

Výpadky v dodávkách elektrické energie

Nikola Peřinová

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Nikola Peřinová
Osobní číslo: A21574
Studijní program: B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia: Prezenční
Téma práce: Výpadky v dodávkách elektrické energie
Téma práce anglicky: Blackouts

Zásady pro vypracování

- Analyzujte odbornou literaturu a případové studie týkající se blackoutů a elektrické energetiky včetně historických blackoutů ve světě.
- Prozkoumejte a popište historické případy blackoutů a jejich důsledky na společnost a ekonomiku.
- Pojednejte o příčinách výpadků v dodávkách elektrické energie a identifikujte klíčová rizika spojená s elektrickou energetikou.
- Provedte analýzu postupů řízení a obnovy po blackoutu.
- Zhodnoťte současná opatření a technologii používané k prevenci blackoutů.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. ŘEHÁK, David. Kritická infrastruktura elektroenergetiky: určování, posuzování a ochrana. Spektrum (Sdružení požárního a bezpečnostního inženýrství). V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2013. ISBN 978-80-7385-126-2.
2. Trh s elektřinou: úvod do liberalizované energetiky. Druhé aktualizované vydání. Praha: Asociace energetických manažerů, 2016. ISBN 978-80-260-9212-4.
3. HRUBÝ, Zdeněk a KOL. LUKÁŠEK LIBOR A. Energetická bezpečnost České republiky. Karolinum, 2016. ISBN 978-80-246-2974-2.
4. GRIGSBY, Leonard L. (ed.). Power system stability and control. The electrical engineering handbook series. Boca Raton: CRC Press, c2007. ISBN 9780849392917.
5. MARTÍNEK, Zbyněk a HÁJEK, Josef. Analýza spolehlivosti přenosových a rozvodných sítí ES ČR. V Plzni: Západočeská univerzita v Plzni, 2002. ISBN 8070828951.

Vedoucí bakalářské práce: **Ing. Tomáš Martínek, Ph.D.**
Ústav elektroniky a měření

Datum zadání bakalářské práce: **11. prosince 2024**

Termín odevzdání bakalářské práce: **2. června 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 11. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Blackouty jsou stále častějším jevem. V posledních letech došlo k několika významným blackoutům v Evropě, Severní Americe i dalších částech světa. Cílem této práce je poskytnout přehled faktorů, které k výpadkům přispívají, a navrhnout strategie ke snížení jejich výskytu a omezení negativních dopadů. Teoretická část zahrnuje analýzu odborné literatury související s výpadky elektrické energie. Dále jsou popsány vybrané historické případy blackoutů včetně jejich důsledků na společnost a ekonomiku. V praktické části je provedena analýza hlavních příčin a identifikace klíčových rizik spojených s elektrizační soustavou, rozbor postupů řízení a obnovy po blackoutu a zhodnocení současných opatření a technologií používaných k jejich prevenci.

Klíčová slova: výpadek proudu, elektrická energie, kritická infrastruktura, energetická bezpečnost, odolnost sítě

ABSTRACT

Blackouts represent an increasing threat to modern energy infrastructure. In recent years, several major power outages have occurred in Europe, North America, and other parts of the world. The aim of this thesis is to provide an overview of the factors contributing to these outages and to propose strategies for reducing their frequency and mitigating their negative impacts. The theoretical part focuses on the analysis of relevant literature related to blackouts. It also includes a description of selected historical blackout events and their impacts on society and economic situation. The practical part analyses the main causes and key risks associated with the power system, examines blackout response and recovery procedures, and evaluates current preventive measures and technologies.

Keywords: blackout, electrical energy, critical infrastructure, energy security, grid resilience

Děkuji vedoucímu práce panu Ing. Tomášovi Martínkovi, Ph.D. za odborné vedení, čas, trpělivost, proaktivní přístup a rady, které mi poskytoval při zpracovávání bakalářské práce. Dále chci poděkovat všem, kteří mi poskytovali podporu v průběhu studia, zejména svému otci.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	12
1 VYMEZENÍ ZÁKLADNÍCH POJMŮ	13
1.1 BLACKOUT	13
1.2 PŘENOSOVÁ SOUSTAVA.....	13
1.3 DISTRIBUČNÍ SOUSTAVA.....	13
1.4 KRITICKÁ INFRASTRUKTURA ELEKTROENERGETIKY	14
1.5 PREVENCE BLACKOUTŮ	15
1.6 OBNOVA PO BLACKOUTU.....	15
1.7 KASKÁDOVÝ EFEKT.....	16
2 HISTORICKÉ PŘÍPADY BLACKOUTŮ A JEJICH DŮSLEDKY	17
2.1 NEW YORK CITY 1977	17
2.2 SEVEROZÁPAD SPOJENÝCH STÁTŮ AMERICKÝCH A KANADA 2003	19
2.3 ITÁLIE 2003.....	20
2.4 BRAZÍLIE 2009	21
2.5 PORTORIKO 2017.....	23
2.6 TEXAS 2021	24
2.7 SROVNÁNÍ BLACKOUTŮ	25
II PRAKTICKÁ ČÁST.....	27
3 ANALÝZA PŘÍČIN VÝPADKŮ V DODÁVKÁCH ELEKTŘINY	28
3.1 VLIVY POČASÍ	34
3.2 PŘÍRODNÍ KATASTROFA.....	35
3.3 PORUCHA	37
3.4 LIDSKÝ FAKTOR	38
3.5 ORGANIZAČNÍ SELHÁNÍ	38
3.6 KYBERNETICKÝ ÚTOK	39
3.7 TERORISTICKÝ ÚTOK	40
3.8 ZÁVĚR.....	41
4 POSTUPY ŘÍZENÍ A OBNOVY PO BLACKOUTU	42
4.1 TYPOVÝ PLÁN NARUŠENÍ DODÁVEK ELEKTRICKÉ ENERGIE VELKÉHO ROZSAHU	42
4.2 KOMPARATIVNÍ ANALÝZA PŘÍPADŮ	43
4.2.1 Blackout New York City (1977) – řízení a obnova	43
4.2.2 Blackout Severovýchod USA a Kanada (2003) – řízení a obnova	43

4.2.3	Blackout Itálie (2003) – řízení a obnova	44
4.2.4	Blackout Brazílie (2009) – řízení a obnova.....	44
4.2.5	Blackout Portoriko (2017) – řízení a obnova	44
4.2.6	Blackout Texas (2021) – řízení a obnova.....	44
4.2.7	Srovnání blackoutů – řízení a obnova	45
4.3	SHRNUTÍ A DOPORUČENÍ.....	46
4.3.1	Doporučení pro české prostředí.....	47
5	ZHODNOCENÍ SOUČASNÉ PREVENCE.....	48
	ZÁVĚR.....	50
	SEZNAM POUŽITÉ LITERATURY	51
	SEZNAM OBRÁZKŮ	57
	SEZNAM TABULEK.....	58
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	59

ÚVOD

Moderní společnost je ve stále větší míře závislá na spolehlivých dodávkách elektrické energie. Elektrická energie představuje základní podmínku fungování nejen běžného života domácností, ale také průmyslu, zdravotnictví, dopravy, informačních technologií a dalších klíčových infrastruktur. Jakékoli narušení její dostupnosti může mít vážné důsledky pro bezpečnost, ekonomiku i každodenní životy obyvatel. Právě z tohoto důvodu přitahuje fenomén tzv. blackoutů stále větší pozornost odborné i laické veřejnosti.

V posledních desetiletích došlo k několika významným blackoutům ve vyspělých i rozvojových zemích. Čímž se ukázalo, že i technicky vyspělá energetická soustava může být zranitelná vůči různým druhům poruch, systémových selhání, extrémních povětrnostních jevů či kybernetických útoků. S rostoucí složitostí a provázaností energetických sítí narůstá nejen riziko takových událostí, ale také nároky na jejich prevenci a zvládání.

Tato práce si klade za cíl analyzovat příčiny a důsledky blackoutů, identifikovat hlavní faktory zvyšující jejich pravděpodobnost a popsat současné přístupy k řízení krizových situací a obnově dodávek. Dále budou zhodnoceny aktuální technologie a opatření, která mohou přispět ke zvýšení odolnosti energetické infrastruktury. Zvláštní pozornost bude věnována případovým studiím významných blackoutů, z nichž lze čerpat cenné poznatky pro budoucí prevenci a krizové plánování.

I TEORETICKÁ ČÁST

1 VYMEZENÍ ZÁKLADNÍCH POJMŮ

Vymezení základních pojmů je klíčovým krokem k pochopení problematiky blackoutů. Vzhledem k tomu, že některé termíny mohou mít více různých definic v závislosti na kontextu, je nezbytné je jasně a jednoznačně vymežit. Tato kapitola poskytne pevný základ pro další analýzu a umožní čtenářům lépe porozumět argumentaci i závěrům bakalářské práce.

1.1 Blackout

Blackout je úplná ztráta elektrické energie v jedné nebo více oblastech distribuční soustavy způsobená přetížením či selháním jednoho či více prvků soustavy. Tato ztráta může být dočasná nebo trvalá a má za následek výpadek dodávek elektrické energie pro spotřebitele v dané oblasti či oblastech. Blackout může být způsoben různými faktory, včetně přetížení přenosových linek, selhání generátorů nebo přepětí v síti. [1]

1.2 Přenosová soustava

Přenosová soustava je soustava elektrických vedení a zařízení, která slouží k přenosu elektrické energie z výrobních zdrojů k distribučním sítím. Jejím hlavním úkolem je zajišťovat tok elektrické energie na velké vzdálenosti přes regiony nebo dokonce mezi zeměmi. [2]

Tato soustava se skládá z vysokonapěťových elektrických vedení, transformátorů, spínacích stanic a dalšího vybavení, které umožňuje efektivní přenos elektrické energie přes dlouhé vzdálenosti s minimálními ztrátami. [2]

Zpravidla jsou přenosové soustavy navrhovány tak, aby byly schopny přenášet velké množství elektrické energie s vysokým napětím, což zvyšuje efektivitu přenosu a umožňuje minimalizaci energetických ztrát. [2]

1.3 Distribuční soustava

Distribuční soustava v elektrické energetice je druhým klíčovým prvkem elektrických sítí a tvoří spojení mezi přenosovou soustavou a koncovými spotřebiteli. Jejím hlavním účelem je distribuovat elektrickou energii přímo do míst spotřeby, což zahrnuje domácnosti, průmyslová zařízení, obchody a další spotřebitelské body. [2]

Tato soustava zahrnuje nízkonapěťová elektrická vedení, transformátory, rozvodny a další prvky, které umožňují rozvádět elektrickou energii na místní úrovni. Na rozdíl od přenosové soustavy, která přenáší elektrickou energii na velké vzdálenosti s vysokým napětím, distribuční soustava pracuje s nižším napětím a je určena k přímému napojení na koncové uživatele. [2]

1.4 Kritická infrastruktura elektroenergetiky

Kritická infrastruktura je „prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.“ [3]

V případě kritické infrastruktury elektroenergetiky se jedná o klíčové prvky a systémy v oblasti výroby, přenosu a distribuce elektrické energie, na nichž závisí fungování ekonomiky, infrastruktury a každodenního života obyvatel. Přestože elektroenergetika je nezbytná pro moderní společnost, je zároveň citlivá na různé hrozby, včetně přírodních katastrof, kybernetických útoků, teroristických činů nebo technických poruch. [2]

Pro zařazení prvku do kritické infrastruktury musí splňovat určité podmínky stanovené nařízením vlády ze dne 22. prosince 2010, o kritériích pro určení prvku kritické infrastruktury. Nařízení rozlišuje průřezová a odvětvová kritéria. Průřezová kritéria identifikují prvky kritické infrastruktury na základě jejich potenciálního dopadu na společnost, ekonomiku a veřejné služby. Podle těchto kritérií je prvek považován za součást kritické infrastruktury, pokud jeho selhání či narušení může způsobit významné ztráty na životech a zdraví obyvatelstva, tedy úmrtí více než 250 osob nebo hospitalizaci více než 2500 osob na dobu delší než 24 hodin. Z ekonomického hlediska se za prvek kritické infrastruktury považuje ten, jehož selhání by vedlo k hospodářské ztrátě přesahující 0,5 % hrubého domácího produktu. Posledním průřezovým kritériem je dopad na veřejnost, přičemž mezní hodnotou je rozsáhlé omezení poskytování nezbytných služeb či jiné závažné narušení každodenního života, které postihne více než 125 000 osob. [4]

Odvětvová kritéria jsou uvedena v příloze k danému nařízení a vymezují podmínky pro zařazení prvku do kritické infrastruktury v jednotlivých odvětvích. Pro účely této práce jsou stěžejní kritéria pro určení prvků kritické infrastruktury v elektroenergetice. Ta podrobně vymezují, které konkrétní součásti elektrizační soustavy jsou považovány za kritické pro zajištění stability a bezpečnosti dodávek elektrické energie. Mezi tyto prvky patří výroby

elektřiny s celkovým instalovaným výkonem alespoň 500 MW, případně výrobní poskytující podpůrné služby s výkonem nejméně 100 MW, vedení pro vyvedení výkonu a zabezpečení vlastní spotřeby výrobní elektřiny a dispečink výrobce elektřiny. Z přenosové soustavy zde řadí vedení o napětí nejméně 110 kV, elektrické stanice s napětím minimálně 110 kV a technický dispečink provozovatele přenosové soustavy. V rámci distribuční soustavy jsou zde řazeny elektrické stanice a vedení o napětí 110 kV, pokud jejich strategický význam v distribuční síti odůvodňuje jejich zařazení, a také technický dispečink provozovatele distribuční soustavy. [4]

Narušení kritické infrastruktury elektroenergetiky, například masivní blackout nebo systematické selhání elektrických sítí, znamenat ohrožení bezpečnosti státu a způsobit značné obtíže v zajišťování základních potřeb obyvatelstva, fungování nemocnic, komunikací a dalších klíčových odvětví. [2]

Zabezpečení kritické infrastruktury elektroenergetiky zahrnuje opatření na prevenci, detekci a reakci na hrozby, stejně jako plány obnovy v případě jejího selhání. Tato opatření jsou zaměřena na minimalizaci rizik a maximalizaci schopnosti infrastruktury odolat a rychle se zotavit ze situací, které by mohly ohrozit její integritu a funkčnost. [2]

1.5 Prevence blackoutů

Prevence blackoutů zahrnuje širokou škálu opatření a strategií, jejichž cílem je minimalizovat riziko vzniku blackoutů nebo snížit jejich dopady v případě, že k nim dojde. Tato preventivní opatření jsou klíčová pro udržení spolehlivosti a bezpečnosti elektroenergetických systémů. [5]

1.6 Obnova po blackoutu

Obnova po blackoutu zahrnuje celou řadu postupů a opatření, která jsou přijímána a implementována po vzniku výpadku elektřiny, s cílem co nejrychleji obnovit normální fungování energetického systému. Tento proces je klíčový pro minimalizaci dopadů blackoutu na společnost, hospodářství a zabezpečení základních životních potřeb obyvatelstva. Obnova po blackoutu je náročným procesem, který vyžaduje systematický a koordinovaný přístup, a to nejen technický, ale i organizační a komunikační. [5]

1.7 Kaskádový efekt

Kaskádový efekt je situace, kdy jedna událost spustí další události. V případě problematiky blackoutů je důležité zmínit hlavně kaskádové poruchy. Tedy situaci, kdy porucha jednoho prvku energetické soustavy vede k výpadkům dalších prvků. [5]

Tento efekt pak může z malého lokálního výpadku udělat rozsáhlý blackout. Tento jev je možné zpozorovat u mnoha případů blackoutů z minulosti, kdy selhání jednoho prvku způsobilo přetížení dalšího. Kaskádové výpadky jsou ovlivněny mnoha faktory jako jsou například stav komponent systému, vnitřními předpisy firmy a jejich dodržování. Obecně platí, že takové výpadky vznikají v důsledku odpojení obvodových přepínačů. K tomu může dojít buď manuálně, kdy člověk aktivuje přepínač, nebo automaticky pomocí relé. Provozovatelé elektrických sítí se samozřejmě snaží zabránit vzniku tohoto efektu, proto k němu obvykle nedochází, pokud selže pouze jeden systém. [6]

2 HISTORICKÉ PŘÍPADY BLACKOUTŮ A JEJICH DŮSLEDKY

V historii energetického sektoru se vyskytlo několik významných blackoutů, které nejen ovlivnily místní komunity, ale také měly dalekosáhlé dopady na formování bezpečnostních standardů a politik v oblasti energetiky. Tyto incidenty nesloužily pouze jako varování, ale také jako katalyzátory pro změny směřující ke zvýšení odolnosti a spolehlivosti energetických sítí.

V minulosti jsme byli svědky událostí, jako například blackoutů v Evropě, Severní Americe a dalších částech světa, které zdůraznily křehkost energetických infrastruktur a potřebu systematického přístupu k prevenci a řízení výpadků. Tyto události se staly klíčovými momenty, které nás vedou k hlubšímu pochopení vývoje problematiky a vytváření efektivnějších strategií pro budoucí zvládání krizových situací.

Blackouty, ačkoliv jsou většinou považovány za negativní události, mohou sloužit jako důležité učební příležitosti. Analýza příčin, průběhu a následků těchto událostí nám umožňuje identifikovat klíčové body selhání, které lze následně adresovat prostřednictvím lepších technologických řešení, procedurálních změn a investic do infrastruktury.

V dnešní době, kdy je spolehlivost dodávek elektrické energie klíčovým faktorem pro udržení normálního fungování společnosti, je důležité poučit se z minulosti a podniknout opatření k prevenci budoucích blackoutů. Získané znalosti a zkušenosti z historických incidentů nám slouží jako cenný základ pro posílení odolnosti energetických sítí a zajištění stabilní dodávky elektrické energie v budoucnosti.

2.1 New York City 1977

V červenci 1977 zasáhla město New York událost, kterou do té doby nikdo ani nepovažoval za možnou. To ostatně situaci činilo tak vážnou. Nikdo na ni nebyl připravený. Tento blackout trval celkem 25 hodin a zasáhl 9 milionů lidí. [7]

Výpadek byl způsoben souběhem několika událostí, včetně přírodních jevů, nesprávně fungujících ochranných zařízení, nedostatečného poskytování dat dispečerovi systému a komunikačních problémů. Blesk zasáhl vysokonapěťové vedení mezi dvěma rozvodnami a způsobil problém na obou jeho okruzích. Vypínače v rozvodně zareagovaly na poruchu a odpojily postižené okruhy od zbytku sítě, aby se zabránilo dalšímu šíření problému. Systém měl automaticky odpojit jen problematické okruhy, ale kvůli chybě v jeho návrhu došlo k tomu, že se odpojilo i vedení, které nebylo přímo postižené úderem blesku. Přibližně

18 minut po prvním incidentu způsobil další úder blesku další poruchy a došlo tak k vypnutí jističů na dalších dvou vedeních. Po druhém incidentu se síť ocitla ve velmi vážné nouzi. Během následujících přibližně 23 minut, kdy se síť zdála stabilní, docházelo na dvou zbývajících klíčových propojeních k vážnému přetížení. Přetížení se ještě zvýšilo, když došlo k odpojení dalšího vedení kvůli kontaktu vodičů se stromem. Následně došlo k odpojení transformátoru z důvodu přetížení ochrannými relé a v důsledku poruchy na přetíženém fázově posuvném regulačním transformátoru došlo k odpojení posledního vedení. [8]

Během výpadku zůstala telefonní síť sice funkční, ale byla přetížená, což vedlo k prodlevám při doručování oficiálních zpráv a častému obsazení linek. Vzhledem k tomu, že se výpadek odehrál v roce 1977, tedy v době před rozšířením mobilních telefonů a internetu, představovaly přenosné radiopřijímače na baterie hlavní zdroj informací pro obyvatelstvo. Zatímco televizní stanice a noviny nemohly kvůli výpadku fungovat, místní rozhlasové stanice aktivně informovaly o aktuálním dění. Přenosné rádio tak pro miliony zasažených obyvatel představovalo jediný přímý zdroj oficiálních pokynů a zpráv. [8]

Mnohé klíčové služby byly stále v provozu díky záložním generátorům elektrické energie. Některá zdravotnická zařízení a další instituce však měly nefunkční nouzové vybavení, v dalších bylo nutné provést opravy či údržbu, aby bylo možné zajistit dostatečný provoz náhradních zdrojů energie. Policejní stanice a energetická společnost, která spravovala postiženou síť, jim však poskytly potřebné vybavení. Za účelem udržení důležitých služeb napříč městem tato energetická společnost poskytla celkem 18 malých přenosných diesellových generátorů. Vybavení policie a hasičů fungovalo nepřetržitě. Bylo udrženo spojení a vybavení související s jejich činností a odborné znalosti policie byly využity ke zmírnění problémů v dalších oblastech. [8]

Doprava byla částečně omezena, i přes to se však podařilo uskutečnit některé naplánované lety z postižené oblasti. Metro bylo zcela paralyzováno. Naštěstí si však pracovníci dopravního podniku všimli, že systém nefunguje tak, jak by měl, a všem vlakům tak bylo přikázáno, aby zůstaly v nejbližší následující stanici. Z celkové počtu 213 vlaků jich tak pouze sedm uvízlo mezi stanicemi. Uvázlo tak méně než 1 000 cestujících, z nichž všichni byli evakuováni bez zranění. Autobusová doprava a zařízení správy přístavů byly k dispozici po celou dobu. [8]

Ekonomické ztráty byly značné. Podílelo se na tom i rabování a vandalismus, které se v době výpadku odehrávali. Celkové přímé ekonomické ztráty byly vyčísleny na více než 55

milionů amerických dolarů, nepřímé na téměř 300 milionů amerických dolarů. Největší přímé ekonomické ztráty byly v podnicích finančního průmyslu, jejichž značnou část tvoří náklady na obnovu elektrické sítě. Více než polovinu nepřímých ekonomických ztrát tvoří ztráty malých podniků. [7]

2.2 Severozápad Spojených států amerických a Kanada 2003

V srpnu roku 2003 potkal státy Ohio, Michigan, Pensylvánie, New York, Vermont, Massachusetts, Connecticut, New Jersey a kanadskou provincii Ontario jeden z nejrozsáhlejších výpadků elektrické energie. Úkolové uskupení pověřené šetřením události odhadlo, že počet obyvatel postižených tímto incidentem činil přibližně 50 milionů. V některých oblastech výpadek trval až 4 dny. V některých částech Ontaria docházelo k opakovaným přerušením dodávky elektřiny po dobu delší než týden, než byla obnovena plná zásoba energie. [9]

Při takto rozsáhlém výpadku je pochopitelné, že neměl jednu příčinu. Spíše se jednalo o kombinaci několika faktorů. Hlavní příčinou bylo podcenění důležitosti a zanedbání bezpečnostních standardů a ochranných systémů. Došlo například k porušení pravidla N-1, které stanovuje, že i při ztrátě jedné z klíčových částí soustavy bude systém nadále fungovat. To způsobilo, že se kaskádový efekt spustil již po selhání jednoho prvku soustavy. Navíc selhal systém pro sledování stavu sítě. K závažnosti blackoutu přispěla kombinace nedostatečné kapacity přenosové soustavy, chyb v provozních postupech, nedostatečné komunikace a koordinace mezi provozovateli a selhání ochranných systémů. Přenosová soustava nezvládala držet krok s rostoucí poptávkou po elektrické energii. Nedostatečná kapacita vedení a transformátorů vedla k přetížení a nestabilitě sítě. Došlo k automatickému vypnutí jedné elektrárny. Následně, v důsledku zanedbání správy růstu stromů v přístupových cestách k přenosovému vedení, došlo k výpadku některých vedení vysokého napětí. Nedostatek komunikace pak způsobil, že si jednotliví provozovatelé nebyli vědomi vzájemných dopadů jejich operací a nemohli tak adekvátně reagovat na vznikající problémy. Selhalo hned několik ochranných systémů včetně řady relé. Zařízení se kaskádově vypínala, dokud nedošlo k úplnému blackoutu. [9]

Celá událost měla výrazný dopad na obyvatelstvo postižených oblastí. Zvýšila se úmrtnost, zejména u starších osob a jedinců s chronickými onemocněními. Výpadek elektřiny narušil fungování lékařských zařízení a domácí péče, což vedlo ke zhoršení stavu pacientů s chronickými onemocněními, jako jsou osoby s respiračními problémy či

srdečními chorobami, kteří byli závislí na těchto zařízeních. Zvýšení počtu úmrtí přispělo i přehřátí, které bylo zvláště nebezpečné u dětí a starších osob, které neměly přístup k dostatečnému chlazení. Docházelo také k nárůstu trávicích obtíží způsobených konzumací zkažených potravin, neboť vysoké teploty v období výpadku znemožňovaly správné chlazení potravin v lednicích a mrazácích. I když bylo obyvatelstvo informováno o riziku rychlého zkažení potravin, mnozí z nich nebyli schopni nebo ochotni vyhodit veškeré chlazené zásoby. [10], [11], [12]

Celkové náklady ve spojených státech činí mezi 4 až 10 miliardami amerických dolarů. V Kanadě v srpnu klesl hrubý domácí produkt o 0,7 %, došlo k čisté ztrátě 18,9 milionů pracovních hodin a ve výrobním sektoru Ontario utrpělo ztráty v hodnotě 2,3 miliardy kanadských dolarů. [9]

2.3 Itálie 2003

V noci 28. září 2003 se ocitlo bez elektřiny 56 milionů obyvatel Itálie a části Švýcarska. Na některých místech došlo k obnovení dodávek elektrické energie až po 48 hodinách. Výpadek měl dopad i na Francii, Slovinsko a Rakousko. Došlo k úplnému oddělení Italské přenosové soustavy od zbytku Evropy. [13]

Příčinou výpadku bylo přerušení dvou hlavních přenosových linek ze Švýcarska. Prověšení vedení o napětí 380 kV ve Švýcarsku pod vlivem vysoké zátěže způsobilo výboj mezi vedením a stromem, což vyvolalo kaskádový efekt vedoucí k selhání systému. V této situaci byla elektrická soustava schopna po delší dobu převzít zvýšenou zátěž z přerušených linek, ale hlavním problémem bylo, že se nepodařilo tyto linky co nejdříve uvést zpět do provozu. Linky dlouhodobě nebyly navrženy na takovou nadměrnou zátěž. Operátoři nebyli informováni o tom, že v takových podmínkách mohou linky vydržet pouze omezenou dobu, zhruba 15 minut. Což je velice nešťastné, protože vzhledem k rychlé reakci a komunikaci s ostatními zainteresovanými stranami by jinak pravděpodobně k žádnému blackoutu nedošlo. Samotnému výboji mezi stromem a vedením se dalo taktéž předejít udržováním porostu v okolí vedení. [14]

Datum incidentu bylo rovněž poněkud nešťastné, protože v noci z 27. září probíhala v Itálii událost nazývaná Bílá noc. Kvůli této události bylo v ulicích velkoměst stále mnoho lidí i v pozdních hodinách. Náhlý výpadek elektřiny tak vedl k tomu, že tisíce lidí uvízly ve vlacích a dalších dopravních prostředcích. [13]

Blackout měl značný negativní dopad na ekonomiku v Itálii. Celkové makroekonomické škody dosáhly částky 1,182 miliardy eur, což představuje přibližně 0,083 % tehdejšího italského HDP. Téměř čtvrtinu této částky tvořily odhadované ztráty domácností. Výrazně zasaženy byly také sektory zemědělství, výroby a veřejné správy. [15]

2.4 Brazílie 2009

V Brazílii došlo 10. listopadu 2009 k velice nepravděpodobné události. Během nepříznivých meteorologických podmínek došlo vlivem atmosférického výboje, sníženou účinností izolátorů vystavených těmto náročným podmínkám, nebo kombinací obojího k rozsáhlému výpadku. Nepravděpodobná tato událost byla kvůli tomu, že došlo k poruchám na třech vedeních 765 kV téměř současně, čímž došlo k odpojení vodní elektrárny Itaipú, která splňuje kritérium spolehlivosti N-2. Tato elektrárna by tedy byla schopna vyrovnat se s poruchou až dvou prvků soustavy současně. Výsledkem byl rozsáhlý výpadek, který v nejvíce zasažených oblastech trval v průměru 222 minut. Došlo k přerušení dodávek o celkovém výkonu 24 436 MW, což představovalo asi 40 % celkové spotřeby elektrické energie v Brazílii a postihlo tedy přibližně 60 milionů obyvatel. [16]

Výpadek začal v důsledku obloukového záblesku mezi jednou z fází přenosového vedení 765 kV a zemí. Po době dlouhé přibližně 13,5 milisekund, což je doba kratší než jedna perioda síťového napětí, následovala další porucha. Tentokrát to byl jednofázový zkrat na jiném 765kV vedení, ale na odlišné fázi. Asi 3,5 ms poté došlo ke třetímu zkratu, tentokrát na přípojnici v rozvodně Itaberá, opět na jiné fázi. Tři téměř současně vzniklé zkraty na různých fázích vytvořily podmínky podobné třífázovému zkratu. Ochranný systém na základě těchto extrémních proudových hodnot reagoval a automaticky odpojil vedení, aby zabránil dalším škodám a destabilizaci soustavy. Ztráta všech tří vedení mezi rozvodnami Ivaiporã a Itaberá vedla k postupnému odpojování generátorů vodní elektrárny Itaipú, čímž došlo ke snížení zatížení a částečné stabilizaci sítě. Výkon byl následně přesměrován na vedení nižších napětíových úrovní (500 kV, 230 kV a 138 kV), což vedlo k jejich přetížení a následnému odpojení. V důsledku těchto odpojení zůstaly rozvodny Itaberá a Ivaiporã propojeny pouze prostřednictvím jednoho vedení 525 kV, což vedlo k oscilacím výkonu. Tyto výkyvy spustily ochranné systémy v dalších částech sítě a způsobily další poruchy, zejména na vedeních 440 kV. V několika lokalitách došlo k odpojení elektráren a síť se postupně rozpadala na menší ostrovní provozy, které již nebyly schopné udržet stabilní provoz. Výsledkem byl ukázkový případ kaskádových poruch, rychlé a hromadné

odpojování vedení vedlo k postupnému kolapsu napájení v několika brazilských státech. [17]

Blackout měl výrazný dopad na kvalitu života obyvatel. Přerušení dodávky elektrické energie ovlivnilo různé aspekty každodenního života a způsobilo nepohodlí a omezení v mnoha oblastech. Výpadek způsobil nedostatek veřejného i domácího osvětlení, což narušilo pocit bezpečí na ulicích i v domácnostech. Zároveň to ztížilo či dokonce znemožnilo vykonávání činností, které osvětlení vyžadují a v nočních hodinách téměř všech činností. Například i jen jít v noci na toaletu se stalo velice obtížným úkolem. Bez elektrické energie bylo rovněž obtížné uchovávat chlazené potraviny. Obyvatelé tak museli řešit alternativní způsoby, jak zabránit zkažení rychle se kazících výrobků, například pomocí ledu, který však také bez mrazáku časem roztál. Tím se značně zvýšilo riziko požití zkažených potravin. Příprava jídla také byla značně ztížena. Bez možnosti tepelně upravit kazící se jídlo tak byli mnozí nuceni ho vyhodit. Dále byl ovlivněn provoz komunikačních systémů, včetně pevných i mobilních telefonů, internetu a televizního vysílání. Bez dostupných komunikačních prostředků byla výměna informací mnohem obtížnější a lidé tak neměli snadný přístup k informacím o svých blízkých ani ke zprávám o aktuálním dění. Postižena byla i dodávka vody, jelikož mnoho čerpacích stanic přišlo o zásobování elektrickou energií a nebyly tak schopny provozu. Omezený přístup k vodě negativně ovlivnil hygienu, úklid i další běžné činnosti. S omezením provozu se musela potýkat i zdravotnická zařízení. Výpadek narušil poskytování zdravotní péče, provádění chirurgických zákroků, některá vyšetření a také uchovávaní léků a zdravotnického materiálu citlivého na teplotu. To zvýšilo riziko zdravotních komplikací pro pacienty. [18]

Způsobené ekonomické ztráty byly značné a týkaly se několika sektorů národní ekonomiky. Ekonomický dopad blackoutu byl nejvíce patrný v oblastech průmyslu a výroby, dopravy, služeb, zdravotnictví a bezpečnosti. Výpadek vedl k finančním ztrátám, poklesu výroby, ztrátám pracovních míst a negativně ovlivnil mezinárodní mínění o zemi. [18] Ačkoliv žádné z dostupných oficiálních vládních nebo akademických dokumentů neuvádí konkrétní finanční vyčíslení ztrát způsobených tímto výpadkem elektrické energie, lze na základě dostupných údajů provést kvalifikovaný odhad. Vhodným nástrojem pro tento účel je Value of Lost Load (VoLL), tedy odhadovaná hodnota ztráty z každé nedodané kilowatthodiny elektrické energie. Hodnoty VoLL se liší dle sektoru (průmysl, služby, domácnosti) i regionu, za průměrnou hodnotu lze však považovat 3 500 amerických dolarů za 1 MWh. [19] Pro výpočet přímých ekonomických ztrát je potřeba z dřívějších odstavců

vzít v úvahu celkovou ztrátu výkonu 24 436 MW a průměrnou dobu trvání výpadku 222 minut, což je v přepočtu na hodiny 3,7 hodiny. Součinem těchto hodnot zjistíme celkový objem nedodané elektrické energie, který vynásobíme hodnotou VoLL pro získání přímých ekonomických ztrát. Celkový objem nedodané elektrické energie se tedy odhaduje na [20]:

$$24\,436\text{ MW} \times 3,7\text{ h} = 90\,413,2\text{ MWh} \quad (1)$$

Při aplikaci zmíněného odhadu VoLL:

$$90\,413,2\text{ MWh} \times 3\,500\text{ USD/MWh} = 316\,446\,200\text{ USD} \quad (2)$$

Lze tedy přibližně stanovit, že přímé ekonomické ztráty způsobené výpadkem elektriny dosáhly částky přibližně 316 milionů amerických dolarů, což je v přepočtu téměř 7 miliard českých korun. Tento odhad nezahrnuje nepřímé dopady, jako jsou ztráty způsobené přerušением výroby, logistickými problémy, poklesem produktivity, ani reputační či psychologické povahy. Reálné celkové vzniklé ztráty tak mohly být výrazně vyšší.

2.5 Portoriko 2017

V roce 2017 Portoriko zastihly hurikány Irma a Maria, které vážně poškodily tamější elektrickou síť. Nejdříve přišel hurikán Irma a 12 dní po něm následoval hurikán Maria. Následky těchto hurikánů trvají dodnes, v daném roce ale způsobily ten nejdelší blackout v historii USA. Tento blackout totiž trval téměř 11 měsíců. Celkové škody a náklady na následné opravy se pohybují v řádech stovek miliard amerických dolarů. Hrubý národní produkt v Portoriku poklesl o 15 procent a statisíce lidí se rozhodly pro opuštění ostrova. Finanční ztráty v energetickém sektoru byly vyčísleny na přibližně 9,4 miliard amerických dolarů. [21], [22], [23]

Tento dlouhotrvající blackout měl velký dopad na životy obyvatel, ekonomiku a celou infrastrukturu ostrova. Po této katastrofě bylo téměř nemožné sehnat čistou vodu. Hurikány si vyžádaly životy téměř 3 000 lidí, což je více než pětikrát vyšší hodnota, než kterou uváděla zpráva amerického ministerstva zdravotnictví z listopadu 2017. [22], [24]

Mnozí lidé měli problém se sháněním potravin. S tímto problémem se jim snažilo pomoci hned několik humanitárních organizací, aby nedošlo k podvyživení obyvatel a dalším možným zdravotním problémům. Hurikán způsobil značné poškození vodárenské soustavy, které připravilo obyvatele ostrova o přístup k vodě. Ještě dva měsíce po něm byly bez přístupu k vodě statisíce lidí. Těm, kteří přístup měli, bylo doporučeno, aby vodu před použitím raději stále převařovali. Testování veřejného zdraví bylo přerušeno kvůli škodám

vzniklým během bouře, proto je těžké stanovit, s jakými zdravotními problémy se potýkali občané ostrova. [24]

2.6 Texas 2021

V únoru v roce 2021 v Texasu způsobilo extrémní počasí sérii výpadků. Celkově blackout postihl přes 4,5 milionu domácností, což činí zhruba 10 milionů lidí. Z nichž mnozí byli bez přístupu k elektrické energii po dobu delší než dva dny. V době výpadků byly rekordně nízké teploty, což způsobilo, že bylo zdokumentováno přes 100 úmrtí. [25]

Hlavní příčinou tohoto incidentu byl příchod nezvykle mrazivé fronty. Ty vedly k prudkému nárůstu poptávky po elektrické energii na vytápění, na což nebyly výrobní připraveny. Mnoho výroben, zejména ty poháněné zemním plynem a větrem, nebylo navrženo tak, aby odolávaly tak extrémním mrazům. Elektrárny nebyly schopné odolat poklesu teplot začaly postupně vypovídat službu. V reakci na pokles výroby elektrické energie, pokles frekvence v síti a ve snaze zabránit kaskádovým výpadkům a úplnému blackoutu, dispečerů společností provozující texaskou elektrickou síť začali vydávat příkazy k rotačním odstávkám dodávek elektrické energie pro zákazníky. Rotační odstávky znamenaly, že dodávky elektrické energie byly dočasně přerušeny pro různé skupiny odběratelů v různých časových intervalech. To pomohlo snížit celkovou spotřebu elektrické energie, stabilizovat frekvenci a zabránit kolapsu sítě. Nad některými částmi sítě ztratili kontrolu, ale alespoň část byli schopni udržet v provozu. [25]

Většina domácností v dnešní době je závislá na dodávkách elektrické energie obzvláště v zimě. Téměř žádná domácnost již nemá elektricky nezávislé vytápění ani ohřev vody. I přes to, že se dispečerům podařilo minimalizovat škody, v některých domácnostech byly přerušeny dodávky elektrické energie po dobu delší 48 hodin. Teploty v některých postižených oblastech se pohybovaly kolem $-14\text{ }^{\circ}\text{C}$, což byla příčina mnohých úmrtí. V důsledku narušení dodávek elektrické energie a plynu se mnoho lidí dostalo do situace, kdy nebyli schopni ve svém obydlí zajistit a udržet nejen optimální, ale ani bezpečnou teplotu. Někteří byli schopni najít útočiště u rodiny, známých či v hotelech a ohřívacích stanicích, kde byl bezpečný zdroj tepla. Vzhledem k počasí a stavu komunikací však tato možnost nebyla dostupná pro všechny. Někteří se tak snažili zahřát nebezpečnými způsoby jako zapnutím plynových trub, vytopením auta nebo rozděláním ohně v uzavřených prostorách. Tyto činy také vedly v některých případech k úmrtí. Texas má také vysoký počet

lidí bez domova. Výpadek proudu je sice přímo nezasáhl, ale vzhledem k extrémnímu počasí, které výpadky způsobilo, i mezi nimi pravděpodobně došlo k úmrtím. [25]

Ekonomické ztráty byly vyčísleny na částku v rozsahu 80 až 130 miliard amerických dolarů. Odhadovaná hodnota ztracené zátěže v době výpadků přesáhla čtyři miliardy amerických dolarů. Celostátní zimní údržba elektráren byla odhadnuta na částku 430 milionů amerických dolarů. Export chemikálií, plastů a pryže, který představuje téměř 17 procent veškerého vývozu státu Texas, poklesl v únoru 2021 o více než 20 procent. [26], [27]

2.7 Srovnání blackoutů

Tato část práce se zabývá několika významnými blackouty, které v různých obdobích postihly odlišné regiony světa: New York City v roce 1977, Severozápad USA a Kanadu v roce 2003, Itálii v roce 2003, Brazílii v roce 2009, Portoriko v roce 2017 a Texas v roce 2021. Každá z těchto událostí měla závažné dopady na zasažené oblasti a zdůraznila důležitost spolehlivé a odolné infrastruktury. Následující tabulka shrnuje klíčové informace o těchto výpadech elektrické energie s cílem usnadnit jejich vzájemné porovnání.

Tabulka 1 Srovnání rozsahu a dopadu historických blackoutů

Rok	Místo	Počet postižených v milionech	Doba trvání	Hlavní příčina	Ekonomické ztráty v miliardách Kč
2021	Texas	4,5	4 dny	Extrémní mrazy	1 830
2017	Portoriko	3,3	11 měsíců	Hurikány Irma a Maria	215
2003	Severozápad USA a Kanada	50	4 dny	Podcenění bezpečnostních standardů	130
2003	Itálie	56	48 hodin	Nedostatečná údržba vegetace v okolí vedení	29
1977	New York City	9	25 hodin	Selhání ochranných zařízení	8
2009	Brazílie	60	222 minut	Nepříznivé meteorologické podmínky	7

Přehled je seřazen sestupně podle výše finančních ztrát, které způsobily. Z tabulky lze vyčíst, že blackouty mohou být způsobeny mnoha různými příčinami jako přírodními

katastrofami, lidským selháním, nebo technickými poruchami. Největší počet postižených zaznamenala Brazílie v roce 2009, kde výpadek zasáhl přibližně 60 milionů obyvatel, ačkoliv trval pouze 222 minut. Oproti tomu výpadek v Portoriku v roce 2017, který postihl pouze 3,3 milionu lidí, měl nejdelší trvání, přibližně 11 měsíců. To ukazuje, že závažnost následků blackoutů není vždy úměrná počtu postižených osob nebo době trvání.

Finanční ztráty uvedené v tabulce představují minimální odhadovanou částku. Tabulka poukazuje na to, že u novodobějších blackoutů nejsou dopady menší, spíše naopak. Je rovněž možné říci, že čím déle výpadek trval, tím vyšší byly ztráty. U blackoutu v Portoriku to vypadá, že je výjimkou. To je však způsobeno tím, že většina dopadů je přisuzována hurikánům, ne výpadku samotnému. Z hlediska ekonomických ztrát dominuje výpadek v Texasu v roce 2021, kde extrémní mrazy způsobily škody ve výši 1 830 miliard Kč. To ukazuje, že ekonomické dopady blackoutů nejsou vždy přímo úměrné počtu postižených obyvatel nebo délce trvání. Zásadní roli hraje ekonomická vyspělost daného regionu, připravenost infrastruktury a schopnost krizového řízení.

Blackouty představují vážnou hrozbu s potenciálně dlouhodobými následky. Je proto nezbytné investovat do modernizace a posilování elektroenergetické infrastruktury. Kromě technických řešení je důležité zdůraznit i roli lidského faktoru. Je také důležité zavést efektivní plány pro zvládání krizových situací a rychlé obnovení dodávek elektrické energie v případě výpadku. Efektivní prevence blackoutů a zmírňování jejich dopadů vyžaduje úzkou spolupráci mezi státním sektorem, energetickými společnostmi a veřejností.

II PRAKTICKÁ ČÁST

3 ANALÝZA PŘÍČIN VÝPADKŮ V DODÁVKÁCH ELEKTŘINY

Tato kapitola se zaměřuje na identifikaci klíčových rizik spojených s elektrickou energetikou prostřednictvím analýzy příčin výpadků v dodávkách elektrické energie. Cílem provedené analýzy je určit takové kombinace hrozeb a aktiv, jejichž narušení může s vysokou pravděpodobností vést k blackoutu, tedy rozsáhlému výpadku v elektrické síti. Pro účely této analýzy byla zvolena metoda PNH, která umožňuje ohodnotit jednotlivé hrozby na základě tří složek celkového rizika: pravděpodobnosti výskytu (P), závažnosti následků (N) a subjektivního názoru hodnotitele (H). Každé složce je přiřazena hodnota od 1 od 5. Výsledná hodnota rizika (R) je získána jejich součinem. Na základě hodnoty R je následně stanoven stupeň rizika (viz Tabulka 2). [28]

Tabulka 2 Určení stupně rizika

Rizikový stupeň	R	Míra rizika
I.	101 - 125	Nepříjemné riziko
II.	51 – 100	Nežádoucí riziko
III.	11 – 50	Mírné riziko
IV.	3 - 10	Akceptovatelné riziko
V.	< 3	Bezvýznamné riziko

(zdroj: [28])

V rámci analýzy bylo nezbytné nejprve vymezit aktiva elektrizační soustavy, jejichž narušení by mohlo mít významný dopad na bezpečnost a stabilitu dodávek elektrické energie. Výběr aktiv vychází z principu hodnocení kritické infrastruktury, přičemž zahrnuje jak prvky přímo zařazené do této kategorie, tak i další, jejichž selhání by mohlo přispět ke kaskádovému šíření poruch v síti.

Identifikace relevantních hrozeb vycházela z dostupných odborných zdrojů, zkušeností z minulých událostí i vlastních odborných poznatků získaných v průběhu studia. Cílem bylo pokrýt široké spektrum potenciálních scénářů, které mohou vést k výpadkům, a to jak v důsledku technických selhání či lidské chyby, tak v důsledku záměrných škodlivých činů nebo přírodních událostí.

Důležitou součástí procesu byla kategorizace hrozeb i aktiv. Při ní byla zohledněna specifika prostředí elektrizační soustavy i praktická využitelnost výstupů analýzy. Zvolený přístup tak vedl k určitému zjednodušení a zároveň cílenému rozlišení některých pojmů tam,

kde bylo účelné. Některé prvky, jako jsou záložní zdroje napájení, ochranné systémy nebo infrastruktura pro dodávku paliv, nejsou v rámci současných metodik hodnocení kritické infrastruktury samostatně vymezovány. V této analýze však byly zohledněny jako samostatné kategorie aktiv mimo prvky KI (kritické infrastruktury), a to kvůli jejich potenciálnímu vlivu na funkčnost klíčových zařízení elektrizační soustavy.

Vzhledem k systémové povaze blackoutů se analýza nesoustředí na vybranou lokalitu či konkrétní uzel v síti. Výpadky dodávek elektřiny totiž často vznikají kaskádovým šířením poruch napříč různými částmi soustavy, a proto je vhodné zaměřit se na obecné příčiny a zranitelnosti celého systému. Hodnocena je tedy soustava České republiky jako celek.

Tabulka 3 PNH analýza

Hrozba	Prvek soustavy		P	N	H	R
Vlivy počasí	Primární aktiva splňující kritéria pro zařazení do kritické infrastruktury	Výrobní elektřiny	1	5	2	10
		Vedení přenosové soustavy	2	4	2	16
		Elektrické stanice přenosové soustavy	2	4	2	16
		Vedení distribuční soustavy	4	3	3	36
		Elektrické stanice distribuční soustavy	2	3	3	18
		Zařízení dispečerského řízení	1	4	2	8
		Vedení pro vyvedení výkonu a napájení výroben	4	4	3	48
	Sekundární aktiva nepatřící mezi prvky kritické infrastruktury	Menší výrobní elektřiny	4	2	2	16
		Vedení VN	4	3	3	36
		Vedení NN	5	1	1	5
		Transformační stanice	3	2	2	12
		Měničny	1	2	2	4
		Kompenzační stanice	2	2	1	4
		Rozvodny	3	2	2	12
		Řídící centra a operační střediska	1	3	2	6
		Komunikační infrastruktura	2	2	1	4

Hrozba	Prvek soustavy		P	N	H	R
Vlivy počasí	Sekundární aktiva nepatřící mezi prvky kritické infrastruktury	Ochranné prvky	2	2	2	8
		Záložní zdroje napájení	1	3	2	6
		Infrastruktura pro dodávku paliva	2	3	3	18
Přírodní katastrofa	Primární aktiva splňující kritéria pro zařazení do kritické infrastruktury	Výrobní elektřiny	2	5	4	40
		Vedení přenosové soustavy	2	5	4	40
		Elektrické stanice přenosové soustavy	1	5	3	15
		Vedení distribuční soustavy	3	4	3	36
		Elektrické stanice distribuční soustavy	2	4	3	24
		Zařízení dispečerského řízení	1	5	3	15
		Vedení pro vyvedení výkonu a napájení výroben	3	4	3	36
	Sekundární aktiva nepatřící mezi prvky kritické infrastruktury	Menší výrobní elektřiny	3	2	3	18
		Vedení VN	3	3	3	27
		Vedení NN	3	2	2	12
		Transformační stanice	2	2	2	8
		Měničny	2	2	2	8
		Kompenzační stanice	2	1	2	4
		Rozvodny	2	3	3	18
		Řídící centra a operační střediska	1	4	3	12
		Komunikační infrastruktura	3	4	3	36
		Ochranné prvky	2	3	2	12
		Záložní zdroje napájení	2	4	2	16
		Infrastruktura pro dodávku paliva	2	4	2	16

Hrozba	Prvek soustavy		P	N	H	R
Porucha	Primární aktiva splňující kritéria pro zařazení do kritické infrastruktury	Výrobní elektřiny	2	5	4	40
		Vedení přenosové soustavy	1	5	4	20
		Elektrické stanice přenosové soustavy	3	5	4	60
		Vedení distribuční soustavy	2	3	3	18
		Elektrické stanice distribuční soustavy	3	3	3	27
		Zařízení dispečerského řízení	2	5	4	40
		Vedení pro vyvedení výkonu a napájení výroben	2	4	3	24
	Sekundární aktiva nepatřící mezi prvky kritické infrastruktury	Menší výrobní elektřiny	3	2	2	12
		Vedení VN	3	3	2	18
		Vedení NN	4	2	2	16
		Transformační stanice	4	3	2	24
		Měničny	4	3	2	24
		Kompenzační stanice	2	2	2	8
		Rozvodny	4	3	3	36
		Řídící centra a operační střediska	2	4	3	24
		Komunikační infrastruktura	2	3	2	12
		Ochranné prvky	3	4	3	36
		Záložní zdroje napájení	2	4	3	24
		Infrastruktura pro dodávku paliva	2	4	3	24
Lidský faktor	Primární aktiva splňující kritéria pro zařazení do kritické infrastruktury	Výrobní elektřiny	1	5	3	15
		Vedení přenosové soustavy	2	5	3	30
		Elektrické stanice přenosové soustavy	2	5	3	30
		Vedení distribuční soustavy	3	4	3	36
		Elektrické stanice distribuční soustavy	3	4	3	36

Hrozba	Prvek soustavy		P	N	H	R
Lidský faktor	Primární aktiva splňující kritéria pro zařazení do kritické infrastruktury	Zařízení dispečerského řízení	2	5	5	50
		Vedení pro vyvedení výkonu a napájení výroben	2	4	3	24
	Sekundární aktiva nepatřící mezi prvky kritické infrastruktury	Menší výrobní elektrárny	3	2	2	12
		Vedení VN	3	2	2	12
		Vedení NN	4	1	2	8
		Transformační stanice	3	2	2	12
		Měnič	3	2	2	12
		Kompenzační stanice	3	2	2	12
		Rozvodny	3	3	3	27
		Řídící centra a operační střediska	4	3	3	36
		Komunikační infrastruktura	3	3	3	27
		Ochranné prvky	2	4	3	24
		Záložní zdroje napájení	2	4	3	24
		Infrastruktura pro dodávku paliva	3	4	3	36
Organizační selhání	Primární aktiva splňující kritéria pro zařazení do kritické infrastruktury	Výrobní elektrárny	1	5	4	20
		Vedení přenosové soustavy	1	5	4	20
		Elektrické stanice přenosové soustavy	1	5	4	20
		Vedení distribuční soustavy	2	3	3	18
		Elektrické stanice distribuční soustavy	2	4	3	24
		Zařízení dispečerského řízení	2	5	4	40
		Vedení pro vyvedení výkonu a napájení výroben	2	4	3	24
	Sekundární aktiva nepatřící mezi prvky kritické infrastruktury	Menší výrobní elektrárny	3	3	3	27
		Vedení VN	3	2	2	12
		Vedení NN	4	2	2	16

Hrozba	Prvek soustavy		P	N	H	R
Organizační selhání	Sekundární aktiva nepatřící mezi prvky kritické infrastruktury	Transformační stanice	3	3	3	27
		Měničky	3	2	3	18
		Kompenzační stanice	3	3	3	27
		Rozvodny	3	4	3	36
		Řídící centra a operační střediska	4	3	4	48
		Komunikační infrastruktura	3	3	3	27
		Ochranné prvky	2	4	3	24
		Záložní zdroje napájení	2	4	3	24
		Infrastruktura pro dodávku paliva	2	4	3	24
Kybernetický útok	Primární aktiva splňující kritéria pro zařazení do kritické infrastruktury	Výrobní elektřiny	3	4	4	48
		Elektrické stanice přenosové soustavy	2	5	4	40
		Elektrické stanice distribuční soustavy	2	4	3	24
		Zařízení dispečerského řízení	3	5	5	75
	Sekundární aktiva nepatřící mezi prvky kritické infrastruktury	Menší výrobní elektřiny	2	3	2	12
		Transformační stanice	1	3	2	6
		Měničky	1	2	2	4
		Kompenzační stanice	1	2	2	4
		Rozvodny	2	3	2	12
		Řídící centra a operační střediska	3	4	3	36
		Komunikační infrastruktura	3	4	3	36
		Ochranné prvky	3	4	4	48
		Záložní zdroje napájení	2	3	3	18
		Infrastruktura pro dodávku paliva	2	4	3	24

Hrozba	Prvek soustavy		P	N	H	R
Teroristický útok	Primární aktiva splňující kritéria pro zařazení do kritické infrastruktury	Výrobní elektrárny	2	5	3	30
		Vedení přenosové soustavy	1	5	3	15
		Elektrické stanice přenosové soustavy	2	5	3	30
		Vedení distribuční soustavy	1	4	2	8
		Elektrické stanice distribuční soustavy	2	4	3	24
		Zařízení dispečerského řízení	2	5	3	30
		Vedení pro vyvedení výkonu a napájení výroben	1	3	2	6
	Sekundární aktiva nepatřící mezi prvky kritické infrastruktury	Menší výrobní elektrárny	1	3	2	6
		Vedení VN	2	3	3	18
		Rozvodny	2	3	3	18
		Řídící centra a operační střediska	2	4	3	24
		Komunikační infrastruktura	1	3	2	6
		Infrastruktura pro dodávku paliva	2	5	3	30

(zdroj: vlastní)

3.1 Vlivy počasí

Meteorologické jevy, jako jsou silný vítr, vydatné srážky, sucho, mráz, bouřky či krupobití, patří k nejčastějším vlivům, které negativně ovlivňují provoz elektrizační soustavy. Na rozdíl od přírodních katastrof se jedná o běžné jevy, a proto jsou prvky soustavy již při návrhu a provozování přizpůsobeny místním klimatickým podmínkám. I přesto může za určitých okolností dojít k poškození více částí sítě současně a v extrémních případech ke kaskádovým poruchám.

Z historického hlediska patří mezi nejvýznamnější události zcela jistě již zmiňovaný blackout v Texasu v roce 2021 způsobený extrémními mrazy. Ten je blíže popsán výše a zdůrazňuje, že tato hrozba je stále aktuální, zejména když uvažíme probíhající klimatické změny. Z událostí, které jsou nám blíže je možné zmínit například orkán Kyrill (2007) nebo orkán Herwart (2017). Tyto události sice nezpůsobily úplný blackout, ale poškodily některé prvky a způsobily výpadky. Došlo při nich převážně k poškození vedení, v některých

případech došlo i k požárům v důsledku pádu stromů na vedení či trafostanice. Orkán Kyrill připravil o elektrinu přes milion odběratelů, orkán Herwart přes půl milionu. [29], [30]

Zranitelnost jednotlivých aktiv se liší podle jejich konstrukce a umístění. Nejvíce ohrožená jsou venkovní vedení, zejména v zalesněných nebo exponovaných oblastech. Významný vliv má také jejich délka a rozprostření v terénu. Nejvyšší hodnota rizika ($R = 48$) byla proto přiřazena vedením pro vyvedení výkonu a napájení výroben, protože jejich porucha může přímo ovlivnit stabilitu celé soustavy a často se nacházejí v otevřeném terénu. Stejně tak vedení distribuční soustavy v KI a vedení VN mimo KI vykazují zvýšenou míru rizika (R mezi 30 a 36), neboť jsou častěji vystavena působení větru, padajících stromů nebo námraze, přičemž výpadky těchto prvků mohou výrazně ovlivnit zásobování obyvatelstva.

Naopak prvky jako elektrické stanice, zejména měnirny, jsou zpravidla dobře chráněny. Elektrické stanice přenosové soustavy jsou obvykle robustní, velice odolná a dobře chráněná zařízení. Elektrické stanice distribuční soustavy, jsou sice podstatně méně chráněny, ale obvykle jsou umístěny v objektech s dostatečnou konstrukční ochranou, nebo jsou alespoň částečně zastřešeny. Běžné vlivy počasí tak obvykle nemají potenciál ovlivnit jejich provoz. Hodnoty R se zde pohybují mezi 6 a 18, tedy v pásmu akceptovatelného až mírného rizika. Velké výrobní elektrárny, například jaderné nebo uhelné elektrárny, mají robustní konstrukci a jsou navrženy k dlouhodobému provozu i v náročných klimatických podmínkách. Pravděpodobnost jejich narušení běžnými meteorologickými jevy je proto velmi nízká.

Je však třeba dodat, že vlivy počasí mohou postihnout větší území současně, a tím narušit více prvků během krátkého časového intervalu. Právě kombinace výpadků několika vedení a následných přetížení zbylých prvků může vytvořit podmínky pro kaskádové poruchy, ačkoliv se tak zatím na území České republiky nestalo v rozsahu vedoucím k blackoutu. Přestože se zatím daří udržet rizika pod kontrolou, probíhající klimatické změny zvyšují výskyt extrémních jevů. Je tedy nutné pravidelné přehodnocování rizik a zvyšování odolnosti infrastruktury se zohledněním lokálních specifik.

3.2 Přírodní katastrofa

Přírodní katastrofy, jako jsou zemětřesení, sesuvy půdy, povodně, extrémní vichřice nebo laviny, představují hrozbu s nízkou pravděpodobností výskytu, ale potenciálně vysokými následky i pro kritickou infrastrukturu. Na území České republiky se s nimi sice příliš často neseťkáváme, ale například povodně a extrémní bouře zde již v minulosti opakovaně způsobily vážné škody.

Například povodně v letech 1997, 2002 a 2013 ukázaly, že nízko položené transformační stanice, rozvodny nebo vedení NN/VN vedená v blízkosti vodních toků jsou vůči těmto jevům obzvláště zranitelná. Výpadky napájení v některých oblastech Ústeckého, Olomouckého či Jihomoravského kraje vedly ke ztrátě zásobování elektrickou energií na celé dny. [31], [32], [33]

Rizikovitost přírodních katastrof se výrazně liší podle typu a umístění aktiv. V hodnocení byla zohledněna nejen pravděpodobnost výskytu daného jevu, ale i konstrukční odolnost, předchozí zkušenosti a kritičnost daného prvku pro zachování provozu soustavy.

Například velké výrobní elektrárny, jako například uhelné nebo jaderné elektrárny, bývají chráněné a mají stabilní, robustní základy. Ty tedy pravděpodobnost narušení snižují. Naopak vodní elektrárny, jejichž provoz závisí na průtocích, mohou být silně ovlivněny povodněmi. Takže i výroba elektriny v KI se tato hrozba týká, ačkoliv u většiny typů je pravděpodobnost velmi nízká.

Vedení přenosové soustavy často protíná nezastavěné území a svahy, je zde tedy jistá pravděpodobnost poškození v důsledku sesuvů půdy, u jejich projektování je však obvykle dbát zřetel i na tuto hrozbu a pravděpodobnost tak není příliš vysoká. Vedení distribuční soustavy však byla v minulosti sesuvy půdy postižena v důsledku nadměrného nasycení půdy (např. Beskydy v roce 2010). Tyto jevy vedly k narušení stability podpěrných bodů a výpadkům napájení. [34]

Elektrické stanice přenosové soustavy a stanice distribuční soustavy v KI jsou obvykle konstruovány s ohledem na dlouhodobé provozní bezpečnostní standardy a lokalizovány mimo bezprostředně ohrožená území. U stanic mimo KI, případně u menších je zranitelnost nepatrně vyšší, zejména pokud se nacházejí v údolích nebo v blízkosti vodních toků. Příkladem může být zatopení části distribuční infrastruktury v Ústeckém kraji během povodní v roce 2013. [32]

Celkově lze konstatovat, že přírodní katastrofy představují hrozbu s nízkou pravděpodobností, ale vysokým potenciálním dopadem. Mohou vést k narušení více prvků současně, čímž se zvyšuje pravděpodobnost kaskádových poruch a následně tedy i blackoutu. Současná opatření v projektování infrastruktury významně snižují zranitelnost, nicméně i nadále je vhodné pravidelně přehodnocovat rizika na základě aktuálních povodňových map, geologických studií a scénářů extrémního počasí. Především je však

důležité zajišťovat krizové plány pro obnovu provozu v postižených oblastech, jelikož pravděpodobnost vzniku přírodních katastrof nelze nijak ovlivnit.

3.3 Porucha

Technická porucha je běžnou a očekávanou součástí provozu energetické infrastruktury. Může mít příčinu v opotřebením materiálu, výrobní vadě nebo konstrukčním selhání. I přes pravidelné revize a monitoring se poruchy vyskytují, obvykle však bez vážnějších následků díky redundantním systémům a rychlému zásahu obsluhy. V některých případech však může jít o iniciační událost většího rozsahu, zejména pokud zasáhne klíčový bod v síti nebo nastane za situace, kdy je soustava více zatížena.

Nejvíce ohrožená jsou mechanicky namáhaná zařízení, jako jsou elektrické stanice nebo ochranné prvky, které se mohou porouchat vlivem stárnutí, zkratu nebo přepětí. Kompenzační stanice jsou sice méně poruchové, ale jejich selhání může vést k poklesu kvality napětí, což může sekundárně způsobit další poruchy u citlivých zařízení. Výrobní elektriny v KI mohou být postiženy zejména poruchami ve vnitřní technologii (např. turbíny, generátory, napájecí systémy). Vzhledem k vysoké robustnosti a údržbě je pravděpodobnost poruchy nižší, avšak její dopady mohou být značné, pokud dojde k odstavení významného zdroje.

Naopak nejméně ohrožena poruchami jsou pasivní části soustavy, zejména vedení. Pokud k nim dojde, tak obvykle v důsledku mechanického poškození izolátorů nebo zkratu. U vedení distribuční jsou častější kvůli nižším standardům, ale jejich vliv na síť nebývá tolik významný.

Dobrým příkladem možných následků poruchy je dříve zmíněný výpadek v New Yorku v roce 1977. Sice při něm došlo ke kombinaci několika příčin, ale konkrétně porucha ochranných prvků vedla k rychlé eskalaci situace. Došlo totiž k odpojení nepoškozených vedení, což způsobilo přetížení aktivních vedení. Je tedy možné, že nebýt poruchy ochranných prvků, situace by neskončila úplným blackoutem.

Výsledky analýzy ukázaly, že porucha je hrozbou se střední pravděpodobností a proměnlivými následky, které závisí především na schopnosti systému přeměrovat zatížení. Klíčové jsou preventivní kontroly stavu jednotlivých prvků sítě, prediktivní údržba, dostupnost náhradních dílů a školení personálu pro rychlé zásahy. Dále se doporučuje

sledovat vývoj životního cyklu kritických komponent a postupně nahrazovat zařízení po uplynutí určité doby i v případě bezporuchového chodu.

3.4 Lidský faktor

Ačkoli moderní elektroenergetika čím dál více spoléhá na automatizaci, lidský faktor zůstává významným zdrojem rizika. Selhání člověka může vést nejen ke vzniku poruchy, ale i k jejímu nesprávnému zvládnutí, čímž roste riziko eskalace lokální události do rozsáhlého blackoutu. Z hlediska PNH analýzy se lidský faktor projevuje napříč mnoha aktivy, přičemž míra rizika se výrazně liší.

Vysoké riziko zde představují převážně zařízení dispečerského řízení. U těch, která jsou součástí kritické infrastruktury bývá brán větší zřetel na volbu kvalifikovaného personálu a patřičná školení, zároveň bývají do jisté míry automatizovány, nicméně ani tam nelze opomenout lidskou chybovost. Dispečerů rozhodují o rozložení výkonu, přepínání režimů i zvládání mimořádných stavů. Špatná komunikace, opomenutí varování nebo chybná interpretace dat může vést k rychlé destabilizaci celé soustavy. Právě chyba v komunikaci dispečerů značně zkomplikovala situaci při blackoutu na Severozápadě USA a v Kanadě v roce 2003. Tomu je v předchozí kapitole věnována celá podkapitola.

Lidský faktor představuje komplexní hrozbu, která zasahuje různé úrovně řízení i provozu. Minimalizace rizika u této hrozby vyžaduje důsledné školení personálu, validaci dispečerských rozhodnutí, pravidelnou údržbu zařízení a především posilování schopnosti koordinace v reálném čase. Přestože plné odstranění lidské chyby není možné, je možné omezit její dopady důrazem na prevenci.

3.5 Organizační selhání

Organizační selhání představují specifickou kategorii hrozeb, která se liší od lidského faktoru tím, že nejde o chyby jednotlivých pracovníků, ale o systémové nedostatky. Tyto nedostatky se mohou projevovat v řízení, plánování, komunikaci, dokumentaci nebo bezpečnostní kultuře organizací. Mohou dlouhodobě snižovat odolnost infrastruktury a za určitých okolností vést k selháním s rozsáhlými dopady.

Z pohledu aktiv vykazují nejvyšší riziko zařízení dispečerského řízení, u nichž selhání na úrovni organizačních procesů (např. nedostatečná krizová připravenost, neaktuální schémata, chybějící koordinace s ostatními provozovateli) může mít závažné následky. I drobný procesní nedostatek zde může během krizové situace eskalovat do systémového

kolapsu. Také elektrické stanice mimo kritickou infrastrukturu jsou organizačními faktory silně ovlivněny. Typicky jde o zanedbanou údržbu, neaktuální provozní dokumentaci nebo nedostatečnou evidenci konfigurací. V praxi se to může projevit například pozdním zásahem při poruše nebo špatně provedenou rekonstrukcí.

Výrazným příkladem organizačního selhání je nedostatečná údržba vegetace v okolí venkovních vedení, zejména vysokého a nízkého napětí. Je to poměrně běžná situace, která však může mít i závažné následky, jak tomu bylo například v Itálii v roce 2003. Obvykle k tomu dojde v důsledku nevhodného nastavení plánů údržby, špatné koordinace s vlastníky pozemků nebo podcenění revizí. Kontakt větví s nadzemním vedením často vede k poruše, a v kombinaci s dalšími faktory může vyvolat rozsáhlý výpadek elektrické energie.

Velká část historických případů blackoutů měla společné právě organizační selhání. Obvykle nebývá tak vážné, aby způsobilo větší výpadek samo o sobě, ale v případě mimořádné události představuje vážný problém. Bez organizačních selhání je většina mimořádných událostí zvládnutelná bez vzniku blackoutu. Jsou tedy důležitým bodem této analýzy. Jsou však těžko postihnutečné preventivně, protože vyplývají ze zažitých návyků, nedostatečné kultury bezpečnosti nebo slabé vnitřní kontroly.

Pro minimalizaci tohoto typu rizik je klíčové budovat odolnou organizační strukturu, pravidelně revidovat vnitřní procesy a kontrolní mechanismy, provádět simulace krizových scénářů a zajišťovat koordinaci napříč subjekty. Zejména v oblasti dispečerského řízení a údržby kritické infrastruktury by mělo být organizační selhání chápáno jako reálná hrozba, nikoli jen administrativní nedostatek.

3.6 Kybernetický útok

Kybernetické útoky představují rostoucí hrozbu pro energetickou infrastrukturu, zejména s ohledem na digitalizaci řídicích systémů, závislost na datových sítích a propojenost mezi jednotlivými provozovateli. Ačkoliv fyzické poškození infrastruktury tímto způsobem obvykle nehrozí, může dojít k vážnému narušení provozu, chybnému řízení sítí, výpadkům dodávek nebo dokonce k nekontrolovatelnému odstavení výroby.

Nejvíce ohroženými aktivy jsou dispečerská centra, řídicí systémy SCADA, komunikační infrastruktura, centrální servery a databáze a IT infrastruktura elektrických stanic. Právě SCADA systémy (Supervisory Control and Data Acquisition), jež slouží ke

sběru dat a dálkovému řízení, bývají častým cílem útoků. Jejich kompromitace může narušit dohled a řízení nad rozvodem elektřiny.

Naopak fyzické části elektrizační soustavy, jako jsou vedení, jsou kybernetickými útoky přímo neohrožitelné. Lze u nich uvažovat pouze o sekundárním dopadu například při výpadku řídicích systémů, proto byly ze seznamu aktiv u této hrozby vynechány.

Nejvýznamnější známý případ spojený s blackoutem po kybernetickém útoku na evropském území se odehrál na Ukrajině v prosinci 2015. V tomto případě útok skupiny Sandworm způsobil odpojení více než 200 000 odběratelů v několika regionech. Útočníci se dostali do dispečerských systémů, převzali kontrolu nad přepínači a zablokovali operátorům přístup k SCADA systémům. [35]

V rámci České republiky zatím nedošlo k zásadnímu narušení dodávek elektřiny v důsledku kybernetického útoku, ale NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost) opakovaně varuje před rostoucí aktivitou v oblasti energetiky. Zprávy o kybernetické bezpečnosti z let 2021 a 2022 obsahují varování před sofistikovanými pokusy o infiltraci do systémů provozovatelů kritické infrastruktury. [36], [37]

Kromě zařízení dispečerského řízení a komunikační infrastruktury byly za zranitelné považovány i výroby elektřiny s vlastním IT zázemím a připojením do dispečerských systémů. Ačkoliv je to o něco méně pravděpodobné, některým útočníkům by se mohly jevit jako atraktivní cíl.

Pro snížení rizika jsou klíčová opatření v oblasti síťové segmentace, monitoringu provozu, školení personálu, aktualizace systémů, testování odolnosti pomocí penetračních testů a především záložní scénáře řízení v případě ztráty centrální kontroly.

3.7 Teroristický útok

Teroristický čin představuje záměrný útok motivovaný ideologií, politikou nebo cílem vyvolat rozsáhlý chaos a strach. I když je v České republice pravděpodobnost takového útoku nízká, nelze tuto hrozbu zcela vyloučit, zejména s ohledem na zvyšující se napětí v Evropě a světové precedenty. Riziko vyplývá především z možnosti cíleného útoku na klíčové prvky kritické infrastruktury, jehož dopady by mohly být závažné a obtížně řešitelné.

Z hlediska aktiv představují nejrizikovější cíle velké elektrárny, zejména jaderné a uhelné elektrárny, které patří do kritické infrastruktury. Jejich narušení může mít nejen okamžitý dopad na dodávku elektrické energie, ale i sekundární účinky, v případě jaderné

elektrárny i ekologické a radiační riziko. Zabezpečení těchto objektů je však na vysoké úrovni a zahrnuje i fyzickou ostrahu, režimová opatření a krizové plány. Motivace útočníků u těchto symbolicky významných a mediálně sledovaných objektů však může být značná. Vyšší pravděpodobnost dostat se na seznam možných cílů mají i elektrické stanice přenosové soustavy v kritické infrastruktuře, zejména rozvodny. Tyto objekty, i když obvykle dobře oplocené a monitorované, nebývají chráněny tak důsledně jako výroby. I jejich vyřazení však může vést k přetížení nebo přerušení přenosové trasy. Z pohledu přímého dopadu a mediálního ohlasu mohou být cílem i zařízení dispečerského řízení. Výběr tohoto aktiva by jim poskytl zvýšenou šanci na ztráty na životech.

Naopak mnoho aktiv je ze seznamu pro tuto hrozbu vynecháno kvůli nižší míře následků. Je velmi nepravděpodobné, že by si někdo za cíl teroristického činu zvolil prvek, u nějž by došlo k natolik zanedbatelným následkům, že by se nikdo o jeho činu nemusel ani dozvědět.

Celkově lze říci, že teroristické činy vůči energetické infrastruktuře v Evropě zatím nenabýly masového rozsahu, ale i přesto nelze tuto možnost zcela ignorovat. Vzhledem k nízké pravděpodobnosti, ale potenciálně vysokým následkům, je třeba zaměřit se zejména na fyzické zabezpečení aktiv, pravidelné cvičení bezpečnostních složek a spolupráci se zpravodajskými službami. Dále je důležité budovat schopnost sítě se zotavit i při výpadku části systému, a to zejména u aktiv s nejvyšší kritičností.

3.8 Závěr

Analýza rizik jednotlivých hrozeb pro elektrizační soustavu České republiky ukazuje, že odolnost systému výrazně kolísá v závislosti na typu prvku a charakteru hrozby. Nejvyšší hodnoty rizika (R) jsme zaznamenali u vedení pro vyvedení výkonu a napájení výroben (R = 48 při vlivech počasí i kybernetických útocích) a u zařízení dispečerského řízení (R = 50 při lidském faktoru, R = 75 při kybernetickém útoku).

Celkově analýza potvrzuje potřebu diferencovaného přístupu k ochraně elektrizační soustavy podle typu aktiva a charakteru hrozby. Zvláštní důraz je nutné klást na zajištění provozuschopnosti řídicích a dispečerských systémů, zvyšování fyzické a kybernetické odolnosti přenosových a distribučních sítí a pravidelnou revizi připravenosti na přírodní a technické havárie.

4 POSTUPY ŘÍZENÍ A OBNOVY PO BLACKOUTU

Analýza příčin i případové studie historických blackoutů ukazují, že k přerušení dodávek elektrické energie může skutečně dojít i ve vyspělých státech s rozvinutou infrastrukturou. V takové situaci hrají klíčovou roli postupy řízení a obnovy dodávek elektrické energie, tedy soubor prvků technické i fyzické ochrany, který má za cíl minimalizovat dopady blackoutů a co nejrychleji se vrátit k běžnému provoznímu režimu.

Pro analýzu těchto postupů bude využit především Typový plán narušení dodávek elektrické energie velkého rozsahu, vydaný Ministerstvem průmyslu a obchodu v roce 2018. Dalším důležitým zdrojem budou poznatky získané při analýze hrozeb a zranitelnosti v předchozích částech této práce, stejně jako zkušenosti vyplývající z vybraných historických případů rozsáhlých blackoutů.

4.1 Typový plán narušení dodávek elektrické energie velkého rozsahu

Typový plán narušení dodávek elektrické energie velkého rozsahu, vydaný Ministerstvem průmyslu a obchodu, představuje základní koncepční rámec pro řešení mimořádné události typu rozsáhlého blackoutu na území České republiky. Dokument vychází ze zákona č. 240/2000 Sb., o krizovém řízení, a stanovuje doporučené kroky pro orgány krizového řízení, provozovatele kritické infrastruktury i další zainteresované subjekty. [38]

Základním cílem plánu je minimalizace dopadů výpadku elektrické energie na společnost, ochrana životů a zdraví obyvatel a obnova dodávek v co nejkratším čase. Důraz je kladen na předem definované koordinační mechanismy, rozdělení kompetencí a připravenost na různé scénáře vývoje krizové situace. [38]

Prvním krokem při vzniku blackoutu je identifikace rozsahu a charakteru události. V případě výpadku přenosové nebo distribuční soustavy je odpovědný provozovatel povinen okamžitě informovat Ministerstvo průmyslu a obchodu, Hasičský záchranný sbor České republiky a další dotčené orgány. Následně se aktivuje pracovní skupina pro krizové řízení MPO (Ministerstvo průmyslu a obchodu) a v případě vážné situace může být svolán Ústřední krizový štáb. V dokumentu je popsáno i možné vyhlášení nouzového stavu, pokud je to nezbytné. [38]

Koordinace při řešení blackoutu probíhá na několika úrovních řízení: centrální (MPO, krizový štáb), regionální (krajské úřady) a technické (ČEPS, provozovatelé distribuční soustavy, výrobci). Klíčovou úlohu hraje spolupráce mezi státními a nestátními subjekty.

V plánu je podrobně rozpracována struktura komunikačních toků a zajištění přenosu klíčových informací mezi jednotlivými aktéry. [38]

Zmiňována je rovněž potřeba zajištění fyzické bezpečnosti strategických zařízení a kontrola nad pohybem osob v zasažených oblastech. Důležitým aspektem je také zajištění ochrany veřejného pořádku (např. přes nasazení Policie ČR nebo Armády ČR), jelikož rozsáhlý výpadek může vést ke společenskému napětí. Jedním z hlavních nástrojů zvládnutí krize je prioritizace obnovy dodávek pro kritickou infrastrukturu. Součástí přípravy na krizovou situaci by podle plánu mělo být vybavení těchto subjektů záložními zdroji napájení (např. diesela agregáty) a jejich pravidelné testování. [38]

Postupná obnova musí být velmi precizně koordinována, aby nedošlo ke kolapsu z důvodu nesouladu mezi výrobou a spotřebou. Klíčovou roli v tomto procesu hraje ČEPS (provozovatel přenosové soustavy), který koordinuje fáze obnovy dodávek a zajišťuje stabilizaci sítě. [38]

4.2 Komparativní analýza případů

Pro potřeby porovnání jednotlivých blackoutů z hlediska postupů řízení a obnovy bude nejdříve provedeno shrnutí úspěšných a neúspěšných přístupů u každého z případů. Následně dojde k samotnému porovnání za účelem zjištění častých chyb, efektivních strategií a rozdílů ve zvládnutí situace.

4.2.1 Blackout New York City (1977) – řízení a obnova

Během blackoutu zůstala funkční telefonní síť, ale byla přetížená. Hlavním zdrojem informací se stalo vysílání rádiových stanic. Chyběla koordinovaná krizová komunikace napříč složkami. V některých zdravotnických zařízeních chyběly nebo byly poškozeny záložní zdroje napájení. Policie a hasiči byli zapojeni do krizového řízení. Došlo k úspěšnému včasnému zastavení většiny souprav v metru a následné evakuaci cestujících. Postupná obnova trvala 25 hodin.

Zdůrazněna nutnost záložních zdrojů napájení a pravidelné údržby. Rádio může být v podobných situacích významné. Krizová komunikace je stěžejní.

4.2.2 Blackout Severovýchod USA a Kanada (2003) – řízení a obnova

Došlo k selhání ve sdílení informací mezi provozovateli, což situaci zhoršilo. Nefungoval monitorovací systém, dispečeri nevěděli o přetížení. Byly porušeny bezpečnostní standardy

(pravidlo N-1, správa vegetace). Obnova dodávek trvala dny. Státy utrpěly velké ekonomické ztráty.

Koordinace je důležitá i na mezinárodní úrovni. Systémy SCADA je nutno pravidelně modernizovat. Bylo by vhodné nespolehat se pouze na jediný systém monitorování.

4.2.3 Blackout Itálie (2003) – řízení a obnova

Chyběla včasná reakce operátorů na přetížení zbylých vedení. Operátoři neznali limity sítě. Koordinace na mezinárodní úrovni byla značně opožděna. Správa porostu v okolí vedení byla zanedbána. Obnova trvala až 48 hodin.

Důraz je zde především na organizační selhání. Personál nebyl dostatečně vyškolen, bezpečnostní standardy nebyly dodržovány. Koordinace na mezinárodní úrovni by měla být zlepšena.

4.2.4 Blackout Brazílie (2009) – řízení a obnova

Reakce ochranných systémů byla okamžitá. Systém automaticky odpojil postižená vedení na základě detekce extrémních proudových hodnot. Výkon ze zasažených vedení byl převeden na vedení nižších napěťových úrovní, což vedlo k jejich přetížení. Došlo ke kaskádovým poruchám a izolaci jednotlivých oblastí. Oprava probíhala po stabilizaci ostrovních provozů a ověření jejich připravenosti na zpětné připojení. Kritická infrastruktura a klíčové uzly byly upřednostněny. Rychlá obnova dodávek elektrické energie.

Identifikace slabých míst hrála klíčovou roli. Ochranné systémy při vícenásobných poruchách nebyly koordinované.

4.2.5 Blackout Portoriko (2017) – řízení a obnova

Okamžitě po hurikánu došlo ke zřízení týmů pro vyhodnocení škod a prioritizaci kritických oblastí. Vzhledem k příčině a souvisejícím následkům nebyla elektrizační síť nejvyšší prioritou, takže pro tuto kapitolu se příliš nehodí.

4.2.6 Blackout Texas (2021) – řízení a obnova

Byly nařízeny rotační odstávky pro zachování stability frekvence a prevenci úplného kolapsu sítě. Dispečerů se snažili upřednostnit kritickou infrastrukturu, ale přetížení a výpadky části výroby vedly ke ztrátě kontroly nad částmi sítě. Obyvatelům bylo doporučeno šetřit energií a zůstat uvnitř. V některých oblastech vznikly dočasné ohřívací stanice. Guvernér vyhlásil

stav nouze a požádal o federální pomoc. FEMA (Federal Emergency Management Agency) poskytla podporu ve formě nouzového zásobování, generátorů a přístřeší. Obnovení se pohybovalo v rámci dnů, záviselo na rozmrazení zařízení, zajištění dodávek plynu a restartu elektráren.

Odolnost infrastruktury je nutno zvyšovat dříve, než dojde ke zhoršení klimatu.

4.2.7 Srovnání blackoutů – řízení a obnova

Komparativní analýza ukázala, že i přes odlišné příčiny a geografické podmínky blackoutů se v jejich zvládání opakují některé klíčové faktory úspěchu či selhání. Ty lze rozdělit do několika tematických oblastí:

Koordinace a krizová komunikace

- Silná stránka: Rychlá a přehledná komunikace mezi složkami byla klíčem k úspěchu např. v Brazílii (2009), kde se povedlo rychle stabilizovat ostrovní provozy.
- Slabina: Naopak v USA (2003) a Itálii (2003) došlo k vážným zpožděním v koordinaci, přičemž chyběla funkční výměna informací mezi dispečery nebo jednotlivými státy.
- Poučení: Jednotné komunikační standardy a předem domluvené kanály (včetně záložních) jsou zásadní.

Záložní napájení a připravenost kritické infrastruktury

- Silná stránka: V některých případech (např. Texas 2021) byla snaha udržet provoz klíčových objektů pomocí rotačních odstávek a generátorů.
- Slabina: V New Yorku (1977) i Itálii (2003) selhaly záložní zdroje nebo chyběly, což zhoršilo situaci v nemocnicích a dalších objektech.
- Poučení: Kritická infrastruktura musí být schopna minimálně 72hodinového autonomního provozu.

Automatizace a reakce ochranných systémů

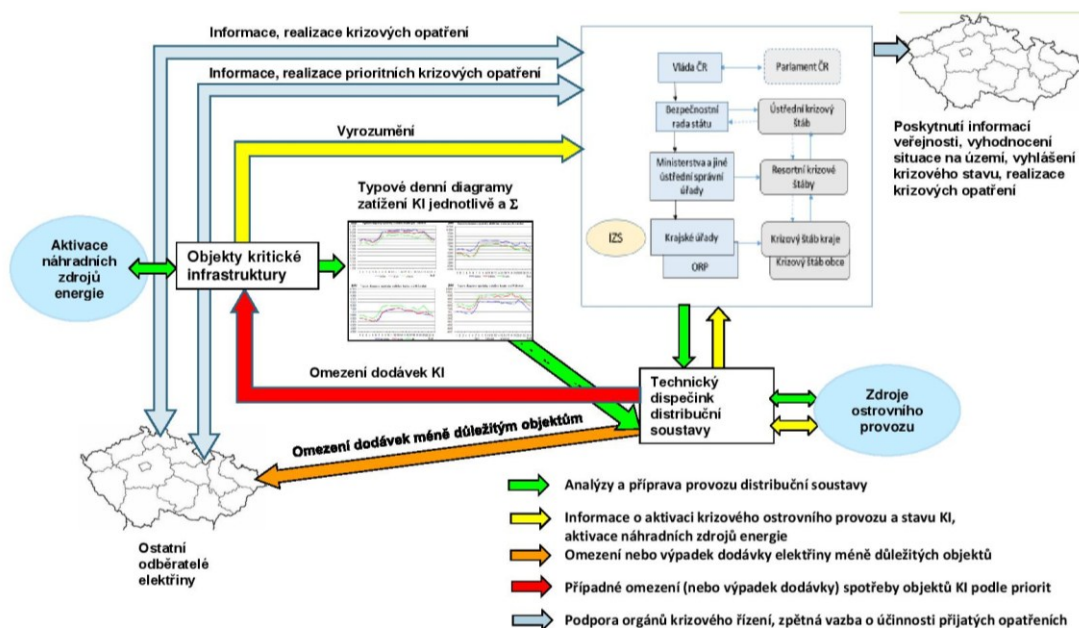
- Silná stránka: Brazilský systém (2009) ukázal sílu rychlé reakce automatické ochrany, ale také její limity při kaskádových poruchách.

- Slabina: V USA (2003) nebyly SCADA systémy dostatečně moderní ani redundantní, což vedlo k přehledové slepotě dispečerů.
- Poučení: Modernizace řídicích systémů a kombinace automatického a lidského řízení je nutná pro adaptivní reakci na krizový vývoj.

4.3 Shrnutí a doporučení

Analýza typového plánu MPO (2018) a komparativních případových studií historických blackoutů ukázala, že účinné řízení a obnova dodávek elektřiny závisí na třech vzájemně propojených pilířích:

- Příprava a prevence – dokonale otestované krizové plány, jasně rozdělené kompetence a pravidelné cvičení mezi všemi zainteresovanými subjekty (MPO, HZS, ČEPS, DS, provozovatelé KI)
- Koordinace a komunikace – rychlé a bezproblémové předávání informací napříč centrální, regionální a technickou úrovní řízení, podpořené robustními záložními komunikačními kanály (např. rádiové vysílání, satelitní spoje)
- Obnova a stabilizace – fázované znovuzapojování zdrojů a sítí podle předem definovaných kritérií, s prioritou kritické infrastruktury (zdravotnictví, vodohospodářství, doprava), a současnou stabilizací frekvence a napětí.



Obrázek 1 Schéma krizového řízení při narušení dodávek elektrické energie

(zdroj: [38])

4.3.1 Doporučení pro české prostředí

Pro zvýšení připravenosti na rozsáhlý blackout je vhodné zavést pravidelné simulace krizových situací zahrnující všechny klíčové subjekty – Ministerstvo průmyslu a obchodu, krizové štáby, ČEPS, distributory, Hasičský záchranný sbor, Policii ČR i Armádu ČR. Taková cvičení by měla probíhat minimálně jednou ročně a je žádoucí při nich využívat odborný dohled externích expertů a inspirovat se nejlepšími mezinárodními praxemi, například standardy IEEE (Institute of Electrical and Electronics Engineers) či postupy ENTSO-E (Evropská síť provozovatelů přenosových soustav elektřiny).

Dále je třeba zajistit záložní komunikační a řídicí kanály, které by měly být nezávislé na běžných sítích. Doporučuje se zavést například satelitní nebo HF-rádiové spoje v dispečerských centrech a na klíčových uzlech sítě. K dispozici by měly být také mobilní krizové jednotky vybavené přenosnými SCADA terminály, které umožní rychlé obnovení řízení i v případě výpadku hlavních řídicích prostředků.

Při obnově provozu po blackoutu je vhodné aplikovat fázovaný přístup podle brazilského modelu z roku 2009. Ten počítá s udržením tzv. ostrovních provozů, tedy lokálních částí sítě napájených z dostupných zdrojů, které se postupně propojují a obnovují celkový provoz. Pro tento postup je nutné definovat minimální soubor kritických zdrojů, které musí být schopné okamžité aktivace.

Pro zvýšení odolnosti sítě je rovněž důležité pravidelně revidovat logiku automatických ochran, zejména reléových, aby při vícenásobných poruchách spolupracovaly správně a předešly nežádoucím odpojením. Dispečeri by měli být pravidelně školeni v manuálním přepínání do ostrovního režimu, aby mohli rychle a správně reagovat v krizových situacích.

Nakonec je nezbytné posílit integrovanou mezinárodní součinnost. Koordinace s přílehlými provozovateli v rámci ENTSO-E, tedy se Slovenskem, Rakouskem či Německem, by měla zajistit sjednocení standardů jako N-1 a společné krizové postupy. Dále je přínosné sdílet cvičné scénáře a varovné signály pro včasné varování před kaskádovými poruchami.

Implementace těchto doporučení zajistí, že v případě rozsáhlého blackoutu dokážeme nejen co nejrychleji obnovit dodávky, ale i minimalizovat sekundární škody na kritických službách a společnosti jako celku.

5 ZHODNOCENÍ SOUČASNÉ PREVENCE

Současná opatření a technologie používané k prevenci blackoutů tvoří komplexní systém složený z technických, organizačních a legislativních prvků. Přestože došlo v posledních letech k významnému posunu směrem k vyšší odolnosti energetických soustav, vývoj ukazuje, že riziko rozsáhlých výpadků nelze nikdy zcela eliminovat, pouze řídit a minimalizovat jejich dopady.

Základem prevence jsou moderní monitorovací a řídicí systémy, zejména systémy SCADA, které umožňují detailní dohled nad provozem přenosové a distribuční sítě. V České republice jsou tyto systémy na vysoké úrovni, nicméně i zde existuje riziko přetížení nebo kybernetických útoků. Důležitá je proto pravidelná modernizace a zavádění bezpečnostních opatření, včetně zálohování dat, segmentace sítí a rozvoje prediktivní analytiky.

Významným prvkem obrany proti důsledkům blackoutů jsou záložní zdroje napájení. Nemocnice, dispečerská pracoviště a další prvky kritické infrastruktury bývají vybaveny dieselaagregáty nebo bateriovými úložišti. Je však nutné zajistit, aby tyto zdroje byly pravidelně testovány a měly dostatečnou kapacitu pro delší výpadky.

Rostoucí význam mají také decentralizované energetické systémy a možnost tzv. ostrovního provozu, díky nimž lokalita zůstává energeticky soběstačná i při výpadku nadřazené sítě. [39] Fotovoltaické systémy, bateriová úložiště či kogenerační jednotky mohou významně přispět k odolnosti lokálních sítí, ale v současnosti většina z nich není konfigurována pro autonomní provoz. Podpora hybridních systémů a komunitní energetiky by mohla tento nedostatek v budoucnu zmírnit. [40]

Chytré sítě a aktivní řízení spotřeby představují moderní nástroje, které mohou významně posílit prevenci blackoutů. Smart grids umožňují rychlejší detekci poruch, flexibilnější reakce na výkyvy a efektivnější integraci obnovitelných zdrojů energie. Díky digitalizaci a decentralizaci usnadňují komunikaci mezi výrobou, distribucí i spotřebiteli a podporují autonomní řízení lokálních sítí. Součástí těchto systémů je také demand side management (DSM), tedy aktivní řízení spotřeby. DSM umožňuje přizpůsobit spotřebu aktuální situaci v síti například prostřednictvím cenových signálů nebo automatizovaných systémů řízení spotřeby. Tím se snižuje zatížení během špiček a zvyšuje stabilita soustavy. I když jsou tyto technologie zatím ve fázi rozšiřování a implementace, mají potenciál zásadně změnit přístup k prevenci blackoutů a posílit odolnost i flexibilitu energetické infrastruktury v budoucnu. [41], [42]

V neposlední řadě hraje důležitou roli i krizová připravenost. Typový plán Ministerstva průmyslu a obchodu definuje jasné kompetence, komunikační kanály i možné scénáře vývoje krizové situace. Přesto lze identifikovat slabá místa, která tvoří hlavně obce a obyvatelstvo, jelikož povědomí o tom, jak se chovat v případě blackoutu není příliš rozšířené. Pravidelné cvičení krizových složek, školení pracovníků by tedy mělo být doplněno o program na seznámení obyvatelstva s výpadky elektrické energie velkého rozsahu.

Důležitou roli v prevenci blackoutů hraje také mezinárodní propojení přenosových soustav a koordinovaná spolupráce provozovatelů. V evropském kontextu tuto roli zajišťuje zejména organizace ENTSO-E (European Network of Transmission System Operators for Electricity), která koordinuje přeshraniční tok elektřiny, plánování provozu a nouzové postupy v rámci celé Evropy. Díky synchronizaci sítí, harmonizaci provozních pravidel a sdílení rezerv dochází ke zvýšení celkové odolnosti systému vůči poruchám a k lepšímu zvládání nepředvídaných událostí. V případech lokálních přetížení či výpadků tak mohou sousední státy přispět k rychlé stabilizaci situace. Přestože vyšší míra propojení přináší i určitou míru rizika systémového šíření poruch, její přínos pro stabilitu a flexibilitu převažuje, zejména pokud je doprovázen účinnou koordinací mezi provozovateli. [43]

Rostoucí význam v oblasti prevence blackoutů získávají také simulační nástroje, modelování scénářů a využití umělé inteligence (AI). Pomocí pokročilých predikčních modelů lze analyzovat rizikové situace v reálném čase, simulovat chování elektrizační soustavy při poruchách či extrémních odběrech a optimalizovat reakční strategie. AI nachází uplatnění například při predikci zatížení, vyhodnocování anomálií, adaptivním řízení spotřeby či návrhu optimálních dispečerských zásahů. Tyto nástroje výrazně přispívají ke zvyšování preventivní připravenosti a umožňují rychlejší a přesnější rozhodování v krizových situacích. Simulace a predikční algoritmy se tak stávají integrální součástí moderního řízení přenosových i distribučních sítí, a to jak ve fázi plánování, tak při samotném provozu. [44], [45]

Z výše uvedeného vyplývá, že současná opatření sice představují solidní základ pro zvládnutí mimořádných událostí, avšak v kontextu narůstajících rizik je třeba pokračovat v jejich rozvoji. Klíčová je především adaptabilita systému, schopnost rychle reagovat na nečekané události a řídit tok energie. Prevence blackoutů se tak čím dál více stává otázkou nejen technologií, ale i spolupráce a plánování.

ZÁVĚR

Tato bakalářská práce se zaměřila na problematiku blackoutů jako komplexního rizika pro moderní společnost. Z provedené analýzy vyplynulo, že výpadky elektrické energie mohou být způsobeny celou řadou faktorů, od technických poruch a systémových selhání přes extrémní klimatické jevy až po lidskou chybu či kybernetické útoky. Historické případy blackoutů navíc ukázaly, že důsledky takových událostí mohou být rozsáhlé a dlouhotrvající. Zasahují nejen ekonomiku, ale i každodenní život obyvatel, veřejnou bezpečnost a fungování kritické infrastruktury.

Přestože v České republice zatím k úplnému blackoutu nedošlo, nelze toto riziko zcela vyloučit. Právě proto má klíčový význam připravenost státu i energetických společností na krizové situace. Typový plán narušení dodávek elektrické energie velkého rozsahu představuje důležitý rámec pro řízení krizí, avšak jeho účinnost závisí na koordinaci, dostupnosti záložních zdrojů a schopnosti rychlé reakce všech zúčastněných subjektů.

Zvláštní pozornost si zaslouží současné trendy v oblasti prevence, zejména rozvoj chytrých sítí, decentralizovaných energetických systémů a komunitní energetiky. Tyto technologie mají potenciál významně zvýšit odolnost energetických sítí a umožnit ostrovní provoz v případě výpadku nadřazené soustavy. Je však nutné, aby byly tyto systémy koncipovány s důrazem na autonomii, flexibilitu a bezpečnost.

Závěrem lze říci, že blackouty představují reálnou hrozbu, kterou nelze zcela eliminovat, ale lze ji účinně zvládat kombinací technických, organizačních i legislativních nástrojů. Klíčová je prevence, včasná identifikace rizik a důsledná příprava na krizové scénáře. Jen tak lze minimalizovat dopady případného výpadku a zajistit rychlou obnovu běžného provozu.

SEZNAM POUŽITÉ LITERATURY

- [1] ÚŘAD PRO TECHNICKOU NORMALIZACI, METROLOGII A STÁTNÍ ZKUŠEBNICTVÍ [ÚNMZ]. ČSN IEC 60050-692, *Mezinárodní elektrotechnický slovník - Část 692: Výroba, přenos a rozvod elektrické energie - Spolehlivost a kvalita služby elektrizačních soustav*. Praha: Česká agentura pro standardizaci, 2019. Dostupné z: ČAS, <https://csnonlinefirmy.agentura-cas.cz/>. [cit. 2025-05-05]. [paywall].
- [2] ŘEHÁK, David. *Kritická infrastruktura elektroenergetiky: určování, posuzování a ochrana*. SPBI Spektrum. Modrá řada. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2013. ISBN 978-80-7385-126-2.
- [3] Zákon č. 240 ze dne 28. června 2000, o krizovém řízení a o změně některých zákonů (krizový zákon). Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-240>. [cit. 2025-03-09].
- [4] Nařízení vlády ze dne 22. prosince 2010, o kritériích pro určení prvku kritické infrastruktury. Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2010-432>. [cit. 2025-03-10].
- [5] Glossary. In: *Encyclopedia of Energy*. Elsevier, 2004. ISBN 978-0-12-176480-7.
- [6] VAIMAN; BELL; CHEN; CHOWDHURY; DOBSON et al. Risk Assessment of Cascading Outages: Methodologies and Challenges. Online. *IEEE Transactions on Power Systems*. 2012, roč. 27, č. 2, s. 631–641. ISSN 0885-8950. Dostupné z: <https://doi.org/10.1109/TPWRS.2011.2177868>. [cit. 2025-05-05]. [paywall].
- [7] CORWIN, J. L. a MILES, W. T. *Impact assessment of the 1977 New York City blackout. Final report*. Online. Arlington, VA: System Control, 1978. Dostupné z: <https://doi.org/10.2172/6584645>. [cit. 2025-05-07].
- [8] FEDERAL ENERGY REGULATORY COMMISSION. *Con Edison power failure of July 13 and 14, 1977. Final staff report*. Online. Washington, D.C.: Federal Energy Regulatory Commission, 1978. Dostupné z: <https://doi.org/10.2172/6673953>. [cit. 2025-05-07].
- [9] U.S.-CANADA POWER SYSTEM OUTAGE TASK FORCE. *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. Online. Washington, D.C.: U.S. Department of Energy, 2004.

- Dostupné z: <https://www.energy.gov/oe/articles/blackout-2003-final-report-august-14-2003-blackout-united-states-and-canada-causes-and>. [cit. 2025-05-05].
- [10] ANDERSON, G. Brooke a BELL, Michelle L. Lights Out. Online. *Epidemiology*. 2012, vol. 23, no. 2, s. 189-193. ISSN 1044-3983. Dostupné z: <https://doi.org/10.1097/EDE.0b013e318245c61c>. [cit. 2025-05-08].
- [11] MARX, Melissa A.; RODRIGUEZ, Carla V.; GREENKO, Jane; DAS, Debjani; HEFFERNAN, Richard et al. Diarrheal Illness Detected Through Syndromic Surveillance After a Massive Power Outage: New York City, August 2003. Online. *American Journal of Public Health*. 2006, vol. 96, no. 3, s. 547-553. ISSN 0090-0036. Dostupné z: <https://doi.org/10.2105/AJPH.2004.061358>. [cit. 2025-05-08].
- [12] LIN, Shao; FLETCHER, Barbara A.; LUO, Ming; CHINERY, Robert a HWANG, Syni-An. Health Impact in New York City during the Northeastern Blackout of 2003. Online. *Public Health Reports*. 2011, vol. 126, no. 3, s. 384-393. ISSN 0033-3549. Dostupné z: <https://doi.org/10.1177/003335491112600312>. [cit. 2025-05-08].
- [13] JOHNSON, Chris W. *Analysing the causes of the Italian and Swiss Blackout, 28 th September 2003*. Online. In: ResearchGate. 2007. Dostupné z: https://www.researchgate.net/publication/229005282_Analysing_the_causes_of_the_Italian_and_Swiss_Blackout_28_th_September_2003. [cit. 2025-05-08].
- [14] UNION FOR THE COORDINATION OF TRANSMISSION OF ELECTRICITY (UCTE). *Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy*. Online. Brusel: UCTE, 2004. Dostupné z: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/ce/otherreports/20040427_UCTE_IC_Final_report.pdf. [cit. 2025-05-08].
- [15] SCHMIDTHALER, Michael a REICHL, Johannes. Assessing the socio-economic effects of power outages ad hoc. Online. *Computer Science - Research and Development*. 2016, vol. 31, no. 3, s. 157-161. ISSN 1865-2034. Dostupné z: <https://doi.org/10.1007/s00450-014-0281-9>. [cit. 2025-05-08].
- [16] OPERADOR NACIONAL DO SISTEMA ELÉTRICO [ONS]. *The Disturbance on November 10th, 2009*. Online. Rio de Janeiro, 2009. Dostupné z: <https://www.ons.org.br/sites/multimedia/Documentos%20Compartilhados/relatorios%20anuais/2009/en/02-disturbance-Nov10th2009.html>. [cit. 2025-05-10].

- [17] OPERADOR NACIONAL DO SISTEMA ELÉTRICO [ONS]. *Relatório de Análise da Perturbação – RAP ONSRE 32522009*. Online. Rio de Janeiro, 2009. Dostupné z: https://www.gov.br/mme/pt-br/assuntos/conselhos-e-comites/arquivos/conselhos-e-comites/Anexo_2_Relatorio_de_Analise_da_Perturbacao_RAP_xONSRE32522009_x.pdf/view. [cit. 2025-05-27].
- [18] FURTADO, Matheus dos Santos; SOUZA, Lucas Araujo Nora de a ANDRADE, José Antônio Bento de. O Apagão de 2009 no Brasil: Causas e Impactos. Online. *Revista Ibero-Americana de Humanidades, Ciências e Educação*. 2023, roč. 9, č. 11, s. 3264-3278. ISSN 2675-3375. Dostupné z: <https://doi.org/10.51891/rease.v9i11.12616>. [cit. 2025-05-27].
- [19] MIDCONTINENT INDEPENDENT SYSTEM OPERATOR [MISO]. *Value of Lost Load (VOLL): Development and Use*. Online. 30 August 2022. Dostupné z: [https://cdn.misoenergy.org/20220830%20RECBWG%20Item%2002%20Value%20of%20Lost%20Load%20\(VOLL\)%20Development%20and%20Use626134.pdf](https://cdn.misoenergy.org/20220830%20RECBWG%20Item%2002%20Value%20of%20Lost%20Load%20(VOLL)%20Development%20and%20Use626134.pdf). [cit. 2025-05-27].
- [20] GORMAN, Will. The quest to quantify the value of lost load: A critical review of the economics of power outages. Online. *The Electricity Journal*. 2022, roč. 35, č. 8, article 107187. ISSN 10406190. Dostupné z: <https://doi.org/10.1016/j.tej.2022.107187>. [cit. 2025-05-27].
- [21] U.S. Government Accountability Office. *Puerto Rico Disasters: Progress Made, but the Recovery Continues to Face Challenges*. Online. Dostupné z: <https://www.gao.gov/products/gao-24-105557>. [cit. 2025-05-27].
- [22] NASA Earth Observatory. *Night Lights Show Slow Recovery from Maria*. Online. Dostupné z: <https://earthobservatory.nasa.gov/images/144371/night-lights-show-slow-recovery-from-maria>. [cit. 2025-05-27].
- [23] FEMA. *DR-4339 Hurricane Maria By The Numbers*. Online. 2021, January 21, 2025. Dostupné z: <https://www.fema.gov/fact-sheet/hurricane-maria-numbers>. [cit. 2025-05-27].
- [24] MICHAUD, Josh a KATES, Jennifer. *Public Health in Puerto Rico after Hurricane Maria*. Online. Menlo Park, CA: Henry J. Kaiser Family Foundation, 2017. Dostupné z: <http://resource.nlm.nih.gov/101727510>. [cit. 2025-05-27].

- [25] BUSBY, Joshua W.; BAKER, Kyri; BAZILIAN, Morgan D.; GILBERT, Alex Q.; GRUBERT, Emily et al. Cascading risks: Understanding the 2021 winter blackout in Texas. Online. *Energy Research & Social Science*. 2021, vol. 77, article 102106. ISSN 2214-6296. Dostupné z: <https://doi.org/10.1016/j.erss.2021.102106>. [cit. 2025-05-27].
- [26] GOLDING, Garrett; KUMAR, Anil a MERTENS, Karel. *Cost of Texas' 2021 deep freeze justifies weatherization*. Online. Federal Reserve Bank of Dallas. 2021. Dostupné z: <https://www.dallasfed.org/research/economics/2021/0415>. [cit. 2025-05-27].
- [27] DONALD, Jess. *Winter Storm Uri 2021*. Online. Texas Comptroller Glenn Hegar. October 2021. Dostupné z: <https://comptroller.texas.gov/economy/fiscal-notes/archive/2021/oct/winter-storm-impact.php>. [cit. 2025-05-27].
- [28] KOUDELKA, Ctirad a VRÁNA, Václav. *Rizika a jejich analýza*. Online. Ostrava: VŠB – Technická univerzita Ostrava, Fakulta elektrotechniky a informatiky, Katedra obecné elektrotechniky, 2006. Dostupné z: <https://docplayer.cz/421968-Rizika-a-jejich-analyza.html>. [cit. 2025-05-27].
- [29] *Větrná smršť – orkán Kyrill 2007*. Online. POŽÁRY.cz. 2007. Dostupné z: <https://www.pozary.cz/clanek/6490-vetrna-smrst-orkan-kyrill-2007/>. [cit. 2025-05-27].
- [30] Skupina ČEZ. *ČEZ Distribuce vyčíslila škody způsobené orkánem Herwartem*. Online. ©2025. Dostupné z: <https://www.cez.cz/cs/pro-media/tiskove-zpravy/cez-distribuce-vycislila-skody-zpusobene-orkanem-herwartem-44007>. [cit. 2025-05-27].
- [31] FIRE RESCUE SERVICE OF THE CZECH REPUBLIC. *POVODNĚ 1997 dvacet let poté aneb co všechno je už jinak*. Online. ©2025. Dostupné z: <https://hzscr.gov.cz/hasicien/docDetail.aspx?docid=22052994&docType=ART&chum=3>. [cit. 2025-05-27].
- [32] SKUPINA ČEZ. *ČEZ Distribuce přijala po povodních řadu opatření*. Online. ©2025. Dostupné z: <https://www.cez.cz/cs/pro-media/tiskove-zpravy/cez-distribuce-prijala-po-povodnich-radu-opatreni-43814>. [cit. 2025-05-27].
- [33] SKUPINA ČEZ. *Deset let poté: Vodní elektrárny ČEZ jsou díky masivním investicím modernější a ekologičtější*. Online. ©2025. Dostupné z: <https://www.cez.cz/cs/pro-media/tiskove-zpravy/deset-let-pote-vodni-elektrarny-cez-jsou-diky-masivnim-investicim-modernejši-a-ekologictejsi-48887>. [cit. 2025-05-27].

- [34] KUBICOVÁ, Romana. *Sesuv půdy pod Gírovou v Beskydech se v roce 2010 stal jedním z největších sesuvů u nás*. Online. Český rozhlas Střední Čechy. 2018. Dostupné z: <https://strednicechy.rozhlas.cz/sesuv-pudy-pod-girovou-v-beskydech-se-v-roce-2010-stal-jednim-z-nejvetsich-7637406>. [cit. 2025-05-27].
- [35] CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY [CISA]. *Cyber Attack Against Ukrainian Critical Infrastructure*. Online. Washington, D.C., 2016. Dostupné z: <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>. [cit. 2025-05-27].
- [36] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST [NÚKIB]. *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2021*. Online, pdf. Brno, 2022. Dostupné z: <https://nukib.gov.cz/cs/infoservis/aktuality/1852-zverejnili-jsme-zpravu-o-stavu-kyberneticke-bezpecnosti-za-rok-2021/>. [cit. 2025-05-27].
- [37] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST [NÚKIB]. *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2022*. Online, pdf. Brno, 2023. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf. [cit. 2025-05-27].
- [38] MINISTERSTVO PRŮMYSLU A OBCHODU [MPO]. *Typový plán narušení dodávek elektrické energie velkého rozsahu*. Online. Praha, 2018. Dostupné z: <https://mpo.gov.cz/assets/cz/energetika/typove-plany-reseni-krizi/2018/5/1--Typovy-plan-naruseni-dodavek-elektricke-energie-velkeho-rozsahu.docx>. [cit. 2025-05-28].
- [39] NEOTOWER. *Ostrovní systémy*. Online. ©2025. Dostupné z: <https://neotower.cz/jak-to-funguje/ostrovni-systemy/>. [cit. 2025-05-28].
- [40] MISE KLIMA. *Komunitní energetika*. Online. ©2025. Dostupné z: https://www.miseklima.cz/opatreni/komunitni-energetika/?utm_source=chatgpt.com. [cit. 2025-05-28].
- [41] ION POWER GRID. *HOW SMART GRIDS PREDICT AND PREVENT POWER OUTAGES*. Online. Medium. 2025. Dostupné z: <https://ionpowergrid.medium.com/how-smart-grids-predict-and-prevent-power-outages-874c84baacde>. [cit. 2025-05-28].

- [42] UNITED NATIONS INDUSTRIAL DEVELOPMENTAL ORGANISATION [UNIDO]. *Demand-side management*. Online, pdf. Vídeň, 2009. Dostupné z: https://www.unido.org/sites/default/files/2009-02/Module14_0.pdf. [cit. 2025-05-28].
- [43] ENTSO-E. *Mission Statement*. Online. Dostupné z: <https://www.entsoe.eu/about/inside-entsoe/objectives/>. [cit. 2025-05-28].
- [44] NEALON, Cory a HORNER, Kim. *University at Buffalo engineers, partners create model to make nation's grid more resilient amid extreme weather, projected spikes in demand*. Online. University at Buffalo. 2024. Dostupné z: https://www.buffalo.edu/news/releases/2024/06/study-ai-could-prevent-future-power-outages.html?utm_source=chatgpt.com. [cit. 2025-05-28].
- [45] NATIONAL RENEWABLE ENERGY LABORATORY [NREL]. *Generative Artificial Intelligence for the Power Grid* [online]. Golden, CO: NREL, 2024 [cit. 2025-05-28]. Dostupné z: <https://www.nrel.gov/grid/generative-artificial-intelligence-for-the-power-grid>

SEZNAM OBRÁZKŮ

Obrázek 1 Schéma krizového řízení při narušení dodávek elektrické energie	46
---	----

SEZNAM TABULEK

Tabulka 1 Srovnání rozsahu a dopadu historických blackoutů.....	25
Tabulka 2 Určení stupně rizika	28
Tabulka 3 PNH analýza	29

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AI	Artificial Intelligence (umělá inteligence)
DSM	Demand side management (aktivní řízení spotřeby)
ENTSO-E	Evropská síť provozovatelů přenosových soustav elektřiny
FEMA	Federal Emergency Management Agency (Federální agentura pro krizové řízení)
IEEE	Institute of Electrical and Electronics Engineers (Institut elektrotechnických a elektronických inženýrů)
KI	Kritická infrastruktura
MPO	Ministerstvo průmyslu a obchodu
NN	Nízké napětí
VN	Vysoké napětí
VOLL	Value of Lost Load (hodnota nedodaného zatížení)
SCADA	Supervisory Control And Data Acquisition (Dispečerské řízení a sběr dat)