraných údajov*: Elektromer umožňuje ako pravidelný odpočet tak aj odpočet na vyžiadanie.
6. Funkcionalita s názvom *Pravidelná a automatizovaná synchronizácia dátumu a času určeného meradla a ďalších TP.*
7. Funkcionalita s názvom *Spínanie taríf podľa aktuálnej sadzby.*
8. Funkcionalita s názvom *Možnosť zmeny času platnosti sadzieb určeného meradla z centrály IMS*: Možnosť diaľkovej zmeny aktuálnej sadzby.
9. Funkcionalita s názvom *Registrácia udalostí neštandardných a poruchových stavov a ich zasielanie do centrály IMS*: Kontrola a zaznamenávanie neštandardných stavov.
10. Funkcionalita s názvom *Možnosť diaľkovej parametrizácie a aktualizácie programového vybavenia určeného meradla.*
11. Funkcionalita s názvom *Možnosť parametrizácie alebo odpočtu určeného meradla cez lokálne rozhranie.*
12. Funkcionalita s názvom *Priebehové štvorkvadrantné meranie odberu a dodávky činnej energie a jalovej energie*: Meranie dodávky a odberu činnej a dodávky a odber jalovej energie.
13. Funkcionalita s názvom *Možnosť diaľkového odpojenia OM povelom z centrály IMS.*
14. Funkcionalita s názvom *Možnosť diaľkového pripojenia OM povelom z centrály IMS alebo jeho lokálneho pripojenia*: Diaľkové ovládanie odberného miesta.
15. Funkcionalita s názvom *Prúdové a výkonové obmedzenie v určenom meradle*: Prúdové a výkonové obmedzenie v určenom meradle.
16. Funkcionalita s názvom *Meranie efektívnych hodnôt napätia a prúdu po fázach*: Meranie vo fázach pre potreby prevádzkovateľa distribučnej sústavy.
17. Funkcionalita s názvom *Vyhodnocovanie účinníka počítaného z činnej a jalovej*

energie: Pomer činnej a jalovej energie.

18. Funkcionalita s názvom *Registrácia alarmov a napadnutie určeného meradla.*
19. Funkcionalita s názvom *Možnosť výmeny komunikačného modulu bez zásahu do meracej časti určeného meradla*: Možnosť výmeny komunikačného modulu napríklad z typu GSM na PLC.
20. Funkcionalita s názvom *Priebehové štvorkvadrantné meranie zdanlivej energie a vyhodnocovanie výkonových parametrov*: Registrácia špeciálnych elektrických parametrov pri vyhodnocovaní kvality elektriny.
21. Funkcionalita s názvom *Meranie kvality elektriny pre potreby prevádzkovateľa distribučnej sústavy.*
22. Funkcionalita s názvom *Vyhodnocovanie účinníka počítaného z nameraných hodnôt činnej energie a zdanlivej energie*: Presnejšie určenie účinníka.
23. Funkcionalita s názvom *Rozhranie a komunikácia s dispečerským riadiacim systémom.*

Tabuľka stručne zobrazuje rozdelenie týchto funkcionalít podľa jednotlivých skupín meradiel 3.1.

3.3.1 Typy elektromerov

Základná

- Meranie typu A: kategória číslo 3 – 2.4.
- V tejto skupine sa používa elektromer Sanxing- typ SX5A2.
- Podrobný popis funkcionalít tohto typu zariadenie je v podkapitole 3.3 body **1-11** a v tabuľke 3.1.

Pokročilá

- Meranie typu A: kategória číslo 1 a 2 – 2.4.
- Do tejto skupiny patria elektromer Addax- typ NP73E pre priame trojfázové pripojenie a elektromer Sanxing- typ P43S02.
- Podrobný popis funkcionalít tohto typu zariadenie je v podkapitole 3.3 body 1-19 a v tabuľke 3.1.

Špeciálna

- Meranie typu A: kategória číslo 4 – 2.4.
- Inštalovaný elektromer EMH- typ LZQJ-XC.
- Podrobný popis funkcionalít tohto typu zariadenie je v podkapitole 3.3 body 1-23 a v tabuľke 3.1.

Tab. 3.1: Tabuľka rozdelenia funkcionalít podľa kategórií elektromerov.

Funkcionalita	**Základná**	**Pokročilá**	**Špeciálna**
Obojsmerná komunikácia medzi OM a centrálou IMS	x	x	x
Monitoring OM lokálnym pripojením k IMS	x	x	x
Priebehové meranie odbru a dodávky činnej energie s diaľkovým odpočtom	x	x	x
Registrácia odberu a dodávky elektriny vo viacerých sadzbách	x	x	x
Pravidelný odpočet určeného meradla a diaľkový prenos nameraných údajov	x	x	x
Pravidelná a automatizovaná synchronizácia dátumu a času určeného meradla a ďalších TP	x	x	x
Spínanie taríf podľa aktuálnej sadzby	x	x	x
Možnosť zmeny času platnosti sadzieb určeného meradla z centrály IMS	x	x	x
Registrácia udalostí neštandardných a poruchových stavov a ich zasielanie do centrály IMS	x	x	x
Možnosť diaľkovej parametrizácie a akturalizácie programového vybavenia určeného meradla	x	x	x
Možnosť parametrizácie alebo odpočtu určeného meradla cez lokálne rozhranie	x	x	x
Priebehové štvorkvadrantné meranie odberu a dodávky činnej energie a jalovej energie		x	x
Možnosť diaľkového odpojenia OM povelom z centrály IMS		x	x
Možnosť diaľkového pripojenia OM povelom z centrály IMS alebo jeho lokálneho pripojenia		x	x
Prúdové a výkonové obmedzenie v určenom meradle		x	x
Meranie efektívnych hodnôt napätia a prúdu po fázach		x	x
Vyhodnocovanie účinníka počítaného z činnej a jalovej energie		x	x
Registrácia alarmov a napadnutie určeného meradla		x	x
Možnosť výmeny komunikačného modulu bez zásahu do meracej časti určeného meradla		x	x
Možnosť diaľkovej parametrizácie a akturalizácie programového vybavenia určeného meradla			x
Priebehové meranie zdanlivej energie a vyhodnocovanie výkonových parametrov			x
Meranie kvality elektriny pre potreby prevádzkovateľa distribučnej sústavy			x
Vyhodnocovanie účinníka počítaného z nameraných hodnôt činnej energie a zdanlivej energie			x
Rozhranie a komunikácia s dispečerským riadiacim systémom			x

3.4 Implementácia High Level Security v inštalovaných elektromeroch

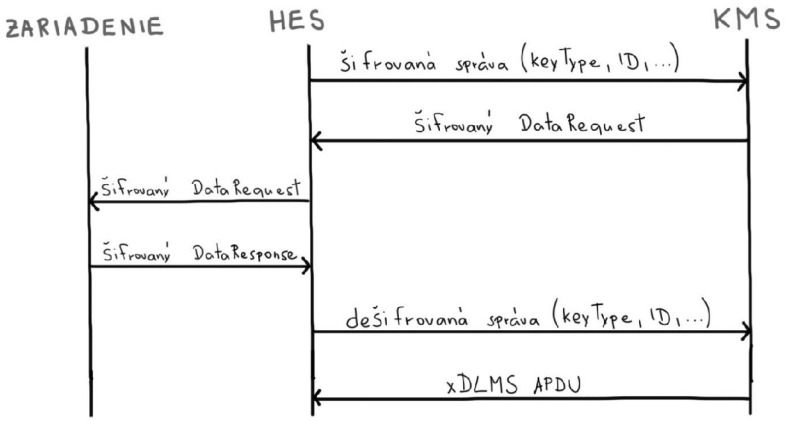
Pri využití zabezpečenej komunikácie je však potrebné zabezpečiť správu kľúčov. V optimálne zabezpečenom prostredí sa o to stará Key Management System teda Systém správy kľúčov. Ten by mal zaistiť bezpečné úložisko kľúčov, zabezpečiť predávanie kľúčov, sledovať ich možnú expiráciu, generovať nové kľúče a šifrovať a dešifrovať rámce DLMS. Tento KMS je teda implementovaný ako samostatná služba alebo súbor služieb, ktoré budú poskytovať potrebné metódy pre šifrovanie a dešifrovanie datových rámcov, generovania a výmeny kľúčov.

3.4.1 Key Management System – bezpečné úložisko kľúčov

Súčasťou implementácie bezpečnostných mechanizmov je správa kľúčov a citlivých dát, ktoré je nutné bezpečne ukladať. V rámci riešenia bezpečnostných politík je v spoločnostiach využívaný systém slúžiaci ako databáza v *Key Management System*, ktorý musí spĺňať prísne bezpečnostné a prevádzkové požiadavky s vysokou dostupnosťou v čase zberu dát. V štruktúre KMS sa okrem tejto databázy nachádzajú a samostatné služby obsluhujúce rôzne varianty komunikačnej technológie. Spolu tvoria systém ukladania a poskytovania hesiel všetkým odlišným formám komunikácie a ich obsluhujúcim systémom ktoré sa potrebujú dostať do zariadení. Medzi hlavné schopnosti systému KMS patria:

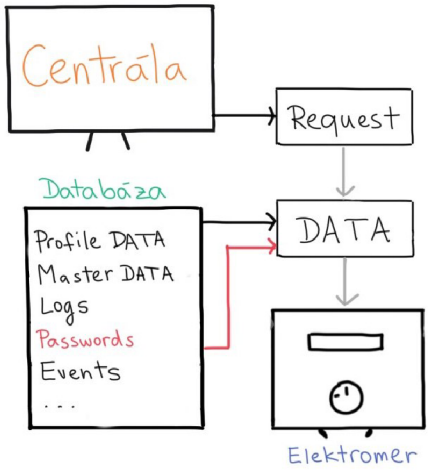
- import jedinečných kľúčov pre aktuálne technológie,
- evidencia o rôznych typoch kľúčov: master key, unicast key, broadcast key, authentication key v tabuľke 1.2,
- evidencia o výmenách a expirácii kľúčov,
- generovanie nových kľúčov,
- overovanie, šifrovanie a dešifrovanie dátových rámcov pri komunikácii so zariadeniami.

Na obrázku 3.1 je znázornená všeobecná schéma komunikácie medzi inteligentným elektromerom a KMS. Komunikačný driver nepracuje priamo s kľúčmi ale posiela dáta k šifrovaniu alebo dešifrovaniu KMS, ktorý operácie prevedie. KMS kľúče drží po celý čas ako prebieha komunikačné spojenie. Komunikácia KMS s takouto databázou prebieha na začiatku spojenia a pri potrebe zmeny úrovne komunikácie.



Obr. 3.1: Schéma bežnej komunikácie meradla s KMS.

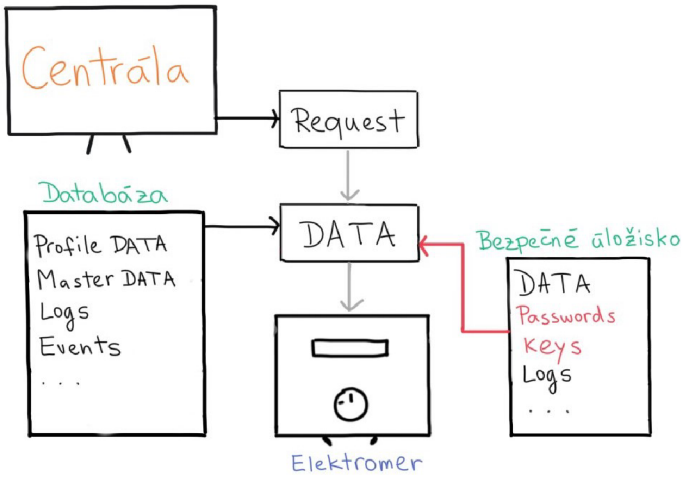
Systém, ktorý obsahuje iba prostú databázu je zobrazený na obrázku 3.2. Pred zahájením spojenia sú citlivé informácie (heslá a kľúče) uložené v databáze. V momente prijatej požiadavky sa z databázy načítajú kľúče potrebné na vytvorenie rámca DLMS (*encryption, authentication key*), ktorý zašifrovaný a podpísaný smeruje do elektromera. Prijatý rámec zariadenie následne verifikuje a použitím vlastných kľúčov vygeneruje odpoveď a zašifrovanú ju odošle naspäť serveru.



Obr. 3.2: Riešenie iba s databázou.

Zloženie systému s využitím KMS patrí do definície ideálneho stavu zaistenia bezpečnosti. Vytvorený rámec je prvotne zaslaný do systému KMS, ktorý využitím bezpečne uložených kľúčov podpíše a zašifruje správu a zašle ju elektromeru. Zariadenie rámec verifikuje a bezpečne zabalený ho pošle späť centrále, do ktorej sa

však dostane až po autentizácii systémom KMS. Na obrázku 3.3 je v jednoduchosti znázornený proces s využitím KMS.



Obr. 3.3: KMS s bezpečným úložiskom kľúčov.

Rozdielne systémy so sebou prinášajú rôzne výhody a nevýhody. Pri využívaní databázy bez KMS vystavujeme komunikačný kanál väčším rizikám ako pri systéme s KMS. Aplikovanie KMS teda vedie k vyššej forme zabezpečenia, no jeho prevádzka je finančne náročnejšia.

4 Súčasný stav Smart Meteringu v Českej republike

4.1 PREdistribuce, a.s.

V súčasnosti pražská PRE distribuce využíva inteligentné elektromery hlavne pre účely pilotných projektov, ktoré sú osobitne definované. Sú to hlavne odberné miesta väčších podnikateľov, fotovoltických elektrární a nabíjačiek elektromerov, hlavne elektromery typu A a B. Kumulatívne je ich v distribučnej sústave inštalovaných cca 7000 kusov.

Vrámci prípravy na rollout na základe novej *Vyhlášky č.359/2020 o měření elektřiny* [7], PRE distribuce realizuje technologické testy rôznych funkcionalít a typov komunikácie hlavne G3, PRIME, BPL (Broadband Power Line) a Corinex. Sú to následujúce typy elektromerov:

- ADD N7x– test PRIME,
- Landis+Gyr E450– test G3,
- Landis+Gyr E350 modul Corinex- BPL Corinex,
- Linyang CLMS x00– BPL Corinex,
- ZPA GS. 303– test nemeckého modelu so Smart Energy Gateway.

Vzhľadom na dátum vydania vyhlášky koncom roka 2020 a jej uvedenie do platnosti začiatkom roka 2021, spoločnosť PRE distribuce v súčasnosti v štádiu prípravy koncepcie implementácie inteligentného merania. Do úvahy sú brané najmä tieto varianty:

- 1. varianta, splnenie požiadavok legislatívy [7] tj osadiť tie odberné miesta, ktoré majú ročnú spotrebu vyššiu než 6 MWh (cca 70 tis.).
- 2. varianta je prvá varianta rozšírená o všetky dvojtarifové miesta (cca 140 tis.).
- 3. varianta počíta s tým, že pokiaľ distribučná trafostanica napája viac ako napríklad 30 odberných miest z kategórií variant 1 a 2, tak dôjde k plošnému nasadeniu inteligentných meradiel napájaných touto trafostanicou.

4.2 ČEZ Distribuce

Podobne ako PREdistribuce sa v súčasnosti ČEZ venuje pilotným projektom zameriavacím sa na komplexné testovanie prevádzky systémov v reálnych podmienkach na svojom distribučnom území. Zámer v budovaní Smart Meteringu je v súlade s *Vyhláškou č.359/2020 o měření elektřiny* [7], ktorá definuje typy a spôsoby merania.

Výber elektromerov je v procese výberového konania podľa plnenia rôznych kritérií a požiadaviek ako typy komunikácie, typ spojenia, sieťové služby, bezpečnostné požiadavky a mnoho iných.

Spoločnosť ČEZ plánuje osadenie odberných miest komunikačnými technológiami ako sú:

- PLC (Power Line Communication),
- BPL (Broadband Power Line),
- GSM (Global System for Mobile Communications),
- rádio technológie.

5 Tvorba ekonomického a hodnotiaceho modelu založeného na NPV, jeho naplnenie a vyhodnotenie

5.1 Hodnotiaci model dopadov kybernetickej bezpečnosti na prevádzkové, ekonomické, regulačné, právne aspekty spoločnosti

Pri riešení a kompletizácii podkladov pre zhodnotenie dopadov kybernetickej bezpečnosti bolo potrebné zhromaždiť a vyhodnotiť množstvo údajov či už v teoretickej rovine (algoritmy, rôzne úrovne bezpečnosti) ale aj v rovine ekonomickej a rovine prevádzkovej. Teoretická časť je popísaná v kapitolách 1 až 3. Táto kapitola hodnotenia je venovaná problematike prevádzkových a ekonomických dopadov pre prevádzkovateľov distribučných sústav (PDS).

Všetky nasledovné atribúty boli posúdené na základe konzultácií s predstaviteľmi PDS pre nasledovné scenáre zavedenia prvkov kybernetickej bezpečnosti:

1. **Minimálna úroveň zabezpečenia**- model s minimálnou úrovňou zabezpečenia reprezentuje LLS štruktúru (podkapitola 1.1.2), kde neexistuje systém prideľovania hesiel Key Management Systémom ani žiadna forma šifrovanej komunikácie. Správy sa medzi entitami prenášajú v prostom tvare.
2. **Optimálna úroveň zabezpečenia**- pri optimálnej úrovni zabezpečenia je do systému zakomponovaný aj Key Management System, ktorý vytvára štruktúru HLS (podkapitola 1.1.2) kde sa bezpečné kľúče predávajú zariadeniam. Komunikácia medzi zariadením a centrálnym systémom prebieha v šifrovanej podobe a využíva zabezpečenú komunikáciu.

5.1.1 Úvod do pravidiel pre spoločnosti, ktoré sú považované za prirodzené monopoly

Podstatou regulácie je simulácia trhových podmienok medzi spoločnosťami, ktoré sú považované za prirodzené monopoly. U spoločností s monopolným postavením nie je zabezpečená dostatočná konkurencia, alebo ich infraštruktúra je jedinečná a ťažko nahraditeľná, ako napríklad telekomunikácie, dopravná či energetická infraštruktúra.

Prevádzkovatelia týchto infraštruktúr pôsobia v prostredí bez konkurencie a ich monopolné postavenie na príslušnom území je dané lokalitou kde infraštruktúru prevádzkujú. Bez účinných regulačných opatrení by monopolné spoločnosti svoju

výhodu bezkonkurenčnosti mohli zneužívať vo svoj prospech, často na úkor zákazníkov, ktorí nemajú na výber. Podstatou regulácie monopolného trhu je najmä ochrana spotrebiteľa a dosiahnutie rovnováhy medzi výhodami pre spotrebiteľov a motiváciou regulovaných spoločností investovať do odvetvia, kde pravidlá hry neurčuje trh, ale regulátor.

Regulácia umožňuje rovnocenný prístup a využitie jedinečnej infraštruktúry každému záujemcovi, pri dodávaných službách definuje štandardy kvality a minimálny rozsah informácií, ktoré monopolné spoločnosti musia poskytovať. Zároveň chráni spotrebiteľov pred vysokými bezkonkurenčnými poplatkami alebo ich neprimeraným zvyšovaním. Dobrým príkladom je elektroenergetika, distribúcia alebo prenos elektriny. Prevádzkovatelia prenosových a distribučných sústav sú rovnako považovaní za prirodzené monopoly a platia pre nich pravidlá regulácie.

V Slovenskej republike sú tieto spoločnosti regulované ÚRSOm, Úradom pre reguláciu v sieťových odvetviach, v Českej republike ERÚ – Energetickým regulačným úradom. Ďalším dôležitým pojmom pre pochopenie regulovaného prostredia je liberalizácia trhu s elektrinou. Liberalizácia umožňuje nastaviť pre spotrebiteľa konkurenčné prostredie, kde má na výber a môže si vybrať svojho najvýhodnejšieho obchodníka s elektrinou. Na Slovensku a v Českej republike sa trh s elektrickou energiou liberalizoval predovšetkým vďaka rozsiahlym regulačným opatreniam, ktoré v plnej miere odrážajú vývoj európskej legislatívy v oblasti liberalizácie trhu. Legislatíva okrem iného zakazuje prirodzeným monopolom ako sú prenosové a distribučné spoločnosti obchodovať s elektrinou a prikazuje týmto spoločnostiam definovať také pravidlá, ktoré umožnia rôznym obchodníkom rovnaký (nediskriminačný) prístup k distribučne alebo prenosovej sústave. Tým je zaručené že pre každého obchodníka existujú rovnaké pravidlá a záleží od jeho schopností ako dokáže motivovať spotrebiteľa. Od týchto pravidiel sú v ďalšom odvodené aj následné úvahy pri hodnotení ekonomického modelu, ktorý je predmetom tejto práce v reťazci *Prevádzkovateľ distribučnej sústavy – Obchodník s elektrinou – Zákazník.*

5.1.2 Teoretický hodnotiaci model rizík spojených s porušením kybernetickej bezpečnosti v problematike IMS

Bezpečnosť informácií predstavuje vytvorenie bezpečného informačného systému, v ktorom je zaistená ochrana údajov, ktoré systém spracováva a uchováva tak, aby nedochádzalo k úniku alebo manipulácii neoprávnenými osobami. Tieto riziká možné simulovať v teoretickom hodnotiacom modeli rizík napríklad Gordon-Loeb Modelom [12]. Porušenie bezpečnosti sa v praxi rozdeľuje a hodnotí v troch hlavných vrstvách (atribútov) podľa triády CIA (Confidentiality, Integrity, Availability) [16] a to sú:

1. Zaistenie dôvernosti

Tento atribút zabezpečuje aby údaje neboli sprístupňované alebo odhalené neautorizovaným osobám alebo entitám. Do tejto kategórie patrí hlavne zaručenie dôveryhodnosti citlivých informácií a dát. Predchádza sa neautorizovanému fyzickému prihláseniu do elektromera napríklad odchytením hesla počas komunikácie medzi elektromerom a centrálou. Hlavnými rizikami je v tomto prípade únik dát o spotrebe, zmena firmware, manipulácia registrov a taríf alebo jednotlivé až hromadné odpojenie elektromerov.

2. Zaistenie dostupnosti

Zaisťuje sa schopnosť byť dostupný a použiteľný na požiadanie autorizovanej entity. Dostupnosť je časová charakteristika, ktorá vyjadruje závislosť medzi požiadavkami riadeného systému a splnením týchto požiadaviek [14]. Tento atribút zahrňuje riziká týkajúce sa nedostupnosti komunikácie teda neschopnosti nadviazania komunikácie. Zabraňuje sa tak útokom na dostupnosť komunikácie medzi serverom a klientom.

3. Zaistenie integrity

Integrita zaisťuje stav zabezpečenia, presnosti a úplnosti aktív. Čítané dáta sú totožné s dátami uloženými čo znamená, že počas prenosu a ukladaní dát nedošlo k neočakávaným zmenám.

Riziká súvisiace s prevádzkovaním systémov na spracovanie zákazníckych dát či už dát meraných alebo fakturačných sú sústredené hlavne u prevádzkovateľa distribučnej sústavy, ktorý tieto dáta získava, spracováva, archivuje a vyhodnocuje. Riziká, ktoré sú prevádzkovateľa distribučnej sústavy relevantné, sa dajú zhrnúť v nasledovnej štruktúre:

- finančné riziká,
- regulačné riziká,
- prevádzkové a organizačné riziká,
- riziká poškodenia mena firmy a vplyv na zákazníka.

Kvantifikácia rizík je zrejmá z tabuliek 5.1 až 5.4, ktoré sú na vertikálnej osi rozdelené do vrstiev podľa poskytovania bezpečnostných atribútov a horizontálna os rozdeľuje tieto tri vrstvy na čas, v ktorom sa riziko uplatňuje. Časy uvedené v tabuľkách označujú časový rámec, v ktorom sa musí proces obnoviť, aby spoločnosť nevstúpila do fázy, v ktorej je z krátkodobého alebo dlhodobého hľadiska ohrozená jej schopnosť prežiť. Tieto časy sa interpretujú ako doba, počas ktorej je potrebné dostať skúmaný proces na minimálnu požadovanú úroveň. Táto úroveň predstavuje

také zabezpečenie funkcionality procesu, aby spoločnosti nevznikali ďalšie škody. Parametre a kvantifikácia štyroch rôznych rizikových oblastí boli vytvorené po konzultácii s distribučnými spoločnosťami a vyhodnotení možných rizík pri prevádzkovaní inteligentného merania.

Finančné riziká

Aké sú finančné dôsledky v prípade prerušenia procesu?

Finančný dopad odvodený od zníženia tržieb a pokút vyplývajúcich z právnych záväzkov. Úrovne dopadu môžeme rozdeliť na:

1. **Mierny** dopad - do výšky 1 mil. Eur.
2. **Stredný** dopad - do výšky 15 mil. Eur.
3. **Vysoký** dopad - do výšky 50 mil. Eur.

Tab. 5.1: Finančné riziká.

Vrstvy	**24 hod**	**3 dni**	**7 dní**	**14 dní**
Dôvernosť	1	2	3	3
Dostupnosť	1	2	2	3
Integrita	2	2	3	3

Regulačné riziká

Aký právny alebo regulačný vplyv sa môže vyskytnúť v prípade prerušenia procesu?

Distribučné spoločnosti sú subjektom regulácie v sieťových odvetviach. Slovenská republika – ÚRSO, Česká republika – ERÚ.

1. **Mierny** dopad - porušenie s menšími následkami, nízkymi kompenzáciami.
2. **Stredný** dopad - porušenie s väčšími následkami, viac civilných žalôb.
3. **Vysoký** dopad - porušenie s vážnymi následkami, vysoké pokuty alebo kompenzácie, pozastavenie činnosti.

Tab. 5.2: Regulačné riziká.

Vrstvy	**24 hod**	**3 dni**	**7 dní**	**14 dní**
Dôvernosť	1	2	3	3
Dostupnosť	1	2	2	2
Integrita	1	2	3	3

Prevádzkové a organizačné riziká

Aké zhoršenie plnenia úloh môže nastať v prípade prerušenia procesu?

Prevádzka distribučnej sústavy, interné a procesné komplikácie.

1. **Mierny** dopad - ovplyvnené viaceré oddelenia v organizácii, proces vykazuje menšie omeškania, malé množstvo ovplyvnených projektov.
2. **Stredný** dopad - ovplyvnené viaceré oddelenia v organizácii, proces vykazuje podstatné omeškania, veľké množstvo ovplyvnených projektov.
3. **Vysoký** dopad - pozastavenie hlavných aktivít, meškanie väčšiny projektov, pozastavené je aj fungovanie iných procesov.

Tab. 5.3: Prevádzkové a organizačné riziká.

Vrstvy	**24 hod**	**3 dni**	**7 dní**	**14 dní**
Dôvernosť	2	3	3	3
Dostupnosť	3	3	3	3
Integrita	3	3	3	3

Riziká poškodenia mena firmy a vplyv na zákazníka

Aký vplyv môže mať na vnímanie spoločnosti/ meno spoločnosti/ vplyv na zákazníka prípadné prerušenie procesu?

Prevádzka distribučnej sústavy, interné a procesné komplikácie.

1. **Mierny** dopad - domácností, firmy: malý počet klientov - postihnutých menej ako 5 % zákazníkov, regionálna resp. lokálna negatívna publicita.
2. **Stredný** dopad - domácností, firmy: 5 až 10 % postihnutých zákazníkov, národná negatívna publicita.
3. **Vysoký** dopad - domácností, firmy: 10 až 25 % postihnutých zákazníkov, intenzívna národná negatívna publicita prechod do medzinárodnej negatívnej publicity.

Tab. 5.4: Riziká poškodenia mena firmy a vplyv na zákazníka.

Vrstvy	**24 hod**	**3 dni**	**7 dní**	**14 dní**
Dôvernosť	1	2	3	3
Dostupnosť	1	2	3	3
Integrita	2	2	3	3

5.2 Kapitálové a prevádzkové náklady IMS, prínosy IMS pre spoločnosť a vplyv podmienok súvisiacich s kybernetickou bezpečnosťou

Pri zhodnocovaní vplyvov kybernetickej bezpečnosti na prevádzkové, ekonomické a užívateľské aspekty som zvolila dva modely, ktoré budem porovnávať. Tieto modely (scénare) sú modelované v prílohe reprezentovanej súborom excel.

Prvý model reprezentuje **minimálnu možnú úroveň zabezpečenia** takzvanú LLS štruktúru (podkapitola 1.1.2), kde neexistuje systém prideľovania kryptovaných hesiel Key Management Systémom. Hardvér elektromerov je v tomto modeli bez možnosti komunikácie HLS. Komunikácia s centrálnym systémom je prostredníctvom GSM komunikácie. Komunikácia s elektromerom v tomto prípade prebieha v otvorenej forme prostým overením hesla, ktoré sa nachádza v meradle.

Druhý model reprezentuje **optimálnu úroveň zabezpečenia**, ktorého súčasťou je Key Management System, hardvér elektromerov podporuje vyššiu formu komunikácie v kryptovanej forme HLS (podkapitola 1.1.2). Druhý model s optimálnou úrovňou zabezpečenia sa oproti prvému modelu líši:

- elektromermi s vyššou hardvérovou úrovňou,
- zriadením systému na prideľovanie hesiel – Key Management System,
- komunikácia medzi centrálou a elektromermi je šifrovaná a zabezpečená,
- prevádzkovanie systému s optimálnou úrovňou zabezpečenia si vyžaduje personál s vyššou kvalifikáciou.

Nižšie uvedené vstupné parametre či už nákladov alebo prínosov sú popísané v rôznych publikáciách ako *Study on cost benefit analysis of smart metering systems in EU Member States* [15] z roku 2015. Vstupné parametre použité v modeli tejto bakalárskej práce viac alebo menej korešpondujú s údajmi z uvedeného zdroja hlavne pre Českú a Slovenskú republiku. Prípadné rozdiely v nákladoch, napríklad cena elektromerov, cena za prevádzku a údržbu systémov sú spôsobené rozdielom cien medzi rokom 2015 a 2021 hlavne z týchto troch dôvodov:

1. Cena ľudskej práce sa medziročne zvyšuje z dôvodu inflácie a to ma vplyv najmä na prevádzku, údržbu a inštaláciu elektromerov, vytváranie IT systémov.
2. Ceny niektorých technologických komponentov pri výrobe elektromerov alebo hardvéru systémov naopak poklesli.
3. Pri vytváraní tohto modelu sa do prínosov zahŕňala hlavne idea prínosov zákazníka. Tento podiel prínosov, vyčíslený približne na 70 % však zďaleka nie je aktuálny.

5.2.1 Vstupné parametre pre CAPEX/OPEX model

Kapitálové výdavky – Capital Expenses CapEx

CAPEX je skratka používaná pre pomenovanie **investičných** (kapitálových) výdavkov. Ide o výdavky vynaložené na nákup zdrojov najmä materiálneho alebo nemateriálneho charakteru (dáta, software, informácie), ktoré majú väčšiu hodnotu a preto nadobúdajú charakter investície. Tá je často realizovaná formou projektov a podnieti nejakú zmenu v organizácii [18].

Prevádzkové výdavky – Operating Expenses OPEX

OPEX je skratka používaná pre pomenovanie **neinvestičných**, bežných **prevádzkových** (operatívnych) výdavkov spoločnosti. Ide o výdavky vynaložené spoločnosťou na zabezpečenie prevádzky, údržby a nákupu služieb [17].

Čistá súčasná hodnota – Net Present Value NPV

Čistá súčasná hodnota je rozdiel medzi súčasnou hodnotou finančných prírastkov a súčasnou hodnotou úbytku financií za určité časové obdobie. Net Present Value sa používa pri kapitálovom rozpočtovaní a plánovaní investícií na analýzu ziskovosti plánovanej investície alebo projektu [19].

Tabuľka 5.5 zobrazuje zoznam vstupných parametrov použitých na výpočet a zobrazenie oboch modelov optimálnej aj minimálnej formy zabezpečenia.
Parametre uvedené v tabuľke sú podrobne popísané v nasledujúcich odstavcoch:

Diskontná sadzba

Diskontná sadzba je druh úrokovej sadzby, za ktorú poskytuje centrálna banka úvery komerčným bankám. Následne komerčné banky poskytujú úvery obyvateľstvu, firmám alebo obciam s úrokovou sadzbou, ktorá sa odvíja od výšky diskontnej sadzby. V praxi používajú firmy najčastejšie ako diskontnú sadzbu na diskontovanie peňažných tokov vážené priemerné náklady na celkový kapitál – **WACC** zo skratky Weighted Average Cost of Capital. WACC predstavuje priemernú mieru výnosu, ktorú požadujú poskytovatelia vlastného kapitálu (majitelia spoločnosti, investori) a poskytovatelia dlhového kapitálu (banky, majitelia dlhopisov) [10].

V tomto prípade sa však jedná o prevádzkovateľa distribučnej sústavy, ktorý pôsobí na vymedzenom trhu a je v monopolnom postavení. V takýchto prípadoch je výška možných výnosov takýchto subjektov regulovaná už vyššie spomínaným SR-ÚRSO a v ČR- ERÚ. Pre roky 2019-2021 regulačný úrad definoval výšku WACC pre prevádzkovateľov distribučných sústav Slovenskej republike na 5,65 % [13].

Tab. 5.5: Tabuľka vstupných parametrov modelu.

Vstupné parametre

Parameter	**Hodnota**
Diskontná sadzba (WACC)	5,65 %
Počet elektromerov	110 000 kusov
Predpokladaná životnosť meradla	12 rokov
Predpokladaná životnosť centrály	12 rokov
Predpokladaná životnosť KMS	12 rokov
Počet rokov rolloutu	7 rokov
Údržba KMS	20,00 %
Údržba meradiel optimálne zabezpečenie	2,00 %
Údržba meradiel minimálne zabezpečenie	1,80 %
Cena elektromera – minimálne zabezpečenie	60 Eur
Cena elektromera – optimálne zabezpečenie	80 Eur
Náklady na inštaláciu elektromera	16 Eur
Jednotková cena za SIM a dátový prenos – minimálne zabezpečenie	1,80 Eur
Jednotková cena za SIM a dátový prenos – optimálne zabezpečenie	2,20 Eur

Počet elektromerov

Pri stanovení počtu elektromerov som vychádzala z Vyhlášky číslo 358 Ministerstva hospodárstva Slovenskej republiky 2.4, ktorá stanovuje rozdelenie odberných miest podľa výšky ročnej spotreby a maximálnej rezervovanej kapacity. Na Slovensku je to 600 000 zákazníkov a v distribučnej spoločnosti, v ktorej som vytvárala a skúmala model to bolo 110 000 meradiel.

Predpokladaná životnosť meradla

Dobu platnosti overenia určeného meradla definuje Zákon o metrológii so svojimi vykonávacími vyhláškami. Na základe tejto legislatívnej normy je doba ciachu (platnosť overenia určeného meradla) stanovená na 12 rokov.

Predpokladaná životnosť centrály a Key Management Systému

Tieto životnosti boli stanovené na základe Best Practice špecialistov v spoločnosti ktorej model som skúmala.

Počet rokov rolloutu

Počet rokov rolloutu predstavuje čas, za ktorý spoločnosť osadí všetky predurčené odberné miesta. V mojom prípade to bolo 7 rokov, definované legislatívou Vyhlášky číslo 358 Ministerstva hospodárstva Slovenskej republiky 2.4.

Údržba Key Management systému, centrály a meradiel

Náklady na údržbu boli stanovené percentom z investičných prostriedkov, ktoré boli vynaložené v danej oblasti. Takto vypočítaná výška prevádzkových nákladov korešponduje s reálnymi nákladmi distribučnej spoločnosti.

Cena elektromera

Ceny elektromerov odzrkadľujú priemerné náklady na nákup rôznych typoch zariadení vhodných pre minimálny a optimálny model. Priemerná cena elektromerov pre minimálny model je 60 Eur a priemerná cela elektromera pre optimálny model s vyššími hardvérovými parametrami je 80 Eur. Cena elektromerov bola vyhodnotená po konzultáciách s distribučnými spoločnosťami. Hardvérové rozdiely elektromerov sú uvedené v tabuľke 3.1.

Náklady na inštaláciu elektromera

Náklady na inštaláciu zahŕňajú podiel hodinovej sadzby montéra, ktorý vykoná montáž elektromera. Tieto náklady sú zahrnuté v kapitálových výdavkoch. Odmena za montáž elektromerov má v oboch modeloch rovnakú cenu.

Jednotková cena za SIM a dátové prenosy

V tejto cene sú zahrnuté nákup samotnej SIM a ta dátové služby.

5.2.2 Štruktúra kapitálových a prevádzkových nákladov IMS

Štruktúra kapitálových a prevádzkových nákladov je konzultovaná s prevádzkovateľmi distribučných sústav ČR a SR a kopíruje procesné nastavenie od vzniku nameraných dát až po doručenie k zákazníkovi: zákazník $\rightarrow$ elektromer $\rightarrow$ GSM komunikačný kanál $\rightarrow$ centrálny merací systém $\rightarrow$ fakturačný systém $\rightarrow$ web portál. Základom je investícia do elektromerov, základnej jednotky celého systému a medzi kapitálové výdavky patrí aj samotná inštalácia elektromerov. Ďalším kľúčovým kapitálovým výdavkom je centrála pre zber nameraných dát a Key Management System. Pre bezporuchový chod týchto zariadení sú potrebné určiť prevádzkové oparenia, ktoré tvoria prevádzkové náklady celého systému. Výšku prevádzkových nákladov

Tab. 5.6: Tabuľka rozdelenia nákladov.

	Náklady		**Zabezpečenie**	
Položky	CAPEX	OPEX	Minimálna úroveň	Optimálna úroveň
Elektromery	✓	✓	✓	✓
Inštalácia elektromerov	✓	-	✓	✓
Komunikácia	-	✓	✓	✓
Centrála	✓	✓	✓	✓
Centrála + KMS	✓	✓	-	✓
Kvalifikovaný personál	-	✓	-	✓

som po konzultácii s prevádzkovateľmi distribučných sústav stanovila percentuálnym pomerom z výšky investícií. Jednotlivé náklady v tabuľke 5.6 boli priradené do skupiny OPEX a CAPEX podľa definícií uvedených v podkapitole 5.2.1.

5.2.3 Štruktúra a kvantifikácia prínosov IMS (prevádzkovateľ IMS, zákazník, obchodník s elektrinou)

Európska komisia (EK) svojim odporúčaním č. 2012/148/EÚ *Commission Recommendation on preparations for the roll-out of smart metering systems* [11] okrem iného odporučila štruktúru a spôsoby kvantifikácie prínosov zavedenia IMS. Prínosy sú štruktúrované podľa reťazca prevádzkovateľ distribučnej sústavy, obchodník s elektrinou a zákazník. Na základe odporúčaní EK a záujmu inštalovať IMS aj na Slovensku, vznikla v roku 2013 pri Ministerstve Hospodárstva Slovenskej republiky pracovná skupina, ktorá mala za úlohu stanoviť podmienky rolloutu IMS pre Slovenskú republiku a vyhotoviť CBA (Cost benefit analýzu) analýzu pre zavedenie IMS v Slovenskej republike. Štruktúra prínosov inteligentného meracieho systému či už z minimálnou alebo optimálnou úrovňou zabezpečenia je rozdelená z celospoločenského hľadiska na tri hlavné subjekty:

1. Prínosy pre zákazníka

Prínosy zákazníka zahŕňajú hlavne následujúce položky.

- Na základe informácií z IMS môže zákazník presunúť časť svojej spotreby do časových pásiem/taríf kedy je cena elektriny nižšia.
- Na základe informácií z IMS môže zákazník presnejšie predikovať svoju spotrebu a tým pádom sa vyhnúť nákladom za spôsobené odchýlky v spotrebe (hlavne priemyselní zákazníci).
- Na základe informácií z IMS môže zákazník optimalizovať/znižovať svoju spotrebu.

- Znižovaním spotreby sa znižujú aj technické straty u zákazníka.

2. Prevádzkovateľ distribučnej sústavy

Prínosy prevádzkovateľa distribučnej sústavy zahŕňajú hlavne následujúce položky.

- Prínosy z nahradenia manuálneho odpočtu elektromera automatickým odpočtom.
- Prínosy plynúce z lepších a adresnejších informácií pre dispečerské riadenie.
- Meranie kvality elektriny a predchádzanie sťažnostiam zákazníkov.
- Nižšie netechnické straty (lepšia identifikácia krádeží).
- Poskytovanie dát na komerčnej báze.
- Presnejšie znalosť podmienok a technických parametrov v distribučnej sústave (elektromery poskytujú na okrem nameranej elektriny aj iné analógové veličiny napr U, I, $\cos\phi$) a tým aj adresnejšia možnosť plánovania obnovy a investícií do distribučnej sústavy.

3. Obchodník s elektrinou

Prínosy obchodníka s elektrinou zahŕňajú hlavne následujúce položky.

- Citlivejšie elektromery, menej obchodných strát.
- Prínosy súvisiace s presnejšími nameranými údajmi menej sťažností, reklamácií, zníženie pohľadávok.
- Prínosy z rôznych tarifných štruktúr v predaji elektriny.

Medzi prínosy som vo svojom modeli zahrnula aj prínosy z odvrátenia rizika podľa modelu popísaného v podkapitole 5.1.2 a to tak, že prípadnú výšku škôd som alokovala do prínosov v optimálnom modeli zabezpečenia, ktorý vyššou úrovňou kybernetickej bezpečnosti tieto riziká odvráti.

5.3 Zhodnotenie ekonomického modelu a vplyvu kybernetickej bezpečnosti na ekonomický model

Zo vstupných hodnôt z tabuľky 5.5 pre výpočet čistej súčasnej hodnoty investície (Net Present Value NPV) sa v oboch modeloch do výpočtu započítavajú:

- diskontované náklady OPEX,
- diskontované náklady CAPEX,
- diskontované prínosy *.

Diskontované náklady OPEX a CAPEX vychádzajú z rozdelenia nákladov v tabuľke 5.6 diskontovaných diskontnou sadzbou WACC z tabuľky 5.5. Modely pracujú

s časovým pásmom rovným životnosti elektromera. Prínosy modelu s **minimálnou úrovňou zabezpečenia** predstavujú skupinu, ktorá pozostáva z prínosov pre distribučnú spoločnosť, prínosy dodávateľa elektriny a prínosov zákazníka, detailne popísanú v podkapitole 5.2.3. V druhom modeli s **optimálnou úrovňou zabezpečenia** prínosy zodpovedajú predošlej skupine rozšírenú o prínosy z odvrátenia stredného rizika pri optimálnej bezpečnosti vychádzajúcej z modelu rizík zobrazenej v podkapitole 5.1.2.

* Prínosy z odvrátenia rizika majú jednorázový charakter a nemajú finančný dopad, ktorý by bolo možno rozdeliť do jednotlivých rokov. Už po jednom vážnom kybernetickom útoku, následnom odpojení zákazníkov a prípadnou zmenou prístupových údajov do elektromerov by sa stal celý systém nefunkčným a bola by potrebné investície do obnovy alebo náhrady celého systému. Preto boli tieto prínosy z odvrátenia rizika pripočítané v plnom rozsahu bez diskontovania.

V XML prílohe sú simulované dva modely:

- model s minimálnou úrovňou bezpečnosti NPV 1,
- model s optimálnou úrovňou bezpečnosti NPV 2.

Modely a ich vstupné parametre sú interaktívne a umožňujú meniť hodnoty. Parametre, ktoré je možno meniť sú:

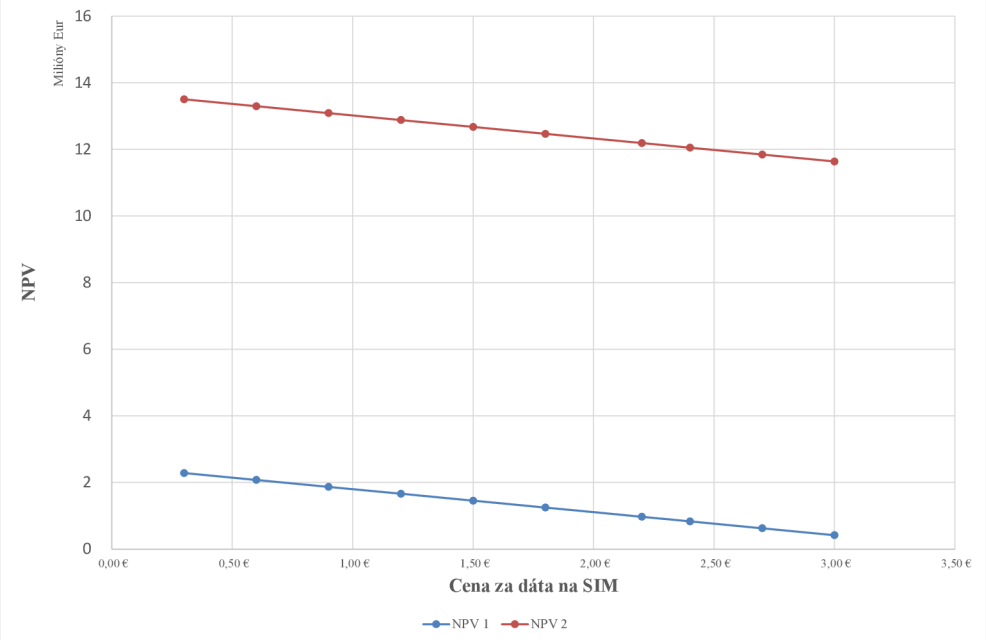
1. diskontná sadzba (WACC),
2. počet elektromerov,
3. počet rokov rolloutu,
4. údržba Key Management Systému,
5. údržba meradiel – minimálne zabezpečenie,
6. údržba meradiel minimálne zabezpečenie,
7. náklady na inštaláciu elektromera,
8. cena elektromera – minimálne zabezpečenie,
9. cena elektromera – optimálne zabezpečenie,
10. jednotková cena za SIM a dátový prenos – minimálne zabezpečenie,
11. jednotková cena za SIM a dátový prenos – optimálne zabezpečenie,
12. jednotlivé prínosy.

Pri skúmaní modelov majú niektoré parametre na ekonomický model projektu IMS väčší a niektoré menší vplyv. Najväčší vplyv má samozrejme výška jednotlivých nákladov (4-11), jednotlivé prínosy (12), diskontná sadzba (1) a najnižšiu kvantitatívny parameter projektu (3).
Pre vizualizáciu vplyvu jednotlivých vstupných parametrov som vybrala parametre ktoré menej ovplyvňujú model (napríklad cena SIM kariet a dátové služby) a pa-

rametre, ktoré viac ovplyvňujú model (cena elektromerov alebo výška prínosov). Keďže je ekonomický model tvorený metódou Net Present Value, vizualizácia je založená na porovnaní NPV 1 a NPV 2 jednotlivých modelov.

Popis parametrov, ktoré majú menší vplyv na ekonomický model

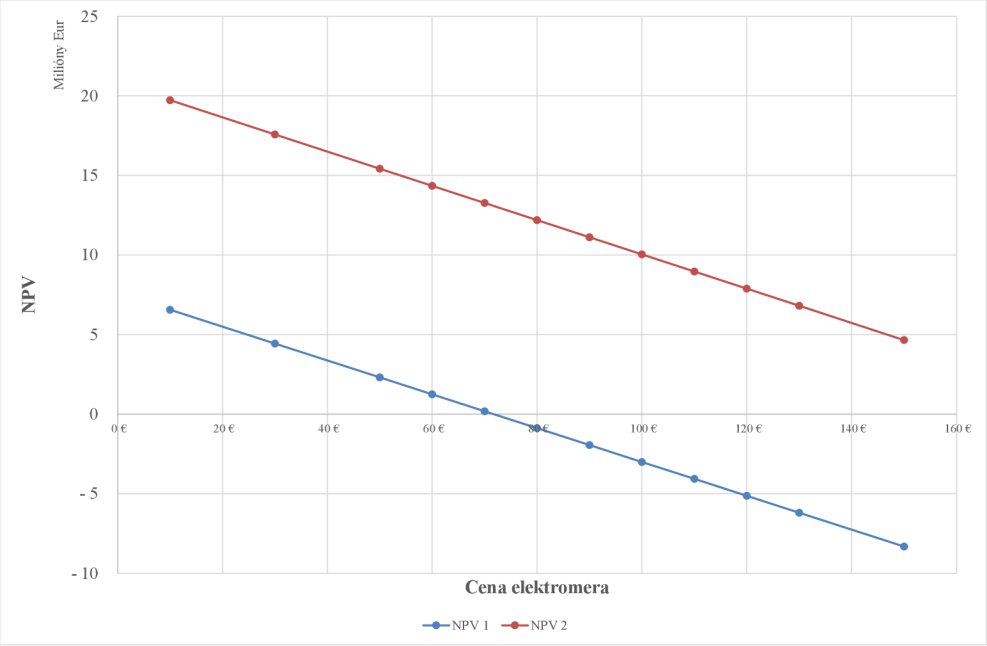
V následujúcom grafe 5.1 je znázornený vzťah čistých súčasných hodnôt na cene za prenos dát po komunikačnom kanáli pomocou GSM siete cez karty SIM. Tieto karty fungujú ako štandardné SIM karty, s výnimkou blokovania určitých služieb. Zvýšenie kybernetickej bezpečnosti nám prinesie zvýšenie objemu prenášaných dát kvôli použitiu šifrovanej komunikácie, hashovaniu a šifrovanému ustanoveniu kľúčov. Porovnanie reálneho toku dát pri dvoch rôznych úrovniach zabezpečenia je popísané v podkapitole 5.4. V našom prípade ma nárast toku dát minimálny vplyv na NPV a nepredstavuje kritický vstupný parameter NPV modelu. Súčasné trhové ceny za dátové služby nespôsobia záporné hodnoty NPV.



Obr. 5.1: Citlivosť NPV na výšku nákladov pre dáta a SIM karty.

V následujúcom grafe 5.2 je znázornený vzťah čistých súčasných hodnôt v závislosti na cene elektromera. Z pohľadu zvýšenia kybernetickej bezpečnosti sú potrebné elektromery so silnejšou hardvérovou výbavou, čo má logický vplyv na čistú súčasnú

hodnotu. V prípade modelu s minimálnou úrovňou zabezpečenia (NPV 1) vidíme, že sa krivka v určitom bode pretne s nulou čo znamená, že pri určitej cene elektromera v našom prípade ≈ 71 Eur za kus sa pri plnom rolloute (110 000 elektromerov) stáva stratovým. V našom prípade vplyv ceny elektromera na čistú súčasnú hodnotu optimálneho modelu (NPV 2) nepredstavuje kritický vstupný parameter kvôli tomu, že prínosy z odvrátenia rizík sú mnohonásobne vyššie ako je rozdiel cien elektromerov.

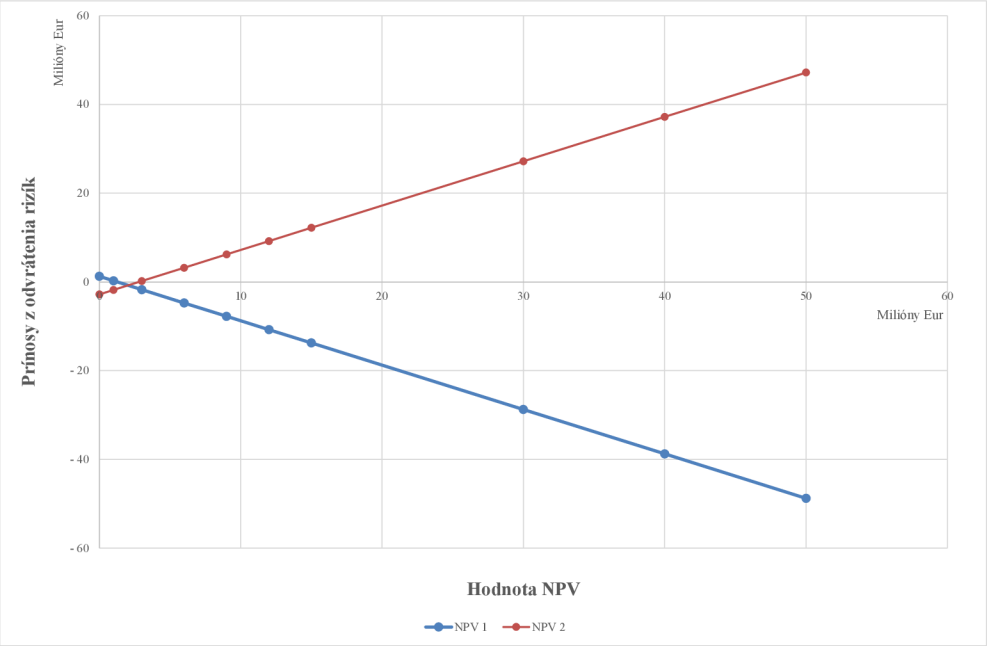


Obr. 5.2: Vplyv ceny elektromerov na ekonomický model.

Popis parametrov, ktoré majú výrazný vplyv na ekonomický model

V následujúcom grafe je vizualizovaný vplyv prínosov z odvrátenia rizika a následných strát. Tieto straty sú alokované do prínosov optimálneho modelu (NPV 2) a naopak pri minimálnom modeli zabezpečenia (NPV 1) sú tieto riziká alokované do nákladov. Tento graf je dôkazom toho, že stanovenie výšky investícií do kybernetickej bezpečnosti, ich správne použitie a minimalizácia rizík z odvrátenia možných kybernetických útokov je kritickým vstupným parametrom. Práve tento parameter poukazuje na zraniteľnosť nezabezpečeného systému, čo v konečnom dôsledku vedie

k finančným stratám v minimálnom modeli (NPV 1). Z tohto grafu jednoznačne vyplýva, že optimálny model zabezpečenia (NPV 2), aj keď je investične a prevádzkovo náročnejší eliminuje prípadné straty spôsobené kybernetickými útokmi.



Obr. 5.3: Vplyv prínosov z odvrátenia rizík.

Zhodnotenie ekonomického modelu a teoretického hodnotiaceho modelu rizík

Z výsledkov predošlých kapitol je jednoznačné, že stanovenie ekonomického rámca kybernetickej bezpečnosti, ktorý môžeme použiť na stanovenie hraničných podmienok pre výdavky na kybernetickú bezpečnosť je obzvlášť dôležitý krok. Tento predpoklad sa potvrdil aj vo vytváraní modelu *Gordon-Loeb Model* [12], kde sa profesori Gordon a Loeb snažili vyčísliť percentuálny pomer možných strát, ktoré ako aj v tejto práci, prevrátili a zobrazili do bezpečnostných prínosov. Po vykonaní týchto výpočtov stanovili hranicu investícií do zvýšenia bezpečnosti na maximálne 37 % z celkových potenciálnych strát vyplývajúcich z hrozieb. Ako však profesori skonštatovali, žiaden model nie je univerzálnym a každá spoločnosť si svoje vlastné riziká musí sama uvedomovať: *„However, this approach is best thought of as a framework, not a panacea, for making sound information-security investments. It is not a magical formula that can be used to churn out exact answers. Rather, it should be used*

as a complement to, and not as a substitute for, sound business judgment.“

5.4 Meranie parametrov GSM komunikácie pri rôznych typoch zabezpečenia

Počas zhotovovania tejto práce mi bola poskytnutá možnosť reálnych testov v laboratóriu využitím jedného z elektromerov implementovaných na východnom Slovensku. Toto meradlo je schopné pracovať v režime LLS (podkapitola 1.1.2) a v režime HLS (podkapitola 1.1.2) pri **Security suite 0** (tabuľka 1.1). Na odpočet profilov sa podľa Vyhlášky č. 358 Ministerstva hospodárstva Slovenskej republiky 2.4 využíva základný merací interval 15 minút. Odčítaval sa jednodenný profil a profil z desiatich dní. Využitím centrálneho systému boli porovnané a testované dostupné formy zabezpečenia a ich:

- čas odpočtu z elektromera do centrálneho systému,
- veľkosť komunikačného logu, ktorý sa odčítaval- súčasťou tohto logu je celý profil elektromera, nie iba namerané hodnoty.

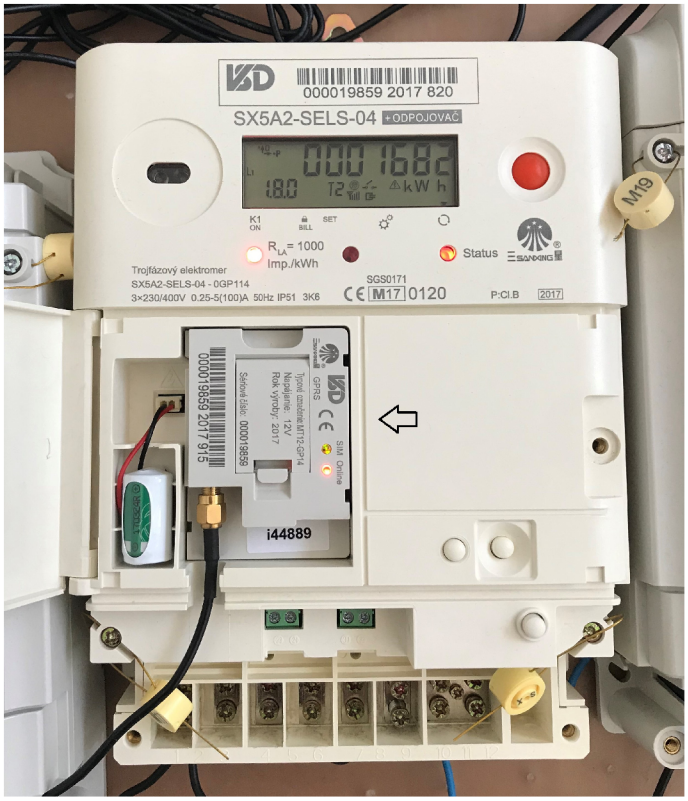
Tab. 5.7: Tabuľka parametrov z testovania elektromeru Sanxing.

Elektromer Sanxing	**LLS**		**HLS**	
Odpočet profilu (15 min)	Čas odpočtu	Veľkosť kom. logu	Čas odpočtu	Veľkosť kom. logu
1 deň	197 sekúnd	28 kB	242 sekúnd	34,7 kB
10 dní	1548 sekúnd	225 kB	1813 sekúnd	285 kB

Z tabuľky 5.7 vyplýva, že iba použitie HLS pri Security Suite 0 spôsobilo vzrast nie len veľkosti prenášaných dát ale aj času odpočtu. Zatiaľ čo v prípade LLS trval odpočet jednodňového profilu 3 minúty 20 sekúnd, odpočet pri využití šifrovanej komunikácie trval cez 4 minúty. Tento rozdiel ale nie je rapídny presne kvôli použitiu úrovne bezpečnosti zodpovedajúcej iba zašifrovaniu prenášaných správ šifrou AES-GCM-128. Táto úroveň zabezpečenej komunikácie nepoužíva digitálny podpis, hash ani šifrované ustanovenie kľúčov. Na obrázku 5.4 sa nachádza typ elektromera, ktorý bol použitý na test v laboratóriu. V ľavej časti elektromera je otvorený kryt, pod ktorým sa nachádza GSM modem, do ktorého je vložená karta SIM. Dióda na tomto modeme svieti čo signalizuje aktívnu službu.

Z výsledkov merania vyplýva, že so zvýšením objemu dát vyššou formou zabezpečenia bude mať každé zvýšenie bezpečnostnej úrovne vplyv aj na celkovú cenu služieb a tým pádom aj na výslednú čistú súčasnú hodnotu (NPV). Ako ale z kapitoly 5 a grafu 5.1 vyplýva, táto položka výslednú hodnotu prudko nezmení, pretože sa cena za prenos dát pomocou siete GSM pohybuje v priaznivých a prijateľných cenách pre

prevádzkovateľov distribučných spoločností. Hlavnou nevýhodou SIM kariet nie je cena dátovej komunikácie ale životnosť SIM karty, ktorá sa nemusí rovnať životnosti elektromera. Je teda možné, že k výmene SIM karty z dôvodu dožitia dôjde ešte pred skončením životnosti elektromera.



Obr. 5.4: Elektromer typu Sanxing SX5A2 použitý na meranie komunikácie.

Záver

Cieľom bakalárskej práce bolo v teoretickej časti preštudovanie problematiky bezpečnosti inteligentných elektromerov a analyzovanie využívaných algoritmov oblasti smart metering so zameraním na protokol DLMS/COSEM a uznávané autority. Tieto teoretické poznatky boli následne využité pri hodnotení dopadov kybernetickej bezpečnosti na prevádzkové, ekonomické a užívateľské aspekty. V závere práce bolo úlohou porovnať scenáre s minimálnymi a optimálnymi požiadavkami pre úroveň bezpečnosti. K tomuto účelu vznikol ekonomický model, ktorý využíva metodiku na porovnanie scenárov založenej na čistej súčasnej hodnote NPV.

Prvým krokom pri tvorbe bolo získanie čo najväčšieho množstva informácií a riešení od konkrétnych spoločností, ktoré sa problematike venujú alebo plánujú venovať. Jedná sa o prevádzkovateľov regionálnych distribučných spoločností v Českej a Slovenskej republike, a to konkrétne VSD (Východoslovenská distribučná, a.s.), PREdistribuce (Pražská Energetika – Distribúcia) a ČEZ Distribuce.

Obsahom prvej a druhej kapitoly je analýza bezpečnostných mechanizmov protokolu DLMS/COSEM a súhrn požiadavok na smart metering ako prvku kritickej infraštruktúry. Tretia a štvrtá kapitola sa venuje popisom súčasného stavu inteligentného merania v Českej a Slovenskej republike.

Piata kapitola sa venuje tvorbe teoretického hodnotiaceho modelu rizík založených na triáde CIA (Confidentiality, Integrity, Availability) a ekonomického modelu založeného na čistej súčasnej hodnote (Net Present Value – NPV). Model bol rozdelený do dvoch scenárov s rôznou úrovňou zabezpečenia. Samotný rollout inteligentného merania v Českej a Slovenskej republike bol daný vyhláškami [6, 7] (legislatívou danej krajiny) a ich ekonomický zmysel bol založený na Cost benefit analýzach (CBA) [15]. Táto práca neanalyzovala potvrdenie odhadovaných prínosov a nákladov pre jednotlivé rollouty inteligentného merania, ale skúmala náklady a prínosy minimálneho a optimálneho modelu zabezpečenia kybernetickej bezpečnosti.

Pri prvotnom skúmaní minimálneho a optimálneho modelu by sme mohli zdanlivo tvrdiť, že z finančného hľadiska je výhodnejším modelom práve model minimálny pre jeho nižšiu finančnú náročnosť, no práve pri analýze rizík a možných dôsledkov nezabezpečeného systému sa na základe modelu rizík ukazuje jeho zraniteľnosť. Táto zraniteľnosť v konečnom dôsledku povedie k finančným stratám, ktoré jednoznačne zvýhodnia optimálny model zabezpečenia, kde sú práve tieto riziká eliminované.

Tak ako rôzne hodnotiace modely napríklad [12], aj výsledky tejto bakalárskej práce odporúčajú spoločnostiam, ktoré prevádzkujú systémy na prenos a spracovanie citlivých dát, na odvrátenie neprimeraných škôd a poškodenie mena, správne vyhodnotiť možné riziká ich systémov a zvoliť efektívne metódy odvrátenia rizík.

Literatúra

[1] HOEVE, M.; PETERS, Ch. *Security requirements for procuring smart meters and data concentrators* [online]. Júl 2019, [cit. 2020-11-9].
Dostupné z: https://www.edsoforsmartgrids.eu/encs-and-e-dso-provide-first-set-of-harmonised-smart-meter-security-requirements/

[2] DLMS User Association. *Green Book Ed.9* [online]. 2019, [cit. 2020-11-9].
Dostupné z: https://www.dlms.com/files/Green_Book_Edition_9-Excerpt.pdf

[3] WEITH, L.J. *DLMS / COSEM protocol security evaluation* [online]. 2014, [cit. 2020-11-9].
Dostupné z: https://pure.tue.nl/ws/files/46962657/773263-1.pdf

[4] JU, Seung-Hwan; SEO, Hee-Suk. *Design Key Management System for DLMS/COSEM Standard-based Smart Metering* [online]. 2018, [cit. 2020-11-30].
Dostupné z: https://www.researchgate.net/publication/336251226_Design_Key_Management_System_for_DLMSCOSEM_Standard-_based_Smart_Metering

[5] *MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY* [online]. 2018, [cit. 2020-11-30].
Dostupné z: https://www.nukib.cz/download/uredni_deska/Kryptograficke_prostredky_doporuceni_v1.0.pdf

[6] *Vyhláška Ministerstva hospodárstva Slovenskej republiky* [online]. 2013, [cit. 2020-11-30].
Dostupné z: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2013/358/

[7] *Vyhláška č. 359/2020 o měření elektřiny* [online]. 2020, [cit. 2020-12-2].
Dostupné z: https://www.zakonyprolidi.cz/cs/2020-359

[8] *Zákon o kybernetickej bezpečnosti* [online]. Január 2018, [cit. 2020-12-2].
Dostupné z: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/69/

[9] *Vyhláška č. 233/2020 Ministerstva hospodárstva Slovenskej republiky* [online]. August 2020, [cit. 2020-12-2].
Dostupné z: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2020/233/

[10] *Výpočet nákladov na kapitál - WACC* [online]. September 2014, [cit. 2021-4-22]. Dostupné z: http://www.cfo.sk/articles/vypocet-nakladov-na-kapital-wacc#.YI07fLUzaXI

[11] *COMMISSION RECOMMENDATION on preparations for the roll-out of smart metering systems* [online]. Marec 2012, [cit. 2021-5-1]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32012H0148

[12] TODOR. *Cybersecurity Economics* [online]. August 2015, [cit. 2021-5-4]. Dostupné z: https://www.cybervelocity.com/cybersecurity-economics-for-cio-and-ciso/

[13] *Hodnoty parametrov pre roky 2020 - 2021 na výpočet maximálnej miery výnosnosti regulačnej bázy aktív WACC* [online]. 2020, [cit. 2021-5-4]. Dostupné z: http://www.urso.gov.sk/?q=Informa%C4%8Dn%C3%BD%20servis/Plyn%C3%A1renstvo/Hodnoty%20parametrov%20WACC%20pre%20rok%202020-2021

[14] HENNYEYOVÁ, K.; GERHÁTOVÁ, G. *Bezpečnostné aspekty spracovania informácií* [online]. [cit. 2021-5-16]. Dostupné z: https://spu.fem.uniag.sk/mvd2016/proceedings/sk/articles/hennyeyova_gerhatova.pdf

[15] *Study on cost benefit analysis of smart metering systems in EU Member States* [online]. [cit. 2021-5-18]. Dostupné z: https://ec.europa.eu/energy/content/study-cost-benefit-analysis-smart-metering-systems-eu-member-states_en

[16] *Confidentiality, Integrity And Availability – The CIA Triad* [online]. [cit. 2021-5-20]. Dostupné z: https://www.certmike.com/confidentiality-integrity-and-availability-the-cia-triad/

[17] *OPEX (Operational Expenditures)* [online]. 2015, [cit. 2021-5-20]. Dostupné z: https://managementmania.com/sk/opex-operational-expenditures

[18] *CAPEX (Capital Expenditures)* [online]. 2015, [cit. 2021-5-20]. Dostupné z: https://managementmania.com/sk/capex-capital-expenditures

[19] *Čistá súčasná hodnota (NPV). (Net Present Value (NPV))* [online]. [cit. 2021-5-20].
Dostupné z: https://investopedia.sk/2020/10/22/cista-sucasna-hodnota-npv-net-present-value-npv/

Zoznam symbolov, veličín a skratiek

OSI	Open Systems Interconnection
AA	Application Association
AES-GCM	Advanced Encryption Standard-Galois Counter Mode
GCM	Galois Counter Mode
AAD	Additional Authenticated Data
EK	Encryption key
IV	Inizialization vector
OID	Object Identifier
ACSE	Association Control Service Element
LLS	Low Level Security
HLS	High Level Security
NÚKIB	Národný úrad pre kybernetickú bezpečnosť
ENCS	European Network for Cyber Security
WAN	Wide Area Network
NCSC	National Cyber Security Centre
PDS	Prevádzkovateľ Distribučnej Sústavy
OM	Odberné Miesto
TP	Technický Parameter
IMS	Inteligentný Merací Systém
GSM	Global System for Mobile Communications
PLC	Power-Line Communication
HDS	Head End System
DT	Datová Trafostanica
PDS	Prevádzkovateľ Distribučnej Sústavy

EK	Európska komisia
WACC	Weighted Average Cost of Capital
OPEX	Operating Expense
CAPEX	Capital Expense
NET	Net Present Value
CIA	Confidentiality, Integrity, Availability
ÚRSO	Úrad pre reguláciu sieťových odvetví
ERÚ	Energetický regulační úřad
SIM	Subscriber Identification Module
BPL	Broadband Powerline
CBA	Cost Benefit Analysis