Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Návrh zabezpečení systému AMM v souladu s požadavky ISO 27001

Diplomová práce

Autor: Bc. Radomír Werner
Studijní obor: IM2-K

Vedoucí práce: Mgr, Josef, Horálek Ph.D.

Odborný konzultant: Titul, jméno, příjmení
Pracoviště

Hradec Králové Duben 2023

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

vlastnoruční podpis

V Hradci Králové dne 28.4.2023 Radomír Werner

Poděkování:

Děkuji vedoucímu diplomové práce Mgr. Josef Horálek Ph.D. za metodické vedení práce a odbornou pomoc při vypracování některých složitějších částí diplomové práce.

Anotace

Obsahem diplomové práce je řešení kybernetické bezpečnosti v rámci organizace, která provozuje AMM měření. V rámci kybernetického řešení také někdy užíváme zkratku (ISMS). V práci je shrnuto, jakým způsobem by se mělo postupovat a co všechno musí splňovat návrh kybernetické bezpečnosti AMM měření podle platné normy ISO/IEC 27001:2013 a její implementaci ISO/IEC 27002:2013. V této normě jsou specifikovány určité oblasti, které je nutné vzít v úvahu při návrhu zabezpečení. Pro účely této práce jsou však použity jen části normy, které jsou zaměřeny přímo na měřící zařízení AMM, a ne na organizační strukturu jako takovou. Dále jsou zde popsány základní principy AMM měření. Součástí práce je také BIA analýza dat, jenž je nutné v rámci kybernetické bezpečnosti ochránit jako cenná aktiva.

Annotation

Title: Security design of the AMM system in accordance with the requirements of ISO 27001

The content of the diploma thesis is the solution of cyber security within the organization that operates AMM measurements. We also sometimes use the abbreviation (ISMS) as part of cyber solutions. The work summarizes how the procedure should be followed and what must be met by the cyber security design of the AMM measurement according to the valid standard ISO/IEC 27001:2013 and its implementation ISO/IEC 27002:2013. This standard specifies certain areas that must be considered in security design. However, for the purposes of this work, only parts of the standard are used that are aimed directly at AMM measuring devices and not at the organizational structure as such. Furthermore, the basic principles of AMM measurement are described here. The work also includes BIA analysis of data, which must be protected as valuable assets within the framework of cyber security.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

V dnešní době jde rozvoj ve všech oblastech společnosti mílovými kroky kupředu, vše se postupně digitalizuje a s nástupem internetu věcí je vše postupně online včetně například domácích spotřebičů. Pozadu nezůstává i energetika, kde byla vydaná nová vyhláška o měření č. 359/2020 Sb. Která přímo nařizuje od roku 2027 osazení měření s dálkovou komunikací u odběrných míst typu měření C. U tohoto typu měření se dnes provádí odečet spotřebované energie za pomocí pracovníků v terénu, což by rázem odpadlo. S touto změnou ve vyhlášce ovšem přichází na řadu otázka bezpečnosti dálkové komunikace mezi provozovatelem distribuční soustavy a měřením. Za tímto účelem je tedy nutné správně navrhnou, jakým způsobem se bude měření dle nové vyhlášky provozovat, tak aby byla zákazníkovi zajištěna bezpečná dodávka elektrické energie. Pro tyto účely je vhodné možná i nezbytné postupovat podle určitých standardů, které byly navrženy a odsouhlaseny mezinárodními organizacemi. Jedním ze standardů zabývajícím se zabezpečením je mezinárodně uznávaná norma ISO 27001, které se z velké části věnuje tato diplomová práce. V této práci jsou obsaženy výňatky z normy a jejího popisu implementace obsažené v normě ISO 27002 doplněné o praktické příklady užití v rámci budoucího měření AMM. Jako příklad provozovatele AMM měření je zde uvedena největší distribuční společnost u nás ČEZ Distribuce a.s. Dále je zde provedena analýza rizik BIA a CIA, které určují dopady na organizaci, pokud by nebylo komplexně vyřešeno zabezpečení celého systému měřením. Na závěr na základě poznatků z analýzy je v rámci BCM popsáno, která data z měření jsou důležitá, jakým způsobem je nutné zvolit opatření tak, aby bylo možné měření AMM bezpečně provozovat.

2 Cíl práce

Cílem práce je zmapovat bezpečnostní opatření navržené v rámci normy ISO/IEC 27001 a její implementace ISO/IEC 27002. V rámci popisu důležitých částí, normy je zároveň uveden příklad zavedení dané problematiky kolem zabezpečení AMM měření do praxe. Dalším cílem bylo provést BIA a CIA analýzu nad částmi celého systému AMM měření a informačními aktivy, které jsou se systémem svázané. Analýza má za úkol zmapovat nejen rizika a možné dopady na organizaci, ale její výsledek je použit na určení opatření v rámci BCM na závěr práce. V celé práci se klade důraz na praktické využití v distribučních společnostech, které měření hojně využívají v distribuční soustavě, proto je i zde vše uvedeno na příkladu ČEZ Distribuce a.s.

3 Metodika zpracování

Diplomová práce je tvořena několika body v rámci kybernetické bezpečnosti, které jsou v souladu s používanou metodikou zavádění a jsou důležité pro správný chod organizace:

- Popis zavádění ISMS v organizaci a definice všech kroků při jeho zavádění a začlenění do organizace.
- Definice ISO normy a konkrétní popis normy ISO/IEC 27001.
- Využití výňatku z implementace normy ISO/IEC 27002 pro využití v praxi v rámci zavádění AMM měření v organizaci a obecné shrnutí požadavků, které jsou zaměřené na zabezpečení celého systému, tak aby splňovali minimálně uvedenou normu.
- Provedení komplexní dopadové BIA analýzy nad konkrétním systémem AMM u organizace ČEZ Distribuce a.s. pro určení rizik nedostupnosti služeb a jejich dopadů na organizaci.
- Provedení CIA analýzy nad důležitými informačními aktivy distribuční společnosti v rámci systémů AMM měření.
- Vyhodnocení výsledků analýz a integraci jejich opatření v rámci BCM.

Všechny výše uvedené body mají za cíl, zhodnotit rizika při zavádění ISMS v organizaci do praxe a minimalizaci způsobených škod, v případě nedokonale navrženého systému.

4 Problematika ISMS

Zkratka ISMS (Information Security Management System), již z jejího názvu je patrné, že se zabývá bezpečností informací a je součástí řízení organizace. Implementace druhu zabezpečení v rámci ISMS do firmy je dnes již celkem standard. [3]

4.1 Definice ISMS

Definice dle normy: „Information Security Management System je součást řízení organizace, založená na přístupu k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací.“ Oblasti, kterých se ISMS týká jsou hlavně:

- IT bezpečnost;
- Komunikační bezpečnost;
- Personální bezpečnost;
- Administrativní bezpečnost;
- Fyzická bezpečnost;
- Dokumentace;
- Bezpečnostní funkce a mechanismy.

Z definice je tedy patrné, že jde o souhrn bezpečnostních opatření, která jsou systematická a většinou podpořená i určitou normou například ISO. [3]

4.2 Etapy zavádění ISMS

Zavádění ISMS se při zavádění do provozu v organizaci dělí do různých etap, které jsou více či méně důležité. Tento způsob zavádění by měl pomoci k vyšší efektivitě využití všech bezpečnostních opatření. [3]

4.2.1 Krok první

Jako základ v prvním kroku je nutný souhlas společnosti se zaváděním konkrétních bezpečnostních opatření dle určené normy. Vedení společnosti, ve které se ISMS zavádí, musí dle požadavků dát souhlas s nasazením nového systému a díky tomu se zároveň zavázat, že bude zavádění ISMS podporovat. Vše je nutné

zdokumentovat a nejlépe certifikovat pro případný audit. Pokud by nebyl o tomto kroku společnosti zhotoven žádný dokument, nemohlo by dojít k nasazení systému řízení bezpečnosti. [3]

4.2.2 Krok druhý

Jde o krok, který spočívá v identifikaci aktiv a jejich ocenění což se provádí například inventurou, poté se jednotlivá aktiva ohodnotí za pomocí atributů z CIA analýzy, které jsou tři, jedná se o dostupnost, důvěrnost a integritu. Následně se provede systematicky analýza rizik, tomuto dokumentu je kladena ta nejvyšší důležitost, protože na něm je postaven celý systém. Pokud tedy nebude kvalitně zpracován, může se stát celý systém ISMS nefunkčním. [3]

4.2.3 Krok třetí

Dalším z dokumentů, který je nutné v rámci ISMS vypracovat je návrh opatření, ten je vytvořen na základě analýzy a vyhodnocených rizik. Nejdříve jsou nalezena kritická místa na základě bezpečnostních potřeb, poté jsou určeny priority, podle kterých jsou vybrána bezpečnostní opatření. Tento dokument je v rámci ISMS stěžejní. V případě extrémního nepoměru mezi rizikem, které bude velmi nízké a náklady na opatření, které mohou být neúměrně vysoké, se může provést tzv. akceptace rizika. Podle platné normy se také musí vytvořit dokument s prohlášením o aplikovatelnosti. [3]

4.2.4 Krok čtvrtý

Je certifikace, tento krok je nepovinný, není ho tedy nutné provádět, protože ISMS může fungovat i bez toho. Certifikace se skládá ze dvou částí, první je certifikovaná dokumentace, která je pro tento úkon nezbytná. V druhém kroku se kontroluje praktické zavádění ISMS. Pro tyto účely se využívá certifikace ISO 9001 a ISO 27001, jsou totiž kompatibilní. [3]

5 ISO

Normy ISO (International Organization for Standardization) jsou mezinárodní standardy, vydávané mezinárodní organizací pro normalizaci. Tato organizace funguje mezinárodně a normalizuje technické činnosti. Hlavní sídlo ISO je v Ženevě, tato organizace byla založena v roce 1946 a jejím účelem bylo

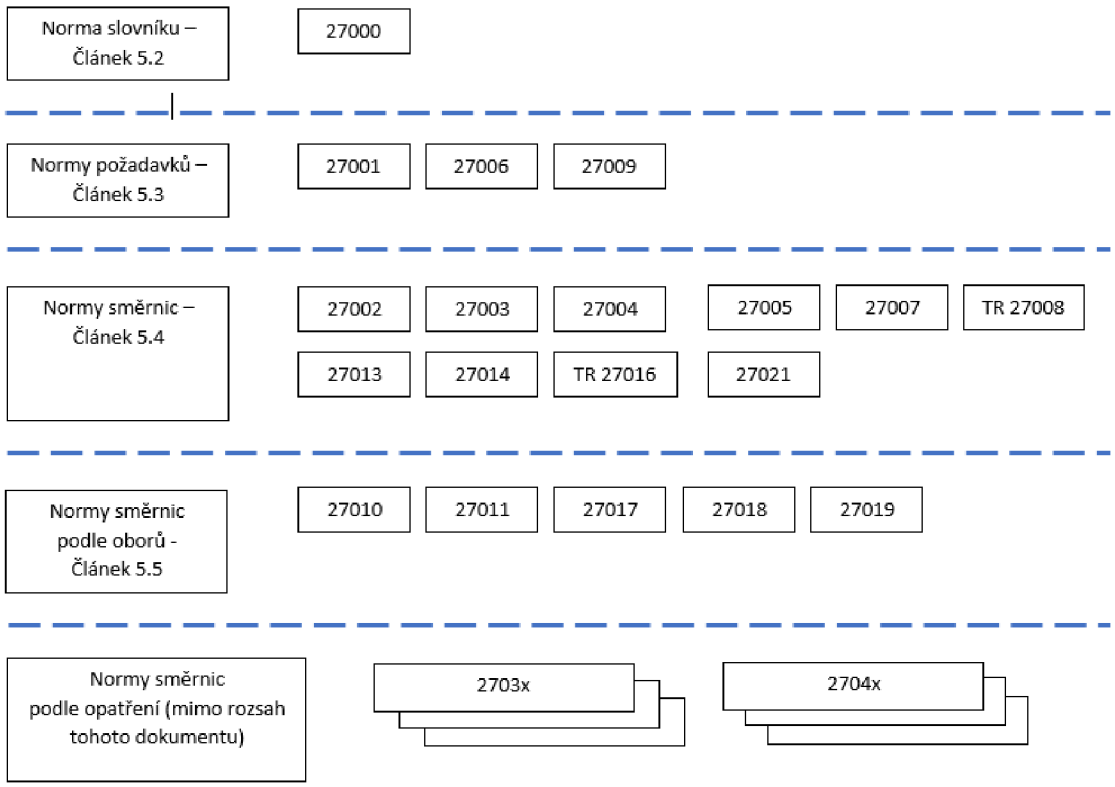
normalizovat technické činnosti v oblasti vědy, techniky a hospodářství. Jedním ze zakládajících členů byla i Československá republika.

Standardy ISO byly vytvářeny technickou komisí, která měla určenou vždy určitou oblast působnosti. Pokud dojde k vytvoření návrhu nějakého standardu v určité oblasti, tak o něm vždy hlasují jednotliví členové Mezinárodní organizace pro normalizaci (ISO), stejnou zkratkou se následně označuje i vydaný standard. Normy ISO jsou dobrovolné a jsou zároveň promítány do norem ČSN například s označením ČSN EN ISO 9001:2016.

Většina moderních firem má snahu splnit všechny požadavky ISO norem, kvůli větší prestiži a zvyšování efektivity. Některé firmy zároveň staví na certifikaci ISO i svou existenci. Dále si díky splnění certifikace firma potvrdí, že prostředky vynaložené na systém zabezpečení nebyly vynaloženy úplně zbytečně a systém ISMS dosahuje dostatečné kvalitativní úrovně. [3] [8] [9]

5.1 Požadavky z ISO 2700x

Obsahem této konkrétní normy je systém řízení bezpečnosti informací v kontextu organizace. V normě jsou zahrnuty požadavky a posouzení rizik bezpečnosti informací, které jsou upravené pro potřeby organizace a jejich případné ošetření. Norma by měla být aplikovatelná v jakékoliv organizaci. Pokud by chtěla organizace získat shodu s touto normou, nesmí vyloučit jakýkoliv požadavek uvedený v této normě. Pro potřeby vypracování diplomové práce bude využita pouze část z této normy, která se týká přímo uvedeného tématu přenosu dat a jejich zabezpečení. Souhrn požadavků je uveden v příloze ČSN ISO/IEC 27001:2013, soubor postupů, opatření a implementace je v ISO normě ČSN ISO/IEC 27002:2013. Vztahy mezi těmito normami jsou zobrazeny níže (Obr. 1). [8] [9]



Obr. 1 Vztahy mezi normami řady ISMS,
zdroj: ČSN ISO/IEC 27000:2020

5.2 Mobilní zařízení a práce na dálku

V tomto bodu je nutné zajistit bezpečnost práce na dálku a při použití mobilních zařízení, případně připojení pomocí PC z privátní či veřejné sítě. [8] [9]

5.2.1 Politika mobilních zařízení

Dle normy je u mobilních zařízení nutné se věnovat převážně zabezpečení informací, které by mohli být využity ke kompromitování organizace (firmy). Dále by měla být věnována pozornost oblasti použití mobilních zařízení, převážně je nutné se zaměřit na použití v nechráněných prostředích.

Začíná to registrací mobilních zařízení, nebo požadavky na fyzickou ochranu, dále omezení v rámci instalace softwaru, požadavky na verze a aktualizace systému, omezení pro připojení k různým informačním službám, řízení jednotlivých přístupů, kryptografii a ochranu proti malwaru. Další částí je řešení vzdálené správy zařízení (nalezení, blokování, mazání), zálohování a využívání služeb na webu a u webových aplikací.

U mobilních zařízení se musí klást důraz na bezpečnost při použití na veřejných místech, tak aby bylo co nejlépe zamezeno se dostat k datům organizace neoprávněnou osobou. Případně zamezit krádeži či ztrátě zařízení. Pokud by došlo ke ztrátě nebo k odcizení zařízení, tak je nutné mít zařízení adekvátně zabezpečené, také je nutné pravidelně školit uživatele. Zařízení celkově rozdělit na pracovní a soukromé účely včetně prostředí a paměť zařízení.

V rámci provozování měření AMM se počítá s tím, že uživatel bude mít k dispozici koncové mobilní zařízení pro přímou komunikaci s měřícím zařízením (elektroměrem) přes optické rozhraní. Tento druh komunikace je nutný pro prvotní aktivaci a nastavení zařízení, případně pro odečet hodnot a nastavení, pro případ nefungující dálkové komunikaci. Zabezpečení zařízení, sloužící pro tyto účely by mělo být zabezpečeno způsobem minimálně takovým, jak uvádí (ČSN ISO/IEC 27002 v kapitole 6.2). [8] [9]

5.2.2 Práce na dálku

V případě práce na dálku je nutné zavést podpůrná bezpečnostní opatření. Při práci na dálku se musí vždy vydat určitá bezpečnostní politika, která řeší zákonem povolené opatření tak, aby připojení splňovalo nejlépe tato kritéria (ČSN ISO/IEC 27002 kapitola 6.2).

V normě je uvedeno že se musí přihlížet k prostředí odkud se uživatel připojuje, důraz se klade především na bezpečnost přenosu, a to i při tvorbě systému připojení na dálku a k citlivosti interního systému. V případě připojení na virtuální vzdálenou plochu ze soukromého zařízení je nutné zamezit ukládání dat do těchto zařízení. Znemožnit přístup do sítě organizace neautorizovaným osobám. Při využití domácí sítě omezit nastavení bezdrátových síťových služeb. Politika za účelem zabránění případných sporů o duševní vlastnictví. Nutná ochrana před malware a požadavek na firewall.

V rámci řešení této problematiky je nutné zavést směrnice a opatření, které by měli zahrnovat optimální a povolené vybavení pro práci na dálku. Toto zařízení by mělo být pod kontrolou organizace. Dále také by mělo řešit fyzickou bezpečnost, hardwarovou a softwarovou podporu, pojištění, zálohu a kontinuitu, audit a monitorování bezpečnosti. Dále pak řešení přístupových práv v rámci zřízení? a ukončení práce na dálku. Zjednodušeně lze tedy říci, že se musí v rámci práce na

dálku ošetřit veškeré možnosti vzdáleného přístupu tak, aby nedošlo ke zneužití nebo neoprávněnému přístupu k informacím organizace. [8] [9]

U AMM měření by se mělo vymezit připojení na dálku pouze pro zařízení vlastněné firmou, důvodem je omezení složitosti zabezpečení. Jednodušší je v tomto ohledu, pokud by bylo zakázáno používat pro připojení soukromá zařízení. V případě AMM měření by se totiž nepřistupovalo na dálku pouze k jednomu měřícímu zařízení, ale k více najednou. Za pomoci různých aplikací je provedeno stahování dat z měření pro jejich úpravy a další zpracování. Dále se také počítá s tím, že bude možné měřící zařízení vzdáleně v omezeném režimu nastavovat. Proto je politika použití pouze firemních zařízení lepší a bezpečnější variantou nad rámec normy, která toto jako jedinou možnost přístupu do firemní sítě striktně nevyžaduje.

5.3 Řízení aktiv

V oblasti řízení aktiv se norma odkazuje na vytvoření seznamu aktiv, které souvisejí se zpracováním informací. Seznam informačních aktiv by měl být uchováván stále aktuální.

V organizaci by mělo dojít ke zmapování všech aktiv a u každého z nich zdokumentovat jakým způsobem se s nimi nakládá, jejich vznik, zpracování, ukládání, přenos, vymazání a zničení. Tyto seznamy ještě více zefektivní ochranu a jdou následně využít také za jinými účely. V normě se klade důraz na to, aby seznam aktiv byl přesný, aktuální, konzistentní a uspořádaný s dalšími inventáři. Příklady aktiv lze najít také v přidružené normě ISO/IEC 27005.

U aktiv je nutné určit vlastníka, který by měl mít k aktivům přístup a zajistit jejich inventarizaci, klasifikaci, přístupy a zajistit správné zacházení. Osoba s přístupem k aktivům by měla mít také určená pravidla pro použití aktiv a případně informace o postupu vrácení aktiv, pokud dojde k ukončení smlouvy v rámci, které aktiva využívá a zpravuje. K dalšímu rozlišení slouží klasifikace a označení informací, to je velmi důležité pro posouzení právních požadavků na informace o aktivech.

Pro účely AMM je důležité určit, ke kterým aktivům bude mít daný zaměstnanec přístup například dle pracovní pozice. Za tímto účelem mu budou poskytnuty zařízení či nástroje pro přístup k určeným aktivům. Předpokládá se, že

v měření AMM jsou aktivy údaje o zákaznicích, zaměstnancích a obchodních partnerech, hlavně pak naměřená data z přístrojů a dále také veškeré nástroje pro jejich zpravování. Pro zjednodušení zabezpečení těchto aktiv je vhodné používat pouze zařízení a média v majetku společnosti a to taková, co nepůjdou použít mimo její síť, případně systém. Vše se totiž při procesu nakládaní s aktivy zjednoduší. [8] [9]

5.4 Řízení přístupu

Pokud jde o řízení přístupu, tak je vždy nutné určit přístupovou politiku, kterou se musí vše řádně přezkoumat a zdokumentovat. Opatření v rámci řízení přístupu se dělí na logická či fyzická a jsou zvažována společně. Zvolená politika přístupu by měla brát v úvahu bezpečnostní požadavky v organizaci, politiku šíření a autorizace informací, přístupová práva a jejich přidělování v rámci klasifikace informací případně celkovou zprávu přístupových práv. Za tímto účelem je nutné určit pravidla v různých oblastech organizace, například přístup k sítím a síťovím službám nebo přístupy určené podle šíře oprávnění uživatelů. [8] [9]

Přidělování přístupových práv u AMM měření je vhodné stanovit podle úrovní a typu zařízení. Uživatel, který bude fyzicky nakládat s přístroji za účelem montáže na odběrném místě u zákazníků bude mít nejnižší přístupová práva, a to jen například synchronizace času, případně odečet hodnot nebo přenastavení sazby dle předem zaslaných dat přímo u zákazníka. Uživatel, který provádí nastavení měřicích zařízení pro konkrétní odběrné místo bude moci přistupovat do měřicího zařízení u zákazníka i vzdáleně pomocí obslužného softwaru a bude moci provést odečet dat, rekonfiguraci přístroje, či za účelem odpojení nebo vypnutí. Dalším druhem přístupu bude například pro výrobce či metrology za účelem kalibrace nebo manipulace s hardwarem či softwarem přístroje. Každá úroveň by měla mít určená přístupová práva u kterých je zapotřebí snižovat či zvyšovat zabezpečení ruku v ruce s šířkou přístupových oprávnění. Pracovník v terénu u zákazníka bude mít tedy nejnižší úroveň, kdežto výrobce či metrolog bude muset pro svou činnost mít nejvyšší úroveň zabezpečení.

5.5 Kryptografie

V případě kryptografie jde o velmi důležitý bod. Zvolená kryptografická opatření mají zásadní vliv na bezpečnost celého systému. V normě je uvedeno, že použití správného druhu kryptografických opatření závisí především na manažerském rozhodnutí, aby vše kolem šifrování a klíčů bylo v souladu s bezpečnostní politikou celé organizace. Týká se to jak použitého šifrování, tak i nakládání s kryptografickými klíči, nutné je především určit odpovědnost za vydávání a ochranu kryptografických klíčů a jejich celkový životní cyklus. V oblasti klíčů by měli být správně zvoleny kryptografické algoritmy v souladu s požadavky a doporučenými postupy.

Kryptografické opatření by mělo být v rámci AMM řešeno a konzultováno ve spolupráci s NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost) na doporučení ENISA (European Network and Information Security Agency) a jiných úřadů, protože se v tomto případě může jednat například při napadení komunikace s velkým množstvím elektroměru i o celostátní problém, energetika se totiž všeobecně označuje jako kritická infrastruktura. Agentura ENISA většinou nespecifikuje konkrétní požadavky na kybernetickou bezpečnost inteligentních sítí, pouze dává doporučení. Pro analýzu požadavků ENISA byly použity dostupné dokumenty na stránkách této organizace www.enisa.europa.eu. Pokud je řešeno kryptografické zabezpečení u jakéhokoliv systému, tak je vždy nutné uvažovat jaké šifry budou na zabezpečení využity.

Na stránkách agentury ENISA jsou na toto téma uvedeny různé studie. Jedna se zajímavých studií se zabývá nově uvažovaným typem šifrování, která by měla zajistit prolomení pomocí kvantového počítače. Jde o postkvantovou kryptografii (PCQ), ve studii je popsáno, jakým způsobem by mohlo probíhat takové šifrování. Zatím však není žádná metoda kvantového šifrování standardizovaná, je to z toho důvodu, že se zatím neobjevil žádný kvantový počítač, který by byl dostatečně výkonný, aby v reálném čase dokázal prolomit současné šifry. Vědci se také domnívají, že k tomu v dohledné době ani nedojde. Jednou z kandidátských postkvantových šifer testovanou NIST (National Institute of Standards and Technology) je CRYSTALS-Kyber, jako jedna z mála by se mohla v brzké době standardizovat, zatím však je toto hudba budoucnosti a dnešní doporučené šifry by měli dle předpokladů ještě nějakou dobu vydržet. [7]

Při návrhu šifrování je nutné vycházet nejlépe z doporučení národních úřadů zabývajících se kybernetickou bezpečností. Pro Českou republiku například na stránkách NUKIB je uvedená vždy aktuální informace o doporučených šifrách a o jejich bezpečnosti. Na stránkách jsou také vždy uvedeny schválené šifry doporučené a dosluhující. [4] [7] [8] [9]

5.5.1 Symetrické algoritmy

a) Schválené blokové a proudové šifry

- Advanced Encryption Standard (AES) s délkou klíčů 128, 192 a 256 bitů
- Twofish s využitím délky klíčů 128 až 256 bitů
- Camellia s využitím délky klíčů 128, 192 a 256 bitů
- Serpent s využitím délky klíčů 128, 192, 256 bitů
- SNOW 2.0, SNOW 3G s využitím délky klíčů 128, 256 bitů
- ChaCha20 s délkou klíče 256 bitů se zatížením klíče menším než 256 GB

b) Doporučené blokové a proudové šifry

- Použití blokových šifer před proudovými.
- V případě blokových šifer: AES, Camellia a Serpent (v uvedeném pořadí).
- Délku klíče 256 bitů.

c) Dosluhující blokové a proudové šifry

- Triple Data Encryption Standard (3DES) s využitím délky klíčů 112 bitů, omezené použití jen se zatížením klíče menším než 10 MB, postupně přecházet na AES. Doporučeno použití jedinečného klíče pro každou zprávu.
- Blowfish s využitím minimální délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB.
- Kasumi s využitím délky klíčů 128 bitů, omezené použití jen se zatížením klíče menším než 10 GB.

5.5.2 Asymetrické algoritmy

a) Schválené algoritmy pro technologii digitálního podpisu

- Digital Signature Algorithm (DSA) s využitím délky klíčů 3072 bitů a více, délky parametru cyklické podgrupy 256 bitů a více
- Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 256 bitů a více
- Rivest-Shamir-Adleman Probablistic Signature Scheme (RSA-PSS) s využitím délky klíčů 3072 bitů a více
- Elliptic Curve Schnorr Signature Algorithm (EC-Schnorr) s využitím délky klíče 256 bitů a více

b) Dosluhující algoritmy pro technologii digitálního podpisu

- Digital Signature Algorithm (DSA) s využitím délky klíčů 2048 bitů, délky parametru cyklické podgrupy 224 bitů
- Elliptic Curve Digital Signature Algorithm (EC-DSA) s využitím délky klíčů 224 bitů
- Rivest-Shamir-Adleman Probablistic Signature Scheme (RSA-PSS) s využitím délky klíčů 2048 bitů
- Elliptic Curve Schnorr Signature Algorithm (EC-Schnorr) s využitím délky klíče 224 bitů

c) Schválené algoritmy pro procesy dohod na klíči a šifrování klíčů

- Diffie-Hellman (DH) s využitím délky klíčů 3072 bitů a více, délky parametru cyklické podgrupy 256 bitů a více
- Elliptic Curve Diffie-Hellman (ECDH) s využitím délky klíčů 256 bitů a více
- Elliptic Curve Integrated Encryption System – Key Encapculation Mechanism (ECIES-KEM) s využitím délky klíčů 256 bitů a více
- Provably Secure Elliptic Curve – Key Encapculation Mechanism (PSEC-KEM) s využitím délky klíčů 256 bitů více
- Asymetric Ciphers and Key Encapculation Mechanism (ACE-KEM) s využitím délky klíčů 256 bitů a více
- Rivest Shamir Adleman – Optimal Asymetric Encryption Padding (RSA-OAEP) s využitím délky klíčů 3072 a více
- Rivest Shamir Adleman – Key Encapsulation Mechanism (RSA-KEM) s využitím délky klíčů 3072 a více [4] [7] [8] [9]

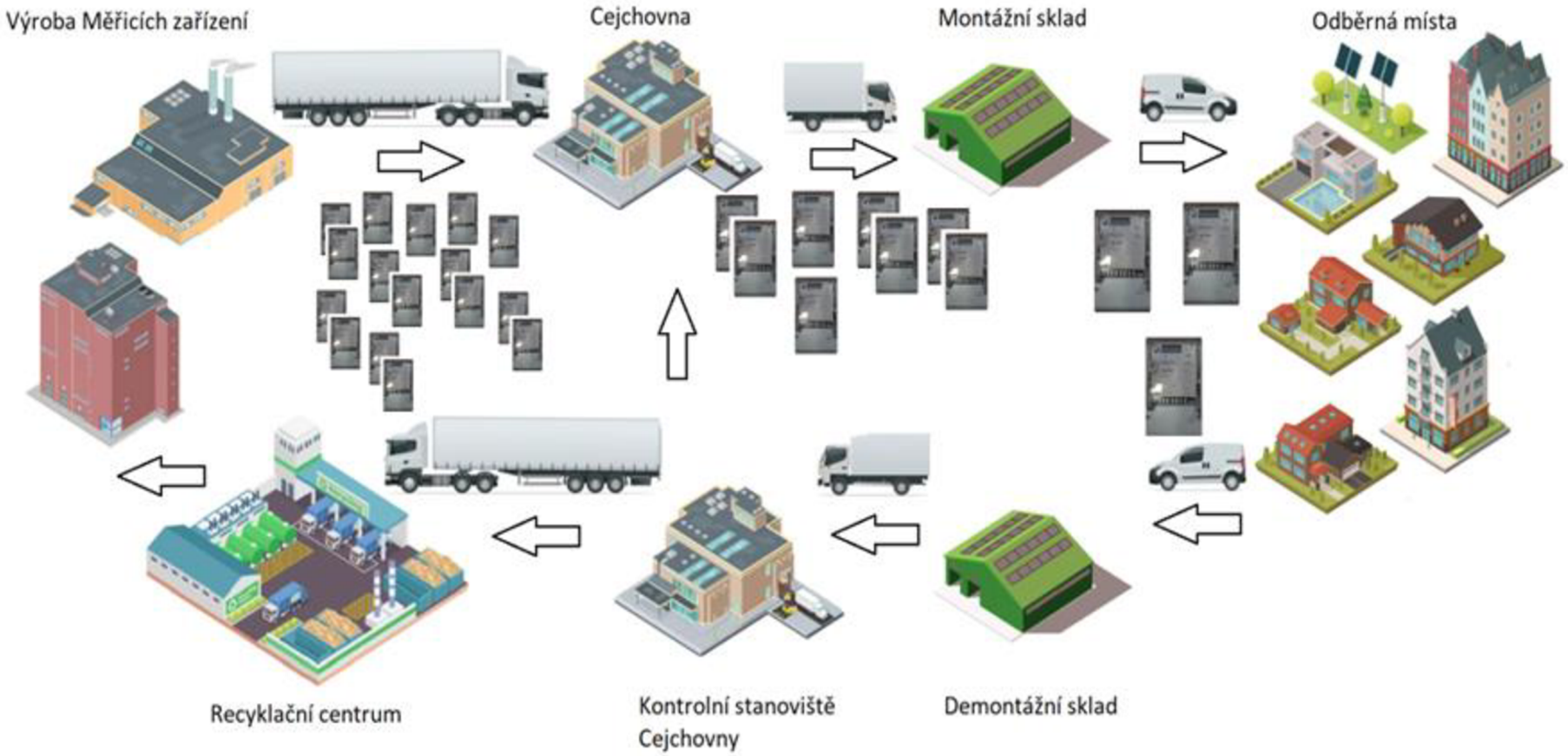
V případě měření AMM je nutné také uvažovat v dlouhodobějším horizontu z hlediska možného prolomení šifer. Životnost měřidla AMM pro přímé měření je dle metrologického zákona 12 let (statické měřidlo) a pokud budeme uvažovat o tom, že se měřidlo bude znovu ověřovat tak se životnost prodlouží o dalších 12 let. Proto tedy je nutné uvažovat o šifrách, které budou bezpečné alespoň po dobu 24let do ukončení životního cyklu měřidla. Životnost měřidel se dá také prodloužit ještě pomocí tzv. SVZ (Statistickou výběrovou zkouškou) jde o proces při kterém se vezmou vzorky elektroměrů stejného materiálového typu a provede se na nich ověření a testy. Pokud tyto měřidla projdou, tak je následně prodloužena jejich životnost o další 4 roky (na 16 let), proto je nutné v této oblasti uvažovat dlouho do budoucnosti. Odhadovaná životnost šifrování je uvedena v tabulce 1.

Tabulka 1 Kryptografické požadavky
Zdroj: Výtah studie ze VUT o KB (mpo.cz) [4] [7]

Kryptografické požadavky	N <2020	S 2020–2030	D> 2030
Zajištění důvěrnosti			
Použití blokové šifry AES-256			
Použití blokové AES-128, AES-192			x
Použití blokové 3DES-168		x	x
Zajištění integrity			
Použití módu blokové šifry GCM, CCM			
Použití módů CTR, OFB, CBC, CFB v kombinaci s bezpečnými MAC v režimu EncryptThenMAC se schválenými šiframi			x
Mód pro ochranu integrity HMAC, CMAC			
Mód pro ochranu integrity HMAC-SHA1		x	x
Digitální podpis DSA 15360 (pozn. ENISA PV Signatures) a více, EC-DSA512 (pozn. ENISA EC-KDSA) a více, RSA 15360 a více			
Digitální podpis DSA 3072, EC-DSA-256, RSA 3072			x
Digitální podpis DSA 2048, EC-DSA-224, RSA 1024		x	x
Hashe SHA2-512, SHA3-512			
Hashe SHA2-256, SHA2-384, SHA3-256, SHA3-384			x
Hashe SHA2-224, SHA3-224		x	x
Zajištění klíčového managementu			
DH-15360, ECDH-512			
DH-3072, ECDH-256			x
DH-2048, ECDH-224		x	x

Generátor náhodných bitů			
HMAC_DRBG, Hash_DRBG obě pro SHA-1, SHA-224, SHA-512/224, SHA256, SHA-512/256, SHA-384, SHA-512, SHA3-512			
CTR_DRBG s 3DES-168 X X		**x**	**x**
Operační režimy pouze důvěrnost			
EME			
OFB, CFB, CTR, CBC, XTS X			**x**

5.6 Životní cyklus měřícího zařízení



Obr. 2 Životní cyklus měřicího zařízení
Zdroj: vlastní zpracování

5.6.1 Externí dodavatelé:

Dodavatelský řetězec je většinou na začátku a případně konci celého životního cyklu měřicího zařízení. Proto je právě tato část životního cyklu měřidla nejnáročnější na bezpečnostní opatření a spolehlivost v rámci dodavatelského řetězce.

Na začátku ještě vůbec, než měřidlo vznikne je nutné provést důkladné testy vzorků měřidel od různých dodavatelů, což je stěžejní pro další části životního cyklu měřidla. Při výběru měřidla a jeho dodavatele se vždy vychází z nějakých předem stanovených kritérií, které musí budoucí měřidlo splňovat, následně v rámci výběru se musí provádět jak zkoušky funkčnosti či přesnosti, tak se testuje také softwarová výbava a bezpečnost měřidla. Testy se provádí na hardwaru a případně krytu měřidla a jeho zabezpečení. Pokud vše dodavatel měřidla splní, tak se musí určit přesný harmonogram dodávek a způsob jejich přepravy. V první fázi jde vždy o přepravu většího počtu měřidel, na které se musí využít speciální přepravní boxy či kontejnery.

V poslední fázi jsou měřidla na konci životního cyklu. Pokud například neprojdou testy a kontrolou v cejchovně či jsou již technicky zastaralá, pak jsou předána k likvidaci nejčastěji externí firmě, která následně zajistí jejich rozebrání a recyklaci dílů.

5.6.2 Cejchovna:

V cejchovně je po výrobě u dodavatele v celém cyklu asi nejpřísnější režim, co se týká bezpečnosti. V cejchovně jsou vždy určené jednotlivé zóny a perimetry, mezi kterými měřidla putují, jde o vykládku, vizuální kontrolu, potom kontrolu funkčnosti a přesnosti, pak zavedení do systému a logistiku. Měřidla se zde ověřují buď způsobem SVZ (statistická výběrová zkouška) pro měření typu C a B bez fakturačního měření jalové energie, to znamená že se například z každých sta kusů vybere náhodně 7 kusů a ty se přezkouší. V případě měřidel s fakturačním měřením jalové energie se musí ověřovat každé měřidlo. Měřidla se přezkušují buď jako nová po přijetí od výrobce, který si je přezkušuje sám, nebo pokud se vracejí již jako použitá po uplynutí platnosti cejchu (tabulka 2).

Tabulka 2 Lhůta platnosti ověření elektroměru
Zdroj: Zákon o metrologii [15]

Typ Elektroměru	Rok výroby	Lhůta platnosti cejchu	Způsob měření
indukční	do 31.12.1989	10 let	přímé
indukční	od 1.1.1990	16 let	přímé
indukční	x	5 let	převodové
statický	x	12 let	přímé
statický	x	5 let	převodové

V tabulce je patrný zejména rozdíl mezi platností cejchu u měřidel přímých a převodových, kde je platnost cejchu poloviční, to z důvodu připojení měřícího řetězce přes transformátory proudu a většímu průtoku energie během doby osazení měřidla na odběrném místě. [15]

Obr. 3 vlevo indukční Elektroměr, vpravo Statický Elektroměr

5.6.3 Montážní/Demontážní Sklad:

Montážní sklad je místo kde se měřidla nacházejí před samotným osazením na odběrné místo u zákazníka. Většinou to jsou skladové prostory, kde se nacházejí jednotlivé menší kontejnery s měřidly, které zpravují pověřené osoby a slouží pro dočasné uskladnění měřidel před jejich osazením výkonnými pracovníky v terénu. Někdy se takto může označovat i vozidlo daného výkonného pracovníka, ve kterém jsou měřidla umístěna před montáží v určený den.

Demontážní sklad je prakticky to samé, jen s tím rozdílem, že jsou zde umístěna měřidla, která již byla těsně před demontáží použita u zákazníka. Zde se ještě musí rozlišovat mezi měřidly, která lze ještě dále využít, protože mají platné ověření a měřidly, která se nedají využít, protože jim uplynula doba platnosti ověření (Tabulka 2).

5.6.4 Odběrná místa:

Jako odběrné místo se označuje místo, kde dochází k měření výroby či spotřeby elektrické energie u zákazníka, ať už jde o jalovou či činnou energii. V rámci měření zde distribuční společnost po určenou dobu a v souladu s platnou smlouvou osadí měřící přístroj. Data z tohoto měřidla jsou dále využita jako podklad pro fakturaci vyrobené či spotřebované elektrické energie odběratelem. Měřidlo (elektroměr) je v majetku distribuční společnosti ať už se jedná o přímé či převodové měření.

V případě převodového měření jsou na OM osazeny měřicí transformátory, ty jsou však již v majetku zákazníka i když jsou součástí celé měřicí soupravy. Distribuční společnost si však podmiňuje doložit zprovoznění jakéhokoliv odběrného místa revizí a v případě měřicích transformátorů protokolem o ověření. Také je nutné, aby měl zákazník na odběrném místě správně připravený rozváděč podle platných připojovacích podmínek. Distribuční společnost si vždy celý rozvaděč a veškeré přístroje v něm zabezpečí úředními plombami proti neoprávněné manipulaci. [1]

5.7 Fyzická bezpečnost a bezpečnost prostředí

Fyzické zabezpečení musí zabránit neoprávněnému přístupu k informacím které jsou umístěné na určitém místě či fyzicky v nějakém zařízení, aby nedošlo k jejich zneužití, poškození či narušení. Norma definuje i použití a definici bezpečnostních perimetrů budov, fyzické kontroly vstupu, zabezpečení kanceláří místností a vybavení, ochranu před vnějšími a přírodními hrozbami atd. Definuje se zde i způsob práce v zabezpečených oblastech. Dále práce a životní cyklus fyzických zařízení, jejich zprávu, užívání a likvidaci. [8] [9]

Obr. 4 Druhy plomb od výrobců měřicích zařízení
Zdroj: vlastní zpracování

Pokud jde o měřicí zařízení typu AMM, tak je nutné především dostatečně zabezpečit přístroje v místě uskladnění a v místě, kde dochází k jejich manipulaci. Za tímto účelem mohou s měřicími zařízeními manipulovat pouze pověření zaměstnanci organizace a při logistických a testovacích činnostech by se měli přístroje nacházet nejlépe na zabezpečených pozemcích anebo budovách. Jednotlivá měřidla jsou zajištěná plombou již od výrobce v místech na krytu přístrojů, tak aby ho nebylo možné odstranit bez jejich znehodnocení a získat přístup do mechanických a elektronických částí měřidla, které mají vliv na správnost měření a neslouží přímo k jeho montáži na odběrném místě u zákazníka. Minimálně jedna z těchto plomb by měla být evidovaná po celou dobu životnosti měřícího zařízení. Pro větší bezpečnost je vhodné také přístroje při uskladnění ve větším množství umístit do přepravních kontejnerů zabezpečených evidenční plombou zvláště pro případy dočasného umístění ve venkovních prostorách. Montáž, přemístění, údržba či

kontrola měřicích přístrojů AMM by měla být prováděna pouze pověřenou osobou nebo zaměstnancem společnosti, který má oprávnění s těmito přístroji nakládat. Veškeré prvky na přístroji, které slouží k jeho montáži či demontáži na odběrném místě u zákazníka by měli být také zajištěny kryty s evidenční plombou nebo plombou samotnou. [1]

5.8 Bezpečnost provozu

Bezpečnost provozu v normě zahrnuje dokumentaci provozních postupů, dále řízení změn, kapacit a s tím související činnosti, které musí být v mnoha případech od sebe oddělené. V tomto bodě je také uvedena ochrana před malwarem a vše s tím související, v neposlední řadě záznamník událostí (logů) a monitorování. Poslední částí jsou řízení a kontrola software, správa a řízení technické zranitelnosti a audity. [8] [9]

Pro účely chytrého měření AMM je bezpečnost provozu důležitý bod. Data z měření jsou využita pro fakturaci za spotřebované či vyrobené množství elektrické energie. Proto musí být data z měření přesná a v nezměněné podobě. Pro montáž měřicího zařízení a jeho manipulaci před instalací na odběrné místo se musí zaměstnanci řídit platnými pracovními postupy, které musí být pravidelně aktualizované. Pro účely nastavení, vzdálené zprávy a odečítání měřidel by se měly používat pouze zařízení ve vlastnictví společnosti, která měření provozuje. Tato zařízení by měla mít odpovídající zabezpečení a měla by pro pracovní účely fungovat pouze v rámci interní sítě, aby se co nejvíce eliminovala možnost napadení pomocí malware z venkovní sítě. Dále by měla odpovídat určitým standardům včetně možnosti tyto zařízení pravidelně aktualizovat o nové prvky zabezpečení. [8] [9]

5.9 Bezpečnost komunikací

Bezpečnost komunikací musí být zajištěna v rámci bezpečnosti sítě a síťových služeb, pozornost je zvlášť věnovaná bezpečnosti přenosu informací a dohodám o důvěrnosti a mlčenlivosti.

Co se týká opatření v sítích, tak by sítě měli být stále pod kontrolou a řízeny za účelem ochrany informací v systémech a aplikacích. Tato problematika je řešena například normou ISO/IEC 27033. Zvláštní pozornost je nutné věnovat bezpečnosti síťových služeb u kterých by měly být zahrnuty různé bezpečnostní mechanismy a

při zajišťování interně by měla být jasně definována odpovědnost. V sítích je také nutné zajistit oddělení jednotlivých skupin uživatelů a systémů, tak aby se navzájem neovlivňovali.

Při zajišťování bezpečnosti přenosu informací je důležité vyřešit přenos informací mezi organizací a externími stranami. Pokud jsou informace přenášeny v elektronické zprávě, tak je nutné, aby byly zprávy přiměřeně chráněné. V normě je také uvedeno, že je nutné ošetřit a pravidelně revidovat veškeré dohody o zachování mlčenlivosti a důvěrnosti. [8] [9]

Pro účely měření AMM je nutné vyřešit všechny uvedené opatření. Komunikace mezi měřícími zařízeními může probíhat přímo bod vs. bod, anebo přes data koncentrátor pomocí technologie BPL po silových kabelech. V obou případech je nutné zajistit komunikaci mezi uvedenými zařízeními za pomoci technologií třetích stran, nejvhodnější technologie pro přenos informací jsou LTE, 5G nebo NarrowBand IoT (LPWA). Nejvhodnější pro tyto účely a již celkem ověřená je technologie LTE, dále se na této technologii prodávají komunikační jednotky, jako další alternativou jsou jednotky NB-IoT zatím však se tato varianta testuje a není tolik rozšířená jako LTE.

GPRS (2.5G) technologii lze spatřit také ve variantě tzv. GPRS+ (2.5+G), tedy případy, kdy GPRS SIM podporuje technologii EDGE (2.75G). Z pohledu bezpečnosti slučujeme skupinu GPRS, GPRS+ i EDGE na tzv. „2G“. V rámci autentizace je využíván principu „výzvy“ a „odpovědi“, schéma je podobné jako u GSM a je tedy téměř shodné napříč „2G“ technologiemi. Výzva je 128 b pseudo-náhodné číslo, kde odpovědí je 32 b vypočtené číslo. Akceptace/Odmítnutí je na základě správného výpočtu funkce A3 (derivace algoritmu COMP128). Šifrování v rámci „2G“ sítí probíhá na základě nastavení sítě dle parametru GEA (GEA0-GEA3). GEA0 je nešifrovaný provoz. GEA1 a GEA2 jsou v podstatě shodné a představují 64 b, proprietární nezdokumentovanou šifru LFSR, která je dnes považována za prolomenou. GEA3 je šifra KASUMI v OFB módu s klíčem 64 b s možným rozšířením na 128 b, šifra je velmi obdobná algoritmu A5/3. GEA4 je pak jen rozšíření klíče na 128 b. Zařízení v tomto případě využívá 128 b algoritmu pouze pokud má podporu UMTS, kde je tedy následně použit 128 b klíč jako HMAC-SHA256(CK || IK, „\x32“) zkrácený na 128 b. Integrita v rámci „2G“ sítí není na této úrovni řešena.

UMTS (3G) a technologie HSDPA (3.5G) budeme považovat za skupinu „3G“, kde jednotlivé bezpečnostní prvky jsou obdobné. Z pohledu autentizace je využíváno nestandardizovaných derivátů funkcí f1, f2 a f5, resp. setu nazývaného jako MILENAGE (založeného na AES) či TUAK (založeného na SHA3). Síť generuje 128bitové pseudo-náhodné číslo na jehož základě jsou funkcemi f1, f2 a f5 provedeny výpočty AK, XRES a MAC, které jsou verifikovány oproti stanici. Šifrování je opět závislé na nastavení sítě, a to v rámci algoritmů přes parametr UEA (UEA0-UEA2). UEA0 je nešifrovaný provoz. UEA1 je šifra KASUMI v OFB módu se 128 b klíčem (KASUMI je obdoba šifry A5/3). UEA2 je pak šifra SNOW 3G také se 128 b klíčem.

LTE A (4G) společně s klasickým LTE (3.75G), ale i novými NB-IoT a LTE-Cat-M budeme z pohledu bezpečnosti považovat za skupinu „4G“. Autentizace je zde obdobná jako v případě UMTS, využívá se však i klíčů CK a IK pro ochranu provozu již na této úrovni, společně s 256 b deriváty KASME a KeNB. Derivační funkce je pak založena na HMAC-SHA256. Šifrování je založeno na jednotlivých derivátech z hlavního klíče, obdobně jako u autentizace. Šifrovací algoritmus pak závisí na nastavení sítě EEA (EEA0-EEA3), kde EEA0 je opět nešifrovaný provoz. EEA1 je shodný s UEA2 v UMTS, tedy šifra Snow3G. EEA2 je pak šifra AES v CTR módu se 128 b klíčem. EEA3 je šifra ZUC s klíčem o velikosti 128 b. Integrita je v tomto případě závislá na parametru EIA (EIA0-EIA4), kde EIA0 je nechráněna (určeno pro nouzové přenosy). EIA1 je UIA2 tedy Snow3G MAC. EIA2 je 32 b MAC generovaný pomocí AES v CMAC módu se 128 b klíčem. EIA3 je 32 b MAC generovaný pomocí algoritmu ZUC s velikostí klíče 128 b.

5G-NR (5G) je nadcházející technologie, která je v mnohých ohledech velmi podobná „4G“ předchůdci z pohledu bezpečnosti. Z pohledu autentizace je využíváno EAP-AKA či 5G AKA (upravené verze UMTS), kde deriváty klíčů jsou opět založeny na SHA-256. Parametry pro šifrování a integritu jsou obdobné, kde parametr se nazývá NEA namísto EEA (u šifrování) a NIA namísto EIA (u integrity). Nicméně jednotlivé hodnoty sobě odpovídají, tedy např. EEA1 = NEA1. [4] [5]

Tabulka 3 Mobilní sítě
Zdroj: Vlastní zpracování

	GPRS, GPRS+, EDGE 2.5G, 2.5+G, 2.75G	**UMTS, HSDPA 3G, 3.5G**	**LTE, LTE A, NB-IoT, LTE Cat-M 3.75G, 4G, 4.5G**	**5G-NR, 5G**
Autentizace	A3 (COMP128)	TUAK Milenage	TUAK Milenage	EAP-AKA 5G-AKA
Integrita		UIA0 – N/A UIA1 – MAC (Kasumi CBC-MAC) UIA2 – MAC (Snow3G)	EIA0 – N/A EIA1 – MAC (Snow3G) EIA2 – MAC (AES CMAC) EIA3 – MAC (ZUC)	NEA0 – N/A NIA1 (EIA1) NIA2 (EIA2) NIA3 (EIA3)
Šifrování	GEA/0 – N/A GEA/1 – LFSR GEA/2 - LFSR GEA/3 – Kasumi OFB GEA/4 – Kasumi OFB	UEA0 – N/A UEA1 – Kasumi OFB UEA2 – Snow3G	EEA0 – N/A EEA1 – Snow3G EEA2 – AES CTR EEA3 – ZUC	NEA0 – N/A NEA1 (EEA1) NEA2 (EEA2) NEA3 (EEA3)

V rámci jednotlivých kritérií je nutno podotknout, že všechny vybrané technologie umožňují implementovat a následně využít vlastní zabezpečovací dostupné klasické techniky jako např. protokoly TLS/SSL, IPSec a další, které z velké části řeší jejich případné nedostatky.

5.10Akvizice, vývoj a údržba systémů

Při vývoji informačních systémů jsou požadavky normy zcela zjevné. Systém by měl být odpovídajícím způsobem bezpečný během celého životního cyklu. Zároveň by v návrhu systému nemělo chybět zabezpečení pro případ vzdáleného připojení z veřejné sítě. Navržené zabezpečení systému by vždy mělo být úměrné k hodnotě v něm obsažených informací. U transakcí v systému by měli být také zabezpečeny přenosy, tak aby se zabránilo porušení důvěrnosti či integrity při nedokončeném přenosu nebo chybném přenosu. V rámci vývoje systému v jeho životním cyklu by pro jeho kontrolu měli být použity formální postupy, které jsou řádně dokumentovány. Dále by neměli být žádoucí modifikace softwarových balíků,

které je nutné omezit na minimum, případně by měly být řízeny. Všechny změny se musí vždy přezkoumávat a testovat, zda nemají neblahý vliv na kritickou činnost organizace. Organizace by měla vždy dohlížet či monitorovat vývoj aplikací a systémů externími zdroji. Základem při vývoji všech systémů by měl být i předem schválený proces průběžného testování a akceptace, což je dnes běžně součástí všech návrhů systému. [8] [9]

Při vývoji systému pro odečty AMM se organizace neobejde bez vývojářů z řad externích firem. Jedná se totiž o tak rozsáhlé projekty napříč několika odvětvími, prakticky žádná organizace nedisponuje zdroji, aby si vývoj odečtových systémů a výrobu všech klíčových komponent mohla zajistit vlastními silami. U AMM měření je nutné pohlídat celý dodavatelský řetězec a správně zvolit klíčové komponenty, tak aby zajistili bezpečný chod celého systému.

5.11 Vztahy s dodavateli

Při výběru dodavatelů výrobků a služeb by se v rámci bezpečnosti mělo postupovat velmi obezřetně. V normě je definované, že všechny přístupy dodavatelů k aktivům organizace by měli být zdokumentovány a dohodnuty. Organizace by měla určit míru zabezpečení v oblasti bezpečnosti informací a všem dodavatelům nařídit, aby se řídily pokyny organizace při přístupu k informacím organizace. Jde o to, aby pokyny a postupy, které v rámci bezpečnosti informačních aktiv dodržuje organizace, dodržoval i ve stejném rozsahu dodavatel. Při řešení smluv s dodavateli by mělo dojít k stanovení a odsouhlasení veškerých bezpečnostních opatření při přístupu k aktivům organizace všemi dodavateli.

V případě že dodavatelé dodávají nebo spravují v organizaci nějaký informační systém, musí se do smluv vždy zahrnout bezpečnostní rizika a jejich řešení v rámci dodávané služby či IT technologií, dále by se toto mělo přenést i na případné subdodavatele. Organizace by také měla v rámci svých pravomocí provádět pravidelné kontroly, audity a přezkoumávání bezpečnosti jednotlivých dodavatelů. Pokud u dodavatelů docházelo ke změně v rámci dodávané služby či produktu, mělo by dojít znovu k přezkoumání a posuzování rizik a v rámci nových zjištění k implementaci nového řešení zabezpečení. [8] [9]

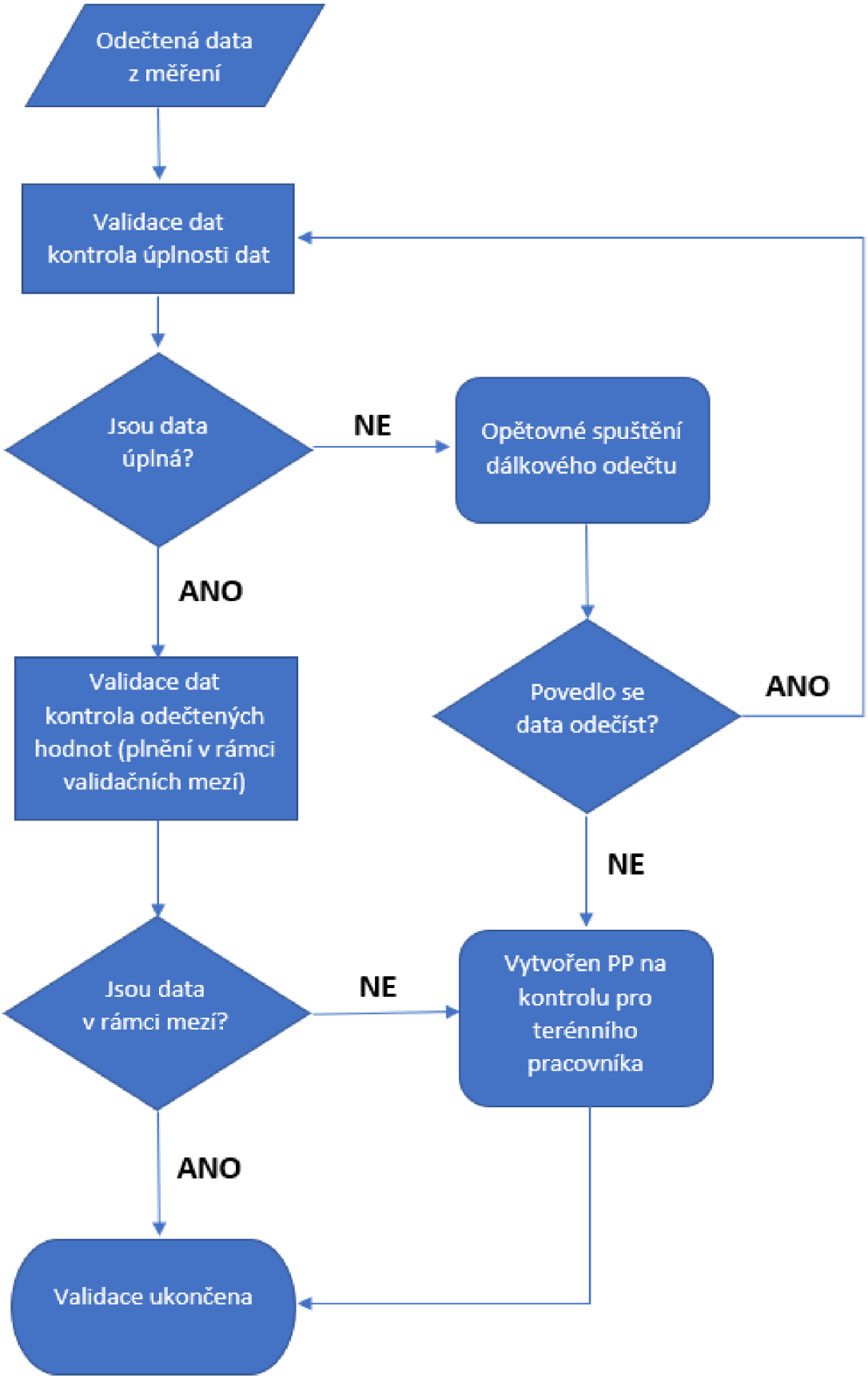
V organizaci jako jsou například distribuční společnosti je hodně důležité, aby dodavatel měl vysokou úroveň bezpečnosti a zároveň plnil spolehlivě své

závazky v rámci dodávek měřicích zařízení. Protože měření AMM budou ve velké míře využívat největší distributoři v ČR, jde také částečně o národní bezpečnost, protože energetika je zařazena do kritické infrastruktury. Proto také se s dodavateli uzavírají smlouvy o mlčenlivosti a dále také je kladen velký důraz na bezpečnost v jejich celém dodavatelském řetězci. Podmínky, za kterých obvykle dodávají měřící zařízení jsou přísné a kontrola jejich splnění také, obzvlášť z pohledu bezpečnosti.

5.12 Řízení incidentů bezpečnosti informací a zlepšování

Při řízení již funkčního systému by měl být zajištěn efektivní přístup k řízení bezpečnostních incidentů a případných slabých míst. Za tímto účelem je nutné zřídit vhodné informační kanály, které zajistí, aby všechny informace o případných incidentech dorazily co nejrychleji tam kam mají. Ať už by šlo o komunikační kanál směrem k obsluze systému, k zaměstnancům nebo poskytovatelům služby. Všechny tyto zprávy o incidentech by se měli správně klasifikovat a posoudit, zda se jedná či nejedná o bezpečnostní incident. [8] [9]

Pro účely AMM měření by měl být zřízen odečtový systém, ve kterém je vhodné také integrovat ověření správnosti odečtených dat pomocí validace dat. Ve validaci musí být určena správná kritéria podle, kterých dojde k vyhodnocení, zda odečtené hodnoty jsou validní. Pokud dojde k tomu, že nějaká z odečtených hodnot u měřicího zařízení není korektní, musí se dle určené závažnosti podnikat určité kroky, viz. Diagram. Do validace vstupují odečtená data z měřících zařízení a v první fázi se zjišťuje úplnost dat, podle toho se určí, zda je nutné provést odečet znovu nebo bude nutný zásah terénních pracovníků. V rámci první fáze validace je nutné vhodně určit počet opakování (pokusů o odečet dat), pokud dojde validace může se je dále využít k například jako podklady pro fakturaci nebo bilance atd. Pokud se v některé fázi určí, že jsou data nevalidní, tak je nutné počkat na výsledek kontroly terénního pracovníka a podle toho určit následné kroky. Komunikace mezi člověkem provádějícím validaci a terénním pracovníkem je nutné provádět nejlépe elektronickou formou zabezpečenými kanály.



Obr. 5 Validace odečtených dat
Zdroj: vlastní zpracování

6 Hlavní principy AMM

6.1 PPDS – typy měření

Pravidla provozování distribuční soustavy (PPDS) jsou vytvořeny jednotlivými energetickými subjekty podnikajícími v distribuci elektrické energie. Jsou schvalovány Energetickým regulačním úřadem a navazují na Pravidla provozování přenosové soustavy.

Tyto pravidla sdružují dohromady veškeré zákony a vyhlášky do přehledné formy a zároveň rozšiřují o různé lokální podmínky v rámci provozování určité distribuční soustavy. V rámci daného tématu měření elektrické energie je důležitý bod v PPDS popisující druhy jednotlivých měření. Zde se především rozlišuje odběrná místa u zákazníka:

Podle druhu měření:

- Přímé – jde o měření u kterých není zapotřebí použití měřicích transformátorů k měření elektrické energie.
- Převodové – jde o měření kde z důvodu toku většího množství energie je zapotřebí použít převodových transformátorů. U napěťové hladiny NN je nutné použít měřící transformátory proudu. V případě měření u odběrných míst s napětím vyšším, než je 1kV je nutné použít společně s měřicími transformátory proudu i měřicí transformátory napětí.

Podle způsobu měření

- Průběhové – jde o měření při kterém dochází k odečtu elektrické energie v intervalu 15 minut což je průměrná hodnota naměřené elektrické energie za 15 minut ať už jde o hodnotu činné či jalové energie.
- Neprůběhové – zde jde o odečet opisu registru (stavu) z elektroměru zpravidla jednou ročně

Podle typu měření:

- Měření typu A – jedná se o průběhové měření elektřiny s denním přenosem údajů.
- Měření typu B – průběhové měření elektřiny s jiným než denním přenosem údajů zpravidla nejdéle jednou za měsíc.

- Měření typu C – donedávna se to týkalo pouze neprůběhového měření, dnes to může být i měření AMM.
- Měření typu S – měření elektřiny s dálkovým přenosem údajů mimo A, B zatím se nevyužívá, do budoucna by to mělo být měření AMM.

6.2 AMM – historie

V začátcích dálkového měření se data zasílala pouze v podobě opisu registrů, následně se začalo na velkých odběrný místech s největší spotřebou používat měření typu AMR. Toto měření se vyznačovalo tím, že kromě měsíčního opisu registrů se dálkově odečítal i profil LP 15, což je aktuální průměrná spotřeba za 15 minut, a to z toho důvodu, že u velkoodběru připojeného ze sítě VN probíhá vyhodnocení čtvrthodinového maxima. Takto odečty velkoodběru probíhají již nějakých 20 let. Postupem času a z důvodu postupných změn v legislativě se dálkový odečet začal rozšiřovat i na menší odběrná místa s jističem nad 80 A.

S nástupem velkého boomu fotovoltaických elektráren v roce 2010 se začalo dálkové měření osazovat i na napěťové hladině NN u odběrných míst s výrobou elektrické energie a jističem do 80 A. Zde se však jednalo stále o měření AMR. kde je možné data pouze odečítat a měřicí přístroj nemá žádné jiné přidružené funkce. Ovšem ještě před tím začaly úvahy o tom jak efektivně a minimálními náklady odečítat všechna odběrná místa. V roce 2007 už byly na světě dokonce první projekty AMM měření, které měli různé varianty komunikace.

V dnešní době mohou být při provozování dálkového odečtu využity různé technologie, záleží především množství přenášených dat a jakým způsobem budou data z elektroměru následně využita. Ve většině případů je pomocí elektroměrů zaznamenávána spousta fyzikálních veličin v datové podobě, ale pouze část je pravidelně využita pro účely zpracování dat k fakturaci. Často je také vybrána technologie zasílání dat na dálku na základě legislativních požadavků.

Obr. 6 vlevo Echelon Type 83500, vpravo Schrack DMTZ-XC
Zdroj: vlastní zpracování

6.3 AMM – datový pohled

Elektroměr AMM se řadí jako všechny elektroměry, které měří elektrickou energii pomocí elektronických součástek bez mechanicky pohyblivých částí, do skupiny statických elektroměrů. Každý statický elektroměr určuje odečtené hodnoty pomocí OBIS kódů. Dříve se jednalo pouze o pár hodnot jako je například hodnoty napětí, proudů a činné energie. Později se postupně přidávali další a další data. Dnes je možné z dat elektroměru určit i zda nedošlo k narušení bezpečnosti například odejmutím krytu nebo případně pokus o narušení dat magnetem, a to z informace chybového registru elektroměru, jak je vidět v tabulce OBIS kódů.

Tabulka 4 OBIS kódy registry
Zdroj: vlastní zpracování

Orgie. OBIS	Veličina	Popis veličiny
1.0.12.4.0.255	U	Střední hodnota napětí je průměr sdružených hodnot
1.0.12.6.0.255	U max	Minimální hodnota napětí. Elektroměr měří, resp. počítá každou sekundu sdružené hodnoty napětí a uloží maximální hodnotou za 15 minut z třech hodnot.

1.0.12.3.0.255	U min	Minimální hodnota napětí. Elektroměr měří, resp. počítá každou sekundu sdružené hodnoty napětí a uloží minimální hodnotou za 15 minut z třech hodnot.
1.0.21.4.0.255	+P (+Ri) L1	Střední hodnota činného výkonu odběru za vyhodnocovací periodu (průmět fázoru do osy X v I a IV kvadrantu) ve fázi 1
1.0.22.4.0.255	-P (- Ri) L1	Střední hodnota činného výkonu dodávky za vyhodnocovací periodu (průmět fázoru do osy X ve II a III kvadrantu) ve fázi 1
1.0.23.4.0.255	+Q (+Rc) L1	Střední hodnota jalového výkonu (induktivní při odběru činného) za vyhodnocovací periodu (průmět fázoru do osy Y v I a II kvadrantu) ve fázi 1
1.0.24.4.0.255	-Q (-Rc) L1	Střední hodnota jalového výkonu (kapacitní při odběru činného) za vyhodnocovací periodu (průmět fázoru do osy Y v III a IV kvadrantu) ve fázi 1
1.0.31.4.0.255	I L1	Střední hodnota proudu za vyhodnocovací periodu ve fázi 1
1.0.41.4.0.255	+P (+Ri) L2	Střední hodnota činného výkonu odběru za vyhodnocovací periodu (průmět fázoru do osy X v I a IV kvadrantu) ve fázi 2
1.0.42.4.0.255	-P (- Ri) L2	Střední hodnota činného výkonu dodávky za vyhodnocovací periodu (průmět fázoru do osy X ve II a III kvadrantu) ve fázi 2
1.0.43.4.0.255	+Q (+Rc) L2	Střední hodnota jalového výkonu (induktivní při odběru činného) za vyhodnocovací periodu (průmět fázoru do osy Y v I a II kvadrantu) ve fázi 2
1.0.44.4.0.255	-Q (-Rc) L2	Střední hodnota jalového výkonu (kapacitní při odběru činného) za vyhodnocovací periodu (průmět fázoru do osy Y v III a IV kvadrantu) ve fázi 2
1.0.51.4.0.255	I L2	Střední hodnota proudu za vyhodnocovací periodu ve fázi 2
1.0.61.4.0.255	+P (+Ri) L3	Střední hodnota činného výkonu odběru za vyhodnocovací periodu (průmět fázoru do osy X v I a IV kvadrantu) ve fázi 3
1.0.62.4.0.255	-P (- Ri) L3	Střední hodnota činného výkonu dodávky za vyhodnocovací periodu (průmět fázoru do osy X ve II a III kvadrantu) ve fázi 3
1.0.63.4.0.255	+Q (+Rc) L3	Střední hodnota jalového výkonu (induktivní při odběru činného) za vyhodnocovací periodu (průmět fázoru do osy Y v I a II kvadrantu) ve fázi 3
1.0.64.4.0.255	-Q (-Rc) L3	Střední hodnota jalového výkonu (kapacitní při odběru činného) za vyhodnocovací periodu (průmět fázoru do osy Y v III a IV kvadrantu) ve fázi 3

1.0.71.4.0.255	I L3	Střední hodnota proudu za vyhodnocovací periodu ve fázi 3
1.0.1.8.0.255	+A	Elektrická energie (práce) odběr – opis kumulativního číselníku na konci vyhodnocovací periody (odběr – z pohledu PDS) v sumě za 3 fáze
1.0.2.8.0.255	-A	Elektrická energie (práce) dodávka – opis kumulativního číselníku na konci vyhodnocovací periody (dodávka – z pohledu PDS) v sumě za 3 fáze
1.0.1.8.1.255	+A T1	Elektrická energie v tarifu 1 (práce) odběr – opis kumulativního číselníku na konci vyhodnocovací periody (odběr – z pohledu PDS) v sumě za 3 fáze
1.0.1.8.2.255	+A T2	Elektrická energie v tarifu 2 (práce) odběr – opis kumulativního číselníku na konci vyhodnocovací periody (odběr – z pohledu PDS) v sumě za 3 fáze
1.0.1.8.3.255	+A T3	Elektrická energie v tarifu 3 (práce) odběr – opis kumulativního číselníku na konci vyhodnocovací periody (odběr – z pohledu PDS) v sumě za 3 fáze
1.0.1.8.4.255	+A T4	Elektrická energie v tarifu 4 (práce) odběr – opis kumulativního číselníku na konci vyhodnocovací periody (odběr – z pohledu PDS) v sumě za 3 fáze
1.0.0.2.1.255	IDTOU	číslo TOU
1.0.96.1.0.255	SN n	sériové číslo elm
1.0.0.0.0.255	C kod	BAR kód
1.0.0.2.0.255	Firmware	verze FW

Při odečtení hodnot z přístroje se datový soubor většinou rozděluje na dvě části, odečet registrů a odečet profilů. Tabulka 4 zobrazuje příklad první část datového souboru s registry elektroměru, zde jsou obsaženy stavové veličiny jako jsou stavy a maxima odebrané a dodané činné energie, dále hodnoty napětí a proudů na jednotlivých fázích nebo případně chybové registry. U každé hodnoty je uvedena časová značka, která uvádí datum, ve kterém byla hodnota odečtena.

Tabulka 5 OBIS kódy profil LP15
Zdroj: vlastní zpracování

Orig. OBIS	Veličina	Popis veličiny
1.0.1.4.0.255	+P	Střední hodnota činného výkonu odběru za vyhodnocovací periodu (průmět fázoru do osy X v I a IV kvadrantu) v sumě za 3 fáze
1.0.2.4.0.255	-P	Střední hodnota činného výkonu dodávky za vyhodnocovací periodu (průmět fázoru do osy X ve II a III kvadrantu) v sumě za 3 fáze
1.0.6.4.0.255	+Rc	Fázor jalového výkonu v Q2
1.0.8.4.0.255	RC-	Fázor jalového výkonu v Q4
1.0.5.4.0.255	Ri+	Fázor jalového výkonu v Q1
1.0.7.4.0.255	Ri-	Fázor jalového výkonu v Q3

Druhá část datového souboru obsahuje data z profilu elektroměru LP15, tyto hodnoty jsou v souboru uvedeny po 15minutových intervalech a jedná se o střední hodnotu naměřené energie za dobu 15minut. Při provedení odečtu těchto hodnot se vždy definuje, jaké období se odečítá, tak aby na sebe hodnoty navazovaly s hodnotami z předchozího odečtu (Tabulka 5). Díky tomu je možné sledovat průběh odběru nebo dodávky elektrické energie v čase.

6.4 AMM – technický pohled

U měření AMM je jeden z hlavních požadavků cena, protože se bude postupně montovat na prakticky všechna odběrná místa což například v ČEZ Distribuci je přibližně něco kolem cca 3 700 000 míst. Realizace takového rozsahu by byla pochopitelně velmi nákladná a údržba také. Proto bude nutné na začátku zvolit jakou cestou technického řešení se musí Organizace vydat. [1]

6.5 Způsob realizace a komunikace

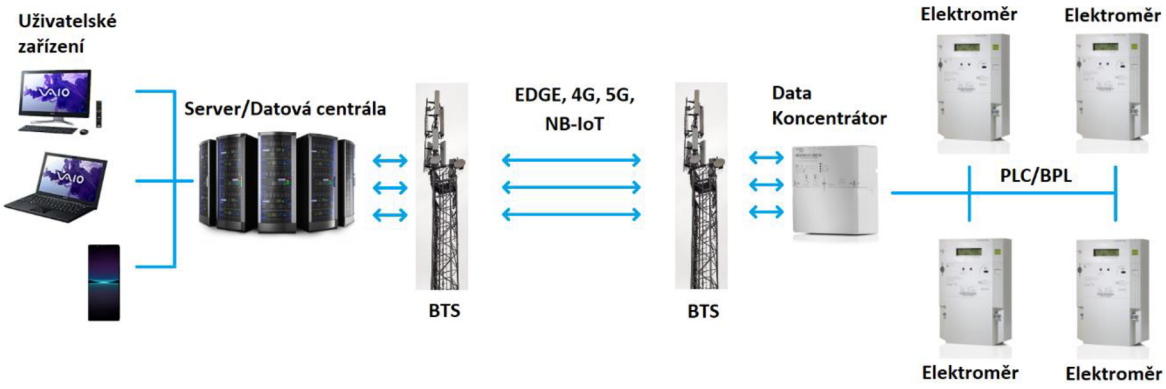
U prvních projektů se v rámci AMM měření testovalo několik různých technologií pro odečet měřicích zařízení. Jednou z prvních variant kolem roku 2007 viz. kapitola (7.1 AMM – historie) byl odečet pomocí přenosu informací po silových kabelech na krátké vzdálenosti v kombinaci s odesíláním dat přes mobilní síť nebo vlastní optickou síť. Elektroměry byly vždy odečítány po skupinách podle

trafostanic, ve kterých byly umístěné data koncentrátory. Od elektroměru ke koncentrátoru byla odesílána data pomocí technologie PLC, později BPL (Obr. 7 komunikace pomocí PLC/BPL).

PLC je úzkopásmová komunikace pouze po kabelech v síti NN/VN, její pásmo je 395 kHz, reálně se však pohybuje nad 18kHz. Přenosová rychlost této technologie je do 2,5kb/s. Nejvíce je tato technologie ovlivněna přeslechy, pokud se v oblasti nachází více data koncentrátorů.

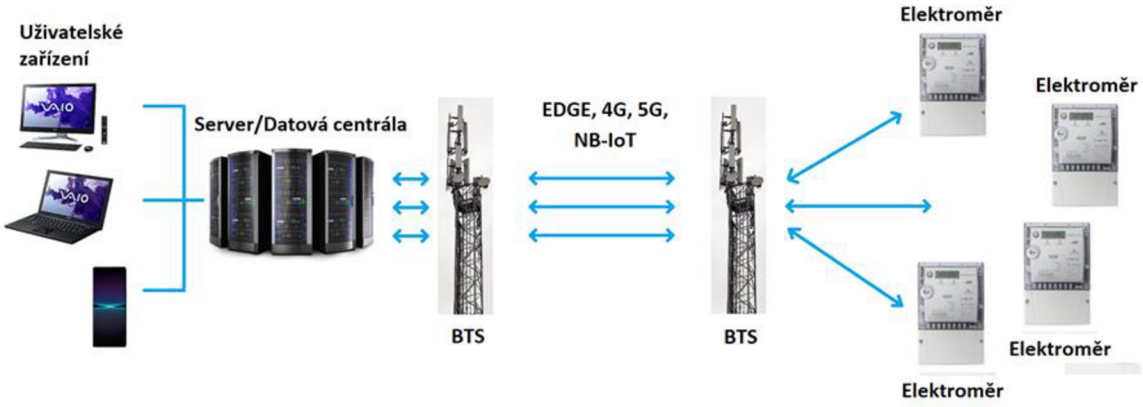
Jako další možnost je komunikace pomocí **BPL**. Jedná se o širokopásmovou technologii v pásmu 2-34 MHz a přenosové rychlosti kolem 40Mb/s. Technologie BPL je však citlivější na rušení díky spínaným zdrojům, střídačům u FVE, dále je mohou rušit výtahy v bytových domech atd. Proto byla vyvinuta technologie s názvem PRIME, což je optimalizovanější BPL technologie, která dosahuje menší rychlosti okolo 500 kb/s. (Obr. 7).

Z data koncentrátorů pak byly odesílány data pomocí mobilní sítě do datového centra nebo se také uvažovalo za tímto účelem o vytvoření optické sítě na internet. Tato varianta měla za cíl snížit závislost na externím dodavateli služeb a zároveň i vyřešit problém se signálem mobilního operátora. Také to mělo být méně nákladně z hlediska použité technologie, protože v té době byly jednotlivé modemy na GPRS a GSM velmi drahé a když se k tomu přičte poplatek za služby operátorovi, tak to celé bylo značně nákladné na provoz. Postupem času a díky zlevňování technologií bezdrátového přenosu a mobilních technologií se karta trochu obrátila a tato varianta získávání odečtu se stala pomalu nákladnější.



Obr. 7 komunikace PLC/BPL
Zdroj: vlastní zpracování

Postupem času se tedy začínalo uvažovat po zkušenostech z měření AMR u velkoodběru, že bude možná daleko jednodušší díky rozvoji rychlejších přenosů dat v mobilní síti a tím i zlevnění nákladů na jeden kB dat, provozovat odečty elektroměrů způsobem bod vs. bod. V praxi to znamená že každý elektroměr má svůj modem se sim kartou operátora a komunikuje pomocí různých bezdrátových technologií přímo s datovým centrem (Obr. 8). Důvodem je jednak ekonomika a hlavně i celkem hodně zkušeností s tímto druhem odečtů z minulosti u velkoodběru kde se takto odečítá data z elektroměrů běžně. Pro přenos se v dnešní době nejlépe hodí technologie 4G sítí (kapitola 5.9 Bezpečnost komunikací), kde jsou jednotlivé technologie rozebrány. Navíc je s nástupem 5G technologií již odstavená technologie 3G o které se ještě v nedávné době uvažovalo.



Obr. 8 komunikace elektroměrů bod vs. bod
Zdroj: vlastní zpracování

7 BIA nad daty AMM

Business Impact Analysis slouží k analýze bezpečnostních rizik v organizaci, které v ní mohou způsobit škody a zhodnotit míru dopadu v případě, že nastanou. (Business Continuity Management, BCM). Součástí BIA je stanovení minimálních úrovní zdrojů potřebných pro obnovení kritických činností ve stanovených časech a na stanovených úrovních. Často se také do BIA analýzy zahrnuje i CIA (Confidentality Integrity Availability), ta se soustředí na data nebo informace jako celek a možnosti výběru stupně ochrany.

Dopadová analýza je zaměřena především na data získaná z měření jako důležité informační aktivum. Data z měření využívají různé distribuční společnosti pro účely zúčtování různých subjektů trhu. Bez těchto dat by nemohl fungovat

energetický trh. Proto je nutné v rámci analýzy zhodnotit rizika jejich nedostupnosti pro distribuční společnost. Jako příklad distribuční společnosti, bude v analýze použita společnost ČEZ Distribuce a.s. (ČEZd) a varianta komunikace elektroměru bod vs. bod (Obr.9). [6]

7.1 BIA/CIA bezpečnostní klasifikace

Před provedením samotné analýzy je nutné vždy provést klasifikaci a stanovit bezpečnostní kritéria. Tyto kritéria se určují podle stupňů závažnosti dopadu na chod organizace. Účelem je převážně zpřehlednění a zjednodušení následného návrhu a opatření s tím spojené. Jako informační aktivum zde budou vstupovat odečtená data z měřicího zařízení, které je nutné chránit před zneužitím. [6]

7.2 Bezpečnostní hlediska pro CIA

Bezpečnostní hlediska jsou tři a vychází již z názvu analýzy. Pro jejich klasifikaci použijeme stupně hodnocení pomocí písmen A, B, C, D, díky kterým určíme důležitost informačních aktiv. [6]

Dostupnost

Tabulka 6 Kritéria dostupnost
Zdroj: Bakalářská práce [6]

Třída Dost.	Zn. BK	Popis
A	[A; *; *]	Narušení dostupnosti systému informačního aktiva není přípustné a je nutné řešit co nejdříve i krátkodobou nedostupnost. Obnovení činnosti by mělo být v řádu minut, jinak může dojít k ohrožení zájmů PDS kritickým způsobem.
B	[B; *; *]	Nedostupnost systému informačního aktiva musí být obnovena v řádu hodin, jinak mohou být důležitě ohroženy zájmy PDS.
C	[C; *; *]	Nedostupnost systému informačního aktiva by nemělo překročit dobu jednoho dne. Dlouhodobější výpadek může mít za následek částečné ohrožení zájmů PDS.
D	[D; *; *]	Nedostupnost systému informačního aktiva ovlivňuje zájmy PDS v nevýznamném měřítku.

Důvěrnost

Tabulka 7 Kritéria důvěrnosti
Zdroj: Bakalářská práce [6]

Třída Dost.	Zn. BK	Popis
A	[*; A; *]	Informační aktiva jsou velmi důvěrná a pokud by došlo k jejich prozrazení, mohlo by to mít fatální následky na PDS a případně i fungování DS.
B	[*; B; *]	Informační aktiva jsou důvěrná a jejich ochranu nařizuje zákon, občanský zákoník, či GDPR.
C	[*; C; *]	Informační aktiva nejsou veřejná a jejich zveřejněním by vedlo k porušení unbundlingu
D	[*; D; *]	Informační aktiva mohou být zveřejněna pouze za určitých podmínek, které stanoví zákon či vnitřní předpisy PDS.

Integrita

Tabulka 8 Kritéria integrity
Zdroj: Bakalářská práce [6]

Třída Dost.	Zn. BK	Popis
A	[*; *; A]	Narušení integrity informačního aktiva by mohlo v konečném důsledku vliv na fungování DS a PDS
B	[*; *; B]	Narušení integrity informačního aktiva by mohlo omezit důležité zájmy a cíle PDS
C	[*; *; C]	Narušení integrity informačního aktiva by mohlo omezit částečně zájmy a cíle PDS
D	[*; *; D]	Narušení integrity informačního aktiva nijak významně neomezuje zájmy a cíle PDS

7.3 Vstupní metrika pro vyhodnocení BIA

Vstupní metrika bude využita pro hodnocení nedostupnosti dat, ztráty dat a jejich vyzrazení či úpravy z pohledu uživatele systému.

Stupnice hodnocení: 1 – žádné
2 – nízké
3 – střední
4 – vysoké
5 – kritické

Dále je zde určena tabulka s dopady:

Tabulka 9 Metrika vyhodnocení BIA
Zdroj: Bakalářská práce [6]

Zkratka	Popis
30M	Nedostupná data 30minut
2 H	Nedostupná data 2hodiny
12 H	Nedostupná data 12hodin
24 H	Nedostupná data 24hodin
2 D	Nedostupná data 2dny
1 W	Nedostupná data 1týden
1 WW	Nedostupná více než 1týden
Z 1	Chybějící záloha 1hodinu
Z 24	Chybějící záloha 24hodin
ZW	Chybějící záloha týden
ZM	Chybějící záloha měsíc
ZALL	Úplná ztráta dat
NP	Neoprávněné prozrazení cizím osobám
CH	Chyby menšího rozsahu – různé překlepy
CHP	Chyby většího rozsahu – chybně naprogramované přenosy dat
CHU	Úmyslná chyba modifikace dat

7.4 Vodítka pro BIA

Vodítka BIA se vždy určují v závislosti na povaze podnikání organizace, u které se zkoumají dopady při narušení informačního aktiva, U společnosti ČEZ Distribuce a.s. je jsou nejcennějším informačním aktivem data z měření, proto se vodítka BIA analýzy musí vztahovat k oblasti využití těchto aktiv. [6]

Zákonné a smluvní povinnosti

Měření elektrické energie nejčastěji využívají distribuční společnosti včetně ČEZd, jako podklad pro fakturaci za dodávku či odběr elektrické energie, proto musí tyto společnosti dodržovat zákony, které se týkají převážně podnikání v energetických odvětvích. Jelikož dnes průběhové měření na OM typu měření C, jehož fungování bude mít na starost právě měření AMM není ještě povinné, jeho povinnost vzniká až v roce 2027, nejsou všechny vyhlášky a zákony zatím na tento způsob měření elektrické energie úplně připraveny. Práva a povinnosti provozu v rámci legislativy řeší, jako hlavní právní předpis **Energetický zákon č. 458/2000 Sb.**, tento zákon zapracovává příslušné předpisy Evropské unie a upravuje předpisy či podmínky podnikání nebo výkon státní správy v energetických odvětvích, kterými jsou elektroenergetika, plynárenství a teplárenství, nebo práva a povinnosti fyzických a právnických osob s tím spojené.

Dále je zde **Vyhláška č. 359/2020 Sb.** dříve **vyhláška č. 82/2011 Sb.** o měření elektřiny, tato vyhláška definuje, jakým způsobem má být realizováno měření elektrické energie na jednotlivých odběrných místech. Od roku 2021 je již do vyhlášky nově integrován způsob měření elektrické energie C1, C2 a C3 s dálkovým přenosem elektrické energie a C4 s možností osazení dálkového přenosu energie. Povinnost takto měřit začíná 1.7.2027 což ještě více tlačí na co nejrychlejší zavedení AMM do praxe. Ve vyhlášce jsou také stanovena pravidla pro předávání dat z měření a podmínky pro jednotlivé typy měření. Stanovuje také termíny a rozsah předávání údajů operátorovi trhu s elektřinou. Poslední část se týká způsobu stanovení náhrady za neoprávněně odebranou elektřinu.

Důležitou je i **Vyhláška č. 540/2005** tato vyhláška stanoví požadovanou kvalitu dodávek a služeb souvisejících s regulovanými činnostmi v elektroenergetice, včetně výše náhrad za její nedodržení, postupy a lhůty pro

uplatnění nároku na náhrady, a postupy pro vykazování dodržování kvality dodávek a služeb.

Vyhláška č. 408/2015 o Pravidlech trhu s elektřinou v této vyhlášce je definované, jakým způsobem má fungovat trh s elektřinou, finanční vypořádání v rámci trhu, formát předávání dat a zákonné lhůty, případně postihy za nedodržení termínů. Dále jsou předmětem této vyhlášky ustanovení týkající se dodávek a výroby elektrické energie, údaje z měření a podporovaných zdrojů. [10] [11] [12] [13] [14]

Řízení a provoz organizace

U řízení a provozu je důležitá zejména efektivita. Dále také je nutné zajistit provoz z hlediska bezpečnosti a stability. Proto je toto hledisko důležité, pokud totiž dojde k nějaké neočekávané situaci v organizaci, tak je nutné, aby měla organizace na pokrytí takovýchto situací dostatečné lidské zdroje a dokázala vše vyřešit v co možná nejkratším čase, než by to mělo nějaký větší dopad na kvalitu dodávané služby v rámci předávání dat z měření. Pokud si mimořádná situace vyžádá využití pouze části kapacity, tak je riziko nějakých vlivů na fungování organizace minimální. Pokud ovšem nelze mimořádnou situaci či výpadek důležitých systémů vyřešit ani za použití všech dostupných kapacit a zdrojů, tak můžou být následky pro organizaci skoro až fatální. [6]

Ztráta důvěryhodnosti

Důvěryhodnost je pro každou organizaci včetně ČEZd velmi důležitá, dokonce i prezentace na venek může hrát roli ve zvolení strategie v rámci podnikatelské činnosti a směřování společnosti. Pokud dojde k nějakému menšímu výpadku či závadě například v rámci komunikace nemusí to mít vůbec zásadní vliv na fungování organizace a nemusí se to ani zásadně projevit ve vztahu k zákazníkovi, a tak i k veřejnosti. Na opačné straně se může stát, že dojde k rozsáhlému a dlouhotrvajícímu výpadku či k veliké ztrátě dat. Pokud by se toto stalo, je možné že následně může dojít k negativní publicitě, která může být řešena na celostátní úrovni nebo dokonce ve vládě a popřípadě ke snížení hodnoty společnosti či jejímu prodeji a velké personální obměně. [6]

Finanční ztráta/Narušení činností

Pokud jde o finanční zátěž v případě problémů s přístupem k datům ze strany ČEZd, tak se to nejvíce liší podle doby, po jakou je toto informační aktivum nedostupné. Pokud se budou brát v úvahu nedostupnosti dat měření typu C u AMM elektroměrů, tak je možné že při krátkém výpadku přístupu k datům nebo malé ztrátě dat bude mít pro organizaci takovýto výpadek skoro nulový finanční dopad. Na druhou stranu, pokud dojde k dlouhodobému výpadku či velké ztrátě dat u 100000 a více odběrných míst, může dojít k finanční zátěži na organizaci, která může být až likvidační. Finanční postihy za nedodržení včasného poskytnutí dat zejména Vyhláška č. 540/2005 Vyhláška o kvalitě dodávek elektřiny a souvisejících služeb v elektroenergetice a lhůty pro odeslání Vyhláška č. 408/2015 Vyhláška o Pravidlech trhu s elektřinou. [6]

a * p * t = P

a – počet OPM t – čas překročení (hod)

p – penalizace v (Kč) P – penalizace (Kč)

Zajišťování nezbytných služeb

Data z měření AMM budou využívány převážně u zákazníku s menším odběrem elektrické energie s jističem do 80 A což je asi 15% spotřeby elektrické energie v ČR což je minoritní podíl. Pokud ovšem jde o počet odběrných míst s tímto typem měření tak se jedná na území ČEZd o 3,5 milionů odběrných míst. Proto v případě malého ovlivnění nedostupnosti dat u malého množství odběrných míst se to na organizaci nijak neprojeví a omezení nebude pro zákazníky téměř žádný problém. Pokud se ovšem omezení dat nebo služeb bude týkat více jak 100000 nebo i 1000000 odběrných míst může to být velký problém pro celou organizaci.

Tabulka 10 Vodítka BIA analýzy Zdroj: Vlastní zpracování

	A	B	C	D	E
	Zákonné a smluvní povinnosti	**Řízení a provoz organizace**	**Ztráta důvěryhodnosti**	**Finanční ztráta/Narušení činností**	**Zajišťování nezbytných služeb**
1 – Nízké	Může zapříčinit porušení interních směrnic, předpisů nebo interních KPI.	Může způsobit určité omezení provozu na krátkou dobu v části organizace.	Může dojít na krátký čas k zhoršení vztahů v organizaci nebo s některými dodavateli	Přímo nebo nepřímo povede ke ztrátám Několika milionů korun.	Omezení systému a služeb pro několik tisíc osob.
2 – Střední	Může zapříčinit správní nebo občanskoprávní řízení S tím spojený finanční postih.	Může zapříčinit omezení důležitých částí organizace na delší dobu.	Může negativně ovlivnit na krátkou dobu vztah s veřejností nebo širokou skupinou lidí.	Přímo nebo nepřímo povede ke ztrátám několika desítek milionů korun	Omezení systému a služeb pro několik desítek tisíc osob.
3 – Vysoké	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání. Případný zákaz činnosti	Může způsobit dočasné zastavení činnosti důležitých částí organizace nebo její velké části.	Může velmi negativně ovlivnit vztah s veřejností na dlouhou dobu s přesahem do celostátní úrovně, či energetickou burzu	Přímo nebo nepřímo povede ke ztrátám několika stovek milionů korun	Rozsáhlé omezení systému a služeb týkající se několika stovek tisíc osob.
4 – Kritické		Může způsobit zastavení činnosti celé organizace v jejichž důsledku může dojít i k ukončení	Může trvale závažným způsobem ovlivnit vztah na celostátní úrovni se zákazníky a dodavateli nebo i politickými důsledky	Přímo nebo nepřímo dojde ke ztrátám více než půl miliardy korun	Rozsáhlé omezení nezbytných systémů nebo služeb pro více než půl milionu osob

7.5 Určení MTPD, MIDP, MTDL

U důležitých informačních aktiv se stanovuje RTO (Recovery Time Objective) a RPO (Recovery Point Objective). RPO je čas poslední zálohy a RTO je čas poslední dostupnosti aplikace. Proto by mělo platit, RPO <=MTDL, RTO <=MIPD a RTO <=MTPD. [6]

MTPD (Maximum Tolerable Period of Disruption)

Je maximální doba tolerance nedostupnosti či výpadku služeb, která by měla za následek vysoký dopad na společnost ČEZd. [6]

Tabulka 11 MTPD
Zdroj: Vlastní zpracování

Stupeň MTPD	**popis**
30M	Do 30 minut je dosaženo vysokých dopadů
2 H	Do 2 hodin je dosaženo vysokých dopadů
12 H	Do 12 hodin je dosaženo vysokých dopadů
24 H	Do 24 hodin je dosaženo vysokých dopadů
2 D	Do 2 dnů je dosaženo vysokých dopadů
1 W	Do 1 týdne je dosaženo vysokých dopadů
1 WW	Za více jak 1 týden je dosaženo vysokých dopadů

MIPD (Medium Impact Period of Disruption)

Je maximální doba tolerance nedostupnosti či výpadku služeb, která by měla za následek střední dopad na společnost ČEZd. [6]

Tabulka 12 MIPD
Zdroj: Vlastní zpracování

Stupeň MIPD	**popis**
30 M	Do 30 minut je dosaženo středních dopadů
2 H	Do 2 hodin je dosaženo středních dopadů
12 H	Do 12 hodin je dosaženo středních dopadů

24 H	Do 24 hodin je dosaženo středních dopadů
2 D	Do 2 dnů je dosaženo středních dopadů
1 W	Do 1 týdne je dosaženo středních dopadů
1 WW	Za více jak 1 týden je dosaženo vysokých dopadů

MTDL (Maximum Tolerable Data Loss)

Jedná se o maximální dobu od poslední zálohy dat, která je pro společnost ČEZd akceptovatelná. [6]

Tabulka 13 MTDL
Zdroj: Vlastní zpracování

Stupeň MTDL	**popis**
1 H	Zálohuje se pravidelně v intervalu 1 hodiny
1 D	Zálohuje se pravidelně v intervalu 1 dne
1 W	Zálohuje se pravidelně v intervalu 1 týdne
1 M	Zálohuje se pravidelně v intervalu 1 měsíc

7.6 Informační aktiva a systémy vstupující do analýzy

Pro účely analýzy se nejdříve určí informační aktiva, které je nutné v rámci měření AMM zabezpečit. U AMM měření je důležité, aby bylo zabezpečení vymyšleno komplexně napříč celými systémy. AMM měření je dnes využíváno pro účely měření typu C. Informační aktiva proudí různými systémy napříč celou strukturou organizace viz. „Obr. 9 Diagram proudu informačních aktiv“. Pro zjednodušení byla vybrána jedna část kudy proudí informační aktiva z měřicích zařízení až k zákazníkovi. Nejdříve jsou zde jednotlivá informační aktiva.

LP15

Jde o takzvaný „last profil“ což jsou střední hodnoty výkonu v intervalu 15.minut viz. kapitola 7.2. AMM – datový pohled. Tento profil se používá především pro lepší přehled o průběhu spotřeby na odběrném místě. Data jsou důležitá pro zákazníka a také obchodníka. Částečně ho lze využít jako kontrolní prvek pro validaci případně se z něj může u budoucích mikrozdrojů vyhodnocovat maximum

a u spotřeb nedovolenou dodávku. S nástupem AMM měření dojde také díky měření LP15 u spousty odběrných míst k přesnějšímu dopočtu v případě reklamací vadného měřidla.

LP60

Tento profil je vždy vypočten z profilu LP15, výsledkem je hodnota odběru elektrické práce za jednu hodinu. Využití najde především v měsíčním zúčtování odchylek na OTE a poskytuje se také jako informace pro zákazníka. Výpočet LP60 je vždy proveden v rámci validace v odečtovém a validačním systému.

BW

Jedná se o zkratku „billing value“ což znamená fakturační hodnota, jde o opis registrů elektroměru. Pro účely fakturace u měření typu C je využívána hodnota činné energie spotřeby nebo výroby. Tato hodnota má vždy časovou značku. V rámci odečtu se z elektroměru vždy odečtou hodnot všech možných veličin viz. kapitola (7.2. AMM – datový pohled). Většina z nich slouží pro účel validace a ověření správnosti měření.

ODP

Tento druh informačního aktiva by měla být zpráva, něco jako pokyn zaslaný k určenému elektroměru za účelem dálkového odpojení z důvodu neplacení. Zatím se to v praxi moc nevyužívá, ale v budoucnu by to mělo být využito v případech, kdy odběratel nezaplatil za odebranou elektrickou energii a má nepřístupné odběrné místo. Tuto funkci definuje i nová vyhláška o měření č. 359/2020 Sb.

PRIPO

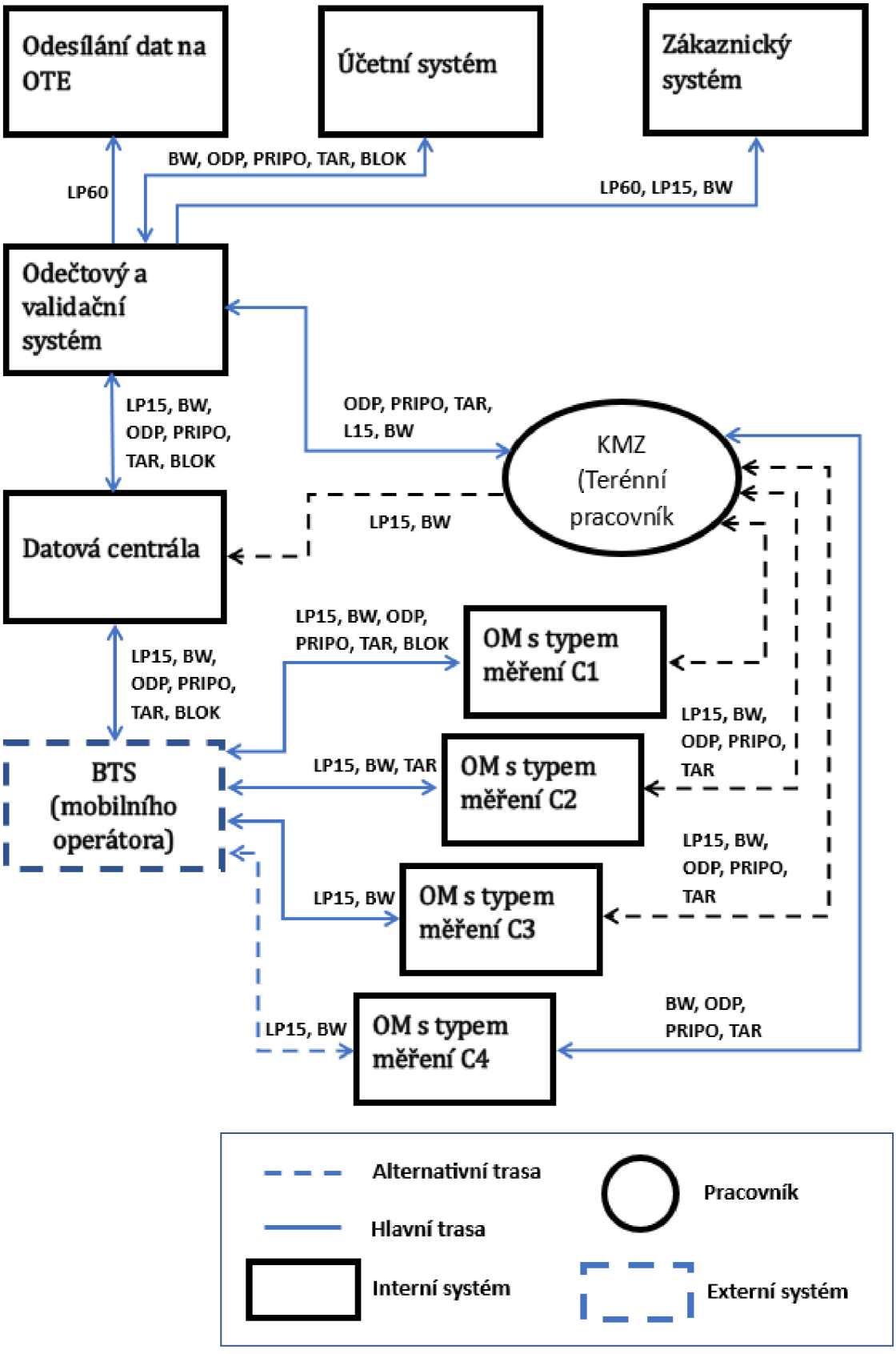
Informační aktivum funguje na podobném principu jako ODP akorát se v tomto případě jedná o připojení odběrného místa například po zaplacení nebo přepisu odběrného místa. Což definuje ta samá vyhláška.

TAR

Dalším informačním aktivem je TAR což je v tomto případě informace o nastavení tarifu, což bude buď zpráva, která nastaví na pevno spínání blokovaných spotřebičů v rámci nízkého a vysokého tarifu nebo půjde přímo o pokyn k sepnutí či vypnutí spotřebičů. Funkce v elektroměru by měla nahradit dnešní HDO a elektroměr by měl umět i díky připojenému relé boxu přepínat více druhů spotřebičů, než bylo možné u AMM měření.

BLOK

Posledním informačním aktivem by měla být funkce BLOK, což zde označuje omezení výkonu. Toto bude využito zejména u mikrozdrojů, kde je nutné v případě velkého přebytku energie v síti omezit výrobu elektrické energie. Dále by se to mohlo použít v případě, že dojde k překročení maxima na výrobě u některého z odběrných míst.



Obr. 10 Diagram proudu informačních aktiv
Zdroj: vlastní zpracování

Z diagramu je patrné kde všude proudí informační aktiva, jednotlivé systémy mají různou funkci a používají informační aktiva různými způsoby.

Elektroměry na **OM s typem měření C1, C2, C3 a C4 (OMC1, OMC2, OMC3, OMC4)** by měly mít podle nové vyhlášky viz. kapitola „8.2.2. Vodítka BIA Zákonné a smluvní povinnosti“ integrovány různé funkce. OM s typem měření C1, C2, C3 by měli disponovat u elektroměru dálkovou komunikací a tím měřením průběhu LP15 a registrů BW, zatímco u typu měření C4 nemusí disponovat dálkovým odečtem a lze ho provozovat jako většinu dnešních elektroměrů typu měření C, a to fyzickým odečtem prováděným pracovníkem v terénu. Elektroměr typu měření C1 a C2 by měl mít možnost ovládání tarifů (TAR) na dálku nebo jeho vzdálené nastavení za pomocí změny TOU tabulky. Elektroměr typu měření C1 by měl disponovat ještě navíc funkcí ODP a PRIPO což je odpojení a připojení na dálku, dále možností BLOK omezení výkonu na dálku.

Jako jeden z hlavních článku v rámci externích dodavatelů služby je zde v řetězci zahrnut mobilní operátor jako **BTS (BTS),** který zajišťuje komunikaci mezi datovou centrálou a elektroměry. Technologie přenosu může být v tomto případě různorodá, pro účel analýzy jí není nutné specifikovat.

Datová centrála (DCT) je určená ke sběru dat a zároveň tvoří přímé spojení s elektroměry. Při odečtu se do ní ukládají veškerá data. Datová centrála by měla být dostatečně zabezpečená vůči napadení zvenčí, proto přístup do ní by měl být pouze z vnitřní sítě. Jde převážně o hardware.

Odečtový a validační systém (OAVS) je software, který slouží k obsluze datové centrály. V odečtovém systému se definuje a plánuje odečty dle harmonogramu, dále zde jsou spouštěné různé reporty. Jelikož jde i o validační systém, tak zde probíhá validace nad daty viz. kapitola „5.12 Řízení incidentů bezpečnosti informací a zlepšování“. Také zde dochází k výpočtu hodinových dat LP60 a k odesílání dat do **Účetního systému (US)** či **Zákaznického systému (ZS)**. Dále z důvodu bezpečnosti se odesílají data určená pro OTE ještě přes mezičlánek v podobě **aplikace odesílání dat na OTE (OOTE)**.

Účetní systém (US) slouží k fakturaci spotřeby a je zde veškerá evidence zákazníků a zaměstnanců, dále se zde vyřizují různé záležitosti kolem provozních

věcí, jako jsou montáže a demontáže měřidel odpojování, připojování a vše kolem servisu měření.

Zákaznického systému (ZS) je vytvořen za účelem poskytování dat z měření zákazníkům, zde je možné zjistit průběh odečtů dat z měření a část opisu registrů.

aplikace odesílání dat na OTE (OOTE) je aplikace která zajišťuje komunikaci s operátorem trhu a odesílá se zní data a zprávy na OTE.

Posledním článkem je **KMZ terénního pracovníka (PKMZ),** ten provádí fyzický periodický odečet na OM s typem měření C4, případně odpojení pro neplacení a parametrizaci elektroměrů, pro případ nefunkční komunikace provádí odečet a nastavení u elektroměrů na OM s typem měření C1, C2 a C3.

7.7 BIA analýza systému AMM měření v ČEZd

7.7.1 Vyhodnocení rizik uživatelem

Je nutné provést hodnocení rizik u analyzovaných systémů z hlediska dostupnosti, ztráty, vyzrazení či chybovosti. Většinou se provádí formou rozhovoru s uživateli daného systému. K tomuto účelu slouží (Tabulka 14). [6]

Tabulka 14 Vyhodnocení rizik uživateli
Zdroj: Vlastní zpracování

Dopad / Název	30 M	2 H	12 H	24 H	2 D	1 W	1 WW	Z 1	Z 24	ZW	ZM	ZALL	NP	CH	CHP	CHU
BTS	1	2	3	3	4	4	5	1	1	1	1	1	3	1	4	5
DCT	1	1	2	3	3	4	5	1	2	3	4	5	5	1	4	5
OAVS	1	1	2	3	4	5	5	1	2	2	4	5	5	2	4	5
ZS	1	1	1	1	2	2	3	1	1	2	3	4	5	1	2	3
OOTE	1	2	3	3	3	4	4	1	1	2	3	3	5	2	4	5
US	1	2	3	3	4	5	5	1	3	4	5	5	5	1	4	5
PKMZ	1	1	2	2	2	3	4	1	1	2	2	3	3	1	3	4
OMC1	1	2	2	3	3	4	5	1	1	2	3	4	5	2	3	4
OMC2	1	1	2	2	3	4	5	1	1	2	3	4	5	2	3	4
OMC3	1	1	1	2	2	3	5	1	1	2	3	4	5	2	3	4
OMC4	1	1	1	1	2	3	4	1	1	1	2	4	5	2	3	4

Z uvedené (Tabulky 14) vyplývá, že krátkodobé výpadky do 2 hodin ve všech částech systému nemají žádný dopad na fungování společnosti. Do větších problémů se společnost ČEZd dostane až při výpadku různých systémů a aplikací na 2 hodiny a více, kritický dopad na všechny systémy a aplikace má samozřejmě výpadek delší než týden. Je to dáno především tím, že měření typu C nemá takovou prioritu jako vyšší typy měření.

Nejvíce choulostivý systém je při výpadku účetní systém **(US)**, dále je problém, pokud nefunguje aplikace na odesílání dat na OTE **(OOTE)**, oba dosahují středních dopadů na společnost už při 12hodinovém výpadku. Je to především tím, že oba systémy jsou koncové a vždy pokud nefunguje systém či aplikace, která je na ně navázaná, tak to tolik nevadí, protože do koncových systémů lze integrovat náhradní způsob či dočasný způsob jakým mohou na venek fungovat. Dalším důvodem je, že například účetní systém obsluhuje nejvíce zaměstnanců a také, že se tam zpracovávají veškeré faktury a finanční toky společnosti a každý jeho výpadek má velký výpadek na ekonomické fungování ČEZd. U aplikace určené k odesílání na OTE**(OOTE)** je rychlejší nástup středních dopadů na společnost z toho důvodu, že pro předání dat na OTE je určen určitý časový limit a sankce za nedodržení termínů jsou pevně dané.

Na druhé straně je zákaznický systém **(ZS),** který slouží pouze k informování zákazníka, a tak by neměl nikdy dosáhnout vyšších než středních dopadů, je to dané také tím, že registrace zákazníků do systému je dobrovolná a pokud vypadne, tak je to nikdy všechny neovlivní.

U **OMC1** je dopad výpadku v čase horší, protože má více funkcí používaných na dálku a počítá se s tím, že ho distributor umístí na odběrná místa s výrobou elektrické energie. Naopak nejmenší dopad by měl případný výpadek na **OMC4,** protože těchto míst bude velmi málo a budou se odečítat zřejmě v intervalu až jednoho roku jako stávající elektroměry typu měření C.

Pokud jde o ztrátu dat, tak zde mají všechny systémy a aplikace společné, že chybějící záloha za 1hodinu nijak moc organizaci neohrozí, nejvíce problematický je v tomto ohledu účetní systém **(US)**, ten už u 24hodin má střední dopad na fungování společnosti. Jediný systém, na který nemá žádný vliv chybějící záloha nebo ztráta dat je **(BTS)**, je to z toho důvodu, že zde nejsou uložena žádná data a (**BTS**) funguje

pouze pro přenos informací. Největší dopad na ztrátu dat je také u datové centrály **(DCT)** a u odečtového a validačního systému **(OAVS).**

Pokud by došlo na vyzrazení údajů z některého ze systémů, tak to může mít až kritické dopady na společnost u všech systémů a aplikací kromě **(BTS) a (PKMZ),** je to převážně z toho důvodu, že mobilní operátor v podobě BTS má mizivé informace o citlivých údajích společnosti. U pracovníků na KMZ **(PKMZ)** je riziko vyzrazení také pouze střední, protože se pracovník v terénu většinou dostane k údajům u maximálně několika tisíc lidí ročně.

V rámci posouzení chybovosti nejsou jednotkové chyby například uživatelů systému nebo nějakých anomálií v systému či aplikaci pro ČEZd až takový problém. Pokud ovšem dojde na systémové chyby tak měřidla na odběrných místech a KMZ **(PKMZ)** dosahují středních dopadů, zákaznický systém **(ZS)** spíše nízkých. Jinak na ostatní systémy má systémová chyba už vysoký dopad.

U úmyslných chyb je ve většině systémů a aplikací dopad na společnost vysoký až kritický, protože lze předpokládat že u takového chování je vždy předpokladem snaha způsobit co největší újmu společnosti.

7.7.2 Hodnocení rizik dle vodítek

BTS (BTS)

Pokud bude průběhové měření osazeno na OM typu měření C v takové míře, jak je plánováno, což znamená, že dálkově bude prováděn odečet minimálně u 95% možná i více míst, tak bude mobilní operátor a jeho přenos dat přes BTS velmi důležitý.

Zákonné a smluvní povinnosti

Pro případ výpadku nějaké BTS či více, nebo například pokud bude operátor provádět nějakou úpravu mobilní sítě v určité oblasti a přestanou se díky tomu odečítat elektroměry, může dojít porušení vyhlášky č. 359/2020 Sb. § 5, § 6, § 8 protože by distributor neplnil povinnosti odečtů a jejich včasné předání. Dále může dojít k porušení vyhlášky č. 540/2005 Sb. § 14 § 15 § 16, kde se stanový kvalita dodávané služby. Počet takových případů může kvůli očekávanému osazení většího počtu měřidel s dálkovým odečtem dosahovat od stovek odběrných míst a do

několika tisíc. Proto zde je riziko hodnoceno jako vysoké. Ve velmi krajním případě k porušení zákona č. 458/2000 Sb. § 11 a vyhlášky č. 408/2015 Sb.

Řízení a provoz organizace

Jelikož při výpadku BTS mobilního operátora jde o externí službu, a tak komunikace s externími dodavateli tvá vždy déle než interní a zároveň je zde určitá forma nejistoty pro provozovatele, že nedojde k včasné opravě komunikace u míst, kde by mohlo dojít k nedodržení zákonných lhůt jsou tyto případy kdy dojde k výpadku komunikace s velkým množstvím míst pro distributora velmi zatěžující. Protože se předpokládá, že rozsáhlé výpadky nebudou moci vykrýt pracovníci v terénu a data poslat náhradní cestou, tak je zde riziko pro ČEZd vysoké.

Ztráta důvěryhodnosti

Pokud jde o ztrátu důvěryhodnosti, tak v tomto případě se uvažuje o tom, že dojde zhruba k ztrátě důvěrnosti na střední úrovni. Výpadek by se neměl nikdy plně dotknout všech odběrných míst na jedné BTS a dále jde o dodávku externího dodavatele, což v takových případech toto pocítí daleko více externí subjekt než samotná ČEZd, která za výpadek neponese plnou odpovědnost.

Finanční ztráta/ Narušení činností

Pokud bychom předpokládali, že půjde o výpadek služeb pro nějakých 1000 OM což by muselo vypadnout hned několik BTS, kterých jsou po celé ČR podle ČTU v počtu cca 16 000 ks pro 4G sítě. Což vychází cca 1BTS na 60 uživatelů. Na tento výpadek by byla nejvíce choulostivá ČEZd v období na začátku měsíce, kdy je nutné včas poskytnout data na OTE. U měření typu C budou stejné lhůty jako u jiných průběhových měření. A tedy dodání dat do 7 pracovních dnů 18hodin. Pokud bychom předpokládali, že by se problém projevoval u 1000 OM ještě 7 pracovní den po 18hodině tak by byl postih vypočten dle vzorce, který je uvedený v kapitole (8.4 Vodítka pro BIA) bod Zajišťování nezbytných služeb.

Nedostupnost služby a neodeslání dat do určité hodiny je postih následující:

1 hodiny od hodiny H

1 000 * 600 * 1 = 600 000 kč

2 hodiny od hodiny H

1 000 * 600 * 2 = 1 200 000 kč

5 hodiny od hodiny H

1 000 * 600 * 5 = 3 000 000 kč

10 hodiny od hodiny H

1 000 * 600 * 10 = 6 000 000 kč

Maximální penalizace

1000 * 30 000 = 30 000 000 kč

V případě nedostupnosti spínání tarifu (nedodržení času vyplývajícího ze smluvené sazby) nebo nedodržení lhůty připojení či odpojení, mohou být sankce ještě vyšší, proto je zde riziko vysoké.

Zajišťování nezbytných služeb

Pokud by došlo na výpadek komunikace, kvůli problémům v mobilní sítí, nemělo by se to nikdy dotknout více než několika tisíc lidí, a to ještě ve velmi omezeném počtu případů. Po zkušenostech z měření AMR lze předpokládat takový rozsáhlý výpadek jednou do roka. V oblasti zajišťování důležitých služeb je toto ohodnoceno jako střední riziko, a to z důvodu postižení malého počtu míst.

Tabulka 15 BTS hodnocení rizik
Zdroj: Vlastní zpracování

Označení	Zákonné a smluvní povinnosti	Řízení a provoz organizace	Ztráta důvěryhodnosti	Finanční ztráta/ Narušení činnosti	Zajišťování nezbytných služeb	MTPD	MIDP	MTDL
BTS	Vysoké	Vysoké	Střední	Vysoké	Vysoké	2 D	12 H	ZM

Datová centrála (DCT)

Jelikož se v případě AMM měření bude ukládat do datové centrály obrovské množství dat a tyto data jsou důležitá především jako podklad pro fakturaci elektrické energie, je důležité, aby jich chybělo co nejméně, nejlépe žádné a byly především konzistentní a pokud možno nezměněné.

Zákonné a smluvní povinnosti

Pokud dojde k výpadku DCT nebude možné následně provádět další zpracování reálných dat, protože k nim nebude přístup, proto takovýto výpadek bude mít vliv prakticky na všechny aplikace, může dojít porušení vyhlášky č. 359/2020 Sb. § 5, § 6, § 8 protože by distributor neplnil povinnosti odečtů a jejich včasné předání. Dále může dojít k porušení vyhlášky č. 540/2005 Sb. § 14 § 15 § 16 § 17 § 18, zákona č. 458/2000 Sb. § 19, § 20 a vyhlášky č. 408/2015 Sb. Znovu však záleží na délce výpadku a stavu požadavků v systémech ČEZd. Kdyby však následkem poškození DCT došlo k veliké ztrátě dat, tak by mohla mít ČEZd obrovské problémy, proto je nutné tuto oblast hodnotit jako kritickou.

Řízení a provoz organizace

Když by se stalo, že vypadne DCT, tak organizace typu ČEZd nemůže nikdy zajistit svými silami data náhradní cestou, aby bylo možné včas dodat data do systémů, také je zde důležité, jaký druh závady na DCT a pokud v ní dojde ke ztrátě dat. V rámci provozu jde asi o nejchoulostivější systém, který může ovlivnit v určitých případech chod celé společnosti. Proto je zde označeno riziko za kritické.

Ztráta důvěryhodnosti

Pokud jde o ztrátu důvěryhodnosti, tak DCT by měla být v plném vlastnictví ČEZd, pouze správu některých částí provádí externí subjekt. Pokud by tedy došlo k narušení dat či k výpadku DCT. Šla by plná odpovědnost na vrub ČEZd. Jestli by šlo o výpadek většího rozsahu a ČEZd by ho nedokázal v rozumné míře napravit, mohlo by to znamenat až kritickou ztrátu důvěry ve společnost na dlouhá léta.

Finanční ztráta/ Narušení činností

Z pohledu financí by se mohla finanční ztráta vyšplhat až do astronomických výšin, pokud by došlo na nejhorší, a to třeba úplnou ztrátu dat z DCT vinou nějaké nehody nebo v případě ztráty velké časti dat, které by již nešlo obnovit. Proto není nutné v tomto případě provádět vyčíslení škod, částky by se totiž mohli bez problémů pohybovat v desítkách miliard korun.

Zajišťování nezbytných služeb

Při výpadku DCT na delší dobu ne je například 1 hodina, je již patrný vliv na funkci celé organizace, pokud dojde k rozsáhlému výpadku či ztrátě dat, může se to týkat i milionu odběratelů a výrobců elektrické energie, proto je zde nutné hodnotit hledisko jako kritické.

Tabulka 16 DCT Vyhodnocení rizik
Zdroj: Vlastní zpracování

Označení	Zákonné a smluvní povinnosti	Řízení a provoz organizace	Ztráta důvěryhodnosti	Finanční ztráta/ Narušení činností	Zajišťování nezbytných služeb	MTPD	MIDP	MTDL
DCT	Vysoká	Kritická	Kritická	Kritická	Kritická	1 W	24 H	ZW

Odečtový a validační systém (OAVS)

V odečtovém systému se provádí přepočty a validace dat, proto je pro tento systém nezbytně nutné, aby zároveň fungovala i DCT. Bez ní by nemohl OAVS pracovat s daty.

Zákonné a smluvní povinnosti

Pokud dojde k výpadku OAVS nebude možné následně poskytovat dat dalším příjemcům jako je US, OOTE a ZS. Takový výpadek bude mít vliv prakticky na všechny návazné aplikace, může dojít porušení vyhlášky č. 359/2020 Sb. § 5, § 6, § 8 protože by distributor neplnil povinnosti odečtů a jejich včasné předání. Dále

může dojít k porušení vyhlášky č. 540/2005 Sb. § 14 § 15 § 16 § 17 § 18, zákona č. 458/2000 Sb. § 19, § 20 a vyhlášky č. 408/2015 Sb. Znovu však záleží na délce výpadku a stavu požadavků v systémech ČEZd. Kdyby však měl výpadek delší trvání mohlo by dojít až k vysokému dopadu na fungování ČEZd.

Řízení a provoz organizace

Výpadek nebo omezení služeb v OAVS může mít až kritický dopad na fungování celé společnosti. Náhradní způsob získání a ověření dat v daném rozsahu není možné. Proto je nutné dbát na to, aby byla aplikace zprovozněna, pokud možno co nejdříve.

Ztráta důvěryhodnosti

Pokud jde o ztrátu důvěryhodnosti, tak je vše stejné jako v případě DCT, kde je riziko ztráty důvěryhodností kritické, protože aplikace navazuje přímo na DCT a její výstupy proudí do všech důležitých systému. Jelikož za aplikaci zodpovídá přímo ČEZd, tak její dlouhodobá nefunkčnost může mít velký vliv na důvěryhodnost celé ČEZd.

Finanční ztráta/ Narušení činností

Pokud by došlo na porušení zákonných limitů v rámci fakturace nebo zasílání dat v důsledku nefunkčnosti aplikace na delší dobu, například prvních 7 dní v měsíci. Mohlo by to mít neblahý vliv na celou společnost ČEZd, protože by náhrady za výpadek šly až do desítek možná stovek miliard.

Pro příklad zde lze uvést výpočet OM s typem měření C1, které jsou výpadkem postiženy nejcitelněji. V roce 2022 bylo v ČR něco kolem 60000 fotovoltaických elektráren. Postih byl vypočten dle vzorce, který je uvedený v kapitole „8.4 Vodítka pro BIA“ bod Zajišťování nezbytných služeb.

Nedostupnost služby a neodeslání dat do určité hodiny je postih následující:

1 hodiny od hodiny H
60000 * 600 * 1 = 36 000 000 kč

2 hodiny od hodiny H

60000 * 600 * 2 = 72 000 000 kč

5 hodiny od hodiny H

60000 * 600 * 5 = 180 000 000 kč

10 hodiny od hodiny H

60000 * 600 * 10 = 360 000 000 kč

Maximální penalizace

60 000 * 30 000 = 1 800 000 000 kč

I když byl výpočet proveden pouze u zlomku míst s konkrétním typem měření C1, tak je vidět, že už jen pouhé nedodržení včasného odeslání dat může způsobit firmě veliké problémy. Proto je zde riziko ohodnocené jako kritické.

Zajišťování nezbytných služeb

Výpadek nebo omezení služeb u OAVS se může vždy dotknout skoro všech zákazníku s typem měření C, proto je nutné toto hledisko označit jako za kritické. Zde jde také hlavně o délku výpadku.

Tabulka 17 OAVS Vyhodnocení rizik
Zdroj: Vlastní zpracování

Označení	Zákonné a smluvní povinnosti	Řízení a provoz organizace	Ztráta důvěryhodnosti	Finanční ztráta/ Narušení činností	Zajišťování nezbytných služeb	MTPD	MIDP	MTDL
OAVS	Vysoká	Kritická	Kritická	Kritická	Kritická	2 D	24 H	ZW

Zákaznického systému (ZS)

Tento systém je možné provozovat i pouze ve formě aplikace, data jsou zde poskytována zákazníkovi pouze pro informativní účely.

Zákonné a smluvní povinnosti

Pokud je na OM realizováno průběhové měření tak je dle vyhlášky 359/2020 Sb. Distributor povinen předávat data z měření zákazníkovi. Za porušení však není stanovena žádná sankce.

Řízení a provoz organizace

Pro organizaci není tento systém úplně stěžejní a jeho výpadek i klidně na měsíc nemusí pro firmu a její chod znamenat nic dramatického.

Ztráta důvěryhodnosti

Výpadek tohoto systému může mít dopad na několik tisíc lidí, v některých případech i desítek tisíc lidí. Je dost pravděpodobné, že to zhorší pověst ČEZd, ale ne na dlouhou dobu a nějak fatálně. Proto je zde střední riziko.

Finanční ztráta/ Narušení činností

Z tohoto hlediska není jisté, zda by došlo na uplatnění sankcí z důvodu nefunkčnosti tohoto systému od nějakého zákazníka na ČEZd. Zřejmě by to ale bylo v mizivém množství a nízké sumě. Proto je zde riziko nízké až velmi nízké.

Zajišťování nezbytných služeb

V rámci zajišťování služeb se výpadek této služby může dotknout desítky tisíc lidí, jde však o služby, které nejsou pro zákazníka stěžejní. Proto je zde riziko kvůli množství zákazníků postižených výpadkem střední.

Tabulka 18 ZS Vyhodnocení rizik
Zdroj: Vlastní zpracování

Označení	Zákonné a smluvní povinnosti	Řízení a provoz organizace	Ztráta důvěryhodnosti	Finanční ztráta/ Narušení činností	Zajišťování nezbytných služeb	MTPD	MIDP	MTDL
ZS	Střední	Nízká	Střední	Nízká	Střední	1WW	1WW	ZM

Aplikace odesílání dat na OTE (OOTE)

Tato aplikace je spojeným komunikačním kanálem s OTE, na který skrz něj proudí data v podobě LP60 z AMM měření. Pro účel analýzy uvažujeme pouze s touto funkcí, ostatní informace z fakturace atd. proudí přímo z US.

Zákonné a smluvní povinnosti

Pokud dojde k výpadku OOTE nebude možné následně provádět odesílání reálných dat, protože k nim nebude mít OTE přístup, proto takovýto výpadek bude mít vliv prakticky jen na nedodržení, č. 359/2020 Sb. § 5, § 6, § 7 protože by distributor neplnil povinnosti jejich včasného předání. Dále může dojít k porušení vyhlášky č. 408/2015 Sb. Znovu však záleží na délce výpadku a stavu požadavků v systémech ČEZd. Z hlediska zákonných povinností je u této aplikace zhruba střední riziko nedodržení zákonných povinností pro typ měření C.

Řízení a provoz organizace

Na fungování organizace nemá fungování této aplikace až takový dopad, protože jde o jednu z mnoha specifických aplikací v rámci ČEZd. Spíše je celkově problém, že tuto aplikaci nelze nijak nahradit, než že by to zatížilo provoz samotný.

Ztráta důvěryhodnosti

Pokud jde o ztrátu důvěryhodnosti, tak je zde vyhodnoceno riziko jako Vysoké, protože jde o komunikaci s důležitým externím subjektem, který je pro

ČEZd strategicky důležitý. Dále z měření typu C se přes tuto aplikace posílá LP60 pro vyhodnocení výroben.

Finanční ztráta/ Narušení činností

Finanční ztráta v tomto případě hrozí podobná jako je výpočet z bodu věnovanému OAVS. Protože nejvíce problémů nefunkčnost systému přidělá všem výrobcům s typem měření C1. Požadovaná náhrada tedy spadá do kategorie vysoká.

Zajišťování nezbytných služeb

V rámci rozmachu mikrozdrojů a s postupným rozšiřováním AMM měření se výpadek systému či omezení služby přibližně může týkat více než 100 000 lidí. Proto toto hledisko je ohodnoceno jako vysokém.

Tabulka 19 OOTE Vyhodnocení rizik
Zdroj: Vlastní zpracování

Označení	Zákonné a smluvní povinnosti	Řízení a provoz organizace	Ztráta důvěryhodnosti	Finanční ztráta/ Narušení činností	Zajišťování nezbytných služeb	MTPD	MIDP	MTDL
OOTE	Střední	Střední	Vysoká	Vysoká	Vysoká	2 D	12 H	ZM

Účetního systému (US)

Jde o systém, ve kterém se vše účtuje a také smluvně vyhodnocuje, dále jsou v něm uloženy veškeré osobní údaje o odběratelích, proto se řadí mezi nejvíce choulostivé systémy.

Zákonné a smluvní povinnosti

Pokud dojde k výpadku US nebude možné následně fakturovat zákazníkům za odběr elektrické energie, dále předávat data z fakturace na OTE, vyřizovat odpojování a pohledávky, případně vyřizovat reklamace, protože takovýto výpadek bude mít vliv na drtivou většinu činností a rázem může dojít k porušení vyhlášky č.

359/2020 Sb. protože by distributor neplnil povinnosti včasné předání fakturačních dat. Dále může dojít k porušení vyhlášky č. 540/2005 Sb. Skoro ve všech směrech, dále zákona č. 458/2000 Sb. a vyhlášky č. 408/2015 Sb. Znovu však záleží na délce výpadku a stavu požadavků v US. Pokud by však došlo k výpadku systému na delší dobu, mohlo by to mít vysoký dopad na ČEZd v rámci žalob za finanční újmy.

Řízení a provoz organizace

Pokud by došlo k rozsáhlému výpadku US mohlo by to zastavit i činnost související s výkonem odečtů v terénu, protože by přestali chodit požadavky na odečet, dále by se neměli kam zasílat fakturační data. Většina systémů napojených na US by mohla směrem k US zastavit činnost a čekat, než se vše zprovozní. Proto bych ohodnotil riziko spjaté s výpadkem jako kritické.

Ztráta důvěryhodnosti

V při rozsáhlém výpadku US hrozí ztráta důvěryhodnosti ve velké míře, protože výpadek má vliv na chod velké části firmy a zároveň i ve vztahu k zákazníkům, pro to je zde dopad ohodnocen jako vysoký.

Finanční ztráta/ Narušení činností

Finanční ztrátu zde není potřeba vyčíslit, protože by v krajním případě při vyplacení náhrad mohla dosahovat astronomických výšin, proto je zde riziko dopadu kritické.

Zajišťování nezbytných služeb

V rámci zajištění nezbytných služeb je riziko dopadu na zákazníky v počtu od několika tisíc až po milion. Pokud by tedy došlo na nejhorší scénář, mohlo by to mít pro ČEZd fatální následky.

Tabulka 20 US Vyhodnocení rizik
Zdroj: Vlastní zpracování

Označení	Zákonné a smluvní povinnosti	Řízení a provoz organizace	Ztráta důvěryhodnosti	Finanční ztráta/ Narušení činností	Zajišťování nezbytných služeb	MTPD	MIDP	MTDL
US	Vysoká	Kritická	Kritická	Kritická	Kritická	12 H	2 D	Z24

KMZ terénního pracovníka (PKMZ)

Pro účely výkonu pracovníků v terénu je nutné, aby dostával pověřený pracovník na své KMZ v čas práci v podobě pracovních příkazů. Pracovník v terénu, řeší převážně odečet u míst s typem měření C4 a dále řeší zprávu všech OM včetně nápravy v případě výpadku komunikace.

Zákonné a smluvní povinnosti

Pokud dojde k výpadku systému spjatým s KMZ nebude možné následně fakturovat operativní požadavky v terénu efektivním způsobem a dojde především k poručení vyhlášky č. 540/2005 Sb. K porušení dalších vyhlášek by došlo pouze v jednotkách případů či v hodně extrémních, jako je například vyhláška č. 458/2000 Sb. a vyhlášky č. 408/2015 Sb. Proto má výpadek tohoto sytému pouze střední dopad na společnost ČEZd.

Řízení a provoz organizace

V případě velkého výpadku systému PKMZ by došlo i na zhoršení efektivity v rámci řízení pracovníků v terénu, dále by mohlo dojít k nesprávnému řešení některých požadavků, které by se k pracovníkům v terénu museli zasílat náhradní cestou. Jelikož ale není práce v terénu díky nefunkčnosti systému tolik omezená. Neměli by být dopady na ČEZd větší než střední.

Ztráta důvěryhodnosti

Pokud by došlo k rozsáhlému výpadku PKMZ, mohlo by se stát, že dojde až na střední dopad na organizaci. Jelikož však jde denně o činnost, která se bude týkat určitých odloučených lokalit, tak důvěra v ČEZd až tolik neutrpí.

Finanční ztráta/ Narušení činností

Finanční ztráta může vzniknout pouze v případě nějakých žalob z důvodu finanční újmy zákazníka nebo nedodržení daných vyhlášek, neměla by však přesáhnout hodnoty několika desítek milionů korun, ale to by už bylo opravdu v extrémních případech. Spíše by tímto byl více zatížen provoz firmy a určitá neefektivita by měla za následek zvýšení nákladů.

Zajišťování nezbytných služeb

Jestliže by trval výpadek nebo nedostupnost systému několik dní nebo i týden, mohlo by se to dotknout maximálně několika desítek tisíc osob napříč celým distribučním územím ČEZd.

Tabulka 21 PKMZ Vyhodnocení rizik
Zdroj: Vlastní zpracování

Označení	Zákonné a smluvní povinnosti	Řízení a provoz organizace	Ztráta důvěryhodnosti	Finanční ztráta/ Narušení činností	Zajišťování nezbytných služeb	MTPD	MIDP	MTDL
PKMZ	Střední	Střední	Střední	Střední	Střední	1 WW	1 W	ZM

OM s typem měření C1 (OMC1)

Průběhové měření kategorie C1 s dálkovou komunikací je možné dálkově omezit či odpojit, dále lze dálkově řídit i ovládání tarifu, v případě výpadku komunikace se na místo posílá pracovník v terénu. Z měření typu C je u tohoto typu elektroměrů velmi důležitá bezpečnost.

Zákonné a smluvní povinnosti

Pokud dojde k výpadku OMC1 nebude možné provádět vzdáleně odečet elektrické energie na OM, dále nebude možné provést odpojení či připojení a také řízení činného výkonu. Pokud by se tak stalo v nepravou chvíli u spousty míst rázem může dojít k porušení vyhlášky č. 359/2020 Sb., č. 540/2005 Sb., dále zákona č. 458/2000 Sb. a vyhlášky č. 408/2015 Sb. Pokud by totiž neměl distributor řídit zátěž a výrobu na těchto odběrných místech mohlo by to to napáchat značné škody na distribuční síti a tím i dojít k porušení všech standardů bezpečné dodávky. Proto je zde riziko nastaveno jako vysoké

Řízení a provoz organizace

Na řízení a provoz organizace by mohl mít zásadní vliv výpadek i několika tisíc míst. Protože by ČEZd nemohla svými silami provést nápravu situace v terénu. Záleželo by na povaze výpadku a délce, v extrémních případech by mohlo dojít k vysokým dopadům na provoz.

Ztráta důvěryhodnosti

Pokud jde o toto hledisko, tak případný výpadek sítě kvůli její nemožnosti ji řídit na u OM jako jsou mikrozdroje, by mohlo mít velký i mediální dopad. Protože by mohlo dojít k narušení bezpečnosti dodávek elektrické energie v některých oblastech. Z tohoto důvodu je zde riziko vysoké.

Finanční ztráta/ Narušení činností

K velké finanční ztrátě by mohlo dojít pouze při výpadku komunikace s několika tisíci místy v době, kdy by bylo nutné za regulovat výrobu elektrické energie. Taková částka bohužel nejde přesně vyčíslit, ale mohla by v případě i soudních sporů přesáhnout hodnotu několika miliard. Proto je zde riziko dopadu určené jako vysoké.

Zajišťování nezbytných služeb

Pokud by výpadek či narušení komunikace s výrobnami zapříčinil pád sítě, tak by se mohlo stát, že bez energie bude v tu ránu 100000 lidí. Proto bylo riziko ohodnoceno jako vysoké.

Tabulka 22 OMC1 Vyhodnocení rizik
Zdroj: Vlastní zpracování

Označení	Zákonné a smluvní povinnosti	Řízení a provoz organizace	Ztráta důvěryhodnosti	Finanční ztráta/ Narušení činnosti	Zajišťování nezbytných služeb	MTPD	MIDP	MTDL
OMC1	Vysoká	Vysoká	Vysoká	Vysoká	Vysoká	1 W	24 H	ZM

OM s typem měření C2 (OMC2)

U průběhové měření kategorie C2 s dálkovou komunikací je možné dálkově odečítat i řídit ovládání tarifu, v případě výpadku komunikace se na místo posílá pracovník v terénu. Z měření typu C jde o jednu z nejpočetnějších skupin Elektroměrů.

Zákonné a smluvní povinnosti

Pokud dojde k výpadku OMC2 nebude možné provádět vzdáleně odečet elektrické energie na OM, dále nebude dodržen čas spínání. Pokud by se tak stalo v nepravou chvíli u spousty míst rázem může dojít k porušení vyhlášky č. 359/2020 Sb., č. 540/2005 Sb., dále zákona č. 458/2000 Sb. a vyhlášky č. 408/2015 Sb. Pokud by totiž neměl distributor řídit zátěž na těchto odběrných místech mohlo by to napáchat značné škody na distribuční síti a tím i dojít k porušení všech standardů bezpečné dodávky. Proto je zde riziko nastaveno jako vysoké.

Řízení a provoz organizace

Na řízení a provoz organizace by mohl mít zásadní rozsáhlý výpadek komunikace, protože by mohlo jít i o desetitisíce míst. Protože by ČEZd nemohla

svými silami provést nápravu situace v terénu. Záleželo by na povaze výpadku a délce, v extrémních případech by mohlo dojít k vysokým dopadům na provoz.

Ztráta důvěryhodnosti

Pokud jde o toto hledisko, tak případný výpadek sítě kvůli její nemožnosti ji řídit u OM s blokovanými spotřebiči. Následně by to mohlo mít velký i mediální dopad. Protože by mohlo dojít k narušení bezpečnosti dodávek elektrické energie v některých oblastech. Z tohoto důvodu je zde riziko vysoké.

Finanční ztráta/ Narušení činností

K velké finanční ztrátě by mohlo dojít pouze při výpadku komunikace s několika tisíci místy v době, kdy by bylo nutné za řídit zátěže pomocí odepnutí nebo sepnutí blokovaných spotřebičů. Taková částka bohužel nejde přesně vyčíslit, ale mohla by v případě i soudních sporů přesáhnout hodnotu několika miliard. Proto je zde riziko dopadu určené jako vysoké.

Zajišťování nezbytných služeb

Co do počtu odběrných míst je toto vůbec nejpočetnější typ měření, proto lze očekávat při rozsáhlejším výpadku komunikace i vysoké dopady na ČEZd. V podobě nedostupnosti služeb zákazníkům.

Tabulka 23 OMC2 Vyhodnocení rizik
Zdroj: Vlastní zpracování

Označení	Zákonné a smluvní povinnosti	Řízení a provoz organizace	Ztráta důvěryhodnosti	Finanční ztráta/ Narušení činností	Zajišťování nezbytných služeb	MTPD	MIDP	MTDL
OMC2	Vysoká	Vysoká	Vysoká	Vysoká	Vysoká	1 W	2 D	ZM

OM s typem měření C3 (OMC3)

U průběhové měření kategorie C3 s dálkovou komunikací je možné OM dálkově odečítat, v případě výpadku komunikace se na místo posílá pracovník v terénu. Z měření typu C jde o jednu z nejpočetnějších skupin Elektroměrů.

Zákonné a smluvní povinnosti

Pokud dojde k výpadku OMC3 nebude možné provádět vzdáleně odečet elektrické energie na OM. Pokud by se tak stalo v nepravou chvíli u spousty míst rázem může dojít k porušení vyhlášky č. 359/2020 Sb., č. 540/2005 Sb., dále zákona č. 458/2000 Sb. a vyhlášky č. 408/2015 Sb. Šlo by však pouze jen o odečty. Proto je zde riziko nastaveno jako vysoké.

Řízení a provoz organizace

Na řízení a provoz organizace by mohl mít zásadní rozsáhlý výpadek komunikace, protože by mohlo jít i o desetitisíce míst. Protože by ČEZd nemohla svými silami provést nápravu situace v terénu. Záleželo by na povaze výpadku a délce, v extrémních případech by mohlo dojít k vysokým dopadům na provoz.

Ztráta důvěryhodnosti

Pokud jde o toto hledisko, tak případný výpadek komunikace s velkým počtem elektroměrů na OM, by Následně mohl mít střední dopad. Protože by mohlo dojít pouze k pozdržení faktur u několika desítek tisíc zákazníků. Na pověsti ČEZd by to takový dopad nemělo.

Finanční ztráta/ Narušení činností

K velké finanční ztrátě by mohlo dojít pouze při výpadku komunikace s několika desítkami tisíc míst v době fakturace, kdy by bylo nutné řešit vyúčtování spotřeby a zasílání dat na OTE. Taková částka bohužel nejde přesně vyčíslit, ale mohla by v případě i soudních sporů přesáhnout hodnotu několika milionů korun. Proto je zde riziko dopadu určené jako střední.

Zajišťování nezbytných služeb

Co do počtu odběrných míst je toto druhý nejpočetnější typ měření, proto lze očekávat při rozsáhlejším výpadku komunikace pouze střední dopady na ČEZd. V podobě nedostupnosti služeb zákazníkům.

Tabulka 24 OMC3 Vyhodnocení rizik
Zdroj: Vlastní zpracování

Označení	Zákonné a smluvní povinnosti	Řízení a provoz organizace	Ztráta důvěryhodnosti	Finanční ztráta/ Narušení činnosti	Zajišťování nezbytných služeb	MTPD	MIDP	MTDL
OMC3	Vysoká	Vysoká	Střední	Střední	Střední	>1 WW	1 W	ZM

OM s typem měření C4 (OMC4)

U měření kategorie C4 s případnou dálkovou komunikací je možné OM dálkově odečítat, ve většině případů bude pracovníkem odečítáno v terénu. V případě výpadku komunikace u těch pár míst, co budou dálkově odečítána se na místo posílá pracovník v terénu. Z měření typu C jde o jednu z nejméně zastoupených skupin Elektroměrů.

Zákonné a smluvní povinnosti

U OM4 by mělo docházet odečtu v terénu jednou za rok a tak k porušení vyhlášky č. 359/2020 Sb., č. 540/2005 Sb., dále zákona č. 458/2000 Sb. a vyhlášky č. 408/2015 Sb. By došlo pouze omezeně. Proto je zde riziko nastaveno jako nízké.

Řízení a provoz organizace

Na řízení a provoz organizace by neměl mít výrazný vliv rozsáhlý výpadek komunikace, protože by se dálkově odečítalo pouze malé procento odběrných míst. Jediné, co by mohlo ovlivnit řízení a provoz v ČEZd je výpadek ostatních odběrných míst, pak by se mohlo stát, že k odečtu elektroměru by nedošlo včas, proto je riziko dopadu ohodnoceno jako střední.

Ztráta důvěryhodnosti

Na ztrátu důvěry by mohlo v tomto případě mít dopad pouze pozdržení faktur z důvodu opožděného odečtu. To by se však projevilo pouze u mizivého počtu OM, a proto by důvěryhodnost ČEZd neutrpěla žádnou újmu. Proto je zde riziko nízké.

Finanční ztráta/ Narušení činností

V tomto případě by mohlo dojít pouze k malé finanční ztrátě, protože jde o malou skupinu OM. Proto je zde riziko nízké.

Zajišťování nezbytných služeb

Co do počtu odběrných míst je toto nejméně početný typ měření, proto lze očekávat při rozsáhlejším výpadku komunikace pouze nízký dopad na ČEZd. V podobě nedostupnosti služeb zákazníkům.

Tabulka 25 OMC4 Vyhodnocení rizik
Zdroj: Vlastní zpracování

Označení	Zákonné a smluvní povinnosti	Řízení a provoz organizace	Ztráta důvěryhodnosti	Finanční ztráta/ Narušení činností	Zajišťování nezbytných služeb	MTPD	MIDP	MTDL
OMC4	nízké	střední	nízké	nízké	nízké	1WW	1W	-

7.7.3 CIA informačních aktiv ČEZd

Tato analýza slouží k určení důležitosti aktiv, se kterými v rámci AMM firma disponuje a využívá. Pro účely analýzy využijeme diagram viz. „Obr. 10 Diagram proudu informačních aktiv“. Dělení bude provedeno dle typů měření u něj se následně rozlišuje dle vyhlášky č.359/2020 Sb. v kapitole „8.4 Vodítka pro BIA“, zda jde o průběhové či neprůběhové měření a zda se jedná o výrobu či spotřebu a dvou tarifní měření nebo jedno tarifní sazbu. [6]

Tabulka 26 CIA Informačních aktiv
Zdroj: Vlastní zpracování

Typ měření / Informační aktivum	C1 Výroba/ Spotřeba 1T/2T průběh	C2 Spotřeba 2T průběh	C3 Spotřeba 1T průběh	C4 Spotřeba 1T/2T neprůběh
LP 15	[B; B; A]	[C; B; B]	[C; B; B]	[C; B; B] *
BW	[B; B; A]	[B; B; A]	[B; B; A]	[C; B; A] *
ODP	[B; A; A]	[B; A; A] **	[B; A; A] **	[B; A; A] **
PRIPO	[B; A; B]	[B; A; B] **	[B; A; B] **	[B; A; B] **
TAR	[A; A; B]	[B; A; B]	-	[B; B; B] ***
BLOK	[A; A; A]	-	-	-
LP60	[B; B; B]	[C; B; C]	[C; B; C]	[C; B; C] *

Poznámka:

** Informační aktivum se u daného typu měření vyskytuje pouze ve výjimečných případech, pokud je realizován dálkový odečet.*

*** Informační aktivum je prováděno pouze terénním pracovníkem pomocí KMZ nebo manuálně.*

**** Informační aktivum je pevně definované pracovníkem v terénu a nastavené pomocí KMZ.*

LP15

U aktiva LP15 jde o surová data odečtená z měřicího zařízení, jeho dostupnost není zase tak důležitá, většinou jí stačí zprovoznit v řádu dnů, protože se nejedná o fakturační hodnoty, ale spíše o informativní, jediný typ měření, u kterého jsou data z měření důležitější je měření typu C1 v případě přítomnosti výroby elektrické energie v OM.

Důvěrnost je u tohoto aktiva nařízena zákonem ve všech případech, jejich prozrazení by mohlo být v rozporu s GDPR a jinými zákony. V nepovolaných rukou by mohlo dojít k jejich zneužití pro obchodní účely.

Narušení integrity by mohlo ve všech případech způsobit minimálně omezení důležitých zájmů PDS. U mikrozdroje či malé výrobny v případě měření typu C1 by

to mohlo znamenat i problém pro fungování DS, pokud by se to týkalo velkého množství odběrných míst.

BW

V případě naměřených dat elektroměrem je BW velmi důležité aktivum, jedná se o opis registrů elektroměru, ze kterého se následně využívají data pro fakturaci. Proto narušení dostupnosti tohoto aktiva by mělo být vyřešeno v řádu hodin zejména v případech kdy je nutné na základě dat vyfakturovat odebranou či vyrobenou elektrickou energii. Rozdíl je, jestli se nedostupnost informačního aktiva objevila uprostřed měsíce nebo na konci, kdy je to větší problém.

Důvěrnost je u tohoto aktiva nařízena zákonem ve všech případech jako u LP15, prozrazení by mohlo být také v rozporu s GDPR a jinými zákony. V nepovolaných rukou by mohlo dojít k jejich zneužití pro obchodní účely.

Narušení integrity u jednoho informačního aktiva na jednom OM nemusí být pro organizaci až takový problém. Pokud však dojde k narušení informačního aktiva u tisíce míst, může to mít vážné důsledky na fungování celé DS.

ODP

Toto aktivum by ve většině případů nemělo být nedostupné déle než několik hodin z důvodu toho, že se jedná o odpojení odběrného místa například z důvodu neplacení, a to je vázáno závaznými termíny od obchodníka, za jehož nedodržení jsou vysoké sankce. Naštěstí taková varianta, aby bylo místo dálkově odpojeno se stává málokdy.

Prozrazením tohoto informačního aktiva by mohlo dojít v případech jeho vyzrazení u spousty odběrných míst k fatálním následkům na DS. Pokud by se informace o odpojování, jakým způsobem fungují atd. dostalo do nepovolaných rukou, může dojít i k narušení bezpečnosti dodávek v distribuční soustavě, úmyslným odpojením většího počtu odběrných míst od elektrické energie.

Narušení integrity v případě tohoto aktiva by mohlo mít za následek, že dojde k odpojení jiného OM než bylo plánováno a následně k ohrožení důvěry ve službu ČEZd a případně nákladným soudním sporům.

PRIPO

Toto aktivum by ve většině případů nemělo být nedostupné déle než několik hodin podobně jako ODP z důvodu toho, že se jedná o připojení odběrného místa například z důvodu zaplacení dlužné částky, a to je vázáno závaznými termíny od obchodníka, za jehož nedodržení jsou vysoké sankce. Dále by mohlo dojít na stížnosti zákazníka, který by na základě včasného nepřipojení mohl po ČEZd vymáhat škodu která mu byla způsobena. Naštěstí taková varianta, aby bylo místo dálkově připojeno se stává málokdy jako v případě ODP.

Prozrazením tohoto informačního aktiva by mohlo dojít v případech jeho vyzrazení u spousty odběrných míst k fatálním následkům na DS. Pokud by se informace o připojování, jakým způsobem fungují atd. dostalo do nepovolaných rukou, může dojít i k narušení bezpečnosti dodávek v distribuční soustavě, úmyslným neplánovaným připojením většího počtu odběrných míst k síti, většinou by to byl, ale problém v kombinaci s vyzrazením informací o ODP.

Narušení integrity v případě tohoto aktiva by mohlo mít za následek, že dojde nedojde k připojení OM, které mělo být připojeno. Následně by mohlo dojít na soudní spory s majitelem OM, avšak tyto případy by se mohli vyskytovat pouze ojediněle.

TAR

Toto aktivum by ve většině případů nemělo být nedostupné déle než hodinu, protože se využívá především ke korekci a připojování zátěže v síti, Toto aktivum se používá zejména k připojování a odpojování elektrických spotřebičů v síti tak aby byla zajištěna její stabilita podle spotřebované či odebrané elektrické energie, jediný případ, kde by to nemělo vadit je měření typu měření C4 u kterého se nastavují časy spínání na pevno pomocí TOU tabulky.

Prozrazením tohoto informačního aktiva by mohlo dojít v případech jeho vyzrazení u spousty odběrných míst k fatálním následkům na DS. Pokud by se informace o způsobu spínání, dostalo do nepovolaných rukou, může dojít i k narušení bezpečnosti dodávek v distribuční soustavě, úmyslným neplánovaným

připojením většího počtu spotřebičů, které zatíží distribuční soustavu a následkem toho může dojít i k blackoutu.

Narušení integrity v případě tohoto aktiva by mohlo mít za následek, že dojde k chybnému spínání spotřebičů. To by mohlo vést k nesymetrii v síti a k jejímu nadměrnému neplánovanému zatěžování a v extrémním případě i k blackoutu.

BLOK

Toto aktivum by ve většině případů nemělo být nedostupné déle než hodinu stejně jako v případě TAR, protože se využívá především řízení činného výkonu elektráren v síti, pokud vyrábějí až moc elektrické energie. Proto jeho nedostupnost v případě přebytků energie v síti může mít za následek výpadek celé sítě.

Prozrazením tohoto informačního aktiva by mohlo dojít v případech jeho vyzrazení u spousty odběrných míst k fatálním následkům na DS. Pokud by se informace o způsobu řízení činného výkonu, dostala do nepovolaných rukou, může dojít i k narušení bezpečnosti dodávek v distribuční soustavě. úmyslným neplánovaným odpojením nebo připojením většího počtu výroben či mikrozdrojů, tímto způsobem lze způsobit i blackout.

Narušení integrity v případě tohoto aktiva by mohlo mít za následek, že dojde k chybnému řízení činného výkonu u výroben či mikrozdrojů. To by mohlo vést k nesymetrii sítě a k jejímu nadměrnému neplánovanému zatěžování nebo blackoutu.

LP60

Toto aktivum se používá v případě typu měření C pouze jako informace. Pouze v případě měření C1 se údaje o výrobě mohou používat na trhu s elektřinou v případě spotových cen.

Důvěrnost je u tohoto aktiva nařízena zákonem ve všech případech, jejich prozrazení by mohlo být v rozporu s GDPR a jinými zákony. V nepovolaných rukou by mohlo dojít k jejich zneužití pro obchodní účely.

Narušením integrity by mohlo dojít k nesprávnému vyhodnocení některých kritérií v případech měření C1 u výroben, jinak by narušení integrity nemělo mít prakticky vliv na chod DS, pouze by si někteří zákazníci mohli stěžovat.

8 BCM pro AMM

V rámci analýzy byly zjištěny případné dopady na organizaci, pokud nebude správně zvolené opatření pro co nejvíce bezproblémový chod celého odečtového systému a spolehlivosti dodávek v celé distribuční soustavě v rámci ČEZd. BCM má za úkol toto zmapovat a určit opatření tak, aby byla zajištěna kontinuita a případná obnova chodu společnosti, pokud nějaká z popsaných hrozeb nastane.

8.1 Opatření vycházející s BIA u sytému pro AMM měření

Z BIA analýzy vyplývá že nejvíce zranitelným systémem je datová centrála **(DCT)**, účetní systém **(US)** a odečtového a validačního systému **(OAVS)**, kde jakýkoliv větší výpadek či omezení v řádu dnů, může mít obrovský dopad na fungování ČEZd.

Jako první bychom mohli řešit opatření u **datová centrála (DCT)**, jedno ze základních opatření, které by mělo být řešené je přístupnost. Jelikož bude denně přistupovat do DCT spousta uživatelů skrze různé systémy je nutné definovat přístupy, které by se měli odehrávat pouze v rámci interní sítě, které jsou definované v kapitole „5.4 Řízení přístupu“, toto by již mělo být v každé společnosti standardem. Dále je zde nutné předem správně definovat uživatele, kteří budou moci k datům v DCT přistupovat v rámci svých uživatelských rolí a přístupových klíčů. Dále by tento systém měl být kompletně nezávislý na ostatních a měla by v něm probíhat úplná záloha dat, která je také kompletně oddělená od hlavního systému DCT jak popisuje kapitola „5.8 Bezpečnost provozu“. U tohoto systému by měl být kladen důraz hlavně na zálohu dat, protože ty jsou zde pro společnost stěžejní a je nutné v případě potřeby provést co nejrychleji jejich obnovu ze zálohy. Z analýzy vyplívá, že tolerovaná maximální ztráta dat je zde týden, což je hodně, proto by bylo vhodné nastavit zálohování dat na 24 hodin.

Jako další z kriticky ohrožených systémů je **odečtová a validační systém (OAVS)**, do tohoto systému vstupují data z DCT, proto by komunikace mezi nimi měla být maximálně zabezpečena pomocí šifrování s dlouhou životností což řeší kapitola „5.5 Kryptografie“. Systém OAVS by měl být také plně oddělený od ostatních

systémů a přístupy řešené podobně jako DCT. Tento systém má v sobě uložená data základní identifikační údaje o odběrných místech, díky kterým může přistupovat ke konkrétním datům v DCT. V systému OAVS by měla být dle analýzy nastavena záloha na jeden týden což je dostatečná doba. Dále by zde bylo vhodné mít v záloze celý záložní systém, který by mohl dočasně vykonávat některé důležité úkony, než se znovu zprovozní hlavní systém OAVS.

Posledním s kritických systémů ČEZd je **účetní systém (US)**, ten je ze všech systémů asi nejkomplexnější, protože do něj vždy bude přistupovat asi nejvíce jiných systémů a aplikací i uživatelů, také zde je proto nutné přistupovat do systému pouze v rámci firemní sítě, a to šifrovaně a pokud možno v rámci co nejvíce definovaných uživatelských rolí. Dále zde nesmírně nutné, pokud dojde k jeho výpadku provést co nejrychlejší zprovoznění. Dle analýzy je určená záloha každých 24hodin což by mělo být dostatečné. I zde by mělo platit, že by bylo vhodné zřídit záložní systém, který by mohl při výpadku hlavního systému dále fungovat. Také by zde měla být data zákazníků pro větší bezpečnost uložena bokem od systému a pro účely maximálního zabezpečení by je měly chránit ty nejmodernější šifry.

U ostatních systémů a aplikací by se mělo komunikovat vždy zabezpečeně, pokud možno v interní síti a pravidelně provádět aktualizace bezpečnostních balíků. Také je zde vhodné pravidelně upravovat dle potřeb bezpečnostní politiku celé organizace, a hlavně se zaměřit na pravidelné audity jak interní, tak i u externích dodavatelů, tak aby se zajistilo co nejbezpečnější a spolehlivý chod společnosti. V neposlední řadě je nutné striktně ve smlouvách zajistit spolehlivost externích dodavatelů služeb a vymezit právní dopady v rámci neplnění standardů a smluvních podmínek.

8.2 Opatření vycházející s CIA informačních aktiv v AMM měření

V případě analýzy CIA byly za nejvíce cenná aktiva pro společnost ČEZd identifikovaná dle „Tabulky 26 CIA Informačních aktiv“ registry elektroměru (BW), pak zprávy, které slouží k řízení funkcí elektroměru jako zpráva o odpojení (ODP), zpráva o připojení (PRIPO), zpráva o blokování spotřebičů (TAR) a zpráva o řízení činného výkonu u výroben (BLOK). Z těchto aktiv je asi nejvíce důležité, aby byl co

nejvíce zabezpečen přenos informace BLOK, jde totiž o nástroj, kterým distributor v reálném čase zajišťuje stabilitu celé sítě, zároveň je zde další z nástrojů řízení sítě, a to je TAR kde se zapíná či vypíná blokované spotřebiče.

Všechna aktiva, co souvisí nějakým způsobem s ovládáním elektroměru by měla být zašifrována dle aktuálních platných doporučení od NUKIB jak řeší kapitola „5.5 Kryptografie“. Následně pokud se pomocí těchto aktiv přistupuje do Elektroměrů, tak by zde měla být vydaná pro každý z elektroměrů zvlášť sada klíčů, která bude zase šifrovaná dle standardů a definovaná podle druhu přístupu k elektroměru, čtení dat, úprava nastavení sazby, vypnutí a zapnutí odpojovače, případně blokování spotřebičů nebo řízení činného výkonu. Komunikace u těchto informačních aktiv by měla být šifrovaná a jen v rámci interní sítě.

Pokud se jedná o data odečtená z elektroměru jako jsou PL15 a BW tak by přístup k nim měl být zabezpečen pomocí hesla. Zároveň by neměl být v žádném případě možný dálkově přepis dat v elektroměru. Pokud by se prováděla komunikace na odběrném místě pomocí KMZ pracovníka v terénu, tak by měl být přístup do měřícího zařízení zajištěn heslem. KMZ pracovníka by mělo fungovat v rámci práce pouze v interní sít. I tak by veškerá komunikace do systémů měla být šifrovaná.

Pro informační aktiva by mělo platit to stejné co pro systémy v ČEZd, jejich bezpečnostní politiky by měli být v souladu s platnými doporučeními NUKIB a pravidelně se aktualizovat.

9 Závěry a doporučení

V rámci diplomové práce byla rozebrána norma ISO/IEC 27001:2013 a její implementace ISO/IEC 27002:2013. Pokud by byl dle doporučení této normy vytvořen funkční systém pro AMM měření, tak bychom ho teoreticky mohli považovat za bezpečný pouze v případě, že bychom zároveň vzali v potaz aktuální doporučení NUKIB. Norma jako taková je již 10 let stará a některé její poznatky v rámci zabezpečení by bylo vhodné rozšířit o jiné. Proto se norma stále rozšiřuje o nové druhy implementací, které jsou lepší i horší.

Jelikož je plošný rozvoj AMM teprve na začátku je spousta věcí v rámci implementace, které zatím nelze popsat či je správně uchopit. V rámci testování v některých projektech AMM zatím nemohlo být vše otestováno dle platných legislativních požadavků. Navíc zatím chybí ještě spousta úprav vyhlášek, tak aby reagovali na nově vznikající typ měření C1, C2, C3, C4, zářným příkladem je Vyhláška č. 408/2015 Pravidla trhu s elektřinou, kde se o tomto vůbec nemluví, a to už má být do roku 2027 osazeno na odběrných místech s odběrem větším než 6MWh. Proto se v některých směrech v rámci BIA analýzy nedá vše konkrétně vyčíslit. Dále je nutné se zajímat o to, zda vůbec lze v rámci AMM měření dosáhnout některých bezpečnostních požadavků, protože je zde nutné brát v potaz náročnost šifrovacích algoritmů, které jdou proti snaze co nejvíce zlevnit nákup hardware v podobě elektroměrů. Proto bude pro ČEZd nelehký úkol zvolit správný poměr cena/výkon. Také je zde riziko, že s rozvojem IT se může vše kolem bezpečnosti šifrování změnit a systém zabezpečení, který byl navržen na životnost třeba 25let, bude potřeba vyměnit nebo razantně upravit již po 10 letech fungování. To vše jsou rizika, se kterými by se mělo počítat v případě implementace AMM měření.

Diplomovou práci by bylo možné do budoucna rozšířit o některé konkrétní informace z oblasti zabezpečení jednotlivých prvků v celém systému, jako jsou síťové prvky a jiné systémy, které zde nebyly uvedeny. Dále je možné ještě popsat, jak by měla správně fungovat struktura organizace ve které se zabezpečení podle ISO/IEC 27001:2013 implementuje což tu nebylo zmíněno.

10 Seznam použitých zkratek

Zkratka	Popis
OM	Odběrné místo
ELM	Elektroměr
MTPD	Maximum Tolerable Period of Disruption - maximální doba tolerance nedostupnosti s maximálním dopadem na organizaci
MIDP	Medium Impact Period of Disruption - maximální doba tolerance nedostupnosti se středním dopadem na organizaci
MTDL	Maximum Tolerable Data Loss - maximální doba od poslední zálohy dat
NN	Nízké napětí
FVE	Fotovoltaická elektrárna
AMM	Automated Meter Management - Systém pro dálkové zpracování odečtů dat elektroměrů a jejich řízení.
LP 15	Last profil (profil spotřeby/výroby v intervalu 15 minut)
LP 60	Last profil (profil spotřeby/výroby v intervalu 60 minut)
BW	Billing value (registr elektroměru)
BTS	Base transceiver station (vysílač rádiových signálů)
GSM	Groupe Spécial Mobile (standart telekomunikační normy)
GPRS	General Packet Radio Service (služba umožňující u GSM telefonů internet)
AMR	Automated Meter Reading (automatický odečet měřidel)
PLC	PowerLine Communication (úzkopásmový a širokopásmový přenos zpráv po elektrické síti)
BPL	Broadband over Powerline (vylepšená technologie širokopásmového přenosu zpráv po elektrické síti)
CSD	Circuit Switched Data (nejstarší metoda přenosu dat u mobilních sítí)
OBIS	Object Identification System (identifikační kódy registrů elektroměru)
TOU	Time of use (tabulka sloužící k nastavení sazby u elektroměru)

ISO	International Organization for Standardization – mezinárodní standardy, vydávané mezinárodní organizací pro normalizaci
IEC	International Electrotechnical Commission – mezinárodní elektrotechnická komise
BIA	Business Impact Analysis – analýza dopadů – je proces analýzy činností organizace a dopadů na ni.
CIA	Confidentiality, availability, integrity – důvěrnost, dostupnost, integrita
ISMS	Information Security Management Systém – Systém řízení bezpečnosti informací
PPDS	Pravidla provozování distribuční soustavy
BCM	Business Continuity Management - Řízení kontinuity činností organizace
ČSN	československé státní normy - chráněné označení českých technických norem
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
ENISA	European Network and Information Security Agency -evropská agentura pro informační a síťovou bezpečnost (kyberbezpečnost)
PCQ	Post Quantum Cryptography – post kvantová cryptografie
SVZ	Statistická výběrová zkouška
DSA	Digital Signature Algorithm – algoritmus digitálního podpisu
RSA	Rivest Shamir Adleman – šifrovací systém s veřejným klíčem
SHA	Secure Hash Algorithm – rozšířená hašovací funkce, která vytváří ze vstupních dat výstup (otisk) fixní délky
CTR	short for Counter - populární režim blokové šifry AES
DES	Data Encryption Standard - algoritmus symetrického klíče pro šifrování digitálních dat
DRBG	Deterministic random bit generator – deterministický generátor náhodných bitů
PRNG	Pseudorandom number generator – Generátor pseudonáhodných čísel

EME	Encrypt Mix Encrypt – široký blok šifrovací režim vyvinutý společností Halevi
OFB	Short for output feedback – blokový šifrovací režim AES podobný režimu CFB
CFB	Cipher feedback – režim blokové šifry AES podobný režimu CBC
CBC	Cipher-block chaining – režim blokové šifry AES, který trumfuje režim ECB ve skrývání vzorů v prostém textu.
4G/LTE	Long Term Evolution – označení technologie pro vysokorychlostní přenos dat v mobilních sítích 4 generace.
LPWA	Low Power Wide Area – komunikace s nižším výkonem než jiné sítě, jako jsou mobilní, satelitní nebo WiFi
5G	Pátá generace bezdrátových systémů – telekomunikační standard mobilní sítě, který technicky navazuje na standard 4G (LTE)
IoT	Internet of Things – je termínem pro moderní síť určenou pro přístroje ovladatelné i na dálku pomocí internetu.
EDGE	Enhanced Data Rates for GSM Evolution – jedná se o technologii 2G určené pro přenos dat po mobilní síti.
GPRS	General Packet Radio Service – služba umožňující uživatelům mobilních telefonů GSM přenos dat a připojení k internetu
GEA	Generic Encryption Algorithm – algoritmus pro zabezpečení sítí GPRS
KASUMI	Bloková šifra používaná v mobilních komunikačních systémech UMTS, GSM a GPRS
COMP128	algoritmus implementovaných funkcí definovaných ve standardu GSM
LFSR	Linear feedback shift register – výpočetní posuvný registr, jehož vstupní bit je lineární funkcí jeho předchozího stavu.
HMAC	Hash message authentication code – ověřovací kód zprávy s klíčem
UEA	Ultra Encryption Algorithm – Symetrický klíč na úrovni bitů krypto systému s náhodnými bity a mechanismem zpětné vazby
EEA	Extended euclidean algorithm – rozšířený euklidovský algoritmus
AES	Advanced Encryption Standard – variantou blokové šifry Rijndael

11 Seznam použité literatury

[1] ČEZ Distribuce a.s. ČEZ Distribuce [online]. Děčín: FG Forrest, 2020 [cit. 2020-08-04]. Dostupné z: https://www.cezdistribuce.cz/

[2] ERU. ERU: Energetický regulační úřad [online]. Jihlava: ERU, 2020 [cit. 2020-08-04]. Dostupné z: https://www.eru.cz

[3] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

[4] BEZPEČNOSTNÍ POŽADAVKY NA MĚŘIDLA A SOUVISEJÍCÍ INFRASTRUKTURU [online]. BRNO, 2020 [cit. 2023-04-25]. Dostupné z: https://www.mpo.cz/assets/cz/energetika/strategicke-a-koncepcni-dokumenty/narodni-akcni-plan-pro-chytre-site/2020/5/Vytah-studie-NAP-SG-kyberneticka-bezpecnost.pdf. Studie. VUT Brno. Zodpovídá Doc. Ing. Jan Hajný, Phd., Doc. Ing. Petr Mlýnek, Ph.d., Ing. Zdeněk Martinsek, Ph.d.

[5] EU CYBERSECURITY MARKET ANALYSIS: IoT in Distribution Grids [online]. April 2022. 95 Nikolaou Plastira 700 13 Vassilika Vouton, Heraklion, Greece: enisa, 2022 [cit. 2023-04-25]. ISBN 978-92-9204-560-9. Dostupné z: https://www.enisa.europa.eu/publications/eu-cybersecurity-market-analysis-iot-in-distribution-grid

[6] Dopady dálkových měření elektrické energie: BIA analýza. Hradec Králové, 2020. Bakalářská práce. Univerzita Hradec Králové. Vedoucí práce Mgr Josef Horálek.

[7] Post-Quantum Cryptography: Integration study. The European Union Agency for Cybersecurity [online]. 2022, october 2022, -(-), 41 [cit. 2023-04-26]. Dostupné z: doi:10.2824/15116

[8] Národní úřad pro kybernetickou a informační bezpečnost. NÚKIB Brno [online]. Brno: NÚKIB Brno, 2023, 2023-04-25 [cit. 2023-04-25]. Dostupné z: https://www.nukib.cz/

[9] ČSN ISO/IEC 27001. Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací: Požadavky. Září 2014. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[10] ČSN ISO/IEC 27002. Informační technologie – Bezpečnostní techniky: Soubor postupů pro opatření bezpečnosti informací. Září 2014. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

[11] Zákon č. 458/2000 Sb. o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů. ČR: ERU, 2000.

[12] Vyhláška č. 408/2015 Sb. o pravidlech trhu s elektřinou. ČR: ERU, 2015.

[13] Vyhláška č. 540/2005 Sb. o kvalitě dodávek elektřiny a souvisejících služeb v elektroenergetice. ČR: ERU, 2005.

[14] Vyhláška č. 82/2011 Sb. o podmínkách měření elektřiny a o způsobu stanovení náhrady škody při neoprávněném odběru, neoprávněné dodávce, neoprávněném přenosu nebo neoprávněné distribuci elektřiny. ČR: MPO, 2011.

[15] Vyhláška č. 359/2020 Sb. Vyhláška o měření elektřiny ČR: MPO, 2020

[16] Zákon č. 505/1990 Sb. Zákon o metrologii. ČR: MPO, 1991

Přílohy – Oskenované zadání práce

Údaje o diplomové práci

Osobní číslo:	I2000710	Datum zadání:	19. ledna 2021
Jméno a příjmení:	Bc. Radomír Werner	Plánované datum odevzdání:	30. června 2022
		Datum odevzdání:	
Studijní program:	N0688A140001 Informační management		
Zadané téma:	Návrh zabezpečení systému AMM v souladu s požadavky ISO 2001		
Stav práce:	Rozpracovaná práce		

Údaje o kvalifikační práci

1. **Hlavní téma**
   Návrh zabezpečení systému AMM v souladu s požadavky ISO 2001
2. **Hlavní téma v angličtině**
   Security design of the AMM system in accordance with the requirements of ISO 2001
3. **Název dle studenta**
4. **Název dle studenta v angličtině**
5. **Souběžný název**
6. **Podnázev**
7. **Anotace (krátký popis práce)**
8. **Klíčová slova (oddělujte čárkou)**
9. **Anotace v angličtině (krátký popis práce)**
10. **Anglická klíčová slova (oddělujte čárkou)**
11. **Přílohy volně vložené**
12. **Přílohy vázané v práci**
13. **Rozsah práce**
14. **Jazyk práce**
    CZ
15. **Záznam průběhu obhajoby**
16. **Zásady pro vypracování**

    Cílem práce je navrhnout zabezpečení systému AMM v souladu s požadavky plynoucícmi z normy ISO 27001.

    V teoretické části práce autor zpracuje relevantní požadavky plynoucí z norym ISO 2001 s ohledem na systém AMM. V praktické části autor nejdříve zpracuje požadavky na kontinuity činností, identifikuje datová aktiva a navrhne relevantí technická opatření pro zajištění informační a kybernetické bezpečnosti s souladu s požadavky ISO 27001.

    Osnova:

    Úvod

    Problematika ISMS

    Hlavní principy AMM

Údaje o diplomové práci

Osobní číslo:	**I2000710**	Datum zadání:	19. ledna 2021
Jméno a příjmení:	**Bc. Radomír Werner**	Plánované datum odevzdání:	30. června 2022
Studijní program:	**N0688A140001 Informační management**	Datum odevzdání:	
Zadané téma:	Návrh zabezpečení systému AMM v souladu s požadavky ISO 2001		
Stav práce:	Rozpracovaná práce		

Definice rozsahu AMM – datový pohled

Deficnice rozsahu AMM – technický pohled

BIA nad daty AMM

BCM pro AMM

Zhodnocení navržených řešení

Závěr

17. Seznam doporučené literatury

ČSN ISO/IEC 27001. Praha: Úřad pro technickou normalizaci, 2013. Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů

18. Osoby VŠKP

Vedoucí diplomové práce: **Mgr. Josef Horálek, Ph.D.**
Katedra informačních technologií

Elektronická forma kvalifikační práce

Zatím není přiložen žádný soubor s elektronickou formou práce...

Posudky kvalifikační práce

Posudek(y) oponenta:

Hodnocení vedoucího:

Soubor s průběhem obhajoby:

Potvrzuji správnost vložených údajů a potvrzuji plnou shodu elektronické verze s odevzdávanou listinnou verzí VŠKP.

Datum: **Podpis:**