

Даниела Борисова

МИКРОРЕЖИ И КИБЕРСИГУРНОСТ



Образование и познание

Даниела Борисова

**МИКРОМРЕЖИ
И КИБЕРСИГУРНОСТ**

София

2025

Даниела Борисова

Институт по информационни и комуникационни технологии
Българска Академия на Науките

Настоящата монография е изготвена с финансовата помощ на проект „Математически модели, методи и алгоритми за решаване на трудни оптимизационни задачи за постигане на висока сигурност в комуникациите и по-добра икономическа устойчивост“ № КР-06-Н52/7/19-11-2021, финансиран от Фонд „Научни изследвания“ на Министерството на образованието и науката.

© Даниела Борисова, автор, 2025

ISBN 978-619-7515-57-2

eISBN 978-619-7515-61-9

Daniela Borissova

**MICROGRIDS
AND CYBERSECURITY**

Sofia

2025

Daniela Borissova

Institute of Information and Communication Technologies
Bulgarian Academy of Sciences

This monograph was prepared with the financial support of the project "Mathematical models, methods and algorithms for solving difficult optimization problems to achieve high security in communications and better economic sustainability" No. KP-06-H52/7/19-11-2021, funded by the Scientific Research Fund of the Ministry of Education and Science.

© Daniela Borissova, author, 2025

ISBN 978-619-7515-57-2

eISBN 978-619-7515-61-9

Предговор

Увеличаващото се навлизане на източниците за производство на възобновяема енергия, базирани на електроника, намаляването на общата ротационна инерция и двупосочният поток на енергия промениха концепцията за стабилност на интелигентната микромрежа и оперативните изисквания. Стабилността на интелигентните микромрежи с ниска инерция и бързи динамични възобновяеми източници е силно зависима от надеждната и осъществима оперативна съвместимост между техните компоненти. Комуникационната инфраструктура е отговорна за осигуряването на тази оперативна съвместимост в рамките на определения времеви хоризонт, като се има предвид поверителността, целостта, наличността и автентичността на обменяната информация. Това прави интелигентните микромрежи уязвими за кибератаки. Нападателите се опитват да нарушат операциите на микромрежата, като манипулират предаваните данни или атакуват физическата система.

Основните предизвикателства, пред които са изправени възобновяемите интелигентни микромрежи по отношение на киберзаплахите, се дължат на остарели наследени системи, което ги прави уязвими на атаки поради остарял софтуер и хардуер. От друга страна, използването на новоразработени методи е предизвикателство поради липсата на съвместимост с настоящата инфраструктура на възобновяема интелигентна микромрежа. Освен това усъвършенстваните решения за киберсигурност често не успяват да отговорят на приложенията в реално време поради времевият им характер, оставяйки възобновяема интелигентна микромрежа все още уязвими за кибератаки. Всичко това обуславя необходимостта от непрекъснати актуализации на решенията за киберсигурност и обучение на човешки ресурси, тъй като нападателите постоянно намират нови начини за проникване в системи.

В тази монография са представени съвременни изследвания в областта на киберзащитата на интелигентните микромрежи. Разгледани са различни форми на киберакатаки както и архитектури за обмен на данни. Анализирани са различните видове комуникации, както и протоколите и стандартите, използвани в тях. Описани се различни типове киберуязвимости, както и основни стъпки за извършване на анализ на риска в микромрежал. Разгледани са някои глобални решения за защита от кибератаки, базирани се на машинно обучение.

Описаните предизвикателства и решения за защита на интелигентните микромрежи от кибератаки в настоящата монография могат да се използват както от специалисти в областта, така и от широк кръг читатели, проявяващи интерес към съвременните решения за защита на интелигентните микромрежи.

Foreword

The increasing penetration of renewable energy sources based on electronics, the reduction of total rotational inertia and bidirectional energy flow have changed the concept of smart microgrid stability and operational requirements. The stability of smart microgrids with low inertia and fast dynamic renewables is highly dependent on reliable and feasible interoperability between their components. The communication infrastructure is responsible for ensuring this interoperability within the defined time horizon, considering the confidentiality, integrity, availability and authenticity of the exchanged information. This makes smart microgrids vulnerable to cyberattacks. Attackers try to disrupt the microgrid operations by manipulating the transmitted data or attacking the physical system.

The main challenges facing renewable smart microgrids in terms of cyber threats are due to outdated legacy systems, which makes them vulnerable to attacks due to outdated software and hardware. On the other hand, the use of newly developed methods is a challenge due to the lack of compatibility with the current renewable smart microgrid infrastructure. Furthermore, advanced cybersecurity solutions often fail to respond to real-time applications due to their time-consuming nature, leaving renewable smart microgrids still vulnerable to cyberattacks. All this necessitates the need for continuous updates of cybersecurity solutions and training of human resources, as attackers are constantly finding new ways to penetrate systems.

This monograph presents contemporary research in the field of cyber security of smart microgrids. Different forms of cyberattacks as well as architectures for bulk data are examined. Different types of communications are analyzed, as well as the protocols and standards used in them. Various types of cyber vulnerabilities are described, as

well as basic steps for performing a risk analysis in a microgrid. Some global solutions for protection against cyberattacks based on machine learning are considered.

The challenges and solutions for protecting smart microgrids from cyberattacks described in this monograph can be used by both specialists in the field and a wide range of readers interested in modern solutions for protecting smart microgrids.

Съдържание

Предговор	v
Foreword	vii
Съдържание	1
Увод	4
1. Микромрежите като план за разширена защита на критична инфраструктура	6
2. Класифициране на различните форми на кибератаки срещу микромрежите	11
2.1. Атака „човек по средата“ (<i>Man-in-the-middle attack – MITM</i>).....	11
2.2. Измамни атаки (<i>Deception attacks or False data injection attack – FDI</i>).....	12
2.3. Отказ от услуга (<i>DoS</i>) и разпределени (<i>DDoS</i>) атаки.....	13
2.4. Повторни атаки (<i>Replay attacks</i>)	14
2.5. Фишинг атаки (<i>Phishing attacks</i>)	15
2.6. Атака със зловреден софтуер (<i>Malware attack</i>)	16
3. Архитектури и математическа основа на структурата за обмен на данни в микромрежи	19
3.1. Видове архитектури на структурата за обмен на данни	19
3.2. Математическата основа на структурите за обмен на данни	24
4. Комуникации в инфраструктурата на микромрежите	29

4.1. Видове комуникации в инфраструктурата на интелигентна микромрежа	29
4.2. Софтуерно дефинирана мрежа	36
5. Протоколи и стандарти в инфраструктурата на интелигентна микромрежа	43
5.1. Концептуален модел на централизирана възобновяема интелигентна микромрежа	43
5.2. Стандарти за комуникация в микромрежи	45
5.3. Комуникационни протоколи в микромрежи	49
6. Интелигентна киберсигурност на микромрежа	60
6.1. Пътната карта за атака на възобновяема интелигентна микромрежа	61
6.2. Атака срещу вградени устройства	65
6.3. Атака върху комуникацията и протоколите	68
7. Киберуязвимости на възобновяемите източници на енергия, защитни мерки и режими на работа на микромрежата	76
7.1. Кибератака срещу фотоволтаичните системи	76
7.2. Кибератака срещу вятърна електроцентрала	82
7.3. Кибератака срещу източници за съхранение на енергия	83
7.4. Класификация на експлоатационните условия на микромрежите	83
7.5. Защитни мерки за противодействие на кибератаки в микромрежите	86
8. Тестове, оценка и анализ на риска в интелигентни мрежи	95
8.1. Тестове за микромрежи	95

8.2. Оценка на уязвимостта на микромрежи	98
8.3. Анализ на риска	101
9. Роля на машинното обучение за осигуряване киберсигурността на микромрежите	108
9.1. Машинно обучение в помощ на киберсигурността на микромрежите	108
9.2. Системи за откриване и предотвратяване на проникване.....	111
9.3. Глобални решения за защита от кибератаки	117
Заклучение	135

Увод

Микромрежите могат да се дефинират като малки енергийни системи с ниско или средно напрежение с децентрализирана група от източници на електроенергия и товари, които могат да работят свързани към или отделени („островни“) от главната енергийна мрежа. За да осигурят правилен контрол, микромрежите често използват широко информационни и комуникационни технологии.

Терминът интелигентни микромрежи се отнася до микромрежи, които са базирани на мрежови системи за управление. Мрежата за управление на интелигентните мрежи като цяло не може да се разглежда като изолирана мрежа: мрежата за управление обикновено е свързана навън, за да получава дистанционни команди или да позволява дистанционна поддръжка. Използваната мрежа може да включва безжични канали и мрежата може да бъде географски разместена, което прави някои устройства физически достъпни и податливи на атаки. Освен това електрическата мрежа е критична инфраструктура, така че може да бъде цел на нападатели с огромен технически и икономически капацитет.

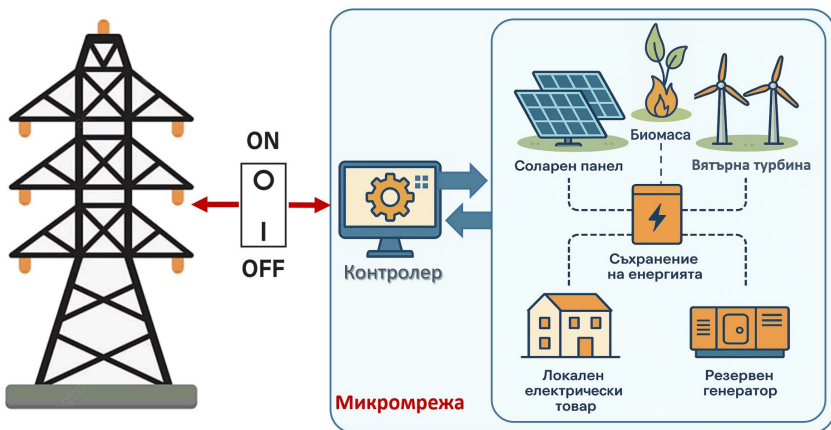
Ефективните микромрежи, които комбинират физически и киберсистеми, изискват надеждно и ефикасно наблюдение и администриране. Въпреки това интегрирането на тези компоненти може да създаде слабости в системата, което налага специално внимание върху тези проблеми, за да се осигури успешно внедряване и работа на микромрежата.

Интелигентните микромрежи, интегриращи сложни механизми, включително разпределени сензори, задвижващи механизми, контролери и захранващи компоненти, изискват прецизна и бърза комуникационна координация. Интелигентните микромрежи трябва да се справят с предизвикателства като осигуряване на надеждна свързаност, подобряване на сигурността на данните и ефективно управление на широкомащабна обработка на данни. Поради всички тези причини киберсигурността е основен въпрос за подобряване на устойчивостта на микромрежите.

1. Микромрежите като план за разширена защита на критична инфраструктура

В днешния свят, зависим от електрическата енергия, стабилността и сигурността на електроснабдяването са от изключителна важност за функционирането на обществото. Критичната инфраструктура – като болници, водоснабдяване, телекомуникации, транспорт и държавни учреждения – не може да си позволи прекъсването на електрозахранването. Уязвимостта на големите електропреносни мрежи към природни бедствия се превърна в належащ проблем, но природата не е единственото нещо, което заплашва мрежата в наши дни. Тъй като обществото става все по-дигитализирано, критичната инфраструктура е изложена на повишена експозиция на киберзаплахи. Няма достатъчно мощност, така че достъпът до нова мощност все повече се превръща в пречка за центровете за данни. Съвременните икономики също се движат с електричество, а без него те блокират. Едно набиращо популярност решение са микромрежите, които предлагат достъп до надеждно захранване и постоянна електрическа устойчивост както за бизнеса, така и за правителството.

Какво представляват микромрежите? Микромрежите са локални енергийни системи, които могат да работят, като се свързват с основната електропреносна мрежа, но могат да бъдат и напълно самостоятелни в т.нар. „островен режим“. Компоненти на типична микромрежа са локалните източници на енергия (соларни панели, вятърни турбини, биомаса, микрогенератори); енергийните хранилища (батерии); интелигентните контролни системи и натоварванията (потребители), както е илюстрирано на Фиг. 1.1.



Фиг. 1.1. Компоненти на типична микромрежа

Микромрежата като самостоятелна енергийна система, може да генерира, разпределя и контролира електроенергия локално. Тя комбинира различни източници на енергия като слънчеви панели, вятърни турбини и генератори на изкопаеми горива, заедно със системи за съхранение на енергия и усъвършенствани технологии за управление. Множество микромрежи могат да бъдат интегрирани в основната електрическа мрежа, като всяка от тях действа като ключов компонент на разпределителната комуникационна мрежа.

В островен режим микромрежата работи независимо, осигурявайки електричество само за своите вътрешни енергийни нужди. Системата за управление на микромрежата взаимодейства с пазарните сигнали и оптимизира характеристики като пиково натоварване и регулиране на честотата. Системата за контрол управлява разпределението и използването на ресурси, включително производство и съхранение на енергия, управление на натоварването и осигуряване на самодостатъчна работа. Всички тези особености са предпоставка за уязвимост на микромрежите от кибератаки. Експертите по сигурността описват кибератаката срещу електрическата мрежа като форма на асиметрична война – средство за унищожаване на обществото чрез прекъсване на доставката на

храна, вода, здравеопазване, търговия и комуникации. От жизненоважно значение е да се приложат всички възможни мерки за сигурност, за да се предотвратят прекъсвания, които могат да оставят хората без основни ресурси. Това, което мнозина не осъзнават, е, че микромрежите предлагат защита срещу кибератаки и предоставят обещаващ път за подобряване на сигурността на мрежата.

Като източник на генериране на електроенергия на място по време на прекъсвания микромрежите гарантират, че съоръженията и операциите остават функционални, но също така могат да помогнат за стабилизиране на мрежата по време на периоди на напрежение в мрежата. Със способността си да работят независимо от основната мрежа, микромрежите могат не само да осигурят непрекъсната защита срещу киберзаплахи, но и да предложат гъвкаво и ефективно решение за развиващия се енергиен пейзаж. В случай на продължителни прекъсвания, микромрежите, захранвани с природен газ, осигуряват допълнителен слой надеждност в сравнение с потенциални закъснения или недостиг на доставка на дигелово гориво. Природният газ е изобилен, с относително чисто изгаряне и с вътрешен произход, което го прави надежден вариант за генериране на енергия.

Появата на изкуствения интелект постави началото на нова ера за мрежова сигурност, представяйки смесица от обещание и опасност. От една страна, изкуственият интелект и технологиите предлагат мощен набор от инструменти за укрепване на устойчивостта на мрежата. Предсказуемият анализ, задвижван от алгоритми за машинно обучение, може да пресее огромни масиви от данни от мрежата и свързаните устройства, за да открие превантивно и да осуети потенциални заплахи. Този проактивен подход позволява по-бързо време за реакция и по-ефективни стратегии за смекчаване в случай на кибератаки или физически пробиви.

И все пак, широкото приемане на изкуствения интелект също така въвежда нови рискове за киберсигурността. Тъй като систе-

мите стават все по-взаимосвързани и автономни, те създават възможности за злонамерени участници да използват уязвимостите. Атаките, насочени към манипулиране на данни, представляват заплаха за целостта на решенията за сигурност, потенциално водещи до фалшиви аларми или компрометирано вземане на решения. Освен това опасенията относно алгоритмичните пристрастия и прозрачността повдигат въпроси относно етичните последици от разчитането на изкуствения интелект за критични мрежови операции.

Въпреки че изкуственият интелект има огромен потенциал за подобряване на мрежовата сигурност, внедряването му трябва да бъде придружено както от стабилни мерки за киберсигурност, така и от електрическа устойчивост, осигурена от микромрежите за природен газ. Чрез възприемането на цялостен подход, който дава приоритет както на иновациите, така и на намаляването на риска, индустрията може да се ориентира в променящия се пейзаж на заплахите и да защити критичната инфраструктура за бъдещите поколения.

Развитието на изкуствения интелект само засилва рязкото нарастване и изискванията на центровете за данни. И тъй като микромрежите служат като план за разширена защита на критична инфраструктура, тяхното практическо приложение за центрове за данни предоставя завладяващ модел за повишаване на устойчивостта и надеждността за всички бизнеси и общности. Тези сложни енергийни системи предлагат ценна представа за внедряването на микромрежи като децентрализирано производство и разпределение на енергия, намалявайки уязвимостите, свързани с централизираните мрежи.

Микромрежите позволяват на местните активи за производство на електроенергия – включително традиционни генератори, възобновяеми източници и съхранение – да поддържат работата на локалната мрежа дори когато по-голямата мрежа има прекъсвания или, за отдалечени райони, където няма връзка с по-голя-

мата мрежа. Освен това микромрежите позволяват на местните активи да работят заедно, за да спестят разходи, да удължат продължителността на енергийните доставки и да генерират приходи чрез участие на пазара.

Чрез децентрализиране на генерирането на енергия и включване на устойчиви технологии микромрежовият модел на центъра за данни може да бъде водеща рамка за укрепване на цялостната сигурност и устойчивост на критичната инфраструктура. Но в крайна сметка силата на публично-частното сътрудничество се очертава като решаващ компонент в колективните усилия за изграждане на киберсигурни микромрежи, които гарантират устойчивостта и надеждността на нашата критична мрежова инфраструктура.

Микромрежите са не само технически иновации, но и стратегически ресурс за защита на обществото. Те осигуряват: непрекъсваемо хранване, гъвкавост и устойчивост, по-ниски разходи в дългосрочен план и енергийна независимост.

2. Класифициране на различните форми на кибератаки срещу микромрежите

Цялостно разбиране на каналите за предаване на микромрежите е от съществено значение за точното разпознаване и ефективно контролиране на кибератаки [1]. Кибератаките могат да доведат до вреда, която се простира отвъд дигиталната област и дори може да засегне физическата среда [2]. Те могат да доведат до проникване в системата, което да предизвика невъзможност на машината да изпълни желаните команди. Следователно пробивът се премества от киберпространството към физическото пространство, което налага разрешаването на последствията от пробива [3].

2.1. Атака „човек по средата“ (*Man-in-the-middle attack –MITM*)

Кибератаката „човек по средата“, често известна като кибератака MITM, е сложна форма на проникване, при която нападателят дискретно прихваща и манипулира комуникацията между двама агенти или системи, като остава незабелязан. Извършителят на тази жестока атака се поставя в стратегическа позиция между подателя и получателя на съобщението. Те създават впечатлението, че комуникират директно един с друг, докато всъщност тайно регулират потока от информация. Това може да бъде представено по следния начин [4]:

Sender → Attacker → Receiver

Тук нападателят прихваща комуникацията от подателя и я променя, ако е необходимо, и я препраща към очаквания приемник. По същия начин атакуващият прихваща отговорите на получателя, променя ги според нуждите и след това ги препраща към подателя. Това скрито прихващане и модифициране на данни може

да се осъществи в множество комуникационни мрежови канали, включително кабелни и безжични мрежи, уебсайтове, имейли и приложения за незабавни съобщения.

Interception $\xrightarrow{\hspace{1.5cm}}$ *Modification* *Impersonation* $\xrightarrow{\hspace{1.5cm}}$ *Interference* *Data Theft*

При MITM атака нападателят може да се представи за единия или и двамата агенти, участващи в комуникацията. Това затруднява легитимните членове да разграничат модифицираното от истинското. Това представяне може да включва подправяне на мрежови IP адреси, домейни и цифрови сертификати. Следователно компрометира доверието и целостта на комуникацията. Междувременно нападателят може да попречи на предаването на данни, като промени съобщенията, въведе злонамерен код или дори напълно блокира или забави комуникационните протоколи. Намесата на нарушителите има за цел да манипулира данните, обменяни между агентите и системите за определени цели. Обикновено това се прави, за да се открадне чувствителна информация като идентификационни данни за вход, лична информация и финансови данни.

2.2. Измамни атаки

(Deception attacks or False data injection attack – FDI)

Тази стратегия е широко известна като false data injection attack (FDI), което означава инжектиране на фалшиви данни. Съгласно тази концепция различни киберсегменти компрометират целостта на изпратената информация. Измамни пробиви или нападения възникват, когато конкретни компоненти като инструменти, тригери или контролни модули се поддават на трика да приемат невярна информация за автентична. Илюстративен пример е Stuxnet, добре познат компютърен вирус с капацитет да променя софтуера в индустриални логически контролери, използвани в индустриални приложения в реалния свят [5]. По време на инжектиране на фалшиви данни нападателите генерират информационни пакети

безразборно или ги конструират с помощта на математически алгоритми [6]. Математическият модел за изследвания на микромрежите, базиран на определението за този тип атака, е следният [7, 8]:

$$x^{att} = x + \alpha \Delta$$

където x^{att} е атакуваният сигнал, който може да бъде напрежение, ток, честота, мощност и т.н. x е здравият сигнал без атаки. Δ са ограничени или неограничени фалшиви данни, инжектирани за коригиране на данни, които биха били постоянни стойности, периодични вълни, шум и т.н. $\alpha=1$ означава, че атаката е стартирана, а $\alpha=0$ определя, че атаката не е налична за сигнала.

2.3. Отказ от услуга (DoS) и разпределени (DDoS) атаки

Атака за отказ на услуга е злонамерена дейност, при която хакер затрупва определен компонент от управляващата система с прекомерен брой запитвания, като по този начин изчерпва възможностите на системата. В такива ситуации обширната обработка кара машината да изпитва прекъсвания или неизправности, което потенциално я прави напълно недостъпна [9, 10]. DoS атаките могат да бъдат насочени както към компютърни мрежи, така и към физически системи. Кибератаките, споменати в този контекст, имат специфична цел да причиняват смущения в информационните канали или да деактивират софтуерния код, който контролира мрежата, информацията от сензорите и информационната топология [11, 12]. Предотвратяването на атака за отказ на услуга е изключително сложно поради трудността при разграничаването на истинската информация от злонамерените заявки, тъй като и двете използват един и същ канал и стандарт. За да се предпази системата от атака за отказ на услуга, трябва да се уверим, че са налични системи за откриване на проникване и решение за предотвратяване на разпределена атака за отказ на услуга. Осигуряването на излишен капацитет в уеб връзката на организацията е от решаващо значение.

Значителният капацитет за изисквания за трафик на услугата помага за предпазване от нискомащабни разпределени атаки за отказ на услуга. Атаката за отказ на услуга не позволява на получателя да получи достъп до информацията, която изпращачът е изпратил. Нашественикът упорито предава идентична информация от множество източници към приемника, докато не блокира комуникационните връзки. При атаката за отказ на услуга, по време на възникването си сигналът, включително командите за измерване или управление, ще бъде прекъснат за известно време. Така полезната математическа формула за тази атака е [7]:

$$x^{att} = (1 - \alpha)x$$

където x^{att} е атакуваният сигнал, който може да бъде напрежение, ток, честота, мощност и т.н., а x е нормалният сигнал без атаки. При $\alpha=1$ се означава появата на атака за отказ на услуга, а при $\alpha=0$ – няма атака за отказ на услуга.

2.4. Повторни атаки (*Replay attacks*)

Повторните атаки са специфичен тип измамна атака. По време на това нарушение нападателят първо придобива данните, извлечени от устройството. След това атакуваният заменя променените данни с файл, съдържащ информация от регистрационния файл, което води до спад в ефективността на системата за управление и потенциално позволява неоткрити физически атаки от различни видове. Откриването на такъв компромат е трудно поради възможността за удостоверяване на шифрованите ключове. Като отговор на нарушението противникът прехвърля предварително видените данни към приемника, без да прави никакви модификации. Например, ако има проблем в енергийните системи, хакерът може да съобщи информация, дори когато всичко останало работи добре. В резултат на това центърът за управление погрешно приема, че оборудването все още функционира според установените норми. В резултат на това решаването на проблема отнема повече време, а пос-

ледствията от грешката се влошават, тъй като защитният механизъм не е взет предвид. Въпреки това, при типичните работни условия на енергийните мрежи, прехвърлянето на информация, докато е в погрешно състояние, може да доведе до изпращане на неточен сигнал за работа от центъра за управление [13, 14]. Една илюстрация на това може да се представи по следния начин [1]:

$$\psi_{ri} = \psi_{si} + \psi_h$$

където ψ_{ri} и ψ_{si} са съответно получената информация и изпратената информация и невярната информация, а ψ_h е колекция от съхранени предишни информационни пакети от противника, обозначени като $\psi_h = (\psi_\alpha, \psi_{\alpha+1}, \dots, \psi_{\alpha+n})$.

2.5. Фишинг атаки (*Phishing attacks*)

Този тип атака е известна като фишинг и включва доставка на фалшиви имейли, които изглежда, че произхождат от надеждни институции. Придобиването на конкретни лични и идентификационни данни е основната цел на този тип атака. Фишинг атаките попадат в категорията психологическа манипулация и технологична измама. Поредица от имейли доставят този вирус на нашата машина, съдържащ интегрирани URL адреси, които зареждат злонамерен софтуер върху него. Има случаи, когато щракването върху тази връзка ще ни отведе до интернет адрес, който не е реален и ще ни принуди да инсталираме злонамерен софтуер или да предоставим личната си информация. Използвайте много различни методи за комуникация като текстови съобщения, обаждания и т.н., за да получите лична информация чрез фишинг нападение. Има няколко различни типа стратегии за фишинг като лов на китове, отравяне с копие и подвеждащи техники.

За да се смекчи възможността от фишинг атаки в микромрежата, могат да се използват разсъждения, проверка на връзката, анализ на имейл, подпис и др. Освен това, чрез повишаване на осведомеността сред енергийния диспечерски персонал и отделни лица, може да се смекчат до известна степен фишинг атаките [15].

2.6. Атака със зловреден софтуер (*Malware attack*)

Операцията със злонамерен софтуер включва неволно поставяне на вреден код на машината на дадено лице. Това е, което днес наричаме вируси, зловреден софтуер или ransomware, наред с други. Нормалният код вгражда заразен код, което му позволява да се разпространява и работи независимо. Зловреден софтуер може да проникне в търговски мрежи, да наруши определени технологични процеси, да експроприира частни файлове или друга лична информация и следователно да генерира незаконни печалби от целта. Понастоящем шпионският софтуер е насочен предимно към търговски или икономически данни, а не към лични данни [16].

Най-често срещаният тип злонамерен софтуер е вирус, злонамерена програма, която се свързва с машинни програми, репликира и модифицира кода при изпълнение. Придобиването на приложение или изпълнението на софтуер може да го разпространи. Друга форма на вируса е троянският кон, считан за най-опасния поради вредната си функционалност. Той се крие в полезен софтуер и не се разпространява като вирусите. Третият тип е ransomware, злонамерена програма, която ограничава достъпа до клиентска информация и изисква плащане за освобождаването ѝ. Въпреки простотата на кода избягването на тази атака е изключително трудно.

Библиография

1. Ahmed, I., El-Rifaie, A.M., Akhtar, F., Ahmad, H., Alaas, Z., Ahmed, M.M.R.: Cybersecurity in microgrids: A review on advanced techniques and practical implementation of resilient energy systems. *Energy Strategy Reviews*, 58, 101654, 2025, <https://doi.org/10.1016/j.esr.2025.101654>.
2. Цочев, Г., Йошинов, Р.: Изследване сигурността на киберфизичните системи. Образование и познание, 2020.
3. AlHidaifi, S.M., Asghar, M.R., Ansari, I.S.: A survey on cyber resilience: Key strategies, research challenges, and future directions. *ACM*

- Computing Surveys, 56(8), 1-48, 2024, <https://doi.org/10.1145/3649218>.
4. Jena, S., Padhy, N.P., Guerrero, J.M.: Multi-layered coordinated countermeasures for DC microgrid clusters under man in the middle attack. IEEE Transactions on Industry Applications, 60(2), 2127-2141, 2024, <https://doi.org/10.1109/TIA.2023.3308557>.
 5. Benmalek, M., Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. Internet of Things and Cyber-Physical Systems, 4, 186-202, 2024, <https://doi.org/10.1016/j.iotcps.2023.12.001>.
 6. Zhang, H., Chen, Z., Yu, C., Yue, D., Xie, X., Hancke, G.P.: Event-trigger-based resilient distributed energy management against FDI and DoS attack of cyber-physical system of smart grid. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 54(5), 3220-3230, 2024, <https://doi.org/10.1109/TSMC.2024.3357497>.
 7. Mahvash, H., Taher, S.A., Guerrero, J.M.: Detecting and mitigating cyber-attacks in AC microgrid composed of marine current turbine DFIGs to improve energy management system. e-Prime - Advances in Electrical Engineering, Electronics and Energy, 7, 100464, 2024, <https://doi.org/10.1016/j.prime.2024.100464>.
 8. Shahbazi, Z., Ahmadi, A., Karimi, A., Shafiee, Q.: Performance and vulnerability of distributed secondary control of AC microgrids under cyber-attack. In 7th International Conference on Control, Instrumentation and Automation (ICCIA), Tabriz, Iran, pp. 1-6, 2021, <https://doi.org/10.1109/ICCIA52082.2021.9403548>.
 9. Chen, H., Yang, S., Wu, H., Song, J., Shui, S.: Advanced hierarchical energy optimization strategy for integrated electricity-heat-ammonia microgrid clusters in distribution network. International Journal of Hydrogen Energy, 97, 1481-1497, 2025, <https://doi.org/10.1016/j.ijhydene.2024.11.428>.
 10. Basit, A., Tufail, M., Rehan, M., Ahmed, W., Radwan, A., Ahmed, I.: Event-based secure filtering under two-channel stochastic attacks and switching topologies over wireless sensor networks. IEEE Transactions on Network Science and Engineering, 11(4), 3704-3717, 2024, <https://doi.org/10.1109/TNSE.2024.3383280>.

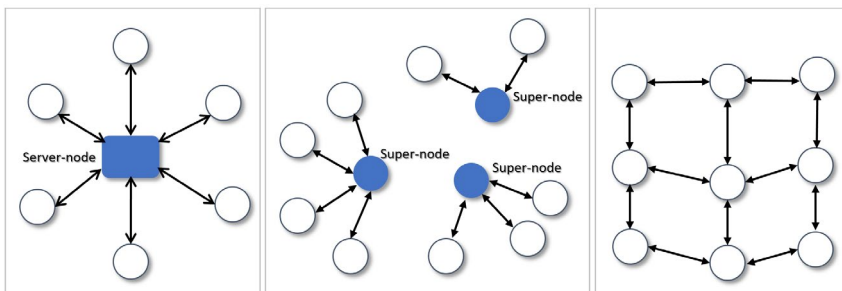
11. Basit, A., Tufail, M., Rehan, M., Riaz, M., Ahmed, I.: Distributed state and unknown input estimation under denial-of-service attacks: A dynamic event-triggered approach. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 70(6), 2266-2270, 2023, <https://doi.org/10.1109/TCSII.2022.3229412>.
12. Shirkhani, M., Tavoosi, J., Danyali, S., Sarvenoei, A.K., Abdali, A., Mohammadzadeh, A., Zhang, C.: A review on microgrid decentralized energy/voltage control structures and methods. *Energy Reports*, 10, 368-380, 2023, <https://doi.org/10.1016/j.egyr.2023.06.022>.
13. Yi, X., Lu, T., Li, Y., Ai, Q., Hao, R.: Collaborative planning of multi-energy systems integrating complete hydrogen energy chain. *Renewable and Sustainable Energy Reviews*, 210, 115147, 2025, <https://doi.org/10.1016/j.rser.2024.115147>.
14. Khalid, M., Ahmed, I., AlMuhaini, M., Savkin, A.V.: A novel computational paradigm for scheduling of hybrid energy networks considering renewable uncertainty limitations. *Energy Reports*, 11, 1959-1978, 2024, <https://doi.org/10.1016/j.egyr.2024.01.047>.
15. Tamal, M.A., Islam, Md K., Bhuiyan, T., Sattar, A., Prince, N.U.: Unveiling suspicious phishing attacks: enhancing detection with an optimal feature vectorization algorithm and supervised machine learning. *Frontiers in Computer Science*, 6, 1428013, 2024, <https://doi.org/10.3389/fcomp.2024.1428013>.
16. Aryal, K., Gupta, M., Abdelsalam, M., Kunwar, P., Thuraisingham, B.: A survey on adversarial attacks for malware analysis. *IEEE Access*, 13, 428-459, 2025, <https://doi.org/10.1109/ACCESS.2024.3519524>.

3. Архитектури и математическа основа на структурата за обмен на данни в микромрежи

За да се анализират ефектите от кибератаките, е важно да се моделират архитектурите за обмен на данни в микромрежите.

3.1. Видове архитектури на структурата за обмен на данни

Мрежовата топология на възли или агенти в децентрализираните архитектури е от решаващо значение по отношение на разработването на ефективна и подходяща микромрежа. Според тяхната логическа топология и степен на децентрализация, разпределените мрежи могат да бъдат широко класифицирани в следните архитектури, както е показано на Фиг. 3.1 [1].



Фиг. 3.1 . Архитектури за обмен на данни в микромрежи: централизирана, децентрализирана/йерархична и разпределена

- **Централизирана топология:** В една централизирана мрежа единичен информационен хъб, известен като контролен хъб, свързва всички единици за достав-ка на енергия и товари, улеснявайки обмена на информация с други свързани агенти или товари. Централният контролен хъб е отговорен за комуникацията между свързани единици като из-точници на зелена енергия, кон-

венционални инсталации, единици за съхранение на енергия, устройства за свързване към мрежата и прикачени товари. Възлите изпращат съобщения до централния сървър, за да определят адресите на възлите, които съдържат необходимите ресурси/данни. Въпреки това, подобно на децентрализирана система, след като даден възел разполага с информацията, той може директно да комуникира с търсения възел без помощта на централния сървър. В тази структура агентите имат повишена интелигентност (в сравнение с типичните възли на комуникационната мрежа) и подобрени комуникационни възможности. Освен това някои контролни задачи се разпределят чрез агенти, въпреки че те все още нямат възможности за вземане на решения. Централизираните архитектури се нуждаят от канали за обмен на данни с повишени разходи и скорости на данни, което ги прави по-уязвими за кибератаки, насочени към тези мрежи.

- **Децентрализирана/йерархична топология:** В децентрализираната система повече от един контролен хъб отговаря за обмена на данни между свързаните елементи или между мултиконтролните хъбове. Тази топология се характеризира с наличието на някои агенти (супер възли), които поемат власт над действията на други агенти. В тази микромрежа съществуват различни агенти, които изпълняват различни йерархични задачи. Повечето микромрежи в литературата използват тристепенна йерархична архитектура, където обикновено агентите от най-високо ниво са отговорни за критичните решения, агентите от средно ниво вземат решения за свързани или изключени задачи на мрежата, а агентите от пониско ниво взаимодействат със сензори и устройства. Изборът и разпределението на тези супер възли е динамичен. Този подход все още е ненадежден, тъй като не всички партньори могат да действат като супер възли поради липса на ресурси.

- **Разпределена топология:** Всяко устройство в разпределена топология се свързва локално и може да действа като контролен център, позволявайки предаването и приемането на данни.

При тази топология всеки локален агент е автономен, има същата роля в мрежата и е отговорен за придобиването на знания за собствената си част от мрежата. Съществена разлика по отношение на другите архитектури е, че на отделните агенти е позволено да откриват друга агентна информация чрез комуникация и координация с техните съседи. Тази топология не използва централен сървър за управление на мрежата, избягвайки единична точка на повреда и позволявайки много високо мащабируема мрежа.

В Таблица 3.1 са показани плюсовете и минусите на централизиран, децентрализиран и разпределен метод на управление [2].

Таблица 3.1. Сравнение на централизиран, децентрализиран и разпределен метод на управление

Тип контрол	Плюсове	Минуси
Централизирана	• Лесен за изпълнение • Лесен за поддръжка в случай на повреда в една точка	• Изчислителна тежест • Трудно се разширява • Единична точка на повреда (силно нестабилна) • Изисква се високо ниво на свързаност
Децентрализирана	• Само местна информация • Оборудван с контролна островна зона също без водачи • Паралелно изчисление	• Липса на комуникационни връзки между агентите • Умерена мащабируемост
Разпределена	• Лесен за разширяване (висока мащабируемост) • Ниска изчислителна цена (паралелно изчисление)	• Нуждае се от синхронизация • Постигането на консенсус отнема време на местните агенти

Тип контрол	Плюсове	Минуси
		• Скорости на конвергенция, повлияни от топологията на комуникационната мрежа • Необходимост от двупосочна комуникационна инфраструктура • Разходи за надграждане на съществуващия контрол и комуникация

Изборът на подходяща мрежова топология има важно влияние върху информационния поток, върху производителността и способността на микромрежата да бъде разширявана и актуализирана. Напълно децентрализираните топологии имат няколко предимства сред останалите.

Разпределените централизиран топологии са приемливи в микромрежи, където предварително дефиниран оператор управлява микромрежата, а производствената и потребителската страна на електроенергийната система имат подобни цели. Централният сървър получава информация за състоянието от всички звена и може да изчисли оптимална глобална стратегия за управление, осигурявайки практическо изпълнение на инфраструктурата за управление и намалявайки разходите за внедряване.

Децентрализираното управление е най-подходящият метод, когато има множество енергийни устройства от страна на производството и потреблението, които трябва да бъдат управлявани, изискващи наблюдение и настройка в реално време. В този случай централизиран контрол не може да отговори на изискванията. Въпреки че разходите за инсталиране на топологиите за децентрализирано управление са по-високи от тези на централизирано управление, оперативните разходи са значително намалени и могат да

бъдат амортизирани за кратко време [3]. В допълнение, в децентрализираните мрежи е възможно да се инсталират модулни и мащабируеми системи с добра точност.

Микромрежите по същество са децентрализирани и разпределени. Следователно децентрализираните методи за контрол ще бъдат ефективни. Всяка зона на микромрежата има своя локална система за управление и така скоростта на реакция на системата ще бъде много висока. Освен това при децентрализираното управление на микромрежата данните се обменят между различни области и следователно ще се получи максимална ефективност от енергийната система.

В Таблица 3.2 е представено сравнение на някои основни характеристики на микромрежите, използващи централизирани и децентрализирани контролни структури [4].

Таблица 3.2. Сравнение на важни характеристики на централизирани и децентрализирани контролни структури

Характеристика	Централизирана	Децентрализирана
Висока надеждност	×	✓
Централен контролер	✓	×
Ниска цена	×	✓
Висока гъвкавост	×	✓
Висока координация	✓	×
Лесно изпълнение	✓	✓

3.2. Математическата основа на структурите за обмен на данни

Математическата основа на многоагентните системи може да се използва, за да се изразят връзките между върхове и ръбове в структура за обмен на данни в микромрежата [5, 6].

Нека разгледаме микромрежа, работеща в островен режим, която се състои от контролирани хардуерни единици, оборудвани с разпределени енергийни ресурси. В рамките на разпределените енергийни ресурси единиците за доставка на енергия се разглеждат като агенти [7]. Следователно съществува множество от N единици или агенти, които се управляват от взаимодействията на динамичната система от по-висок ред. Множеството V се състои от всички агенти или възли в мрежата, означени чрез $\{1, 2, \dots, N\}$. Графът $G = (V, E)$ също изразява и метода, чрез който агентите комуникират. Елементът E принадлежи към декартовото произведение V , което обхваща всички връзки между агентите.

Всеки субект или единица i притежава данни във формат на параметър Y_i , който претърпява промени и актуализации чрез взаимодействия със съседни агенти. Целият набор от агенти, които са съседни на агента i , се означава чрез N_i , при което N_i е равно на подмножеството на $v(I, j)$, съставено от всички j . Освен това, векторът $Y(t)$ включва данни, отнасящи се до всички агенти в текущия момент t . Казано по друг начин, този вектор е съставен от колона и N редове, където всеки ред представлява агентите, изразено по следния начин [8]:

$$Y^T(T) = [Y_1(t), Y_2(t), \dots, Y_n(t)]$$

Поради това данните относно всеки агент могат да бъдат изведени чрез следния израз:

$$Y_i(t) = \sum_{j \in N_i} (Y_j(t) - Y_i(t)), Y_i(0) \in R$$

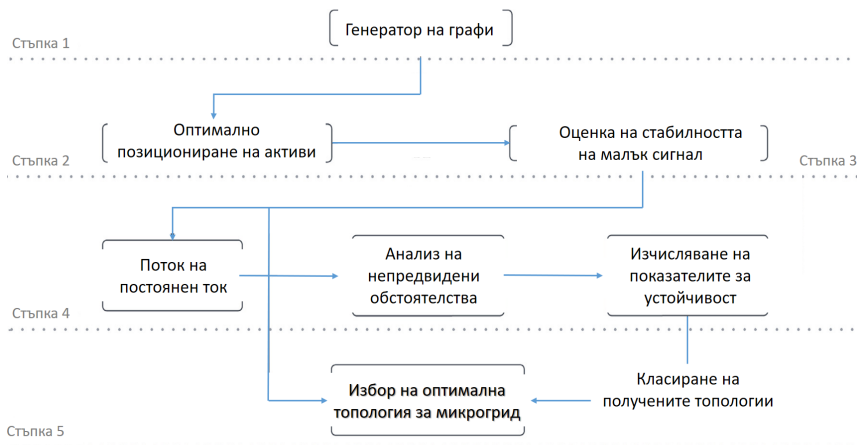
Освен това, съвкупността от вариации между този конкретен агент, както и неговите съседи, определя интервала на актуализиране, който съответства на агента i .

Също така е важно да се отбележи, че гореспоменатото взаимодействие се развива в сценарий, при който на връзките на взаимодействие между агентите не се дава никаква тежест. Всеки път, когато топологията на връзките на взаимодействие се претегля, връзката между тях ще се модифицира по следния начин [9]:

$$Y_i(t) = \sum_{j \in N_i} a_{ij} (Y_j(t) - Y_i(t)), Y_i(0) \in R$$

където чрез променливата a_{ij} е означено теглото, свързано с пътя на взаимодействие между агентите i и j .

За да се реши проблема с планирането на топологията на микромрежата [10] и недостатъците на съществуващи решения, в [11] е предложена нова рамка за проектиране на топология на микромрежа за устойчиви приложения. Тази рамка се основава на предложена методология за проектиране на топология за изолирани микромрежи, която схематично е онагледена на Фиг. 3.2.



Фиг. 3.2. Планиране на оптимална топология на микромрежа

Предложеният холистичен оптимален топологичен дизайн се състои от генератор на графи за извличане на всички възможни свързани, неизоморфни мрежи за даден брой възли; оптимално позициониране на активи върху всяка генерирана графика с помощта на линейно програмиране със смесено цяло число; оценка на стабилността на малък сигнал и поток след прекъсване на матрично изчисление за всяка микромрежа за количествено определяне на последствията от повреда на всички свързващи линии; количествено определяне на показателите за устойчивост, първоначално приложени към разпределителните системи за оценка на уязвимостта и критичността на всяка линия, заедно с класическите теоретични индикатори на графиката и накрая, агрегиране на споменатите показатели за класиране на произведените микромрежови топологии.

Предложената методология получава като вход желания брой възли заедно с агрегираните инсталирани мощности за необходимите активи (слънчеви масиви, съхранение на енергия, критични и регулярни натоварвания). Тя може да произведе оптимална мрежова топология както по отношение на избора на взаимно свързващи линии, така и по отношение на оптималното разположение на активите в шините на микромрежата, като същевременно оценява стабилността и производителността на микромрежата при най-лошите условия на прекъсване на линията.

Библиография

1. Marzal, S., Salas, R., González-Medina, R., Garcerá, G., Figueres, E.: Current challenges and future trends in the field of communication architectures for microgrids. *Renewable and Sustainable Energy Reviews*, 82, Part 3, 3610-3622, 2018, <https://doi.org/10.1016/j.rser.2017.10.101>.
2. Fadda, G., Fadda, M., Ghiani, E., Pilloni, V.: Chapter 9 - Communications and internet of things for microgrids, smart buildings, and homes. Editor(s): R. K. Chauhan, K. Chauhan, *Distributed Energy Resources in*

- Microgrids, Academic Press, 243-273, 2019, <https://doi.org/10.1016/B978-0-12-817774-7.00009-0>.
3. Bayindir, R., Hossain, E., Kabalci, E., Perez, R.: A Comprehensive study on microgrid technology. International Journal Of Renewable Energy Research, 4(4), 2014, 1094-1107, <https://dergipark.org.tr/en/pub/ijrer/issue/16073/168050>.
 4. Shirkhani, M., Tavoosi, J., Danyali, S., Sarvenoe, A.K., Abdali, A., Mohammadzadeh, A., Zhang, C.: A review on microgrid decentralized energy/voltage control structures and methods. Energy Reports, 10, 368-380, 2023, <https://doi.org/10.1016/j.egyr.2023.06.022>.
 5. Ahmed, I., Rehan, M., Iqbal, N., Ahn, C. K.: A novel event-triggered consensus approach for generic linear multi-agents under heterogeneous sector-restricted input nonlinearities. IEEE Transactions on Network Science and Engineering, 10(3), 1648-1658, 2023, <https://doi.org/10.1109/TNSE.2022.3232779>.
 6. Ali, P.R., Rehan, M., Ahmed, W., Basit, A.I., Ahmed, I.: A novel output feedback consensus control approach for generic linear multi-agent systems under input saturation over a directed graph topology. ISA Transactions, 148, 128-139, 2024, <https://doi.org/10.1016/j.isatra.2024.02.029>.
 7. Ahmed, I., El-Rifaie, A.M., Akhtar, F., Ahmad, H., Alaas, Z., Ahmed, M.M.R.: Cybersecurity in microgrids: A review on advanced techniques and practical implementation of resilient energy systems. Energy Strategy Reviews, 58, 101654, 2025, <https://doi.org/10.1016/j.esr.2025.101654>.
 8. Basit, A., Tufail, M., Hong, K.-S., Rehan, M., Ahmed, I.: Event-triggered distributed exponential H_∞ observers design for discrete-time nonlinear systems over wireless sensor networks. In: 13th Asian Control Conference (ASCC), Jeju, Korea, Republic of, 2022, pp. 1730-1735, <https://doi.org/10.23919/ASCC56756.2022.9828291>.
 9. Ahmed, I., Rehan, M., Hong, K. -S., Basit, A.: Event-triggered leaderless robust consensus control of nonlinear multi-agents under disturbances. In: 13th Asian Control Conference (ASCC), Jeju, Korea, Republic of, 2022, pp. 1736-1741, <https://doi.org/10.23919/ASCC56756.2022.9828087>.

10. Che, L., Zhang, X., Shahidehpour, M., Alabdulwahab, A., Al-Turki, Y.: Optimal planning of loop-based microgrid topology. IEEE Transactions on Smart Grid, 8(4), 1771-1781, 2017, <https://doi.org/10.1109/TSG.2015.2508058>.
11. Bintoudi, A.D., Demoulias, C.: Optimal isolated microgrid topology design for resilient applications. Applied Energy, 338, 120909, 2023, <https://doi.org/10.1016/j.apenergy.2023.120909>.

4. Комуникации в инфраструктурата на микромрежите

Увеличаващото се навлизане на източниците за производство на възобновяема енергия, базирани на електроника, намаляването на общата ротационна инерция и двупосочният поток на енергия промениха концепцията за стабилност на интелигентната микромрежа и оперативните изисквания. Стабилността на интелигентните микромрежи с ниска инерция и бързи динамични възобновяеми източници е силно зависима от надеждната и осъществима оперативна съвместимост между техните компоненти.

4.1. Видове комуникации в инфраструктурата на интелигент-на микромрежа

Комуникационната инфраструктура е отговорна за осигуряването на оперативната съвместимост в рамките на определения времеви хоризонт, като се има предвид поверителността, целостта, наличността и автентичността на обменяната информация. Това прави интелигентните микромрежи уязвими за кибератаки. Нападателите се опитват да нарушат операциите на микромрежата, като манипулират предаваните данни или атакуват физическата система.

За да се подобрят защитните техники срещу кибератаки в микромрежата от съществено значение е познаването на комуникацията в инфраструктурата. Центърът за управление на микромрежата е отговорен за координирането между разпределени източници на генериране, ангажимент на блока, защита, оценка на сигурността, контролиране на генерираната активна и реактивна мощност (V/F и PQ контролер), икономическо планиране, участие на пазара, реакция на търсенето, свързване/разединяване, синхронизъм и координация с основната мрежа [1, 2]. Това изисква бърза коригираща реакция поради по-ниската инерция на възобновяема интелигентна микромрежа, особено в островен режим [3].

В Таблица 4.1 са показани някои необходими времеви хоризонти в интелигентните микромрежи [4].

Таблица 4.1. Времеви хоризонти в интелигентните микромрежи

Разменени съобщения	Време
Отговор на търсенето	500 ms до минути
Разпределени източници на генериране и складови системи	20 ms до 15s
Разпределени измервания	1 μ s
Информация за защита	4 ms
Информация за наблюдение	1s
Контролна информация	16 ms до 100 ms
Информация за експлоатация и поддръжка	~ 1s
Непрекъснати потоци от данни от интелигентни електронни устройства	3 ms или 10 ms

Понякога защитните релета неправилно изключват възобновяема интелигентна микромрежа от главната мрежа в определени ситуации, като например, когато напрежението намалява. За да се предотвратят подобни грешки, е необходима бърза и надеждна двупосочна комуникационна инфраструктура за предаване на информация между основната мрежа, контролния център на микромрежата и защитните устройства в точката на общо свързване [5]. Освен това топологията на системата непрекъснато се променя в активните микромрежи поради двупосочен поток на мощност [6, 7]. Тъй като защитните релета изискват информация от топологията на системата, за да зададат времето си, е необходима онлайн настройка за активна микромрежа, за да се повиши надеждността и защитата на системата. За онлайн настройка е необходима и бърза и надеждна комуникация. Следователно комуникационната

инфраструктура играе жизненоважна роля в управлението на възобновяема интелигентна микромрежа.

Комуникационната система е разделена на три вида: (1) *кабелна линия*, (2) *безжична технология* и (3) *комбинирана*. В Таблица 4.2 са представени кратки дефиниции на комуникационни технологии базирана на [8, 9, 10].

В допълнение към наличността, времевият хоризонт (скорост на предаване и латентност) и честотната лента са двата най-съществени фактора при избора на комуникационни технологии за микромрежови операции. Високата честотна лента обикновено не е необходима. Например (14 – 100) kbps са достатъчни за обменени съобщения в отговор на търсенето, а (10 – 60) kbps са достатъчни за разпределените източници на генериране и системи за съхранение. Недостатъчната честотна лента може да доведе до загуба на пакети и изкривяване, намалявайки стойността на забавената информация. Обратно, по-високата честотна лента може да подобри качеството на услугата и устойчивостта на комуникация срещу кибератаки, насочени към честотната лента.

Комуникационната инфраструктура във възобновяема интелигентна микромрежа трябва да надхвърля изискванията за време и честотна лента, като се има предвид нарастващото навлизане на възобновяеми източници на енергия, характеристики на виртуална инерция, по-ниска ротационна инерция и бърза динамика.

Таблица 4.2. Кратка дефиниция на комуникация микромрежи

Тип про- водник	Видове комуникация	Предимства	Недостатъци
Кабелна основа	Оптично vlakно	- Способност за защита от електро-магнитни смущения - Висока скорост на предаване 100 Mbps – 2,5 Gbps за до 60 км - Голям капацитет на предаване - Висока честотна лента и добра поверителност	- Високи строителни разходи - Високи разходи за поддръжка - Подземните оптични влакна са обект на счупване в случай на прекъсване
	Телефонна мрежа	- Ниска цена на окабеляване - Няма нужда от специална комуникационна мрежа	Ниска скорост на предаване (до 24 Mbps)
	Комуникация по захранваща линия	- Лесно - Ниска строителна трудност - Ниски строителни разходи - Ниски експлоатационни разходи - Добра сигурност - Лесно управление	- Ниска скорост на предаване и ниска честотна лента 100–500 Kbps в NB PLC, за (0–150 km) 10–200 Mbps в BB PLC, за (0–1,5 km) - Уязвими на смущения - Намаляване на скоростта на предаване чрез увеличаване на разстоянието, затихване

Тип проводник	Видове комуникация	Предимства		Недостатъци
	Ethernet	• Добра скорост на предаване (до 100 Mbps)		• Ограничена зона на покритие, висока цена и сблъсък
Безжичен	Мобилна мрежа	GPRS	• Покриват широк диапазон • Адаптиране към трудните географски условия • Лесен монтаж • Високи скорости на предаване за нови технологии	• Несигурно забавяне и ниска скорост на предаване (в сравнение с типа проводник) • Проблем при тежки климатични условия • Ниска надеждност • Подходящото приложение на GPRS е система с ниски изисквания за реално време
		EDGE		
		CDMA		
		3G/4G/5G		
	Радиочестота	• Покриват широк диапазон и се адаптират към трудните географски условия • Лесна инсталация и висока скорост на предаване (до 600 Mbps)		• Интерференция с електромагнитни вълни • Проблем при тежки климатични условия

Тип проводник	Видове комуникация	Предимства	Недостатъци
	WiMAX	• Покриват широк диапазон • Голямо разстояние за предаване на данни (до 50 км) • Адаптиране към трудните географски условия • Лесен монтаж • Високи скорости на предаване (до 70 Mbps) • В реално време • Ниска цена • Лесна поддръжка	• Въпреки че ресурсите на спектъра, стандартите и сигурността на WiMAX трябва да бъдат подобрени • Липса на проникване през препятствия (проблем в градските райони) и проблем при тежки метеорологични условия • Загуба на пакети за мрежи на дълги разстояния в градска и селска среда • Скъпа кула • Увеличаване на забавянето във времето с увеличаване на честотата на дискретизация и количеството информация
	Zigbee	• Лесен и лесен за използване • Ниска консумация на енергия • Надежден • Ниска цена • Кратко забавяне	• Ниска скорост на предаване (20–250 kbps) • Късо разстояние за предаване на данни (50m) • Ниска памет • Базиран на батерия • Проблем при тежки климатични условия

Въпреки напредъка на безжичните технологии през последните години технически предизвикателства като изключително шумна среда, проблеми с интерфейса, несигурни закъснения във времето, латентност на пакетите, липса на качество на услугата и податливост на кибератаки ограничиха широкото приемане във възобновяеми интелигентни микромрежи [11].

В комуникационната технология на микромрежите, оптичното влакно предлага превъзходни спецификации, позволявайки предаване на сигнали на дълги разстояния, без да е необходимо усилване на сигнала. Въпреки това, подобно на безжичната технология, оптичните влакна са уязвими за кибератаки, тъй като предаваните данни могат да бъдат прихванати чрез обикновен хардуер, без да се прекъсва връзката. Освен това нападателите могат да използват допълнителен хардуер за стартиране на злонамерени атаки [12]. След оценка на предимствата и ограниченията на комуникационните технологии, изброени в предходната таблица, оптичното влакно се очертава като най-подходящия вариант.

Струва си да се спомене, че оптичната технология може да се използва в софтуерно дефинирана мрежа (SDN – Software-Defined Network) като кабелна комуникационна среда [13]. Това се дължи на факта, че оптичната технология осигурява както висока скорост на предаване на данни, така и надеждна комуникация, и намира приложение при свързването на концентратори, като осигурява и комуникацията между концентратори и контролни центрове [14].

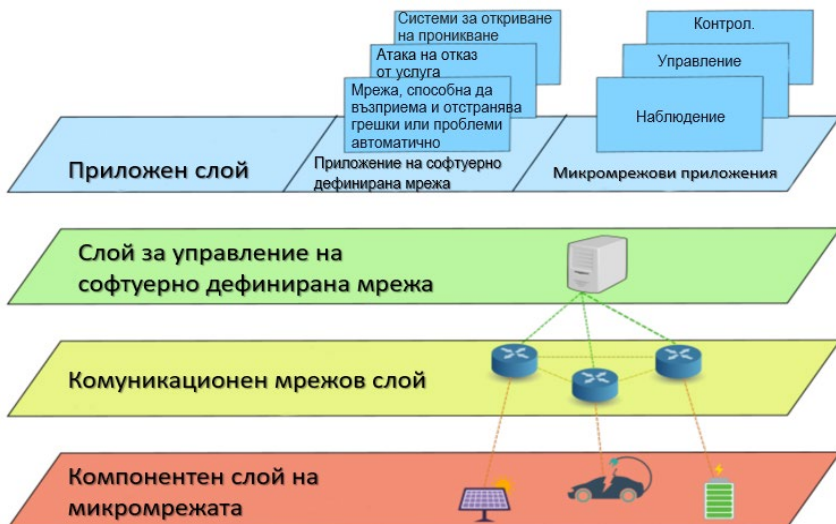
Като се има предвид критичната роля при предаването на важна информация, безжичната комуникация може да служи като резервно копие въпреки увеличените разходи, които са оправдани за осигуряване на надеждна, непрекъсната и сигурна работа на възобновяема интелигентна микромрежа. Не трябва да се пренебрегват някои от предимствата на технологиите за безжична комуникация, превъзхождащи решенията, базирани на кабел, като мобилност, удобство, лесна инсталация и ниска цена.

Комуникационната инфраструктура служи като гръбнак на възобновяемата интелигентна микромрежа, улеснявайки предаването на данни и координацията между различни компоненти на микромрежата. Тази инфраструктура е от решаващо значение за оперативната съвместимост, откриването на грешки и синхронизирането на мрежата, като по този начин подобрява цялостната производителност и надеждност. Отчитайки зависимостта на възобновяемата интелигентна микромрежа от цифрова комуникация за обмен на данни и контролни команди, гарантирането на сигурността и целостта на тези мрежи е от първостепенно значение. Внедряването на усъвършенствани протоколи за криптиране, системи за откриване на проникване и механизми за контрол на достъпа в рамките на комуникационната инфраструктура повишава киберустойчивостта, намалявайки риска от кибератаки и осигурявайки непрекъсната работа [15, 16].

4.2. Софтуерно дефинирана мрежа

Технологията за софтуерно дефинираната мрежа е подход за управление на мрежата, който позволява динамична, ресурсно ефективна и програмируема мрежова конфигурация с цел подобряване на мрежовата производителност и наблюдение [17]. Софтуерно дефинираната мрежа централизира мрежовата интелигентност в един мрежов компонент чрез отделяне на процеса на препращане на мрежови пакети от процеса на маршрутизиране и контролни действия. Софтуерно дефинираната мрежа е полезно решение за подобряване на производителността, безопасността и сигурността на различни типове мрежи, включително интелигентни системи за контрол на мрежата [18].

Прилагането на парадигмата на софтуерно дефинираната мрежа в микромрежи може да обхваща както приложения за сигурност, така и приложения за контрол, както е показано на Фиг. 4.1 [19].



Фиг. 4.1. Архитектура на микрогрид със софтуерно дефинирана мрежа

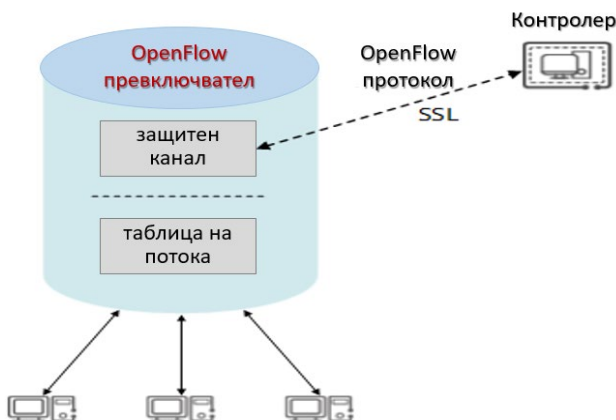
Софтуерно дефинираната мрежа също има интересни приложения за сигурността на индустриалните системи за контрол, особено за реакция при инциденти. Позволява повишаване на устойчивостта на системата за управление, благодарение на възможността за динамично преконфигуриране на мрежата след откриване на повреда или компрометирано устройство, което ѝ позволява да работи дори при влошени условия. Това е особено полезно за контролни мрежи в критични инфраструктури, които изискват изключително висока наличност. В [20] се обсъжда как софтуерно дефинираната мрежа и технологиите за виртуализация на мрежови функции могат да помогнат за проектирането на автоматични механизми за реакция при инциденти в индустриална система за контрол и също така се описва прототип, за да покаже осъществимостта в сценарий, който използва програмируеми логически контролери, управляващи класическа система за контрол на пълнене на резервоар.

В [21] е проучена приложимостта на нововъзникващите технологии в областта на IP мрежите, включително софтуерно дефинирана мрежа, виртуализация на мрежови функции и защитни стени от следващо поколение за защита на индустриална система за контрол. Предложен е алгоритъм за откриване и локализиране на атаки и проектиране на стратегия за намеса в полето за управление на мрежови работи [22]. Софтуерно дефиниран подход за сигурност към защитени полеве зони в индустриалните системи за контрол е показан в [23]. Той се състои от хибриден модул за откриване на аномалии, който инспектира поведението на аномалии в мрежовите комуникации и физическите състояния на процеса. Той предлага многостепенен модул за отговор на сигурността, който позволява изолиране на всяка компрометирана зона.

Софтуерно дефинираната мрежа позволява проверка на цялата комуникационна мрежа по отношение на политики за сигурност и мрежови ситуации. Тази мрежа позволява също така директно внедряване на система за откриване на проникване в мрежа в рамките на контролера на софтуерно дефинираната мрежа, дори ако такова внедряване може да въведе време на латентност, което може да бъде несъвместимо с позволеното забавяне в среда на микромрежа [24].

В допълнение към описаното до тук за софтуерно дефинираната мрежа, трябва да се спомене и най-популярният стандарт/протокол за обмен на съобщения между нивата на управление и данни в нея, а именно OpenFlow [25]. OpenFlow е с отворен код и се поддържа от много доставчици. Може да се използва в изцяло виртуализирана мрежова среда за управление на виртуални комутатори в облачни изчисления. Естеството на OpenFlow на софтуерно дефинираната мрежа позволява бърз отговор на промени и повреди. Освен това е много гъвкав и може да управлява много сложни правила.

Архитектурата OpenFlow се състои от контролер, превключвател OpenFlow и защитен канал, както е показано на Фиг. 4.2.



Фиг. 4.2. Архитектура на OpenFlow

Контролерът контролира мрежата по централизиран начин, за да реализира функциите на контролния слой. Превключвателят OpenFlow отговаря за препращането в слоя данни; той обменя съобщения с контролера чрез защитен канал, за да получава препращащи записи и да докладва статуса си.

Контролерът OpenFlow е мозъкът на архитектурата на софтуерно дефинирана мрежа и се намира на контролния слой, за да инструкира препращането на данни през протокола OpenFlow. За целта се установява защитен канал между контролера и превключвателя OpenFlow. Чрез този канал контролерът контролира и управлява превключвателя и получава обратна връзка от превключвателя. Съобщенията, обменяни по защитения канал на OpenFlow, трябва да отговарят на формата, определена от протокола Open Flow.

Защитеният канал на OpenFlow обикновено е шифрован с помощта на защита на транспортния слой, но може да се изпълнява директно през TCP в обикновен текст в OpenFlow 1.1 и по-нови версии. Превключвателят OpenFlow е отговорен главно за препращането в слоя данни. Може да бъде физически или виртуализиран комутатор/рутер. Превключвателя OpenFlow препраща пакети,

влизаци в превключвателя, въз основа на таблицата на потока, която съдържа набор от записи на правила, инструктиращи превключвателя как да обработва трафика [26]. Записите в потока се генерират, поддържат и доставят от контролер.

Библиография

1. Chen, X., Zhou, J., Shi, M., Chen, Y., Wen, J.: Distributed resilient control against denial of service attacks in DC microgrids with constant power load. *Renewable and Sustainable Energy Reviews*, 153, 111792, 2022, <https://doi.org/10.1016/j.rser.2021.111792>.
2. Sangoleye, F., Johnson, J., Chavez, A., Tsiropoulou, E.E., Marton, N.L., Hentz, C.R., Yannarelli, A.: Networked microgrid cybersecurity architecture design guide: A New Jersey TRANSITGRID Use Case. 2022, <https://doi.org/10.2172/1900087>.
3. Farrokhadi, M. et al.: Microgrid stability definitions, analysis, and examples. *IEEE Transactions on Power Systems*, 35(1), 13-29, 2020, <https://doi.org/10.1109/TPWRS.2019.2925703>.
4. Marzal, S., Salas, R., Gonzalez-Medina, R., Garcera, G., Figueres, E.: Current challenges and future trends in the field of communication architectures for microgrids. *Renewable and Sustainable Energy Reviews*, 82, Part 3, 3610-3622, 2018, <https://doi.org/10.1016/j.rser.2017.10.101>.
5. Gadanayak, D.A.: Protection algorithms of microgrids with inverter interfaced distributed generation units – A review. *Electric Power Systems Research*, 192, 106986, 2021, <https://doi.org/10.1016/j.epsr.2020.106986>.
6. Sarangi, S., Sahu, B.K., Rout, P.K.: Review of distributed generator integrated AC microgrid protection: issues, strategies, and future trends. *International Journal of Energy Research*, 45(10), 14117-13144, 2021, <https://doi.org/10.1002/er.6689>.
7. Habibzadeh, H., Nussbaum, B.H., Anjomshoa, F., Kantarci, B., Soyata, T.: A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, 50, 101660, 2019, <https://doi.org/10.1016/j.scs.2019.101660>.

8. Ghosh, S., Chanda, C.K., Das, J.K.: A comprehensive survey on communication technologies for a grid connected microgrid system. In International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 2021, pp. 1525-1528, <https://doi.org/10.1109/ICAIS50930.2021.9395820>.
9. Miller, D., Mirzaeva, G., Townsend, C.D., Goodwin, G.C.: The use of power line communication in standalone microgrids. IEEE Transactions on Industry Applications, 57(3), 3029-3037, 2021, <https://doi.org/10.1109/TIA.2021.3057343>.
10. Yang, H., Li, Q., Chen, W.: 9 - Microgrid communication system and its application. In hierarchical control, Editor(s): Qiang Yang, Ting Yang, Wei Li, Smart Power Distribution Systems, Academic Press, 179-204, 2019, <https://doi.org/10.1016/B978-0-12-812154-2.00009-2>.
11. Volkova, A., Niedermeier, M., Basmadjian, R., de Meer, H.: Security challenges in control network protocols: A survey. IEEE Communications Surveys & Tutorials, 21(1), 619-639, 2019, <https://doi.org/10.1109/COMST.2018.2872114>.
12. Yan, J., Liu, C. -C., Govindarasu, M.: Cyber intrusion of wind farm SCADA system and its impact analysis. In IEEE/PES Power Systems Conference and Exposition, Phoenix, AZ, USA, 2011, pp. 1-6, <https://doi.org/10.1109/PSCE.2011.5772593>.
13. Kuzlu, M., Pipattanasomporn, M., Rahman, S.: Communication network requirements for major smart grid applications in HAN, NAN and WAN. Computer Networks, 67, 74-88, 2014, <https://doi.org/10.1016/j.comnet.2014.03.029>.
14. Fadda, G., Fadda, M., Ghiani, E., Pilloni, V.: Chapter 9 - Communications and internet of things for microgrids, smart buildings, and homes. Editor(s): R. K. Chauhan, K. Chauhan, Distributed Energy Resources in Microgrids, Academic Press, 243-273, 2019, <https://doi.org/10.1016/B978-0-12-817774-7.00009-0>.
15. Blagoev, I.: Method for evaluating the vulnerability of random number generators for cryptographic protection in information systems. Studies in Computational Intelligence, 902, 391-397, 2021, https://doi.org/10.1007/978-3-030-55347-0_33
16. Blagoev, I.: Application of time series techniques for random number generator analysis. In: Proc. of XXII Int. Conference DCCN, 23-27 September, 2019, pp. 437-446.

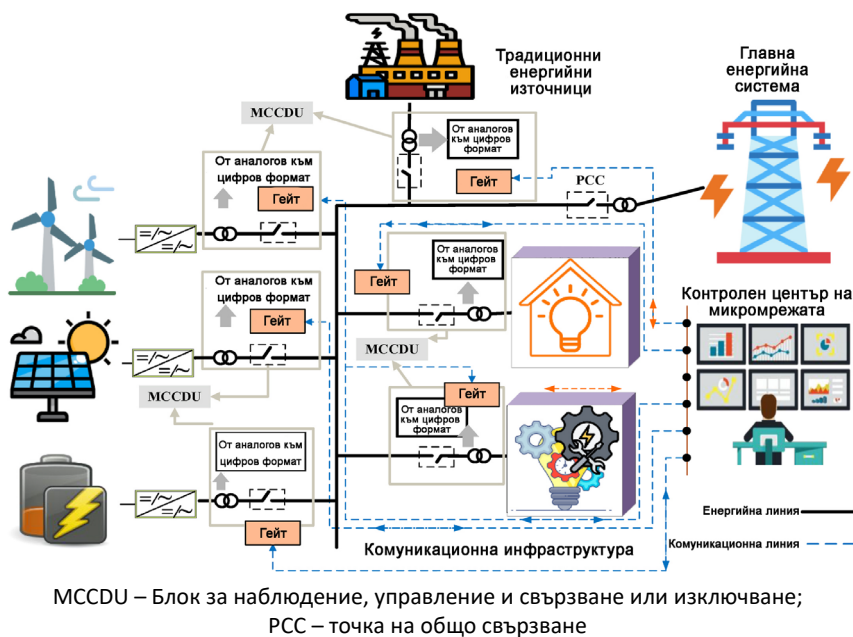
17. Gaggero, G.B.: Microgrids cybersecurity. Encyclopedia. Available online: <https://encyclopedia.pub/entry/16850>. (accessed on 17 April 2025)
18. Fatkueva, R., Evnevich, E., Yoshinov, R.: State-of-the art and trends in network security control. Problems of Engineering Cybernetics and Robotics, 72, 41-44, 2020, <https://doi.org/10.7546/PECR.72.20.05>.
19. Gaggero, G.B.; Girdinio, P.; Marchese, M. Advancements and research trends in microgrids cybersecurity. Applied Sciences, 11(16), 7363, 2021, <https://doi.org/10.3390/app11167363>.
20. Piedrahita, A.F.M.; Gaur, V.; Giraldo, J.; Cardenas, A.A.; Rueda, S.J. Leveraging software-defined networking for incident response in industrial control systems. IEEE Software, 35(1), 44-50, 2018, <https://doi.org/10.1109/MS.2017.4541054>.
21. Genge, B.; Graur, F.; Haller, P. Experimental assessment of network design approaches for protecting industrial control systems. International Journal of Critical Infrastructure Protection, 11, 24-38, 2015, <https://doi.org/10.1016/j.ijcip.2015.07.005>.
22. Sándor, H.; Genge, B.; Szántó, Z.; Márton, L.; Haller, P. Cyber attack detection and mitigation: Software defined survivable industrial control systems. International Journal of Critical Infrastructure Protection, 25, 152–168, 2019, <https://doi.org/10.1016/j.ijcip.2019.04.002>.
23. Yang, J.; Zhou, C.; Tian, Y.C.; Yang, S.H. A software-defined security approach for securing field zones in industrial control systems. IEEE Access, 7, 87002-87016, 2019, <https://doi.org/10.1109/ACCESS.2019.2924800>.
24. Fausto, A., Marchese, M.: Implementation details to reduce the latency of an SDN statistical fingerprint-based IDS. In International Symposium on Advanced Electrical and Communication Technologies (ISAECT), Rome, Italy, 2019, pp. 1-6, <https://doi.org/10.1109/ISAECT47714.2019.9069714>.
25. Li, W., Meng, W., Kwok, L.F.: A survey on OpenFlow-based software defined networks: Security challenges and countermeasures. Journal of Network and Computer Applications, 68, 126-139, 2016, <https://doi.org/10.1016/j.jnca.2016.04.011>.
26. OpenFlow switch specification, <https://opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf>.

5. Протоколи и стандарти в инфраструктурата на интелигентна микромрежа

Този раздел представя систематичен преглед на стандартите, предизвикателствата и решенията за киберустойчивост на възобновяема интелигентна микромрежа, като се фокусира върху комуникационни технологии, стандарти и протоколи.

5.1. Концептуален модел на централизирана възобновяема интелигентна микромрежа

Един концептуален модел на централизирана възобновяема интелигентна микромрежа е показан на Фиг. 5.1 [1].



Фиг. 5.1. Концептуален модел на централизирана възобновяема интелигентна микромрежа

Всички измерени аналогови данни се преобразуват първо в цифров формат от обединяващо устройство (виж. Фиг. 5.1). Тези цифрови данни преминават по-нататъшна обработка, за да отговорят на специфични изисквания, след което модулът за наблюдение, управление и свързване или изключване предава данните и състоянието на разпределените източници на генериране и товарите към контролния център на микромрежата през шлюзове [2]. Центърът за управление на микромрежата получава информация от всички шлюзове и след анализ издава подходящи команди. Следователно, центърът за управление на микромрежата играе решаваща роля в управлението на координацията между контролируемите източници на разпределено генериране, механизми за защита и други оперативни аспекти. Той използва усъвършенствани системи за мониторинг и контрол, за да осигури оптимална работа и баланс между различни източници на генериране и потребление чрез мониторинг в реално време.

Чрез непрекъснато наблюдение на натоварването в реално време контролният център коригира генерираната мощност на управляемите блокове, като издава нови референтни точки. В проучванията на микромрежите неконтролируемите единици често се моделират като товари с отрицателно търсене, влияещи върху вариациите на потреблението в системата на микромрежата.

По отношение на защитата контролният център прилага цялостен набор от схеми за защита на инфраструктурата на микромрежата от електрически повреди и смущения. Това включва откриване на неизправности, изолиране, стратегии за възстановяване и координиране на защитни релета и прекъсвачи. Едновременно с това се провеждат редовни оценки на сигурността, за да се идентифицират и смекчат потенциалните уязвимости в системата за контрол на микромрежата. Този проактивен подход включва оценки на риска, тестове за проникване и сканиране на уязвимости за откриване на слабости в сигурността и прилагане на ефективни контрамерки.

По отношение на мерките за киберсигурност контролният център на микромрежата прилага набор от стратегии за защита срещу киберзаплахи и осигуряване на целостта, поверителността и наличността на критични оперативни данни. Това включва сегментиране на мрежата за изолиране на критични системи за контрол от външни мрежи, внедряване на защитни стени и системи за откриване/предотвратяване на проникване за наблюдение и блокиране на опити за неототоризиран достъп.

Криптирането на комуникационните канали предотвратява подслушването и манипулирането, докато строгите мерки за контрол на достъпа ограничават достъпа само до ототоризиран персонал. Провежда се непрекъснато наблюдение и одит на системните регистрационни файлове, за да се открие незабавно и да се отговори на всяка подозрителна дейност. Контролният център на микромрежата използва различни алгоритми за откриване на проникване и методи за оценка на състоянието на микромрежата, за да се защити срещу киберпрестъпници и да предвиди точно траекториите на системата.

5.2. Стандарти за комуникация в микромрежи

Като фундаментален стандарт за управление на сигурността на информацията ISO/IEC 27001 има широка област, включително тестване на сигурността на системата, съответствие с политиките за сигурност (периодични проверки) и технически преглед на съответствието – тестване на операционни системи, за да се установи, че внедряването на хардуерни и софтуерни контроли е коректно. Спомагателното и практическо ръководство за прилагането на ISO/IEC 27001 е предоставено в ISO/IEC 27002. ISO/IEC 27001 и 27002 могат да се прилагат към всички компоненти на интелигентна мрежа [3].

Стандартът NIST SP 800-82 се отнася до сигурността на промишлена система за управление, която е призната и използвана в световен мащаб. Стандартът потвърждава и удостоверява, че посочените контроли за сигурност са внедрени правилно и те работят и

дават желаните резултати. Този стандарт също така предоставя конкретни препоръки относно инструментите за тестване на уязвимост и проникване [4].

Сигурността остава сериозен проблем особено за протоколи, на които липсват стабилни функции за сигурност, което прави възобновяемите интелигентни микромрежи уязвими към киберзаплахи като хакерство и неоторизиран достъп.

С разширяването на микромрежите възникват проблеми с мащабируемостта, което потенциално възпрепятства оптимизирането и интегрирането на възобновяеми енергийни източници. Предизвикателствата по отношение на оперативната съвместимост произтичат от различните компоненти в рамките на възобновяема интелигентна микромрежа, което усложнява ефективната координация и контрол. Закъсненията могат да повлияят на операциите в реално време във възобновяема интелигентна микромрежи с висока интеграция на възобновяеми източници и бързи ذخаранващи електронни интерфейси.

IEEE 1547 определя технически изисквания и протоколи за безопасна, надеждна и ефективна работа на разпределени енергийни ресурси от жилищни, търговски и промишлени зони, включително слънчеви фотоволтаични системи, вятърни турбини и по-малки генератори, интегрирани в микромрежи [5]. Този стандарт задава насоки за поддържане на стабилността на мрежата чрез управление на нивата на напрежение и осигуряване на контрол на честотата по време на режими на работа. Освен това той определя мерки за безопасност за изключване и повторно включване на мрежата, за да се намалят опасностите, свързани с инсталациите на разпределените енергийни ресурси.

IEEE 1547 очертава и параметри за качество на електроенергията, като гарантира, че електроенергията, инжектирана в мрежата, отговаря на специфични стандарти за хармоници, колебания на напрежението и други аспекти на качеството. Въпреки това липсата на специална рамка за киберсигурност в рамките на IEEE 1547

поражда опасения за потенциално манипулиране на данни, неотризиран достъп или прекъсвания в операциите на разпределени енергийни ресурси, което може значително да повлияе на стабилността на микромрежата.

През 2023 г. бе въведен IEEE 1547.3, който се фокусира върху насоките за киберсигурност за разпределени енергийни ресурси, свързани с електроенергийни системи [6]. Този нов стандарт предоставя основни мерки за киберсигурност, които компаниите за разпределени енергийни ресурси трябва да прилагат, когато проектират интелигентни инвертори, за да подобрят устойчивостта на киберсигурността. От решаващо значение е защитните мерки за киберсигурност непрекъснато да се развиват паралелно. Въпреки че стандартизацията е жизненоважна за установяване на основни нива на сигурност, тя трябва да бъде допълнена от всеобхватна отбранителна стратегия, която включва проактивни мерки като разузнаване на заплахи, оценки на уязвимостта и планиране на реакция при инцидент [7].

IEC 61850 придоби популярност благодарение на лесната си интеграция със съществуващите инфраструктури на електроенергийната система и високата оперативна съвместимост, което го прави най-широко възприетият стандарт за ефективна и надеждна работа. Този стандарт установява стабилни комуникационни протоколи като GOOSE, MMS, Sampled Value и техните маршрутизирани версии заедно със стандартизирани модели на данни, които улесняват оперативната съвместимост между устройства от различни производители. Като поддържа комуникация в реално време за функции за мониторинг и контрол, IEC 61850 подобрява отзивчивостта и ефективността на интелигентните мрежи, позволявайки бързо адаптиране към промените в търсенето и предлагането на енергия.

IEC 61850 предоставя стандартизирани модели на данни, които описват функциите и възможностите на интелигентните елект-

ронни устройства, опростявайки конфигурацията, работата и поддръжката на интелигентни енергийни системи чрез установяване на общо разбиране на функционалностите на устройството. Поддържат се и усъвършенствани функции за автоматизация като откриване на неизправности, изолиране и възстановяване на услугата, което значително повишава оперативната ефективност и надеждността на енергийните системи.

Справянето с опасенията, свързани с киберсигурността, е друг критичен аспект на IEC 61850, включващ широки мерки за сигурност за защита на целостта, поверителността и автентичността на обменените данни в рамките на интелигентни енергийни системи. Механизми като криптиране и удостоверяване предотвратяват неоторизиран достъп и подправяне, като по този начин предпазват критичната инфраструктура от потенциални атаки. Съвместимостта му с други стандарти за киберсигурност като IEC 62351 гарантира цялостен подход към защитата на интелигентни енергийни системи. Първоначално разработен за автоматизация на подстанции, изследователите са проучили и препоръчали прилагането на IEC 61850 в комуникацията между различно оборудване в рамките на възобновяеми интелигентни микромрежи [8, 9, 10, 11]. IEC61850 включва общо десет части [12].

IEC 61850-7-420 дефинира стандартен микромрежов модел на данни, пригоден за разпределени енергийни ресурси, позволяващ безпроблемна интеграция и управление на възобновяеми източници като слънчева и вятърна енергия за подобряване на стабилността и ефективността на мрежата.

Стандартът IEC 62351 предоставя изчерпателна рамка за протоколи за сигурност в микромрежовата комуникация. Той специално се фокусира върху гарантирането, че изискванията за сигурност на оперативните протоколи и протоколите за споделяне на информация са изпълнени. Стандартът IEEE P2030.7 очертава спе-

цифичните критерии за микромрежови контролери с особен акцент върху контролните елементи на работата на микромрежата като автоматизация, стабилност и управление на енергията [13].

Стандартите IEC 61968/61970, известни като общ информационен модел (Common Information Model – CIM), установяват насоки за обмен на данни между електрически разпределителни системи и системи за управление на разпределени енергийни ресурси. Тези спецификации са от съществено значение за гладкото функциониране на микромрежовите операции [14].

5.3. Комуникационни протоколи в микромрежи

Надеждната работа на възобновяема интелигентна микромрежа зависи в голяма степен от точността на предаваните данни. Изследването на протоколите, използвани в двупосочна комуникация между компонентите на микромрежата, е от решаващо значение за разработването на стабилна възобновяема интелигентна микромрежова комуникационна инфраструктура. Тези протоколи трябва да гарантират поверителността, автентичността, целостта, наличността и неотричането на предадените данни [15]. Липсата на тези атрибути може да доведе до сериозни оперативни проблеми в микромрежите. Например липсата на поверителност и цялост може да изложи предадената информация на злонамерени дейности. По същия начин, без удостоверяване, разграничаването между правилни и неправилно получени команди става невъзможно [5].

В енергийната система се използват няколко комуникационни протокола, включително и в микромрежи, като Modbus, OPC/OPC UA, DNP3, IEC 61850/IEC 60870-6, IEC 60870-5-101, IEC 60870-5-104 и IEC 61850. Всеки протокол обслужва специфични функции в енергийната система, като събиране на данни, контрол, мониторинг и оперативна съвместимост между различни устройства и системи. Например DNP3 и IEC 60870-5-104 са пригодени за използване в SCADA системи, докато IEC 61850, най-новият стандарт, е

предназначен за комуникационни мрежи в подстанции [16]. Въпреки важноста им за работата и ефективността на възобновяема интелигентна микромрежа, тези комуникационни протоколи са изправени пред различни ограничения и уязвимости.

Modbus първоначално е разработен, за да улесни обмена на данни между програмируеми логически контролери [17]. Modbus се използва широко в микромрежи поради своята простота. Може да се предава през различните физически мрежи на RS 485, RS 232 и Ethernet TCP/IP. Въпреки това протоколът Modbus е неефективен за широкомащабно предаване на данни от/към мрежата. Той има висока латентност, което го прави неподходящ за комуникационна система, особено такава, включваща аварийно управление.

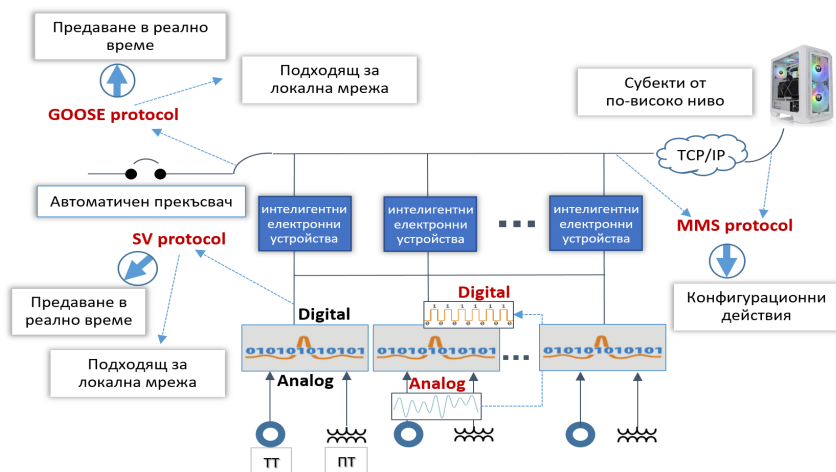
DNP3 (Distributed Network Protocol 3) е колекция от протоколи, използвани за комуникация в системите за автоматизация на процеси. Той придоби популярност в микромрежите поради способността си да осигурява сигурна и ефективна комуникация [18].

Интегрирането на интернет протокол версия 6 (IPv6) в киберсигурността на микромрежата е решаващо развитие, което гарантира сигурна и ефективна комуникация [19]. IPv6 осигурява значителни подобрения в сравнение с предшественика си, главно по отношение на възможностите за удостоверяване и криптиране, поради огромното си адресно пространство и разширени функции за сигурност. Сигурните комуникационни методи са от решаващо значение за поддържане на оперативната цялост и защита срещу кибератаки в разпределени микромрежи. Внедряването на IPv6 подобрява силата и мащабируемостта на мрежовите структури, позволявайки подобро управление на разпределени енергийни ресурси и по-устойчиви комуникационни мрежи. Чрез използване на функционалностите на IPv6 разпределените микромрежи могат да постигнат повишени нива на сигурност в своите контролни и комуникационни протоколи, което е наложително в прогресивно мрежовата среда на съвременните енергийни системи. IPv6 се изпъл-

зва в рамките на комуникационните протоколи и стандарти за разпределен микромрежови киберсигурен контрол, подчертавайки значението му за укрепване на микромрежите срещу киберуязвимости.

В Таблица 5.1 са представени типичните IEC61850 протоколи.

На Фиг. 5.2 е показано как протоколите SV и GOOSE директно предават данни в реално време през Ethernet [1]. Това ги прави подходящи за бърза комуникация в рамките на локални мрежи (LAN), но не са идеални за широкообхватни мрежи (WAN) [20].



ТТ – Токов трансформатор, Потенциален трансформатор (ПТ)

Фиг. 5.2. Схема на местоположението на протоколите в интелигентната енергийна система

Таблица 5.1. Общи IEC61850 протоколи

Протоколи	Специфика					
	Механизъм	ENC или DIC	AUT	Закъснение	Използване на част	61850/ 62351
GOOSE	• Мултикаст • Издател абонат • Въз основа на събития • Съобщение в реално време	Не	Не	~ ms	За изпращане на сигнал за изключване от IED към прекъсвачи	Раздел 8-1 / Раздел 6
SV	• Мултикаст • Издател/абонат • Съобщение в реално време	Не	Не	Детерминистичен 250 μ s (50 Hz) 208 μ s (60 Hz)	Изпращане на стойности на напрежение и ток от обединяващи модули към IED или защитни релета	Раздел 9-2 Леко издание / Раздел 6
MMS	• Клиент/сървър • TCP/IP протокол • Съобщение не в реално време • Може да поддържа повече механизми за сигурност	Не	Да	~ ms Зависи от мрежовата комуникация	Комуникация между обекти от по-високо ниво и IED	Раздел 8-1/ Раздели 3-4, 6

ENC = Криптиране, DIC = Цифров сертификат, AUTHN = Удостоверяване

Протоколът MMS (Multimedia Messaging Service), който работи по модела клиент/сървър, улеснява комуникацията в широкообхватни мрежи, използвайки IP адреси и картографиране на данни към TCP/IP. Тази възможност поддържа по-широки и по-гъвкави комуникационни изисквания, включително приложения в SCADA системи, и подобрява оперативната съвместимост в големи, разпределени интелигентни мрежови среди [21].

Използвайки предимствата на бързата комуникация на GOOSE и SV, е разработена маршрутизирана версия, която позволява предаване на данни през IP мрежи [22]. Това подобрение разширява тяхната полезност отвъд локалните мрежи, улеснявайки използването им в по-широки географски обхвати, като същевременно се запазват техните комуникационни предимства в реално време.

В Таблица 5.2 е представен изчерпателен преглед на комуникационните технологии, използвани в микромрежовите системи, заедно със съответните им стандарти и приложения [23].

Микромрежите използват HAN (Home Area Network), NAN (Neighborhood Area Network), IAN (Industrial Area Network) и BAN (Building/Business Area Network). Интелигентните измервателни уреди, генераторите, енергията и оборудването за битова автоматизация представляват HAN. IAN и BAN имат допълнителни инструменти за автоматизация. Приложенията варират от HAN до WAN (Wide Area Network).

HAN свързаността позволява създаването на по-малка широка мрежова свързаност. Тя осигурява контрол на нивото на достъп на домовете, позволявайки на потребителите да регулират потреблението на енергия. HAN се използва за управление на потреблението, топлинни операции, интелигентни измервателни уреди или наблюдение на системата за домашна сигурност. Тези взаимодействия са осъществими чрез оборудване в сгради или съседни

обекти, които осигуряват интернет скорости от 100 kbps на разстояние от 100 m и консумират по-малко вата мощност. HAN използва Wi-Fi, Bluetooth и ZigBee.

Таблица 5.2. Компилация от комуникационни модалности
в микромрежови системи

Модалност на комуникацията	Стандарти	Приложения
Теснолентов PLC [24]	IEEE P1901.2 [25], G3-PLC [26]	HAN/NAN/WAN
Широколентов PLC [27]	IEEE 1901 [28], домашен щепсел 1.0 [29, 30]	HAN/BAN/NAN
DSL [31]	ADSL [32]	NAN/Вентилатор
VDSL [32]	VDSL [32]	HAN-Вентилатор
HDSL [33]	HDSL [33]	NAN/Вентилатор
Ethernet [34]	IEC 61850 [35]	HAN/BAN/NAN, SAS [36]
Оптично влакно [37]	PON [37], SONET/SDH [37]	WAN
WLAN [38]	IEEE802.11 [38]	Локални мрежи [39]
WPAN [40]	IEEE 802.15 [40]	Bluetooth, ZigBee [41], Домашни мрежи
Клетъчен [42]	Поколения 2 до 5 [42]	V2G, WAN/LTE-A [43]

Библиография

1. Rouhani, S.H., Su, C.-L., Mobayen, S., Razmjoo, N., Elsis, M.: Cyber resilience in renewable microgrids: A review of standards, challenges, and solutions. Energy, 309, 133081, 2024, <https://doi.org/10.1016/j.energy.2024.133081>.
2. Chattopadhyay, A., Ukil, A., Jap, D., Bhasin, S.: Toward threat of implementation attacks on substation security: Case study on fault

- detection and isolation. IEEE Transactions on Industrial Informatics, 14(6), 2442-2451, 2018, <https://doi.org/10.1109/TII.2017.2770096>.
3. Leszczyna, R. (2018) Standards on Cyber Security Assessment of Smart Grid. International Journal of Critical Infrastructure Protection, 22, 70-89; ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements, (Edition 3, 2022), <https://www.iso.org/standard/27001>.
 4. Nejabatkhah, F., Li, Y.W., Liang, H., Ahrabi, R.R.: Cyber-security of smart microgrids: A survey. Energies, 14(1), 27, 2021, <https://doi.org/10.3390/en14010027>.
 5. Premaratne, U., Samarabandu, J., Sidhu, T., Beresh, R., Tan, J. -C.: Security analysis and auditing of IEC61850-based automated substations. IEEE Transactions on Power Delivery, 25(4), 2346-2355, 2010, <https://doi.org/10.1109/TPWRD.2010.2043122>.
 6. IEEE P1547.3/D3.12 IEEE approved draft guide for cybersecurity of distributed energy resources interconnected with electric power systems. pp. 1–158, 2023.
 7. Ahn, B. et al.: An overview of cyber-resilient smart inverters based on practical attack models. IEEE Transactions on Power Electronics, 39(4), 4657-4673, 2024, <https://doi.org/10.1109/TPEL.2023.3342842>.
 8. Hussain, S.M.S., Aftab, M.A., Nadeem, F., Ali, I., Ustun, T.S.: Optimal energy routing in microgrids with IEC 61850 based energy routers. IEEE Transactions on Industrial Electronics, 67(6), 5161-5169, 2020, <https://doi.org/10.1109/TIE.2019.2927154>.
 9. Aftab, M.A., Suhail Hussain, S.M., Latif, A., Das, D.C., Ustun, T.S.: IEC 61850 communication based dual stage load frequency controller for isolated hybrid microgrid. International Journal of Electrical Power & Energy Systems, 130, 106909, 2021, <https://doi.org/10.1016/j.ijepes.2021.106909>.
 10. Chlela, M., Joos, G., Kassouf, M., Brissette, Y.: Real-time testing platform for microgrid controllers against false data injection cybersecurity attacks. In IEEE Power and Energy Society General Meeting (PESGM), Boston, MA, USA, 2016, pp. 1-5, <https://doi.org/10.1109/PESGM.2016.7741747>.
 11. Islam, M., Lee, H.-H.: Microgrid communication network with combined technology. In 5th International Conference on Informatics,

- Electronics and Vision (ICIEV), Dhaka, Bangladesh, 2016, pp. 423-427, <https://doi.org/10.1109/ICIEV.2016.7760039>.
12. Moreira, N., Molina, E., Lazaro, J., Jacob, E., Astarloa, A.: Cyber-security in substation automation systems. *Renewable and Sustainable Energy Reviews*, 54, 1552-1562, 2016, <https://doi.org/10.1016/j.rser.2015.10.124>.
 13. Joos, G., Reilly, J., Bower, W., Neal, R.: The need for standardization: The benefits to the core functions of the microgrid control system. *IEEE Power and Energy Magazine*, 15(4), 32-40, 2017, <https://doi.org/10.1109/MPE.2017.2690518>.
 14. Lv, G., Liu, H.: Study on IEC 61970/61968 based information integration for smart distribution grid. In: *Proc. of International Conference on Electrical and Control Engineering*, Yichang, China, 2011, pp. 5019-5022, <https://doi.org/10.1109/ICECENG.2011.6057309>.
 15. Gunduz, M.Z., Das, R.: Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, 169, 107094, 2020, <https://doi.org/10.1016/j.comnet.2019.107094>.
 16. Volkova, A., Niedermeier, M., Basmadjian, R., de Meer, H.: Security challenges in control network protocols: A survey. *IEEE Communications Surveys & Tutorials*, 21(1), 619-639, 2019, <https://doi.org/10.1109/COMST.2018.2872114>.
 17. Dutertre, B.: Formal modeling and analysis of the Modbus protocol. In: Goetz, E., Shenoi, S. (eds) *Critical Infrastructure Protection. ICCIP 2007*. IFIP International Federation for Information Processing, vol. 253, 189-204, 2008, https://doi.org/10.1007/978-0-387-75462-8_14.
 18. Ayele, E.D., Gonzalez, J.F., Teeuw, W.B.: Enhancing cybersecurity in distributed microgrids: A review of communication protocols and standards. *Sensors*, 24, 854, 2024, <https://doi.org/10.3390/s24030854>.
 19. Zografopoulos, I., Hatziaargyriou, N.D., Konstantinou, C.: Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. *IEEE Systems Journal*, 17(4), 6695-6709, 2023, <https://doi.org/10.1109/JSYST.2023.3305757>.
 20. Wang, W., Sun, K., Zeng, C., Chen, C., Qiu, W., You, S., Liu, Y.: Information and Communication Infrastructures in modern wide-area systems. In: Haes Alhelou, H., Abdelaziz, A.Y., Siano, P. (eds) *Wide Area Power Systems Stability, Protection, and Security*. Power Systems, pp. 71-104, 2021, https://doi.org/10.1007/978-3-030-54275-7_3

21. Wong, T.-Y., Lau, W.-H., Chung, H.S.-H., Shum, C.: A feasibility study of using Manufacturing Message Specification report gateway model for IEC61850 inter-substation type-1 messaging over wide area network. *Sustainable Energy, Grids and Networks*, 30, 100612, 2022, <https://doi.org/10.1016/j.segan.2022.100612>.
22. Ustun, T. S., Farooq, S.M., Hussain, S.M.S.: Implementing secure routable GOOSE and SV messages based on IEC 61850-90-5. *IEEE Access*, 8, 26162-26171, 2020, <https://doi.org/10.1109/ACCESS.2020.2971011>.
23. Ayele, E.D., Gonzalez, J.F., Teeuw, W.B.: Enhancing cybersecurity in distributed microgrids: A review of communication protocols and standards. *Sensors*, 24, 854, 2024, <https://doi.org/10.3390/s24030854>.
24. Shukla, S., Deng, Y., Shukla, S., Mili, L.: Construction of a microgrid communication network. In: *ISGT 2014*, Washington, DC, USA, 2014, pp. 1-5, <https://doi.org/10.1109/ISGT.2014.6816412>.
25. Gungor, V.C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., Hancke, G.P.: Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics*, 7(4), 529-539, 2011, <https://doi.org/10.1109/TII.2011.2166794>.
26. Razazian, K., Umari, M., Kamalizad, A., Loginov, V., Navid, M.: G3-PLC specification for powerline communication: Overview, system simulation and field trial results. In *ISPLC2010*, Rio de Janeiro, Brazil, 2010, pp. 313-318, <https://doi.org/10.1109/ISPLC.2010.5479881>.
27. Jianming, L., Bingzhen, Z., Liang, G., Zhou, Y., Yirong, W.: Communication performance of broadband PLC technologies for smart grid. In *2011 IEEE International Symposium on Power Line Communications and Its Applications*, Udine, 2011, pp. 491-496, <https://doi.org/10.1109/ISPLC.2011.5764448>.
28. Goldfisher, S., Tanabe, S.: IEEE 1901 access system: An overview of its uniqueness and motivation. *IEEE Communications Magazine*, 48(10), 150-157, 2010, <https://doi.org/10.1109/MCOM.2010.5594690>.
29. Chung, M.Y., Jung, M.H., Lee, T.J., Lee, Y.: Performance analysis of HomePlug 1.0 MAC with CSMA/CA. *IEEE Journal on Selected Areas in Communications*, 24(7), 1411-1420, 2006, <https://doi.org/10.1109/JSAC.2006.874404>.
30. Mohassel, R.R., Fung, A.S., Mohammadi, F., Raahemifar, K.: A survey on advanced metering infrastructure and its application in smart grids. In

- IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE), Toronto, ON, Canada, 2014, pp. 1-8, <https://doi.org/10.1109/CCECE.2014.6901102>.
31. Cendrillon, R., Yu, W., Moonen, M., Verlinden, J., Bostoen, T.: Optimal multiuser spectrum balancing for digital subscriber lines. IEEE Transactions on Communications, 54(5), 922-933, 2006, <https://doi.org/10.1109/TCOMM.2006.873096>.
 32. Ginis, G., Cioffi, J.M.: Vectored transmission for digital subscriber line systems. IEEE Journal on Selected Areas in Communications, 20(5), 1085–1104, 2002, <https://doi.org/10.1109/JSAC.2002.1007389>.
 33. Ahamed, S.V., Gruber, P.L., Werner, J.J.: Digital subscriber line(HDSL and ADSL) capacity of the outside loop plant. IEEE Journal on Selected Areas in Communications, 13, 1540-1549, 1995.
 34. Christensen, K., Reviriego, P., Nordman, B., Bennett, M., Mostowfi, M., Maestro, J.A.: IEEE 802.3 az: The road to energy efficient ethernet. IEEE Communications Magazine, 48(11), 50-56, 2010, <https://doi.org/10.1109/MCOM.2010.5621967>.
 35. Brunner, C.: IEC 61850 for power system communication. In IEEE/PES Transmission and Distribution Conference and Exposition, Chicago, IL, USA, 2008, pp. 1-6, <https://doi.org/10.1109/TDC.2008.4517287>.
 36. Ko, M.A.: Layering serial attached small computer system interface (SAS) over ethernet. U.S. Patent US8140696B2, 2012, <https://patents.google.com/patent/US8140696B2/en>.
 37. Stalley, K.D., Clarke, D.E., Rosher, P.A.: Optical fibre communications system. U.S. Patent US5479286A, 1995, <https://patents.google.com/patent/US5479286A/en>.
 38. Jiang, D., Delgrossi, L.: IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments. In Proc. of VTC Spring 2008 - IEEE Vehicular Technology Conference, Marina Bay, Singapore, 2008, pp. 2036-2040, <https://doi.org/10.1109/VETECS.2008.458>.
 39. Guille, C., Gross, G.: A conceptual framework for the vehicle-to-grid (V2G) implementation. Energy Policy, 37(11), 4379-4390, 2009, <https://doi.org/10.1016/j.enpol.2009.05.053>.
 40. Rajagopal, S., Roberts, R.D., Lim, S.K.: IEEE 802.15. 7 visible light communication: Modulation schemes and dimming support. IEEE Communications Magazine, 50(3), 72-82, 2012, <https://doi.org/10.1109/MCOM.2012.6163585>.

41. Lee, J.S., Su, Y.W., Shen, C.C.: A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. In IECON 2007 - 33rd Annual Conference of the IEEE Industrial Electronics Society, Taipei, Taiwan, 2007, pp. 46-51, <https://doi.org/10.1109/IECON.2007.4460126>.
42. Mishra, A.R. Fundamentals of Cellular Network Planning and Optimisation: 2G/2.5 G/3G... Evolution to 4G; John Wiley & Sons: Hoboken, NJ, USA, 2004.
43. Ghosh, A., Ratasuk, R., Mondal, B., Mangalvedhe, N., Thomas, T.: LTE-advanced: Next-generation wireless broadband technology. IEEE Wireless Communications, 17(3), 10-22, 2010, <https://doi.org/10.1109/MWC.2010.5490974>.

6. Интелигентна киберсигурност на микромрежа

Комуникационната инфраструктура, базираните на цифров микро-процесор интелигентни електронни устройства и технологията Интернет на нещата (IoT) [1] излагат възобновяемите интелигентни микромрежи на значителни киберзаплахи. Киберпрестъпниците използват различни методи за насочване към възобновяема интелигентна микромрежа, включително манипулиране на данни, компрометиране на интелигентни електронни устройства, отвличане на комуникация, внедряване на злонамерен софтуер и атаки на физическата система. Тези кибератаки могат да имат сериозни последиствия като оперативни смущения, финансови загуби, компрометирана цялост на данните, дори прекъсвания на тока.

Една критична заплаха включва манипулиране на предавани данни, което може да възникне чрез техники като инжектиране на фалшиви данни, подправяне, забавяния или създаване на трафик, за да се предотврати предаването на данни. Например нападателите могат да инжектират фалшиви данни в предаваната информация, за да подведат контролните системи да вземат неправилни решения като например неправилно балансиране на натоварването или погрешно откриване на грешки. Манипулирането на референтни точки, изпратени до електроцентрали, подстанции и защитни системи, може да доведе до нестабилност или повреда на оборудването.

Нарушенията на поверителността на данните като подслушване или неоторизиран достъп могат да компрометират оперативната информация и да разкрият уязвимостите на системата, потенциално улеснявайки по-вредни атаки като финансова експлоатация на пазарите на енергия. Атаките срещу физически системи

представяват друга сериозна загриженост, при която нападателите получават достъп до ключови точки във възобновяема интелигентна микромрежа като контролни интерфейси, измервателно оборудване и сензори, за да изпращат злонамерени команди. Например промяната на настройките на токовия трансформатор и потенциалния трансформатор или достъпът до вътрешните конфигурации на релето и контролера могат да причинят прекъсвания или повреда на оборудването.

Кибератаките могат да манипулират контролните сигнали, за да претоварят компонентите, което води до прегряване, пожари, физически щети и продължителен престой. Десинхронизиращите атаки, насочени към прецизната синхронизация (напр. GPS), необходима за ефективна работа на микромрежата, могат да предизвикат фазови несъответствия и проблеми с качеството на захранването, потенциално водещи до прекъсване на тока или хаотични работни условия.

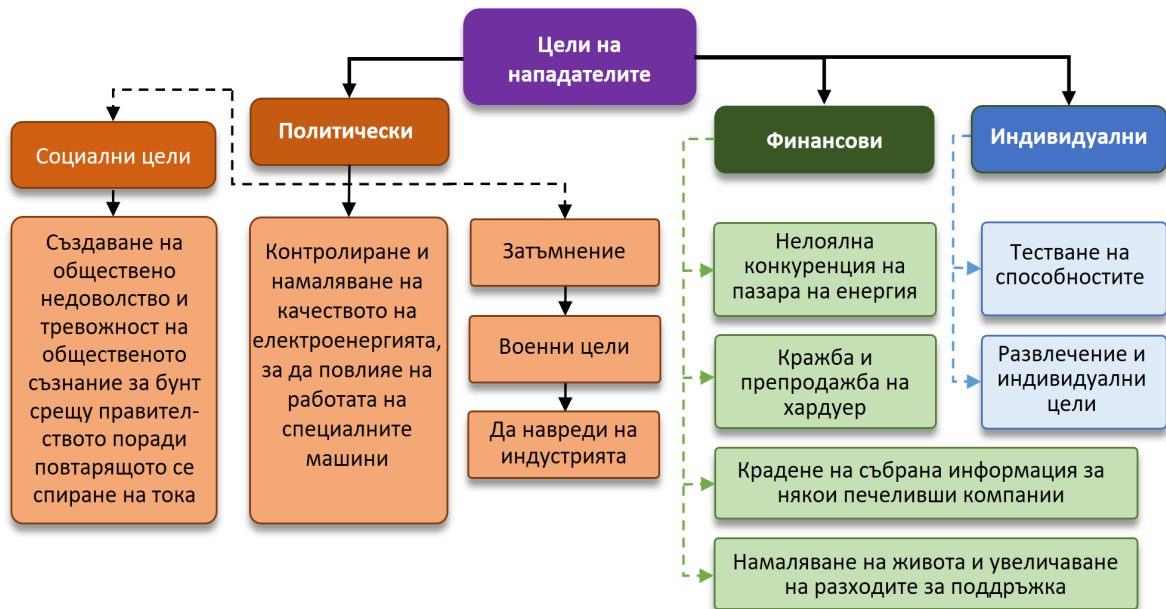
6.1. Пътната карта за атака на възобновяема интелигентна микромрежа

Отчитайки разрушителния ефект на кибератаките върху микромрежите, все повече изследователи се фокусират върху тази област и разработват стратегии, които да предпазват от злонамерени дейности. На Фиг. 6.1 са показани видовете кибератаки.



Фиг. 6.1. Видове кибератаките

На Фиг. 6.2 са показани целите на кибератаките въз основа на поведението на атакуващия.



Фиг. 6.2. Цели на кибератаките и възможни въздействия

Успешната активна атака обикновено изисква предходни успешни пасивни атаки. Например кибератаки, водещи до спиране на тока, като инцидента с Black Energy в Украйна [2], включват координирани атаки срещу различни сегменти на електроенергийната система, което налага успешно проникване във всички целеви зони. Пътната карта за атака на възобновяема интелигентна микромрежа е показана на Фиг. 6.3.



Фиг. 6.3. Пътната карта за атака на възобновяема интелигентна микромрежа

Кибернападателите обикновено използват два основни метода за постигане на целите си.

- Атака срещу вградени устройства.
- Атака срещу комуникация и протоколи.

Тези атаки могат да бъдат стартирани чрез получаване на физически или отдалечен достъп до отделни интелигентни елект-

ронни устройства и контролни центрове, локални мрежи (LAN), широкообхватни мрежи (WAN) или чрез отвличане на безжични комуникации.

6.2. Атака срещу вградени устройства

За да се насочат към вградени устройства, атакуващите разработват зловреден софтуер като троянски коне, вируси и червеи (включително скорошен ransomware като Petya и Not Petya). След това те търсят пътища за заразяване на вградени в микромрежи устройства и контролни центрове, както е показано на Фиг. 6.4.



Фиг. 6.4 Три начина за заразяване на зловреден софтуер

Зловредните софтуери Stuxnet и Black Energy са примери на злонамерени дейности [2, 3]. След като зловредният софтуер проникне във възобновяема интелигентна микромрежа, той се стреми да манипулира различни електронни устройства, сензори, състояния на прекъсвачи, устройства за архивиране и съхранение на исторически данни и други интелигентни устройства. При подобни манипулации се изпращат фалшиви команди и неточни измервания в цялата мрежа, което води до неправилно функциониране на системните компоненти, както е показано на Фиг. 6.5.

Последици от кибератака срещу възобновяема
интелигентна микромрежа

- В резултат на това фалшивото изключване на се променя топологията на мрежата, претоварвайки другите линии;
- Фалшиво свързване или прекъсване на връзката с главната мрежа (атака срещу точката на общо свързване), включване/изключване на островен режим;
- Фалшиво включване или изключване на генераторни и акумулиращи блокове, липса на енергиен баланс;
- Намаляване или увеличаване на генерираната мощност, липса на баланс на производство и потребление;
- Йерархична загуба на товари (от некритично до критично)
- Загуба на времева синхронизация;
- Лошо качество на захранването (чрез създаване на вариации, инжектиране на хармоници);
- Неправилни резервни производствени данни;
- Неуспешно предоставяне на услуга от определен компонент;
- Затъмнение.

Фиг. 6.5. Последици от кибератака срещу възобновяема
интелигентна микромрежа

За да се предпазим от зловреден софтуер, трябва да се приложат няколко стратегии. Тези стратегии са обобщени на Фиг. 6.6, черпейки от източници [4, 5, 6].

Защитните стени и изолацията от интернет могат значително да намалят риска от неоторизиран външен достъп, което налага атакуващите да получат вътрешен достъп, за да изпълнят успешни атаки. Софтуерът против злонамерен софтуер обаче остава от решаващо значение за предотвратяване на инсталиране на злонамерен софтуер и опити за заразяване, въпреки че усъвършенстваните нападатели могат да се опитат да заобиколят тези защиты, както се вижда от зловредния софтуер Stuxnet.

- Използване на изключителна комуникация и протоколи във възобновяемите интелигентни микромрежи вместо интернет;
- Сегментиране на възобновяемите интелигентни микромрежи на няколко секции;
- Инсталирайте защитна стена във всеки сегмент, за да предотвратите външен неоторизиран достъп;
- Инсталирайте антизловреден софтуер за предотвратяване и откриване на вирусна инфекция;
- Създаване на доживот за пароли и използване на удостоверяване в две стъпки за инсталиране на нов софтуер и актуализиране на корекции, както и редовно актуализиране на софтуера и управление на корекции;
- Идентифицирайте възможните точки за достъп и укрепване на физическия достъп чрез политики за силни пароли, многофакторно удостоверяване и ограничаване на достъпа;
- Контрол и втвърдяване на кибернетичен достъп, както и обучение за сигурност на служителите;
- Редовно одитирайте и тествайте споменатите механизми за сигурност;
- Използване на офлайн носител (твърд диск, DVD и др.) за архивиране и редовна ротация на архивиране;
- Използване на многоцелеви интуитивни методи за откриване и предотвратяване с множество алгоритми.

Фиг. 6.6. Някои стратегии срещу зловреден софтуер

Вътрешният достъп обикновено се осъществява чрез несъзнателни или умишлени действия на оторизирани потребители или по време на процеси на въвеждане в експлоатация и тестване, включващи преносими устройства за съхранение [7].

За да се предотвратят непреднамерени злонамерени дейности, повишаването на осведомеността за киберсигурността на оторизираните потребители е от съществено значение [8]. Например обучението за потенциални заплахи като кибератаката в Украйна, която започна с отваряне на заразен имейл, съдържащ злонамерен софтуер Black Energy.

Наложително е да се забрани неоторизирано инсталиране на софтуер или пачове без технически контрол и да се избягва свързването на лични смарт устройства (напр. лаптопи или мобилни телефони) към защитени мрежи [9]. Обратно, за смекчаване на

умишлени злонамерени дейности, прилагането на удостоверяване в две стъпки с вторично удостоверяване от персонал по сигурността, задаване на дати на изтичане на паролата и редовно актуализиране на пароли (за предотвратяване на достъп от вече напуснал персонал) са основни мерки. Освен това подобряването на методите за откриване и превенция остава от решаващо значение за ефективното осуетяване на заплахите за киберсигурността.

6.3. Атака върху комуникацията и протоколите

За разлика от традиционните комуникационни системи, комуникацията във възобновяема интелигентна микромрежа е ограничена както от време, така и от съображения за сигурност. Стандартът IEC 61850 е широко възприет заради своите ефективни протоколи. Въпреки ограниченията във времето IEC 61850 няма стабилни механизми за сигурност, което го прави податлив на кибератаки [10].

Нападателите се възползват от уязвимости, като се опитват да прихванат комуникацията между издател/абонат в протоколи като GOOSE и SV и между клиент/сървър в протокола MMS. Един използван метод е „отравяне“ на протокола за намиране на физическия адрес (Address Resolution Protocol – ARP), при което фалшиви ARP съобщения се изпращат през мрежата, за да подмамат устройствата да асоциират автентичен IP адрес със злонамерен MAC адрес. Тази тактика позволява на нападателите да подслушват и манипулират предаваните съобщения [11].

В Таблица 6.1 са показани потенциалните последици от кибератаки, насочени към IEC61850 протоколи [7, 12, 13].

Таблица 6.1. Последиви от кибератаката срещу IEC61850 протоколи.

Атака		Протокол		
		GOOSE	SV	MMS
Пасивна	Анализ на трафика	Достъп до съобщения за злонамерени политически или финансови цели като проектиране на бъдещи атаки, нелоялна конкуренция на пазара на енергия и др.		
	Подслушване			
Активна	Повторение, отложено	• Неизправност • Фалшива команда към прекъсвачите • Фалшив доклад за статус на прекъсвачи • Невъзможност за комуникация с прекъсвачите	• Неизправност • Невъзможност за комуникация с ТТ и ПТ • Неправилно изпращане • Доклади за извадкови стойности на ТТ и ПТ • Неизправност на релейната защита	• Неуспешна операция • Невъзможност за комуникация с контролния център • Изпращане и получаване на фалшиви команди за управление
	Отказ от услуга			
	Модифициране на контролните данни на протокола и измерените стойности			
	Човек в средата на атаката			
	Инжектиране на фалшиви данни			

ТТ – Токов трансформатор, ПТ – Потенциален трансформатор

Важно е да се отбележи, че естеството на кибератаките при GOOSE и SV се различава от тези при MMS поради използваните съответно модели клиент – сървър и издател – абонат. За подобряване на киберсигурността в рамката на IEC 61850 е разработен IEC62351.

В Таблица 6.2 са обобщени IEC62351 решенията за защита на IEC61850.

Въпреки че IEC62351 предоставя някои решения за защита на IEC61850 срещу кибератаки, някои практически и глобални ограничения правят IEC61850 все още уязвим за кибератаки. Някои от тези ограничения са както следва:

- Високи времена за обработка в някои дадени решения.
- Липса на координация между енергийната система и IEC62351 поради наследено оборудване на енергийната система.
- Високи разходи за внедряване.
- Усложняване на комуникационната мрежа.

Като се имат предвид ограниченията, посочени в предходните таблици, няколко решения за справяне с недостатъците на IEC 62351 при защитата на IEC 61850 са представени в Таблица 6.3.

Таблица 6.2. IEC62351 решения за защита на IEC61850

Стандарт	Раздел	Протокол	Предоставено решение	Недостатъци	Глобален лимит
IEC62351	6	GOOSE / SV	Метод за удостоверяване чрез цифрови подписи, базирани на RSA, времево клеймо (за SV)	- Трудно за изпълнение - Високи времена за обработка - Големи дължини на подписа - Използване на симетрични ключове [14, 15, 16]	Оборудването на наследената система за захранване не поддържа IEC62351
	4	MMS	- Сигурност на транспортния слой за цялост, поверителност и удостоверяване чрез различни комплекти за шифроване (за T-Profile) - Добавяне на полета в блоковете данни на протокола, използвани за удостоверяване на елемент на услугата за контрол на асоциацията (за A-профил)	- Висока латентност - Високи разходи за внедряване - Уязвимост към някои атаки като инжектиране, забавяне и модификация, ако атакуващият има достъп до лични ключове и ключове за криптиране - Някои устройства не поддържат TLS - Сложност на мрежата	

RSA (Rivest–Shamir–Adleman) – криптосистема с публичен ключ, една от най-старите широко използвани за сигурно предаване на данни; TLS – Transport Layer Security – криптографски протокол, предназначен да осигури комуникационна сигурност през компютърна мрежа

Таблица 6.3. Някои решения за отстраняване на недостатъците на IEC62351

Дадени решения за недостатъци	Осигурени предимства	Справка
• Rainbow схема за подпис • Квантов криптографски метод за квантови компютърни заплахи	• Бързо генериране на подпис • Проверка с помощта на асиметрични ключове • Намаляване на времезакъснението • Повишаване на изискванията за сигурност	[14]
• Алгоритъм за прескачане на последователност	• Намаляване на времезакъснението • Лека схема за удостоверяване • Повишаване на изискванията за сигурност	[17]
• Алгоритми, базирани на код за удостоверяване на съобщението	• Подобряване на изискванията за сигурност и време	[18]
• Метод, базиран на удостоверено криптиране със свързани данни	• Подобряване на поверителността и интегритета едновременно • Намаляване на времезакъснението	[19]

Следователно, стандартът IEC62351 описва рамка за сигурност за управление на грид системи и споделяне на информация за тях, включително връзката между различните рискове за киберсигурността и изискванията за сигурност, необходими за намаляване им. Тези рискове са разделени на четири категории: неоторизиран достъп до данни (конфиденциалност), неоторизирана промяна или кражба на данни (интегритет) и неотказ, който гарантира отговорност и отрича неверни твърдения за действие или бездействие.

Изискванията за сигурност са категоризирани в четири основни области: *поверителност, цялост, наличност и отказоустойчивост*. Всеки критерий е допълнен със списък на специфични опасности. Пример за ситуация, при която принципът на „конфиденциалност“ може да бъде нарушен, е чрез „неоторизиран достъп до информация“, което може да бъде постигнато с помощта на техники като подслушване и прихващане.

Случаи на „неоторизирана промяна или кражба на информация“ отслабват идеята за „интегритет“. „Наличност“ се отнася до възпрепятстване на разрешен достъп или отказ на услуга, което включва действия като подправяне на услуга и изчерпване на ресурс. И накрая, „неотричането“ гарантира „отчетност и отказ от действие“, за да се предотвратят атаки за отказ на услуга и да се опровергават твърденията за неизвършени действия, както и да се намалят опасностите като отказ и ретроспективен отказ. Разбирането на тази всеобхватна картина е от решаващо значение за разработването на стабилни мерки за защита на микромрежите от различни киберзаплахи.

Библиография

1. Gonzalez, I., Calderon, A.J., Folgado, F.J.: IoT real time system for monitoring lithium-ion battery long-term operation in microgrids. *Journal of Energy Storage*, 51, 2022, 104596, <https://doi.org/10.1016/j.est.2022.104596>.
2. Liang, G., Weller, S.R., Zhao, J., Luo, F., Dong, Z.Y.: The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, 32(4), 3317-3318, 2017, <https://doi.org/10.1109/TPWRS.2016.2631891>.
3. Langner, R.: Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9(3), 49-51, 2011, <https://doi.org/10.1109/MSP.2011.67>.
4. Birleanu, F.G., Bizon, N.: Control and protection of the smart microgrids using internet of things: Technologies, architecture and applications. In: Mahdavi Tabatabaei, N., Kabalci, E., Bizon, N. (eds) *Microgrid*

- Architectures, Control and Protection Methods. Power Systems. 749–770, 2020, https://doi.org/10.1007/978-3-030-23723-3_31.
5. Venkataramanan, V., Hahn, A., Srivastava, A.: CP-SAM: Cyber-physical security assessment metric for monitoring microgrid resiliency. IEEE Transactions on Smart Grid, 11(2), 1055-1065, 2020, <https://doi.org/10.1109/TSG.2019.2930241>.
 6. Vosughi, A., Tamimi, A., King, A.B., Majumder, S., Srivastava, A.K.: Cyber–physical vulnerability and resiliency analysis for DER integration: A review, challenges and research needs. Renewable and Sustainable Energy Reviews, 168, 112794, 2022, <https://doi.org/10.1016/j.rser.2022.112794>.
 7. Cai, J., Zheng, Y., Zhou, Z.: Review of cyber-security challenges and measures in smart substation. In International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), Chengdu, China, 2016, pp. 65-69, <https://doi.org/10.1109/ICSGCE.2016.7876027>.
 8. Tianxing, M., Yoshinov, R., Osipov, V., Zhukova, N., Schukina, M., Evnevich, E.: Problems of human secure interaction with the Internet space. Problems of Engineering Cybernetics and Robotics, 75, 15-34, 2021, <https://doi.org/10.7546/PECR.75.21.03>.
 9. Alkathairi, M.S., Alqarni, M.A., Chauhdary, S.H.: Cyber security framework for smart home energy management systems. Sustainable Energy Technologies and Assessments, 46, 101232, 2021, <https://doi.org/10.1016/j.seta.2021.101232>.
 10. Habib, H.F., Lashway, C.R., Mohammed, O.A.: A review of communication failure impacts on adaptive microgrid protection schemes and the use of energy storage as a contingency. IEEE Transactions on Industry Applications, 54(2), 1194-1207, 2018, <https://doi.org/10.1109/TIA.2017.2776858>.
 11. Hijazi, S, Obaidat, M.S.: Address resolution protocol spoofing attacks and security approaches: a survey. Security and Privacy, 2(1), 2019, <https://doi.org/10.1002/spy2.49>.
 12. Kang, B. et al.: Investigating cyber-physical attacks against IEC 61850 photovoltaic inverter installations. In IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), Luxembourg, Luxembourg, 2015, pp. 1-8, <https://doi.org/10.1109/ETFA.2015.7301457>.

13. Rajkumar, V.S., Tealane, M., Stefanov, A., Presekal, A., Palensky, P.: Cyber attacks on power system automation and protection and impact analysis. In IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), The Hague, Netherlands, 2020, pp. 247-254, <https://doi.org/10.1109/ISGT-Europe47291.2020.9248840>..
14. Reshikeshan, S.S.M., Koh, M.B., Illindala, M.S.: Rainbow signature scheme to secure GOOSE communications from quantum computer attacks. IEEE Transactions on Industry Applications, 57(5), 4579-4586, 2021, <https://doi.org/10.1109/TIA.2021.3093375>.
15. Rodríguez, M., Lázaro, J., Bidarte, U., Jiménez, J., Astarloa, A.: A fixed-latency architecture to secure GOOSE and sampled value messages in substation systems. IEEE Access, 9, 51646-51658, 2021, <https://doi.org/10.1109/ACCESS.2021.3069088>.
16. Farooq, S.M., Hussain, S.M.S., Ustun, T.S.: Performance evaluation and analysis of IEC 62351-6 probabilistic signature scheme for securing GOOSE messages. IEEE Access, 7, 32343-32351, 2019, <https://doi.org/10.1109/ACCESS.2019.2902571>.
17. Youssef, T., El Hariri, M., Mohammed, O., Wilkerson, C.: Sequence hopping algorithm for securing IEC 61850 GOOSE messages. In IEEE Green Technologies Conference (GreenTech), Houston, TX, USA, 2022, 1-5, <https://doi.org/10.1109/GreenTech52845.2022.9772034>.
18. Hussain, S.M.S., Farooq, S.M., Ustun, T.S.: Analysis and Implementation of Message Authentication Code (MAC) Algorithms for GOOSE Message Security. IEEE Access, 7, 80980-80984, 2019, <https://doi.org/10.1109/ACCESS.2019.2923728>.
19. Hussain, S.M.S., Farooq, S.M., Ustun, T.S.: A method for achieving confidentiality and integrity in IEC 61850 GOOSE messages. IEEE Transactions on Power Delivery, 35(5), 2565-2567, 2020, <https://doi.org/10.1109/TPWRD.2020.2990760>.

7. Киберуязвимости на възобновяемите източници на енергия, защитни мерки и режими на работа на микромрежата

Съвременните енергийни системи разчитат на сложни мрежи от интелигентни измервателни уреди, сензори и автоматизирани системи за управление. В частност източниците за производство на възобновяема енергия са жизненоважна част от възобновяемите интелигентни микромрежи и са основната цел на кибератаки [1, 2, 3]. Следователно изследването на устойчивостта на тези източници срещу кибератаки е приоритет.

7.1. Кибератака срещу фотоволтаичните системи

Фотоволтаичните (photovoltaics – PV) мрежи са свързани към електрическата мрежа чрез интелигентни захранващи електронни интерфейси. Тези интерфейси са от решаващо значение за оптимална работа, тъй като се свързват с контролния център на микромрежата и често предават своя статус (измервания, статус) и получават команди [4]. Във фотоволтаичната система атакуващият се насочва към сензори, прекъсвачи, проследяване на максимална мощност (MPPT – Maximum Power Point Tracking), DC-DC преобразуватели, инвертори, контролери на батерии (по-специално, тези контролери са интегрирани в контролер с много обекти като компонент на черна кутия в търговски настройки и комуникационни инфраструктури).

В Таблица 7.1 е показана подробна киберуязвимост на фотоволтаична система, включително целеви компоненти от атакуващия, метод за изпълнение на атаката, предоставени решения и разсейващи резултати от атаката [5, 6, 7, 8].

Таблица 7.1. Подробна киберуязвимост на фотоволтаична система

Атака върху	Начин на изпълнение	Предоставено решение	Резултати
Физическа атака срещу хардуер	• Физически щети • Кражба на оборудването	• Предотвратяване на нежелан физически достъп: използвайте огради, охранителни камери, охрана и входни системи за сигурност, като вземете предвид потенциалните методи за кражба по време на монтажа и строителството, заедно с прилагането на по-широки мерки за физическа сигурност • Идентификация и удостоверяване на човешки потребители: внедряване на системи за идентифициране и удостоверяване на човешки потребители • Актуализирана система за управление на инвентара • Внедряване на устройства против кражба • Създаване на политика за контрол на физическия достъп	• Загуба на някои фотоволтаични масиви във фотоволтаичната ферма • Провал на фотоволтаичната ферма

Атака върху	Начин на изпълнение	Предоставено решение	Резултати
Интелигентен инвертор, преобразувател, контролери за зарядно устройство за батерии и софтуер	• Софтуерни актуализации/промяна на изходните кодове от: – физически достъп чрез оторизиран персонал или нападатели – отвлечане на комуникация – контролен център • Модифициране на референтните и сензорните измервания чрез: – физически достъп – отвлечане на комуникация – център за управление – физически достъп до LAN • Фалшиви пачове	• Непрекъснато обновяване на софтуера • Предотвратяване на нежелан физически достъп • Използване на сигнатурни и контекстно базирани защитни стени, шлюзове • Подобрено утвърждаване на системата. • Внедряване на софтуер с повишени мерки за сигурност • Използване на решения срещу зловреден софтуер • Редовни проверки на историята на влизане • Ролеви контрол на потребителския достъп • Използване на инфраструктура с публичен ключ	• Нагоре за изключване на хранящите електронни интерфейси • Флуктуация на напрежението в микромрежата чрез промяна на генерираната ШИМ и реактивна мощност или колапс на напрежение и честота • Фалшифициране на изходната мощност и промяна в подаването на мощност • Презареждането или разреждането на батериите намалява живота им и увеличава разходите за поддръжка

Атака върху	Начин на изпълнение	Предоставено решение	Резултати
		- Човешка идентификация на потребителя и удостоверяване - Сканиране на корекции преди инсталиране - Силна автентификация, базирана на парола - Политика за контрол на достъпа с удостоверяване в два етапа	- Прекъсване на MPPT - Разпространение на зловреден софтуер в енергийните системи - Причиняване на необичайни хармоници върху вълнови форми
PV референтни точки	- Модификация на PV референтната точка като PQ от: - отвлечение на получените команди от контролния център на микромрежата - инсталиране на зловреден софтуер	- Внедряване на допълнителен защитен слой за PQ референтни точки - Интегриране на допълнителна защитена комуникация за архивиране - Налагане на политика за контрол на достъпа - Използване на усъвършенствани техники за защита срещу зловреден софтуер	- Скрито намаляване на напрежението на PV терминала поради поглъщане на реактивната мощност - Проблеми с качеството на захранването и стабилността на напрежението - Големи реални загуби на мощност

Атака върху	Начин на изпълнение	Предоставено решение	Резултати
Точката на общо свързване между фотоволтаичната ферма и микромрежата	• Фалшива команда за възпрепятстване на: – физически достъп – отвлечане на комуникация – център за управление на microgrid – местен център за управление на фермата – инсталиран зловреден софтуер на свързаното IED с прекъсвачи	• Предотвратяване на неоторизиран физически достъп • Използване на охранителна техника в ЦОП • Използване на GPRS телекомуникационна система или резервни системи • Налагане на политика за контрол на достъпа • Използване на техники за защита срещу злонамерен софтуер и усъвършенствани техники за защита срещу злонамерен софтуер	• Свързване и изключване от микромрежата • Много проблеми, свързани с по-ниска инерция на островния режим

Глобални резултати:	• Финансови загуби с PV за отказ на услуга поради загубите на икономическата зададена точка за изпращане • Ако PV е жилищна ($\leq 2\text{kw}$), отказът на услугата има малък ефект върху работата на микромрежата • Ако PV е търговска ($2\text{kw} \sim 2\text{Mw}$), отказът от услугата води до следните бедствия: намаляване на инерцията на възобновяемата микромрежа, загуба на някои некритични товари и засягане на икономичното изпращане на микромрежата • Ако PV е от комунален тип ($2\text{Mw} \sim 10\text{Mw}$), загубата на фотоволтаичната ферма е по-опасна със следните ефекти: намаляване на инерцията, икономично разпределение и загуба на някои некритични или дори критични товари • Намаляване стабилността на напрежението на микромрежата поради поглъщане на реактивна мощност
---------------------	---

Важно е да се отбележи, че методите за откриване и предотвратяване на проникване са ефективни срещу различни видове атаки. В Таблицата се предлагат някои решения и също така се изследват атаки срещу комуникационни системи.

7.2. Кибератака срещу вятърна електроцентрала

Електричеството, генерирано от вятърни турбини, се контролира от локални и микромрежови контролни центрове; някои вятърни генератори обаче не могат да се изпращат [9]. Центърът за управление на микромрежата получава измервания от турбината и енергийната система и изпраща поръчки и справки [10, 11]. С интелигентни функции вятърните турбини също са податливи на кибератаки [12, 13]. Целите на нападателя са същите като споменатите за фотоволтаичните. Подобно на фотоволтаичните системи кибератаките срещу офшорни вятърни турбини водят до сравними последиствия, методи на изпълнение, предоставени решения и резултати.

Докато физическият достъп за стартиране на кибератака върху офшорна вятърна ферма е по-труден, физическата ѝ защита е по-ниска и средата е по-тиха, което прави манипулирането на блока за контрол и наблюдение, монтиран на кулата, по-лесен след получаване на физически достъп. Подобно на фотоволтаичните системи атаките срещу вятърни турбини могат да нарушат точното прогнозиране на вятърната енергия (както краткосрочно, така и дългосрочно), което създава предизвикателства за икономическото планиране на изпращането и изисква по-отнемащи време ремонти [14].

По-малките фотоволтаични системи, особено жилищните видове, често нямат стандарти за киберсигурност, разчитайки на интернет свързаност за наблюдение и контрол. Тази достъпност ги прави уязвими за потенциални нападатели.

7.3. Кибератака срещу източници за съхранение на енергия

Батерии, съгъстен въздух, маховици, суперкондензатори и изпомпвани водноелектрически системи са обичайни източници за съхранение на енергия, свързани към мрежата чрез двупосочни инвертори като PCS100-ESS [15]. Тези системи участват в управлението на PV, PQ и Vf. Кибернападателите могат да ги направят недостъпни или да причинят неизправности, като използват пропуските в знанията в техните ограничения за презареждане, като по този начин ограничават възможностите им за доставка на енергия. Могат да манипулират съобщения от контролния център, сензори или вътрешни контролери [16]. Например контролерът на батерията използва данни като ток, напрежение и температура, за да се оцени състоянието на заряд.

Чрез манипулиране на сензорите за измерване нападателите могат да подведат контролера да вземе неправилни решения, което потенциално води до презареждане (като по този начин намалява живота на батерията) или разреждане, когато е необходимо за аварийни условия. Въвеждането на минимални и максимални прагове за зареждане на батериите е защитна мярка срещу подобни атаки [17, 18, 19].

7.4. Класификация на експлоатационните условия на микромрежите

Значителният напредък на информационните технологии, както и на индустриалните рамки за контрол, доведе до повишен интерес към микромрежите като киберфизична система [20]. Микромрежите са съставени от два отделни слоя:

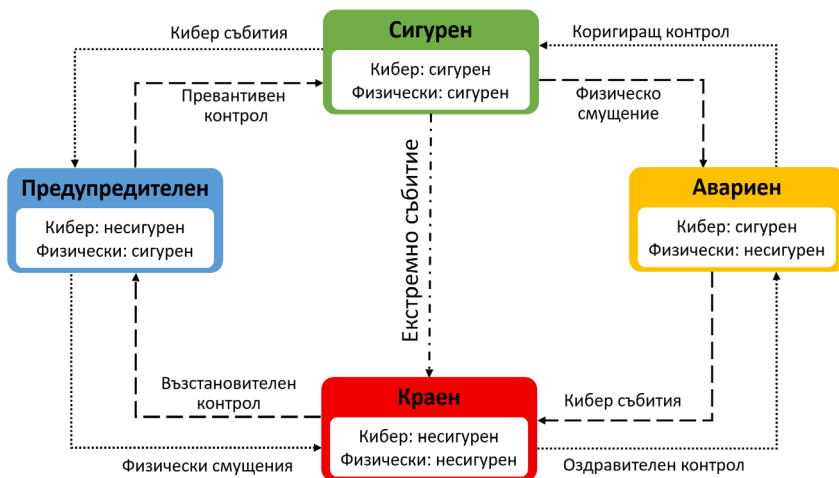
- физически слой, който обхваща материалните компоненти като фотоволтаични панели, вятърни турбини, системи за съхранение на енергия заедно с техните силови електронни преобразуватели,
- кибернетичен слой, който обхваща дигиталните аспекти.

Физическият слой е отговорен за управлението, изчислени-
ята и обработката на операциите за свързване [21]. Киберсисте-
мата на микромрежите представлява технологичната инфраструк-
тура, която обхваща различни взаимосвързани компоненти и про-
цеси [22]. Тя е предназначена да улесни управлението и работата с
цифровата информация и комуникацията в структурата на микро-
мрежата. Тази киберсистема играе решаваща роля за осигуряване
на сигурността, ефективността и надеждността на цифровите опе-
рации на микромрежата.

Системата събира, обработва, показва и съхранява информа-
ция за дейността на микромрежата чрез информационни канали и
чрез потоци от данни [23, 24]. Информацията се представя под
формата на наблюдение и измервания, протоколи, заедно с кон-
фигурации на микромрежата. Работата на непрекъснатите физи-
чески събития зависи до голяма степен от наличието на ефективни
и надеждни потоци от данни. Работните условия на микромрежата
с физически и кибервзаимодействия могат да бъдат категоризи-
рани в четири различни режима: защитен, предупредителен, ава-
риен и екстремн режим.

Тези функционални сценарии на микромрежата са илюстри-
рани на Фиг. 7.1 [20, 25].

- **Защитен режим:** При този режим микромрежата функцио-
нира по нормален начин, при който както киберсигурност-
та, така и физическата сигурност се запазват.
- **Режим на предупреждение:** При този режим физическата
сигурност се запазва, но киберсигурността е разрушена. В
този режим правилата за контрол на мониторинга са бло-
кирани и оборудването трябва да може да стабилизира фи-
зическия процес, като използва настройките си по подраз-
биране.



Фиг. 7.1. Режими на работа на микромрежата

- **Аварийен режим:** При този режим киберсигурността се запазва, но физическата сигурност е компрометирана. В това състояние се случват събития като прекъсване на електрическа линия или източник на захранване, колебания на напрежението, които са твърде високи или твърде ниски, честотни колебания, както и отклонения на честотата и увеличени токове на линията.
- **Екстремен режим:** В този режим всички слоеве са компрометирани в рамките на един и същ период от време, което води до повреда на комуникационното и друго оперативно оборудване. Това състояние може да се дължи на природно бедствие, което унищожава както физическото оборудване, така и комуникационната мрежа.

Обикновено в енергийната индустрия се използват четири категории действия за възстановяване на микромрежата в по-безопасен режим [26, 27]:

- **Превантивен контрол:** Той включва връщане към състояние на сигурност от състояние на предупреждение, така че

операторът да може да си възвърне киберсигурността, като същевременно поддържа физическата сигурност непроменена.

- **Коригиращ контрол:** Чрез възстановяване на физическата сигурност и запазване на киберсигурността той възстановява защитения режим от аварийния режим, като същевременно запазва кибернетичната поверителност и физическата цялост на компонентите на мрежата [28].
- **Коригиращ контрол:** Възстановява аварийния режим от екстремнен режим, като елиминира кибернетични уязвимости и предотвратява от допълнителни нарушения поверителността в киберпространството [29].
- **Възстановяващ контрол:** Той възстановява режим на предупреждение от екстремнен режим, като елиминира всички физически уязвимости и предотвратява от допълнителни щети върху кибер стабилността.

7.5. Защитни мерки за противодействие на кибератаки в микромрежите

За да се предпазят микромрежите от различни кибератаки, е наложително да се създадат подходящи защитни механизми. Въз основа на настоящите академични изследвания тактиките за противодействие могат да бъдат класифицирани в три отделни типа, както е посочено в [30]:

- **Стратегии за превенция:** Този защитен подход ефективно отлага началото на заплахите. Превантивните методи са от изключително значение като основно средство за защита срещу киберпроникване в микромрежи.
- **Стратегии за устойчивост:** Този защитен метод подобрява устойчивостта срещу потенциални вреди и позволява работа, възможно най-подобна на нормално състояние.

- **Идентифициране и сегрегация:** Тази отбранителна методология използва усъвършенстван подход за определяне на източника на злонамерено проникване, изолиране на засегнатите компоненти и бързо възстановяване на мрежата до нормалното ѝ работно състояние.

Защитните техники срещу кибератаки в микромрежите са от съществено значение за запазване на целостта и сигурността на тези системи. Основна стратегия е контролът на достъпа, който смекчава присъствието на неоторизирани лица, които имат достъп до критична информация и оборудване в рамките на микромрежата [31]. Прилагането на строги мерки за контрол на достъпа значително намалява опасността от допускане на неоторизирани лица [32]. Сегментирането на мрежата е жизненоважна тактика; чрез разделянето на микромрежата на отделни части кибератаките могат да бъдат ограничени до едно място, като по този начин възпрепятстват страничното движение и минимизират възможните щети в цялата система [33]. Освен това внедряването на системи за откриване на проникване е от решаващо значение за наблюдение на комуникациите в микромрежите, улеснявайки откриването на аномални или подозрителни модели, които означават киберзаплахи [34].

Ключов защитен механизъм е сигурното удостоверяване, което гарантира, че само оторизирани служители имат достъп до комуникационната инфраструктура на микромрежата. Това може да бъде постигнато чрез строги методи за удостоверяване като например многофакторно удостоверяване, което осигурява допълнителен слой на защита. Криптирането е от съществено значение за опазване на поверителността и целостта на информацията по време на прехвърляне на данни, възпрепятствайки враждебните участници да прихванат или модифицират комуникации [35]. В крайна сметка управлението на корекциите е от съществено значение за запазване на сигурността на системата. Целият софтуер, код и плат-

форми в центровете за данни на микромрежата трябва да получават редовни актуализации и корекции, за да смекчат известните уязвимости и да подобрят устойчивостта на системата срещу потенциални кибератаки [36].

Ефективните стратегии за борба с кибератаките включват предвиждане на атаки и подобряване на сигурността на данните на системата за предотвратяване на проникване чрез използване на софтуерно дефинирани архитектури [37]. Може да се използва усъвършенствана изчислителна мрежа за кодиране на защитен механизъм. Различни методи като контролирано обучение, техники за метаевристична оптимизация, анализ на стабилността, регресионен анализ и др. могат да бъдат използвани за прогнозиране на кибератаки и прониквания.

В Таблица 7.2 е представен общ преглед на различни защитни техники, които могат да се използват за намаляване на въздействието на кибератаките върху микромрежите.

Таблица 7.2. Защитни механизми за кибератаки в микромрежи

Отбранител-на стратегия	Коментар
Контрол на достъпа [31]	Чрез внедряването на строги системи за контрол на достъпа е възможно да се намали броят на неоторизираните лица, които получават достъп до важна информация и оборудване, разположени в рамките на микромрежата.
Сегментиране на мрежата [32]	MG мрежата може да бъде разделена на изолирани сегменти, което позволява ограничаване на всякакви кибератаки и предотвратяване на странично разширение вътре в мрежата.
Системи за откриване на проникване [33]	Създаване на система за откриване на проникване, за наблюдаване на комуникациите, които се осъществяват в микромрежата и идентифициране на всякакви необичайни или странни модели, които може да са показателни за наличието на кибератаки.

Отбранител-на стратегия	Коментар
Системи за предотвратяване на проникване [34]	За да се предотврати компрометиране на архитектурата на микромрежата, е необходимо да се използват системи за предотвратяване на проникване, за да се предотврати или намали ефектът от кибератаки, които са разпознати от системите за откриване на проникване.
Сигурно удостоверяване [38, 39]	За да се гарантира, че само персонал, който е надлежно сертифициран, има достъп до комуникационните инфраструктури на микромрежата, е необходимо да се внедрят строги механизми за удостоверяване, които могат да включват многофакторно удостоверяване.
Криптиране [35]	Трябва да се използват техники за криптиране, за да се защити поверителността и целостта на информацията по време на връзката за обмен на данни. Това ще предотврати появата на злонамерено проследяване.
Управление на корекциите [36]	За да се гарантира, че всички известни дефекти са коригирани, наложително е всички програми, код и компютърни платформи, които се помещават в центровете за данни на микромрежата, да бъдат редовно актуализирани и коригирани.

Всяка от тези мерки играе решаваща роля в защитата на микромрежите от кибератаки в енергийната индустрия, като гарантира защитата на техните процеси, поверителността на информацията и надеждността по време на целия процес.

Библиография

1. Weng, S., Yue, D., Chen, J., Xie, X., Dou, C.: Distributed resilient self-triggered cooperative control for multiple photovoltaic generators under denial-of-service attack. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 53(1), 226-237, 2023, <https://doi.org/10.1109/TSMC.2022.3176460>.

2. Zhang, J., Guo, L., Ye, J.: Cyber-attack detection for photovoltaic farms based on power-electronics-enabled harmonic state space modeling. *IEEE Transactions on Smart Grid*, 13(5), 3929-3942, 2022, <https://doi.org/10.1109/TSG.2021.3121009>.
3. Hemmati, R., Faraji, H.: Identification of cyber-attack/outage/fault in zero-energy building with load and energy management strategies. *Journal of Energy Storage*, 50, 104290, 2022, <https://doi.org/10.1016/j.est.2022.104290>.
4. Judge, M.A., Khan, A., Manzoor, A., Khattak, H.A.: Overview of smart grid implementation: Frameworks, impact, performance and challenges. *Journal of Energy Storage*, 49, 104056, 2022, <https://doi.org/10.1016/j.est.2022.104056>.
5. Su, Q., Wang, H., Sun, C., Li, B., Li, J.: Cyber-attacks against cyber-physical power systems security: State estimation, attacks reconstruction and defense strategy. *Applied Mathematics and Computation*, 413, 126639, 2022, <https://doi.org/10.1016/j.amc.2021.126639>.
6. Tuyen, N.D., Quan, N.S., Linh, V.B., Van Tuyen, V., Fujita, G.: A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy. *IEEE Access*, 10, 35846-35875, 2022, <https://doi.org/10.1109/ACCESS.2022.3163551>.
7. Qiu, W., Sun, K., Li, K.-J., Li, Y., Duan, J., Zhu, K.: Cyber-attack detection: Modeling and roof-PV generation system defending. *IEEE Transactions on Industry Applications*, 59(1), 160-168, 2023, <https://doi.org/10.1109/TIA.2022.3213629>.
8. Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., Ghadimi, N.: A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research*, 215, Part A, 108975, 2023, <https://doi.org/10.1016/j.epsr.2022.108975>.
9. Bevrani, H., François, B., Ise, T.: *Microgrid dynamics and control*. John Wiley & Sons, 2017.
10. Loughney, S., Edesess, A.J.: Applications of industrial IoT and WSNs in O&M programmes for offshore wind farms. In: Tuovinen, T., Periaux, J., Neittaanmäki, P. (eds) *Computational Sciences and Artificial Intelligence in Industry. Intelligent Systems, Control and Automation:*

- Science and Engineering, 76, 223-245, 2022, https://doi.org/10.1007/978-3-030-70787-3_15.
11. Ali, SW, et al. Offshore wind farm-grid integration: a review on infrastructure, challenges, and grid solutions. IEEE Access, 9, 102811-102827, 2021, <https://doi.org/10.1109/ACCESS.2021.3098705>.
 12. Kulev, N., Torres, F.S.: Simulation of the impact of parameter manipulations due to cyber-attacks and severe electrical faults on offshore wind farms. Ocean Engineering, 260, 111936, 2022, <https://doi.org/10.1016/j.oceaneng.2022.111936>.
 13. Zhao, Y., Yao, W., Zhang, C.-K., Ai, X., Wen, J.: Resilient wide-area damping control to mitigate strong cyber attack: A multiple-controller switching approach. IEEE Transactions on Smart Grid, 14(3), 2326-2337, 2023, <https://doi.org/10.1109/TSG.2022.3215785>.
 14. Ren, Z., Verma, A.S., Li, Y., Teuwen, J.J.E., Jiang, Z.: Offshore wind turbine operations and maintenance: A state-of-the-art review. Renewable and Sustainable Energy Reviews, 144, 110886, 2021, <https://doi.org/10.1016/j.rser.2021.110886>.
 15. Liu, X., Shahidehpour, M., Cao, Y., Wu, L., Wei, W., Liu, X.: Microgrid risk analysis considering the impact of cyber attacks on solar PV and ESS control systems. IEEE Transactions on Smart Grid, 8(3), 1330-1339, 2017, <https://doi.org/10.1109/TSG.2016.2622289>.
 16. Mhaisen, N., Fetais, N., Massoud, A.: Secure smart contract-enabled control of battery energy storage systems against cyber-attacks. Alexandria Engineering Journal, 58(4), 1291-1300, 2019, <https://doi.org/10.1016/j.aej.2019.11.001>.
 17. Kharlamova, N., Hashemi, S., Træholt, C.: Data-driven approaches for cyber defense of battery energy storage systems. Energy and AI, 5, 100095, 2021, <https://doi.org/10.1016/j.egyai.2021.100095>.
 18. Ghanbari-Ghalehjoughi, M., Taghizad-Tavana, K., Nojavan, S.: Resilient operation of the renewable energy and battery energy storages based smart distribution grid considering physical-cyber-attacks. Journal of Energy Storage, 62, 106950, 2023, <https://doi.org/10.1016/j.est.2023.106950>.
 19. Kharlamova, N., Træhold, C., Hashemi, S.: Cyberattack detection methods for battery energy storage systems. Journal of Energy Storage, 69, 107795, 2023, <https://doi.org/10.1016/j.est.2023.107795>.

20. Ahmed, I., El-Rifaie, A.M., Akhtar, F., Ahmad, H., Alaas, Z., Ahmed, M.M.R.: Cybersecurity in microgrids: A review on advanced techniques and practical implementation of resilient energy systems. *Energy Strategy Reviews*, 58, 101654, 2025, <https://doi.org/10.1016/j.esr.2025.101654>.
21. Yan, Y., Kunhui, Y.: Novel cyber-physical architecture for optimal operation of renewable-based smart city considering false data injection attacks: Digital twin technologies for smart city infrastructure management. *Sustainable Energy Technologies and Assessments*, 65, 103733, 2024, <https://doi.org/10.1016/j.seta.2024.103733>.
22. Zhang, J., Li, H., Kong, X., Zhou, J., Shi, G., Zang, J., Wang, J.: A novel multiple-medium-AC-port power electronic transformer. *IEEE Transactions on Industrial Electronics*, 71(7), 6568-6578, 2024, <https://doi.org/10.1109/TIE.2023.3301550>.
23. Ma, K., Yang, J., Liu, P.: Relaying-assisted communications for demand response in smart grid: Cost modeling, game strategies, and algorithms. *IEEE Journal on Selected Areas in Communications*, 38(1), 48-60, 2020, <https://doi.org/10.1109/JSAC.2019.2951972>.
24. Shi, L., Dai, Q., Ni, Y.: Cyber–physical interactions in power systems: A review of models, methods, and applications. *Electric Power Systems Research*, 163, Part A, 396-412, 2018, <https://doi.org/10.1016/j.epsr.2018.07.015>.
25. Solat, A., Gharehpetian, G.B., Naderi, M. S., Anvari-Moghaddam, A.: On the control of microgrids against cyber-attacks: A review of methods and applications. *Applied Energy*, 353, Part A, 122037, 2024, <https://doi.org/10.1016/j.apenergy.2023.122037>.
26. Sanchez, H.S., Rotondo, D., Escobet, T., Puig, V., Quevedo, J.: Bibliographical review on cyber attacks from a control oriented perspective. *Annual Reviews in Control*, 48, 103-128, 2019, <https://doi.org/10.1016/j.arcontrol.2019.08.002>.
27. Kumar, A., Singh, A.R., Raghav, L.P., Deng, Y., He, X., Bansal, R.C., Kumar, P., Naidoo, R.M.: State-of-the-art review on energy sharing and trading of resilient multi microgrids. *iScience*, 27(4), 109549, 2024, [https://www.cell.com/iscience/fulltext/S2589-0042\(24\)00771-5](https://www.cell.com/iscience/fulltext/S2589-0042(24)00771-5).
28. Li, L., Sun, Y., Han, Y., Chen, W.: Seasonal hydrogen energy storage sizing: Two-stage economic-safety optimization for integrated energy

- systems in northwest China. *iScience*, 27(9), 110691, 2024, [https://www.cell.com/iscience/fulltext/S2589-0042\(24\)01916-3](https://www.cell.com/iscience/fulltext/S2589-0042(24)01916-3).
29. Zhang, H., Yu, C., Zeng, M., Ye, T., Yue, D., Dou, C., Xie, X., Hancke, G.P.: Homomorphic encryption-based resilient distributed energy management under cyber-attack of micro-grid with event-triggered mechanism. *IEEE Transactions on Smart Grid*, 15(5), 5115-5126, 2024, <https://doi.org/10.1109/TSG.2024.3390108>.
30. AlHidaifi, S.M., Asghar, M.R., Ansari, I.S.: A survey on cyber resilience: Key strategies, research challenges, and future directions. *ACM Computing Surveys*, 56(8), 1-48, 2024, <https://doi.org/10.1145/3649218>.
31. Zografopoulos, I., Hatziaargyriou, N.D., Konstantinou, C.: Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. *IEEE Systems Journal*, 17(4), 6695-6709, 2023, <https://doi.org/10.1109/JSYST.2023.3305757>.
32. Shafei, H., Li, L., Aguilera, R.P.: A comprehensive review on cyber-attack detection and control of microgrid systems. In: Haes Alhelou, H., Hatziaargyriou, N., Dong, Z.Y. (eds) *Power Systems Cybersecurity*. Power Systems, 1-45, 2023, https://doi.org/10.1007/978-3-031-20360-2_1.
33. Ahmad, H., Gulzar, M.M., Aziz, S., Habib, S., Ahmed, I.: AI-based anomaly identification techniques for vehicles communication protocol systems: Comprehensive investigation, research opportunities and challenges. *Internet of Things*, 27, 101245, 2024, <https://doi.org/10.1016/j.iot.2024.101245>.
34. Jamil, N., Qassim, Q. S., Bohani, F. A., Mansor, M., Ramachandaramurthy, V. K.: Cybersecurity of microgrid: State-of-the-art review and possible directions of future research. *Applied Sciences*, 11(21), 9812, 2021, <https://doi.org/10.3390/app11219812>.
35. Martinez-Martinez, J., Carvajal-Jimenez, C., Aponte-Roa, D.A.: A secured IoT scheme for microgrids monitoring. In *10th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2020, pp. 0986-0990, <https://doi.org/10.1109/CCWC47524.2020.9031280>.
36. Khalaf, M., Ayad, A., Tushar, M.H.K., Kassouf, M., Kundur, D.: A survey on cyber-physical security of active distribution networks in smart

- grids. IEEE Access, 12, 29414-29444, 2024, <https://doi.org/10.1109/ACCESS.2024.3364362>.
37. Mustafa, F.E, Ahmed, I., Basit, A., Alvi, U.-E-H., Malik, S.H., Mahmood, A., Ali, P.R.: A review on effective alarm management systems for industrial process control: Barriers and opportunities. International Journal of Critical Infrastructure Protection, 41, 100599, 2023, <https://doi.org/10.1016/j.ijcip.2023.100599>.
38. Sangoleye, F., Johnson, J., Chavez, A., Tsiropoulou, E.E., Marton, N.L., Hentz, C.R., Yannarelli, A.: Networked microgrid cybersecurity architecture design guide: A New Jersey TRANSITGRID Use Case. 2022, <https://doi.org/10.2172/1900087>.
39. Yoshinov, R., Iliev, O.: Sharing local resources within a community by enhancing the potential of Eduroam and EduVPN with mobile application for remote and local resources and through secure user identification over the network (MARLIN). Problems of Engineering Cybernetics and Robotics, 79, 3-36, 2023, <https://doi.org/10.7546/PECR.79.23.01>.

8. Тестове, оценка и анализ на риска в интелигентни мрежи

В съвременните интелигентни мрежи, управлявани от модерни компютърни и мрежови технологии, мониторингът на състоянието разчита на сигурна киберфизична свързаност. Трудно е да се оцени рискът за киберсигурността на интелигентните мрежи поради огромното разнообразие от информационни и комуникационни технологии, които могат да се използват за постигане на широк набор от задачи. Оценка на уязвимостта и анализът на риска са два свързани, но различни процеса, които често се използват в областта на киберсигурността за идентифициране на потенциални заплахи и уязвимости в компютърни системи, мрежи и други цифрови активи. Поради това, изследователи от цял свят полагат огромни усилия за изучаване на микромрежи и за изграждане на тестови полигони и демонстрационни площадки [1, 2].

8.1. Тестове за микромрежи

В условията на нарастващи кибератаки, устойчивите микромрежи са от съществено значение за повишаване на стабилността, надеждността и сигурността на съвременните енергоразпределителни мрежи. Поради това планирането и провеждането на тестове са дейности, които не трябва да се negliжират. Платформите за тестване на микромрежите предоставят реалистична и контролирана експериментална среда за симулиране на реални оперативни сценарии и оценка на реакцията на тези системи при различни условия [3, 4, 5]. От гледна точка на киберсигурността, тези платформи осигуряват сигурна среда за идентифициране на потенциални пътища за атака, уязвимости и защитни стратегии [6, 7].

Платформите за тестване на микромрежите базирани на симулация, са от особено важна важност за определяне дали възможността за генериране на енергия от микромрежата е достатъчна, за да отговорят ефективно на изискванията за натоварване [5]. Тези платформи позволяват на изследователите да моделират различни оперативни сценарии, което позволява идентифицирането на потенциални слабости в микромрежовите системи. Някои често срещани софтуерни тестови платформи за микромрежи са:

- Компютърно проектиране на енергийни системи. Това е симулационен инструмент за управление на силова електроника, динамично поведение на енергийните системи и анализ на преходни процеси [8].

- MATLAB/Simulink – една от най-известните симулационни тестови среди. Интегрирането на хардуер от индустриален клас в тестовата платформа позволява пълна емуляция на работата на микромрежата и улеснява изучаването на ефектите на шума от измерванията, закъсненията при семплиране и комуникация [9]. Процесът на предаване на режими на микромрежата може да се наблюдава чрез комуникациите между емулятори в реално време и Simulink [10]. Приложимостта е описана в [11], където изследователи са постигнали оптимално разпределение на мощността микромрежи, контролирани от Simulink и dSPACE.

- DER-CAM (Distributed Energy Resources Customer Adoption Model – Модел за приемане от клиенти на разпределени енергийни ресурси). Като симулатор на решения, използван за икономично диспечерско управление, DER-CAM осигурява ефективно използване на енергийните ресурси. Въз основа на разходите за поддръжка, кривите на натоварване, разходите за енергия и местни типологии, изследователи провеждат проучвания за осъществимост на внедряването на микромрежи [12].

Предимството на симулационно-базираните тестови платформи за микромрежи е, факта че те са способни да тестват раз-

лични сценарии с минимални разходи и без рискове за безопасността. Ограниченията на симулационно-базираните тестови платформи обаче включват неспособността им да възпроизведат напълно сложността и непредсказуемостта на реалните среди. Фактори като внезапни промени в натоварванията, повреди на оборудването и кибератаки могат да бъдат трудни за точно моделиране, което води до пропуски в тяхната приложимост към реални микромрежови операции [13].

Друга технология за тестване работоспособността и сигурността на микромрежите е цифровият близък знак. Цифровият близък знак е технология, която отразява състоянието, поведението и динамиката на физическите системи в реално време чрез виртуални модели [14]. Цифровите близнаци се използват за подпомагане на мониторинга, симулацията, оптимизирането на производителността и вземането на решения на сложни системи. Физическите тестови платформи за микромрежи често са персонализирани, скъпи и ограничени до локална употреба. Цифровите близнаци имат потенциала да подобрят симулирани и хардуерно свързани тестови платформи за микромрежи след достатъчно тестване на физически тестови платформи за микромрежи [15].

Цифровите близнаци имат потенциала да подобрят тестовите платформи на микромрежите, като подкрепят изследователите при моделирането на сложни и динамични сценарии за кибератаки. За разлика от традиционните симулирани тестови платформи, цифровите близнаци са способни непрекъснато да отразяват състоянието на микромрежата в реално време, като по този начин поддържат адаптивно тестване на киберсигурността, което се развива заедно с поведението на системата [16]. Тази възможност е особено важна в сценарии, при които киберфизическите взаимодействия и техните въздействия в реално време са от решаващо значение за разбирането на уязвимостите и проектирането на ефективни контрамерки в микромрежовите системи.

Чрез първоначално свързване на дигиталния близък към физическа тестова среда на микромрежа, той може точно да възпроизведе динамиката на системата и да валидира надеждността на нейните операции. След като дигиталният близък бъде напълно тестван, той може да разшири възможностите на тестовите среди на микромрежа, базирани на симулация [17]. Например, дигиталният близък може да симулира мрежов трафик, системни реакции и потенциални вектори на кибератаки, предоставяйки гъвкава платформа за изследване на различни стратегии за киберсигурност, без да се нарушават физическите системи [18].

Внимание заслужават и т. нар. хардуерно свързани тестови стендове за симулация на микромрежи, представляващи симулационни платформи, интегрирани с физически компоненти. Използването на хардуер в тестовите стендове за симулация на микромрежи може да симулира проблемите, срещани от микромрежовите системи в действителност, особено в областта на киберсигурността [19]. Едно от основните предимства на този подход е, че той позволява на изследователите да наблюдават взаимодействията в реално време между симулираните и физическите компоненти, осигурявайки по-точна оценка на производителността и устойчивостта на системата [20]. Въпреки това, създаването и поддръжката на такива тестови платформи може да бъде скъпа поради необходимостта от специализирано оборудване и физическо пространство. Освен това, проблеми със синхронизацията и забавянията в комуникацията ще повлияят на интеграцията на хардуера и софтуера.

8.2. Оценка на уязвимостта на микромрежи

Оценката на уязвимостта включва систематично изследване на система или мрежа за идентифициране на уязвимости, които биха могли да бъдат използвани от нападатели. Това може да включва както автоматизирани, така и ръчни техники като сканиране за отворени портове, анализиране на софтуерни конфигурации и тестване за известни уязвимости в конкретни приложения.

Оценката на уязвимостта в микромрежа включва няколко важни стъпки, за да се гарантира, че микромрежата е сигурна и устойчива. Този процес включва идентифициране на активите и инфраструктурата, които трябва да бъдат оценени, идентифициране на потенциални заплахи, анализиране на уязвимости, оценка на вероятността и въздействието на атака, разработване и прилагане на стратегии за смекчаване и непрекъснато наблюдение и актуализиране на микромрежовата система, за да се гарантира постоянна сигурност и устойчивост. Следвайки тези стъпки, оценката на уязвимостта може да идентифицира потенциални заплахи и уязвимости, да оцени въздействието на атаката и да разработи и приложи ефективни стратегии за смекчаване за защита на микромрежовата система.

На Фиг. 8.1 е показана последователността на основните стъпки за извършване на оценка на уязвимостта в микромрежа [21].



Фиг. 8.1. Основни стъпки за оценка на уязвимостта в микромрежа

1) *Идентифициране на заплахите*: Идентифициране на потенциалните заплахи, които биха могли да засегнат микромрежата като природни бедствия, кибератаки, физически атаки и човешка грешка. Внимателно обмисляне както на вътрешни, така и на външни заплахи.

2) *Анализиране на уязвимостите*: Анализиране на уязвимостите, които идентифицираните заплахи могат да използват. Уязвимостите могат да включват слаби пароли, остарял софтуер, лоша физическа сигурност и недостатъчно резервно хранване.

3) *Определяне на вероятността за атака*: Да се оцени вероятността от възникване на атака, като се анализират потенциалните последствия и мотивите на нападателите.

4) *Оценка на въздействието на атаката*: Да се оцени въздействието на атаката върху микромрежата и последствията за критичната инфраструктура или услуги, които микромрежата поддържа.

5) *Разработване на стратегии за смекчаване*: Разработването на стратегии за справяне с идентифицираните уязвимости може да минимизира въздействието на потенциални атаки. Тези стратегии могат да включват мерки за физическа сигурност, софтуерни актуализации, резервни хранващи системи и планове за действие при извънредни ситуации.

6) *Тестване и валидиране на стратегиите за смекчаване*: Тестването и валидирането ефективността на стратегиите за смекчаване е необходимо, за да се гарантира, че те могат адекватно да защитят микромрежата.

7) *Прилагане на стратегии за смекчаване*: Прилагането на разработените и тествани стратегии за смекчаване заедно с непрекъснато наблюдаване и актуализиране микромрежата ще осигури постоянна сигурност и устойчивост.

8.3. Анализ на риска

Анализът на риска се фокусира върху по-цялостно изследване на потенциалното въздействие на пробив в сигурността, включително вероятността от възникване на атака и потенциалните последици за организацията. Това може да включва оценка на стойността на активите, които биха могли да бъдат компрометирани, разходите за възстановяване и потенциалното въздействие върху репутацията, финансовата стабилност и правната отговорност [22, 23].

В допълнение към оценката на уязвимостта, за да се осигури безопасна и надеждна работа на микромрежите, е от съществено значение да се извърши цялостен анализ на риска, който идентифицира потенциалните опасности, оценява тяхната вероятност и въздействие, приоритизира рисковете, разработва подходящи стратегии за намаляване на риска и наблюдава ефективността на процеса на управление на риска във времето [24, 25]. Оценката на риска е важна част от киберсигурността. Рискът се определя като [26]:

$$Risk = Attack_likelihood \times Possible_Actions \times Consequences$$

Първоначалната стъпка в проверката на риска е идентифицирането на активи за киберсигурност, включително хардуер, мрежови настройки, софтуер и комуникационни протоколи. След това трябва да се използват няколко метода за тестване, за да се открият уязвимости в енергийната система. Оценката на уязвимостта изисква изследване на системи, сценарии и точки за достъп. След откриване на кибернетични уязвимости физическите и приложните слоеве на инфраструктурата на интелигентната мрежа трябва да бъдат оценени за щети от атака. Фалшива кибератака може да бъде стартирана, за да се запишат последствията от атаката, докато се симулира модел в реално време. В различни проучвания се анализират възможните уязвимости на интелигентните мрежи [27, 28, 29, 30]. Други инструменти, които могат да се използват за оценка

на степента на атака, включват системи за откриване на проникване и системи за откриване на аномалии, които откриват необичайна активност.

На Фиг. 8.2 е показана последователността на основните стъпки за извършване на анализ на риска в микромрежа [21].



Фиг. 8.2. Основни стъпки за анализ на риска в микромрежа

Тези основни стъпки включват следните дейности:

1) *Идентифициране на опасностите*: Идентифициране на потенциалните опасности, които могат да повлияят на микромрежата, включително природни бедствия, кибератаки, повреди на оборудването и оперативни грешки.

2) *Оценяване на вероятността*: Оценката на вероятността за възникване на всяка опасност може да се реализира чрез изследване на исторически данни, експертни мнения и друга подходяща информация. Оценките на вероятността могат да бъдат качествени, количествени или и двете.

3) *Оценяване на въздействието*: При оценката на потенциалното въздействие на всяка опасност върху микромрежата могат да се вземат предвид последствията от всяка опасност като повреда на оборудването, загуба на електрозахранване или прекъсване на критични услуги.

4) *Приоритизиране на рисковете*: Приоритизирането на рисковете е добре да се основа на комбинацията от оценката на вероятността и оценката на въздействието. Рисковете с голяма вероятност и силно въздействие обикновено се дават с най-висок приоритет.

5) *Определяне толерантността към риска*: Необходимо е да се установи приемливо ниво на риск за микромрежата въз основа на целите на организацията, регулаторните изисквания и очакванията на заинтересованите страни.

6) *Оценяване на съществуващите контроли*: Задължително е да се оцени ефективността на съществуващите контроли, за да се определи тяхната ефикасност за смекчаване на идентифицираните рискове.

7) *Разработване на стратегии за намаляване на риска*: Наложително е разработване на стратегии за намаляване на риска за справяне с идентифицираните опасности. Тези стратегии трябва да бъдат проектирани така, че да минимизират или елиминират рисковете.

8) *Прилагане на стратегии за намаляване на риска*: Прилагането на мерките за намаляване на риска, посочени в стратегиите за намаляване на риска, ще доведе до намаляване или премахване на идентифицираните рискове.

9) *Проследяване и преглед*: Периодичното преглеждане на процеса на управление на риска и установите показатели ще позволи проследяване на ефективността на мерките и стратегиите за намаляване на риска.

Следвайки тези стъпки, организациите могат ефективно да управляват риска в своите микромрежи и да осигурят непрекъснатост на критичните услуги дори при неочаквани събития.

Библиография

1. Hossain, E., Kabalci, E., Bayindir, R., Perez, R.: Microgrid testbeds around the world: State of art. *Energy Conversion and Management*, 86, 132-153, 2014, <https://doi.org/10.1016/j.enconman.2014.05.012>.
2. Wanik, M.Z.C., Krama, A., Jabbar, A.A., Sanfilippo, A., Satar, S.: Development of microgrid testbed for real desert environment testing and evaluation: project experience. In 22nd Wind and Solar Integration Workshop (WIW 2023), Copenhagen, Denmark, 2023, pp. 295-301, <https://doi.org/10.1049/icp.2023.2751>.
3. Zhang, Z., Turnbull, B., Kermanshahi, S.K., Pota, H., Damiani, E., Yeun, C.Y., Hu, J.: A survey on resilient microgrid system from cybersecurity perspective. *Applied Soft Computing*, 175, 113088, 2025, <https://doi.org/10.1016/j.asoc.2025.113088>.
4. Meje, K.C., Bokopane, L., Kusakana, K.: Microgrids control strategies: A survey of available literature. In International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), Kuching, Malaysia, 2020, 167-173, <https://doi.org/10.1109/ICSGCE49177.2020.9275651>.
5. Sedghisigarchi, K., Sicat, C.: Development of smart microgrid research and educational testbed. In IEEE Conference on Technologies for Sustainability (SusTech), Phoenix, AZ, USA, 2017, 1-6, <https://doi.org/10.1109/SusTech.2017.8333524>.
6. Sarker, P.S., Venkataramanan, V., Cardenas, D.S., Srivastava, A., Hahn, A., Miller, B.: Cyber-physical security and resiliency analysis testbed for critical microgrids with IEEE 2030.5. In 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, Sydney, NSW, Australia, 2020, 1-6, <https://doi.org/10.1109/MSCPES49613.2020.9133689>.
7. Gupta, K., Sahoo, S., Panigrahi, B.K., Blaabjerg, F., Popovski, P.: On the assessment of cyber risks and attack surfaces in a real-time co-simulation cybersecurity testbed for inverter-based microgrids. *Energies*, 14, 4941, 2021, <https://doi.org/10.3390/en14164941>.
8. Ashok Kumar, L., Indragandhi, V., Uma Maheswari, Y.: Chapter 8 - Introduction to Power Systems Computer-Aided Design. Editor(s): Ashok Kumar L., Indragandhi V., Uma Maheswari Y., Software Tools for the Simulation of Electrical Systems, Academic Press, 287-347, 2020, <https://doi.org/10.1016/B978-0-12-819416-4.00008-9>.

9. Tu, H., Du, Y., Yu, H., Lukic, S., Metelko, M., Volgyesi, P., Dubey, A., Karsai, G.: A hardware-in-the-loop real-time testbed for microgrid hierarchical control. In IEEE Energy Conversion Congress and Exposition (ECCE), Portland, OR, USA, 2018, 2053-2059, <https://doi.org/10.1109/ECCE.2018.8557737>.
10. Lu, L.-Y., Liu, J.-H.H., Chu, C.-C.: Distributed real-time simulation and on-site development of a micro-grid with renewable energy sources. In IEEE Power and Energy Society General Meeting, San Diego, CA, USA, 2012, 1-7, <https://doi.org/10.1109/PESGM.2012.6345607>.
11. Meng, L., Savaghebi, M., Andrade, F., Vasquez, J.C., Guerrero, J.M., Graells, M.: Microgrid central controller development and hierarchical control implementation in the intelligent microgrid lab of Aalborg University. In IEEE Applied Power Electronics Conference and Exposition (APEC), Charlotte, NC, USA, 2015, 2585-2592, <https://doi.org/10.1109/APEC.2015.7104716>.
12. Essiet, I.O., Sun, Y., Wang, Z.: Analysis of the effect of parameter variation on a dynamic cost function for distributed energy resources: A DER-CAM case study. Applied Sciences, 8, 884, 2018, <https://doi.org/10.3390/app8060884>.
13. Prabaakaran, K., Chitra, N., Kumar, A.S.: Power quality enhancement in microgrid – A survey. In International Conference on Circuits, Power and Computing Technologies (ICCPCT), Nagercoil, India, 2013, 126-131, <https://doi.org/10.1109/ICCPCT.2013.6528830>.
14. Yu, W., Patros, P., Young, B., Klinac, E., Walmsley, T. G.: Energy digital twin technology for industrial energy management: Classification, challenges and future. Renewable and Sustainable Energy Reviews, 161, 112407, 2022, <https://doi.org/10.1016/j.rser.2022.112407>.
15. Bazmohammadi, N., Madary, A., Vasquez, J. C., Mohammadi, H. B., Khan, B., Wu, Y., Guerrero, J.M.: Microgrid digital twins: Concepts, applications, and future trends. IEEE Access, 10, 2284-2302, 2021, <https://doi.org/10.1109/ACCESS.2021.3138990>.
16. Saad, A., Faddel, S., Youssef, T., Mohammed, O.A.: On the implementation of IoT-based digital twin for networked microgrids resiliency against cyber attacks. IEEE Transactions on Smart Grid, 11(6), 5138-5150, 2020, <https://doi.org/10.1109/TSG.2020.3000958>.

17. Kandasamy, N.K., Venugopalan, S., Wong, T.K., Leu, N.J.: An electric power digital twin for cyber security testing, research and education. *Computers and Electrical Engineering*, 101, 108061, 2022, <https://doi.org/10.1016/j.compeleceng.2022.108061>.
18. Shen, Z., Arrano-Vargas, F., Konstantinou, G.: Virtual testbed for development and evaluation of power system digital twins and their applications. *Sustainable Energy, Grids and Networks*, 38, 101331, 2024, <https://doi.org/10.1016/j.segan.2024.101331>.
19. Xiao, B., Starke, M., Liu, G., Ollis, B., Irminger, P., Dimitrovski, A., Prabakar, K., Dowling, K., Xu, Y.: Development of hardware-in-the-loop microgrid testbed. In 2015 IEEE Energy Conversion Congress and Exposition (ECCE), Montreal, QC, Canada, 2015, pp. 1196-1202, <https://doi.org/10.1109/ECCE.2015.7309827>.
20. Zhang, Z., Hu, J., Pota, H., Kermanshahi, S.K., Turnbull, B., Damiani, E., Yeun, C.Y.: Experimental demonstration of risks and influences of cyber attacks on wireless communication in microgrids. In 21st Annual International Conference on Privacy, Security and Trust (PST), Sydney, Australia, 2024, pp. 1-5, <https://doi.org/10.1109/PST62714.2024.10788082>.
21. Irmak, E., Kabalci, E., Kabalci, Y.: Cybersecurity in microgrids. *Encyclopedia*. Available online: <https://encyclopedia.pub/entry/45967>. (accessed on 17 April 2025).
22. Luo, J., Li, H., Wang, S.: A quantitative approach and simplified generic transient motor startup power models for microgrids security assessment. *Sustainable Cities and Society*, 83, 103998, 2022, <https://doi.org/10.1016/j.scs.2022.103998>.
23. Mishra, S., Anderson, K., Miller, B., Boyer, K., Warren, A.: Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies. *Applied Energy*, 264, 114726, 2020, <https://doi.org/10.1016/j.apenergy.2020.114726>.
24. Peng, H., Su, M., Li, S., Li, C.: Static security risk assessment for islanded hybrid AC/DC microgrid. *IEEE Access*, 7, 37545-37554, 2019, <https://doi.org/10.1109/ACCESS.2019.2899347>.
25. Colorado, P.J., Suppioni, V.P., Filho, A.J.S., Salles, M.B.C., Grilo-Pavani, A.P.: Security assessment for the Islanding Transition of Microgrids.

- IEEE Access, 10, 17189-17200, 2022, <https://doi.org/10.1109/ACCESS.2022.3150331>.
26. Banik, S., Banik, T.: Survey on simulation and vulnerability testing in smart grid. Preprints, 2024020047, 2024, <https://doi.org/10.20944/preprints202402.0047.v1>.
27. Sun, C.-C., Liu, C.-C., Xie, J.: Cyber-physical system security of a power grid: State-of-the-art. Electronics, 5, 40, 2016, <https://doi.org/10.3390/electronics5030040>.
28. Paul, B., Sarker, A., Abhi, S.H., Das, S.K., Ali, Md.F., Islam, Md M., Islam, Md. R., Moyeen, S.I., Badal, Md. F.R., Ahamed, Md. H., Sarker, S.K., Das, P., Hasan, Md. M., Saqib, N.: Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies. Heliyon, 10(19), e37980, 2024, <https://doi.org/10.1016/j.heliyon.2024.e37980>.
29. Alonso, M., Turanzas, J., Amaris, H., Ledo, A.T.: Cyber-physical vulnerability assessment in smart grids based on multilayer complex networks. Sensors, 21, 5826, 2021, <https://doi.org/10.3390/s21175826>.
30. Borenus, S., Gopalakrishnan, P., Bertling Tjernberg, L., Kantola, R.: Expert-guided security risk assessment of evolving power grids. Energies, 15, 3237, 2022, <https://doi.org/10.3390/en15093237>.

9. Роля на машинното обучение за осигуряване киберсигурността на микромрежите

Осигуряването на киберсигурността на микромрежите става все по-важно, особено в контекста на нарастващата дигитализация на енергийните системи. Важна роля при осигуряване киберсигурността на микромрежите играе машинното обучение, като предоставя нови методи за откриване, предотвратяване и реакция на киберзаплахи.

9.1. Машинно обучение в помощ на киберсигурността на микромрежите

Киберсигурността на микромрежите може да бъде подобрена чрез използването на алгоритми за машинно обучение. Чрез анализиране на мрежовите данни могат да се идентифицират аномалии на база на които да се предприемат подходящи мерки за предотвратяване или смекчаване на последствията от кибератака. Машинното обучение прави киберсигурността на микромрежата проста, ефективна и рентабилна. Едно цялостно проучване на методи, решения и перспективи на машинно обучение при киберсигурност в интелигентни мрежи е представено в [1]. Три са основните стъпки, последвани от машинното обучение за откриване на атака в микромрежата: предварителна обработка на данни, процес на обучение и процес на откриване.

- **Предварителната обработка на данни** е необходима задача за почистване на данните и превръщането им в подходящи за модел на машинно обучение, което допринася за повишаване точността и ефективността на модела на машинно обучение. Тя включва: получаване на набора от данни; импортиране на библиотеки; импортиране на набори от данни; намиране на липсващи данни; кодиране на категорични данни; разделяне на набор от данни на набор за обучение и тест; мащабиране на функции. Често

използвани техники за предварителна обработка са AutoEncoders (AE), Singular Value Decomposition (SVD) и Principal Component Analysis (PCA). AutoEncoder е вид изкуствена невронна мрежа, която се научава да представя данни в компресирана форма и след това ги реконструира възможно най-близо до оригиналния вход [2].

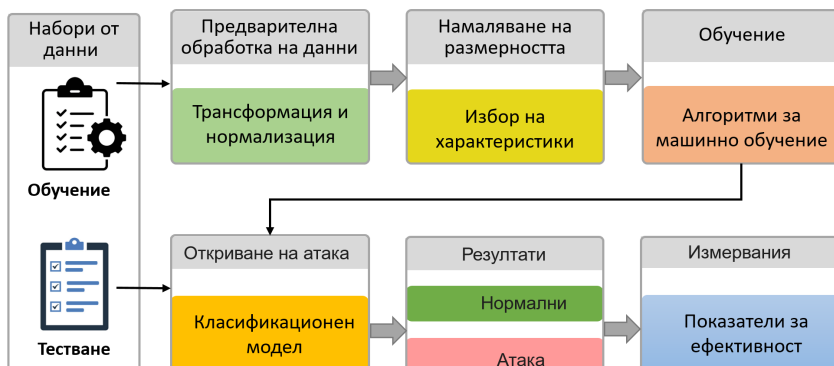
В машинното обучение SVD се дава възможност за опростяване на сложни набори от данни чрез: (1) Намаляване на размерността при запазване на ключова информация; (2) Подобряване на производителността на модела чрез премахване на шума; (3) Улесняване на компресирането на данни за ефективно съхранение [3]. Principal Component Analysis е популярна техника, използвана за намаляване на размерността и трансформиране на голям набор от променливи в по-малък набор, като същевременно се запазва възможно най-много информация.

- **Процесът на обучение и валидиране** при машинното обучение на модел за откриване на атака зависи от наличието на етикет, наличността на данни и отклонението на данните. Наличието на етикети в данните за обучение е необходимо, за да се гарантира дали се използва контролирано, неконтролирано, или укрепващо обучение. При контролирано обучение се предоставят извадкови етикетирани данни за обучение на модела на атака. При неконтролирано обучение данните не се етикетират, класифицират или категоризират и алгоритъмът действа върху данните без никакъв надзор. Неконтролираното обучение открива скрити модели и структури в немаркирани данни, като определя приликите между набор от немаркирани входни данни чрез групиране на примерни данни в различни групи въз основа на приликите между тях [4].

Обучението с подсилване е метод на обучение, базиран на обратна връзка, при който моделът на атака се учи от обратната връзка въз основа на своите предишни отговори и подобрява своята производителност. Типът обучение се решава въз основа на наличието на етикети, обема на данните и балансирането на класове.

Данните за обучение се считат за пълни, когато са налични всички необходими модели. Ако данните са пълни и всички необходими модели в данните са балансирани, тогава може да се приложи подходяща техника на машинно обучение. Ако данните са непълни, се препоръчва да се използва увеличаване на данните или адаптиране на домейна, за да се осигурят значими проби [5].

- **Процес на откриване.** Техниките на машинното обучение при откриване на атаки се могат да се използват за три основни дейности: (1) откриване на атаки, (2) класификация на атаки и (3) анализ на атаките. Данните за обучение преминават през серия от предварителни процеси, преди да бъдат използвани в обучението на модела. Тези операции се състоят от трансформации на данни и нормализиране. Процесът на намаляване на размерите е от решаващо значение за увеличаване на производителността на модела от тези конвертирани данни. За този процес се използват статистически методи за намаляване на измерението или алгоритми за избор на характеристики. След обучението на модела се открива атака с тестови данни. Успехът на модела се оценява с различни показатели за ефективност чрез сравняване на прогнозни резултати с действителни резултати. Диаграмата на тези етапи е показана на Фиг. 9.1 [6].



Фиг. 9.1. Блок-схема за откриване на атаки

Успехът на модела също зависи от хиперпараметрите на избора алгоритъм за машинно обучение, независимо от набора от данни. Възможно е да се използват различни оптимизационни алгоритми за определяне на оптималните стойности на тези параметри. Някои типични примери за това как се използват алгоритми за машинно обучение в киберсигурността са показани в Таблица 9.1.

Таблица 9.1. Приложение на някои алгоритми за машинно обучение в киберсигурността

Алгоритъм	Приложение
Decision tree algorithm	Откриване и класифициране на атаки
Dimensionality reduction algorithms	Премахване на шумни и неподходящи данни
K-means clustering	Откриване на зловреден софтуер
K-nearest neighbors classifier (kNN)	Лицево разпознаване, използвано за удостоверяване
Linear regression	Прогнозиране на резултатите за сигурността на мрежата
Logistic regression	Откриване на измами
Naive Bayes algorithm	Откриване на проникване
Random forest algorithm	Класифициране на фишинг атаки
Support Vector Machine (SVM) algorithm	Класифициране, откриване и прогнозиране на IP адреси и адреси на портове в черен списък

9.2. Системи за откриване и предотвратяване на проникване

Системите за откриване на проникване (Intrusion Detection System – IDS) имат за цел да одитират и анализират събития, свързани със сигурността, за да идентифицират потенциално злонамерени дейности. Те действат като линия на защита чрез подобряване на механизма за криптиране и оторизация в комуникационна мрежа.

Има много различни класификации на системи за откриване на проникване [7]. Най-често срещаните класификации са показани в Таблица 9.2.

Системите за откриване на проникване се основат на две основни методологии:

- *Откриване, базирано на сигнатура*: Първият подход, който е доста ефективен, е откриване, базирано на сигнатура, при което действителните данни се проверяват спрямо база данни, съдържаща сигнатури на известни модели на атака. Той идентифицира прилика и изпраща сигнал за подозрение, че може да има инцидент със сигурността.
- *Откриване въз основа на аномалия*: По този начин, с откриване въз основа на аномалия, потребителят трябва да определи какво ще се счита за типично възникващо поведение в мрежа или система. Всичко, което се отклонява от тази норма, се превръща в аномалия и може да се счита за основание за вероятна заплаха за сигурността. Подобен подход може дори да помогне при откриването на неразпознати вражески удари, което го прави много полезен.

Таблица 9.2. Класификации на системи за откриване на проникване

Тип IDS	Описание	Случай на използване	Ползи	Предизвикателства
Мрежово базирана IDS (NIDS)	Следи мрежовия трафик за подозрителна дейност чрез анализиране на пакети.	Използват се в мрежови периметри или критични сегменти за откриване на атаки като сканиране на портове и DDoS.	Осигурява широка видимост на мрежата и може да открие широк спектър от мрежови атаки.	Може да бъде претоварен от голям обем трафик и може да пропусне криптиран трафик.
Хост-базирана IDS (HIDS)	Наблюдава изчислителната система – системни файлове и файлове с логове на приложенията.	Инсталирани на отделни устройства или сървъри за откриване на аномалии и неоторизиран достъп.	Осигурява подробен мониторинг на отделни хостове и може да открива локални атаки.	Ресурсно интензивен и може да бъде компрометиран, ако хостът е компрометиран.
IDS, базирана на подпис	Използва предварително дефинирани модели на атака	Ефективен за откриване на известни заплахи с установени сигнатури.	Точен за известни заплахи, с ниски фалшиво положителни резултати за	Не може да открие нови или неизвестни заплахи без предварително съществуващи сигнатури.

Тип IDS	Описание	Случай на използване	Ползи	Предизвикателства
	(сигнатури) за идентифициране на потенциални заплахи.		разпознати подписи.	
IDS базирана на аномалии	Открива отклонения от нормалното поведение, за да идентифицира потенциални заплахи.	Ефективен за идентифициране на неизвестни заплахи чрез наблюдение за необичайни дейности.	Може да открива нови атаки и експлойти от нулев ден чрез идентифициране на аномалии.	По-висок процент фалшиво положителни резултати поради трудност при определяне на „нормалното“ поведение.

Решенията на системите за откриване на проникване и системите за откриване и предотвратяване на проникване (Intrusion Detection and Prevention System – IDPS) използват комбинация от базирани на подписи и базирани на аномалии техники за откриване, за да анализират мрежовия трафик и системните дейности. Ето как работят:

- *Откриване на базата на сигнатура:* IDS/IDPS системите поддържат база данни с известни модели на атака или сигнатури, които се сравняват с входящия мрежов трафик или системни събития. Ако бъде намерено съвпадение, се генерира предупреждение, което показва потенциално проникване или заплаха за сигурността.
- *Откриване на базата на аномалии:* Тези системи установяват базова линия на нормално поведение на мрежата и системата във времето. Отклоненията от тази базова линия се маркират като потенциални аномалии. Базираното на аномалии откриване е ефективно при идентифициране на неизвестни преди това заплахи или атаки, които нямат известни сигнатури.
- *Мониторинг в реално време:* IDS/IDPS решенията непрекъснато наблюдават мрежовия трафик, търсейки модели или дейности, които съответстват на известни сигнатури на атака или се отклоняват значително от установената норма.
- *Предупреждение и докладване:* Когато бъде открита подозрителна или злонамерена дейност, IDS/IDPS системите генерират предупреждения, които могат да включват подробности за откритата заплаха, нейната сериозност и засегнатата система или мрежов сегмент. Тези сигнали се изпращат до персонала по сигурността или се интегрират със системите за управление на информация за сигурността и събития за допълнителен анализ и реакция.

- *Механизми за реагиране:* В допълнение към откриването, IDPS решенията имат способността да предприемат автоматизирани действия за блокиране или смекчаване на открити заплахи в реално време. Този проактивен подход помага за предотвратяване на потенциални пробиви в сигурността.

Процесът на анализ и вземане на решения в системите за откриване на проникване се реализира чрез следната последователност от действия:

- *Анализ в реално време:* Непрекъснати процес на оценка на входящите данни в реално време чрез използване на определени техники за откриване се нарича система за откриване на проникване (IDS). Бързото идентифициране и реакция на заплахи изискват анализ в реално време.
- *Генериране на предупреждение:* Когато IDS открие подозрителни дейности се генерират предупреждения, които се изпращат на екипите за киберсигурност. Тези сигнали предоставят жизненоважна информация за естеството на заплахата, което позволява на специалистите по сигурността да направят допълнителни разследвания.
- *Корелация на предупреждения:* Тези сложни системи могат да съпоставят предупреждението, за да генерират цялостна картина на възможни пробиви в сигурността. Корелацията намалява появата на някои фалшиви положителни и някои фалшиви отрицателни резултати, като включва разглеждане на това как една дейност е свързана с друга дейност.

Внедряването на IDPS с помощта на конвенционални техники е неефективно при справяне с нарастващите предизвикателства пред сигурността. Прилагането на техники за машинно обучение е ефективно за намаляване на измеренията и задачите за класификация. Системите за откриване и предотвратяване на проникване, базирани на машинно обучение, се учат от исторически данни за

трафика, състоящи се от нормален и необичаен трафик. Тези системи намаляват сложността на мрежовия трафик, за да намерят корелации между данните. Те откриват атаки от нулевия ден и сложни модели на атаки, като се учат от тренировъчни проби и изграждат модел за откриване. Системите за откриване и предотвратяване на проникване, базирани на машинно обучение, могат да се използват за справяне с динамичен мрежов трафик и непрекъсната промяна в условията на атака. Често използваният алгоритъм на машинно обучение за този вид системи е генетичният алгоритъм, размитата логика, изкуствените невронни мрежи и SVM.

9.3. Глобални решения за защита от кибератаки

Повечето методи за киберсигурност са пригодени за специфични компоненти на възобновяемите интелигентни микромрежи, с присъщи ограничения. Например IEC62351 се фокусира върху комуникационната сигурност и му липсват решения за защита на вградени устройства [8]. За да се справят с глобалните предизвикателства пред киберсигурността, изследователите са разработили базирани на модели и без модели методи за откриване и предотвратяване на проникване, базирани на изкуствен интелект и машинно обучение [8, 9, 10, 11]. При подходите, базирани на модели, кибератаките се откриват с помощта на активни детерминистични методи (като техники, базирани на наблюдател) и стохастични методи (като филтри на Калман), като се използва динамиката на системата и математическите модели [12]. Нека е даден модел на пространството на състоянието на система по следния начин [13]:

$$x_s(t) = A_s x_s(t) + B_s u_s(t) + \theta_{x_s}(t)$$

$$y_s(t) = C_s x_s(t) + D_s u_s(t) + \theta_{y_s}(t)$$

където $A_s, B_s, C_s, D_s, u_{s,i}, y_{s,i}$ са матрици на системата, респективно входи и изходи на системата. Неопределеностите на системата (неопределеност на параметрите, шумове от измерване и т.н.) се

моделират от $\theta_{xs}(t)$ и $\theta_{ys}(t)$. При кибератаката целта на нападателите е да манипулират измерените и предавани данни и следователно моделът се трансформира чрез следното представяне:

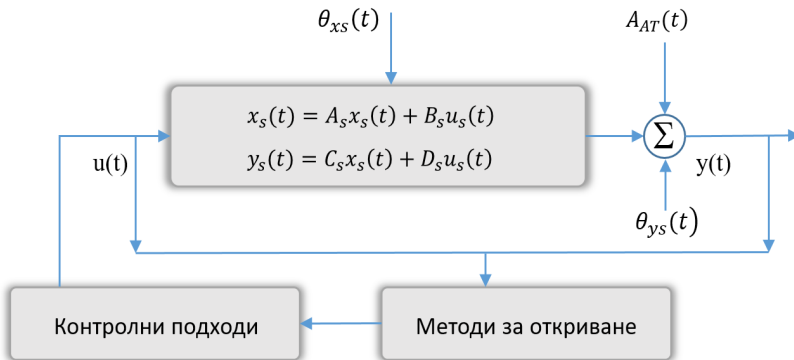
$$x_s(t) = A_s x_s(t) + B_s u_s(t) + \theta_{xs}(t)$$

$$y_s(t) = C_s x_s(t) + D_s u_s(t) + \theta_{ys}(t) + E_{AT} A_{AT}(t)$$

където E_{AT} е матрицата на атаката. Тя показва кой системен изход или кой сензор е атакуван, ако всички сензори или всички изходи са уязвими от кибератака, E_{AT} ще бъде равна на матрицата на идентичността. $A_{AT}(t)$ е моделът на кибератаката.

След откриване на атака, контролните подходи са приложими методи за нейното отстраняване [14].

На Фиг. 9.2 е показан концептуален модел, илюстриращ откриване и отхвърляне на атака чрез обсъждания метод.

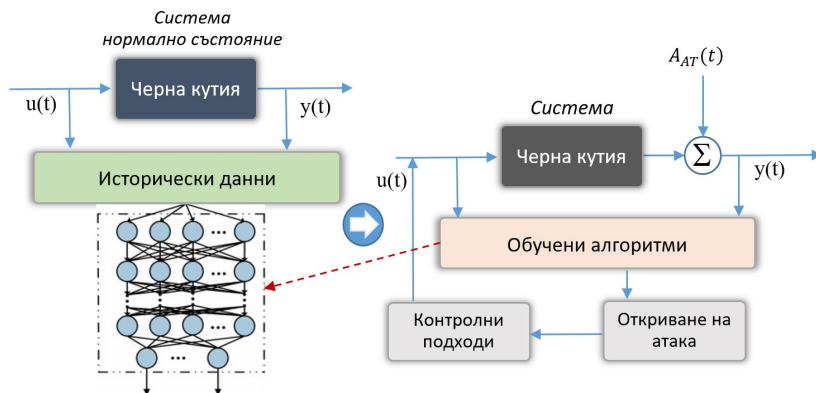


Фиг. 9.2. Концептуален изглед на откриване и отхвърляне на атака в базиран на модел метод

Основният принцип на тези методи включва сравняване на измерените данни с приблизителните данни. Основните предизвикателства, пред които са изправени, включват несигурност на модела и шум при измерване. Следователно, за да се осигури надеждна производителност, тези методи за откриване трябва да са ус-

тойчиви на несигурност в моделите и шум в измерванията. Разработени са методи за идентификация на системи за моделиране на сложни системи [15]. Въпреки това в случаите, когато системата е много сложна или когато извличането на прецизен математически модел е предизвикателство, се приема подход без модели. Този подход използва исторически данни (както входни, така и изходни данни) на системата за обучение на алгоритми за изкуствен интелект или машинно обучение за откриване на проникване [16, 17, 18]. След като бъде открита кибератака, предотвратяването и смекчаването могат да бъдат постигнати чрез стратегии за контрол или други превантивни мерки.

На Фиг. 9.3 е показана концептуална сехама за откриване и предотвратяване на атаки в моделно базирани методи.



Фиг. 9.3. Концептуална схема за откриване на атака

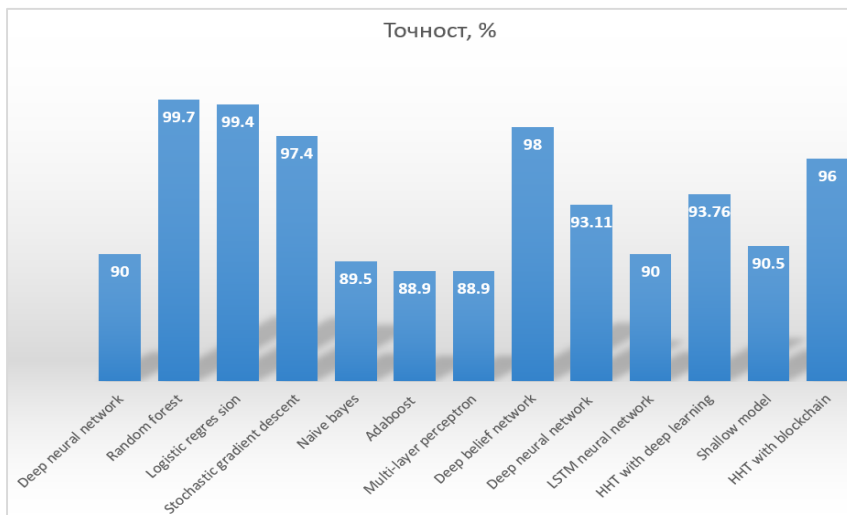
Първоначалната стъпка в тези методологии включва събиране на данни и предварителна обработка, за да се гарантира надеждността и уместността на историческите данни. Този процес включва обработка на проблеми като липсващи стойности, намаляване на шума и адресиране на отклонения, които биха могли да повлияят на точността на анализа. След като данните бъдат събрани и изчистени, следващата критична стъпка е изборът на функция. Това има за цел да идентифицира ключови променливи, които

са от съществено значение за откриване на прониквания или необичайни дейности. Експертите със задълбочени познания за поведението на системата определят „прозорец“, представляващ определен брой точки от данни в рамките на определени интервали от време. Използват се различни статистически техники за извличане на характеристики от тези прозорци като корелационен анализ, оценки на скоростта на промяна и изчисления на максимум, минимум, средна стойност, режим, медиана, стандартно отклонение, дисперсия, сумиране и др.

В [19] е представен метод, управляван от данни, за откриване на кибератаки срещу SCADA системи, избирайки статистически данни от всеки прозорец като набор от функции. След което изкуственият интелект/алгоритмите се обучават за откриване на аномалии въз основа на тези функции. Тези алгоритми непрекъснато наблюдават поведението на системата в реално време, откривайки отклонения от избрани характеристики, показващи необичайни условия. Когато бъдат открити необичайни условия, сигналите се генерират незабавно. Тези сигнали позволяват действия за бърза реакция, вариращи от автоматизирани мерки като изолиране на мрежата до ръчна намеса от персонала по киберсигурността.

Чрез интегриране на усъвършенствани техники за откриване със стратегии за проактивен отговор системите могат да подобрят защитата си срещу непрекъснато развиващите се киберзаплахи, гарантирайки устойчивостта и сигурността на наблюдаваните системи.

Точността на някои алгоритми за откриване на кибератаки с изкуствен интелект е показана на Фиг. 9.4 [13].



Фиг. 9.4. Сравнение на точността на някои методи с изкуствен интелект за откриване на кибератаки

Интересно е да се отбележи, че точността на показаните алгоритми варира от 88.9 до 99.7, което е една добра точност.

В Таблица 9.3 са представени някои от най-изследваните подходи в тази област.

Един съществен недостатък на тези методи е тяхната специфичност към определени видове кибератаки: например алгоритмите, предназначени да откриват инжектиране на фалшиви данни, може да не открият атаки със забавяне във времето.

В Таблица 9.4 е показано сравнение между методологиите за откриване на кибератаки, базирани на модел и без модел.

В Таблица 9.5 са представени предимствата и ограниченията на вторичните контролери, използвани в центровете за управление на микромрежи. Въпреки това от гледна точка на киберсигурността тези подходи често са изправени пред критика, че са предназначени да се справят с конкретни видове кибератаки.

Таблица 9.3. Някои подходи за откриване на атаки

Метод за откриване	Предимства	Предизвикателства	Точност
Неизвестни методи за наблюдение на ввеждане [20, 21, 22]	- Възможност за откриване на кибератаки при наличие на неизвестни входове като смущения - Висока точност - Бързо откриване - Няма нужда от набор от данни	- Проблем в шумна среда (остатъчна точност) - Трудно е да се намери точен праг, за да се направи разлика между здрава и недостатъчна продукция и здрав, за да се намери времево забавяне за неговата производителност - Разглежданата система трябва да има определено условие - Трудно справяне с несигурността на модела - Проблем при отделянето на едновременната кибератака от други грешки - Необходимост от точен модел на системата и предизвикателства в многообластната електроенергийна система	висока
Плъзгащ режим на наблюдение [23, 24, 25]	Възможност за едновременно отделяне на кибератаката от другите системни грешки	Проблеми с тракане поради прекъснат режим на управление	висока

Метод за откриване	Предимства	Предизвикателства	Точност
	• Устойчив срещу несигурност на системата, тъй като не се нуждае от точни параметри за превключване в контролера	• Разглежданата система трябва да има определено условие като ранг на системните матрици и наблюдаемост • Контролният сигнал е ограничен и не може да бъде избран висок, в общата версия на SMO високите печалби ще доведат системата до нестабилност и проблеми с бърборенето • Проблеми, свързани с прекъснатата стратегия • Намиране на подходяща хиперповърхност или колектор (плъзгаща се повърхнина)	
Kalman filter [26, 27]	• Устойчив срещу: – процесен шум и шум от измерване	• Повече изчислителни цикли • Висока сложност • Трудни за изпълнение • Необходимост от първоначално условие • Няма строго доказателство, което да гарантира, че оценката се доближава до действителните състояния	добра

Метод за откриване	Предимства	Предизвикателства	Точност
		Трудно се конструират ковариационните и средните матрици в системата за групова мощност поради сложния модел на системата	
Разширено наблюдение на състоянието [28, 29]	- Лесен за конструиране - Лесна реализация и оптимизация	- Не може да разложи смущенията от кибератаки - Високо усилване - Свързан проблем с голямо усилване, като чувствителност към високочестотен шум при измерване.	
- Размито откриване на проникване, - Размит наблюдател [30, 31]	- Базиран на знания - Няма нужда от системно моделиране - Устойчив срещу: смущения; Системна несигурност; Грешка при моделиране поради база без модел	- Необходимост от задълбочено познаване на системата - Проектирането на правилата и членските функции и припокриването за откриване на атаки е предизвикателство - Неспособност да се учат от грешките си - Необходимост от определяне на точен праг	добра

Таблица 9.4. Сравнение между базирано на модел и без модел откриване на кибератаки

Метод		Предимства	Ограничения	Съобразяване
Базиран на модел [32, 33]	• Базиран на наблюдател • Базиран на паритетно уравнение • Въз основа на оценка на параметри	• Устойчив на шум • Бързо откриване • Реализация в реално време • Наблюдаема процедура на метода	• Необходимост от комп-ресирани и точен математически модел • Липса на адаптация към различни кибератаки • Трудни за моделиране сложни широкомащабни системи • Неуспешно откриване на скрити кибератаки, ако нападателите имат повече познания за системата	• Скорост на откриване на атака • Динамична структура на системата • Времетраеност и вариращи параметри
Без модел [34, 35, 36]		• Няма нужда от системен модел • Офлайн обучение • Може да се разработи за откриване на много видове атаки	• Необходимост от исторически данни за бъдещо откриване • Необходимост от голямо количество измерени данни, тяхната наличност и надеждност	• Скорост на откриване на атака • Здраве на всички исторически данни, могат да се използват детектори за лоши данни

Метод	Предимства	Ограничения	Съобразяване
	• Прогноза за бъдещото поведение на системата • Справяне със закъснението, несигурността на параметрите	• Необходимост от метод на обучение под наблюдение – трябва повече време за обучение – проблем в сложната система • Уязвимост на повторна атака • Липса на висока точност при възобновяемите микромрежи поради стохастичния характер на възобновяемите източници на енергия	• Внимание върху преоборудването, тестването, обучението и валидирането • Шум при измерване
Глобално разглеждане	Нежеланието за инсталиране на тези методи поради трафика на данни, допълнителни разходи		

Таблица 9.5. Предимства и ограничения на контролера в микромрежа

Контролер	Предимства	Ограничения
Fuzzy контролер (без модел) [37]	• Базиран на знания • Няма нужда от системно моделиране • Устойчив срещу: – смущения – системна несигурност – грешка при моделиране – нелинейност на системата поради функцията, независима от модела • Добра способност в комбинация с други методи	• Необходимост от задълбочено познаване на системата • Правилният избор на припокриване на функциите на членовете • Автоматичната настройка на правилата и функциите на членовете е предизвикателство • Неспособност да се учат от грешките си, защото са решили въз основа на дефинираните правила • Въпреки че размитите контролери могат да бъдат внедрени в системи в реално време, тяхната производителност може да бъде ограничена от изчислителни закъснения, особено ако правилата и функциите за членство не са оптимизирани. • Неспособност за разграничаване на грешка от кибератака • Липса на адаптация към внезапни промени поради припокриването на функциите на членовете

Контролер	Предимства	Ограничения
Моделно предсказуемо управление [38, 39]	• Удовлетворяване на системните ограничения • Изчисляване на бъдещото поведение на системата • Висока способност за проследяване на справки • Работа с ограничения в нелинейни и променящи се във времето многопроменливи системи	• Необходимост от моделиране на системата за прогнозиране на бъдещото поведение на системата • Сложен алгоритъм, много параметри за проектиране • Проблеми в шумна среда поради използване на шумно измерване • Изискват много изчислително време в сложни системи
Контролер за плъзгащ режим [40, 41, 42, 43]	• Намаляване на поръчката, когато системата е в плъзгащ се режим • Отхвърляне на смущенията • Устойчив срещу: • Външни смущения, вариация на параметрите и несигурност на модела • Бърза динамична реакция • Добра производителност в нелинейни променливи във времето системи	• Проблеми с тракане поради прекъснат режим на управление • Сложни за изпълнение • Висока скорост на въвеждане на контрол • Намаляване на точността с увеличаване на шума • Нуждае се от междинно звено за откриване на кибератаки • Уникалност и ограничена приложимост към системи с висока размерност • Несигурно време за конвергенция, ниска скорост на конвергенция

Контролер	Предимства	Ограничения
	• Закон за държавен контрол	
Активен контрол за отхвърляне на смущения Active Disturbance Rejection Control [24, 30, 44]	• Устойчив срещу: Системна несигурност; Вътрешни и външни смущения • Няма нужда от детайлен модел на системата • Отхвърляне на смущенията • Прост и лесен за конструиране и осъществяване в реално време • Подобряване на преходния отговор	• Зависимост на производителността от дизайна на наблюдателя • Използване на наблюдател на разширено състояние за откриване на грешки и невъзможност за отделяне на грешки от кибератака от други грешки • Естеството на високото усилване на наблюдателя с разширено състояние и свързаните с него проблеми с високото усилване като чувствителност към високочестотен шум при измерване. • Сложни изисквания за настройка и трудности при справяне с нелинейности

Библиография

1. Berghout, T., Benbouzid, M., Muyeen, S.M.: Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. *International Journal of Critical Infrastructure Protection*, 38, 100547, 2022, <https://doi.org/10.1016/j.ijcip.2022.100547>.
2. Berahmand, K., Daneshfar, F., Salehi, E.S., Li, Y., Xu, Y.: Autoencoders and their applications in machine learning: a survey. *Artificial Intelligence Review*, 57, 28, 2024, <https://doi.org/10.1007/s10462-023-10662-6>.
3. Nanga, S., Bawah, A.T., Acquaye, B.A., Billa, M.-I., Baeta, F.D., Odai, N.A., Obeng, S.K., Nsiah, A.D.: Review of dimension reduction methods. *Journal of Data Analysis and Information Processing*, 9, 189-231, 2021, <https://doi.org/10.4236/jdaip.2021.93013>.
4. Yazici, I., Shaye, I., Din, J.: A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems. *Engineering Science and Technology, an International Journal*, 44, 101455, 2023, <https://doi.org/10.1016/j.jestch.2023.101455>.
5. Shakya, A. K., Pillai, G., Chakrabarty, S.: Reinforcement learning algorithms: A brief survey. *Expert Systems with Applications*, 231, 120495, 2023, <https://doi.org/10.1016/j.eswa.2023.120495>.
6. Ahmetoglu, H., Das, R.: A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions. *Internet of Things*, 20, 100615, 2022, <https://doi.org/10.1016/j.iot.2022.100615>.
7. Azeez, N.A., Bada, T.M., Misra, S., Adewumi, A., Van der Vyver, C., Ahuja, R.: Intrusion detection and prevention systems: An updated review. *Advances in Intelligent Systems and Computing*, 1042, 685-696, 2020, https://doi.org/10.1007/978-981-32-9949-8_48.
8. Ustun, T.S., Hussain, S.M.S., Yavuz, L., Onen, A.: Artificial intelligence based intrusion detection system for IEC 61850 sampled values under symmetric and asymmetric faults. *IEEE Access*, 9, 56486-56495, 2021, <https://doi.org/10.1109/Access.2021.3071141>.

9. Ustun, T.S., Hussain, S.M.S., Ulutas, A., Onen, A., Roomi, M.M., Mashima, D.: Machine learning-based intrusion detection for achieving cybersecurity in smart grids using IEC 61850 GOOSE messages. *Symmetry*, 13, 826, 2021, <https://doi.org/10.3390/sym13050826>.
10. Zhu, R., Liu, C.-C., Hong, J., Wang, J.: Intrusion detection against MMS-based measurement attacks at digital substations. *IEEE Access*, 9, 1240-1249, 2021, <https://doi.org/10.1109/ACCESS.2020.3047341>.
11. Mukherjee, D.: Detection of data-driven blind cyber-attacks on smart grid: A deep learning approach. *Sustainable Cities and Society*, 92, 104475, 2023, <https://doi.org/10.1016/j.scs.2023.104475>.
12. Zhang, J., Ye, J., Guo, L.: Model-based cyber-attack detection for voltage source converters in island microgrids. In *IEEE Energy Conversion Congress and Exposition (ECCE)*, Vancouver, BC, Canada, pp. 1413-1418, 2021, <https://doi.org/10.1109/ECCE47101.2021.9595899>.
13. Rouhani, S.H., Su, C.-L., Mobayen, S., Razmjooy, N., Elsisi, M.: Cyber resilience in renewable microgrids: A review of standards, challenges, and solutions. *Energy*, 309, 133081, 2024, <https://doi.org/10.1016/j.energy.2024.133081>.
14. Rouhani, S.H., Mojallali, H., Baghramian, A.: An optimized fuzzy sliding based active disturbance rejection control for simultaneous cyber-attack tolerant and demand response participation program. *International Transactions on Electrical Energy Systems*, 31(12), e13206, 2021, <https://doi.org/10.1002/2050-7038.13206>.
15. Isermann, R., Münchhof, M.: Identification of dynamic systems: an introduction with applications. Springer, 2011, <https://doi.org/10.1007/978-3-540-78879-9>.
16. Tan, S., Guerrero, J.M., Xie, P., Han, R., Vasquez, J.C.: Brief survey on attack detection methods for cyber-physical systems. *IEEE Systems Journal*, 14(4), 5329-5339, 2020, <https://doi.org/10.1109/JSYST.2020.2991258>.
17. Chen, D., Wawrzynski, P., Lv, Z.: Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Society*, 66, 102655, 2021, <https://doi.org/10.1016/j.scs.2020.102655>.
18. Chang, Q., Ma, X., Chen, M., Gao, X., Dehghani, M.: A deep learning based secured energy management framework within a smart island.

- Sustainable Cities and Society, 70, 102938, 2021, <https://doi.org/10.1016/j.scs.2021.102938>.
19. Roy, S.D., Debbarma, S., Guerrero, J.M.: A data-driven algorithm to detect false data injections targeting both frequency regulation and market operation in power systems. International Journal of Electrical Power & Energy Systems, 143, 108409, 2022, <https://doi.org/10.1016/j.ijepes.2022.108409>.
 20. Qi, J., Taha, A.F., Wang, J.: Comparing Kalman filters and observers for power system dynamic state estimation with model uncertainty and malicious cyber attacks. IEEE Access, 6, 77155-77168, 2018, <https://doi.org/10.1109/ACCESS.2018.2876883>.
 21. Ameli, A., Hooshyar, A., El-Saadany, E.F., Youssef, A.M.: Attack detection and identification for automatic generation control systems. IEEE Transactions on Power Systems, 33(5), 4760-4774, 2018, <https://doi.org/10.1109/TPWRS.2018.2810161>.
 22. Ameli, A., Hooshyar, A., Yazdavar, A.H., El-Saadany, E.F., Youssef, A.: Attack detection for load frequency control systems using stochastic unknown input estimators. IEEE Transactions on Information Forensics and Security, 13(10), 2575-2590, 2018, <https://doi.org/10.1109/TIFS.2018.2824253>.
 23. Tan, C.P., Edwards, C.: Sliding mode observers for robust detection and reconstruction of actuator and sensor faults. International Journal of Robust and Nonlinear Control, 13(5), 443-63, 2003, <https://doi.org/10.1002/rnc.723>.
 24. Aly, A.A., The Vu, M., El-Sousy, F.F.M., Alotaibi, A., Mousa, G., Le, D.-N., Mobayen, S.: Fuzzy-based fixed-time nonsingular tracker of exoskeleton robots for disabilities using sliding mode state observer. Mathematics, 10, 3147, 2022, <https://doi.org/10.3390/math10173147>.
 25. Rouhani, S.H., Abbaszadeh, E., Sepestanaki, M.A., Mobayen, S., Su, C.-L., Nemati, A.: Adaptive finite-time tracking control of fractional microgrids against time-delay attacks. IEEE Transactions on Industry Applications, 60(2), 2153-2164, 2024, <https://doi.org/10.1109/TIA.2023.3312223>.
 26. Qi, J., Taha, A.F., Wang, J.: Comparing Kalman filters and observers for power system dynamic state estimation with model uncertainty and

- malicious cyber attacks. IEEE Access, 6, 77155-77168, 2018, <https://doi.org/10.1109/ACCESS.2018.2876883>.
27. Mansouri, M., Harkat, M.-F., Nounou, H., Nounou, M.N.: Data-driven and model-based methods for fault detection and diagnosis. Elsevier, 2020, <https://doi.org/10.1016/C2018-0-04213-9>.
28. Ran, M., Li, J., Xie, L.: A new extended state observer for uncertain nonlinear systems. Automatica, 131, 109772, 2021, <https://doi.org/10.1016/j.automatica.2021.109772>.
29. Ahmad, S., Ali, A.: On active disturbance rejection control in presence of measurement noise. IEEE Transactions on Industrial Electronics, 69(11), 11600-11610, 2022, <https://doi.org/10.1109/TIE.2021.3121754>.
30. Varshovi, A., Rostampour, M., Sadeghiyan, B.: A fuzzy intrusion detection system based on categorization of attacks. In Proc. of 6th Conference on Information and Knowledge Technology (IKT), 50-55, 2014, <https://doi.org/10.1109/IKT.2014.7030332>.
31. Li, L., Ding, S.X., Qiu, J., Yang, Y., Xu, D.: Fuzzy observer-based fault detection design approach for nonlinear processes. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 47(8), 1941-1952, 2017, <https://doi.org/10.1109/TSMC.2016.2576453>.
32. Isermann. R.: Model-based fault-detection and diagnosis – status and applications. Annual Reviews in Control, 29(1), 71-85, 2005, <https://doi.org/10.1016/j.arcontrol.2004.12.002>.
33. Chen, J., Patton, R.J.: Robust model-based fault diagnosis for dynamic systems. Springer Science & Business Media, 2012, <https://doi.org/10.1007/978-1-4615-5149-2>.
34. Hosseini, S., Azizi, M.: The hybrid technique for DDoS detection with supervised learning algorithms. Computer Networks, 158, 35-45, 2019, <https://doi.org/10.1016/j.comnet.2019.04.027>.
35. Kandaperumal, G., Schneider, K.P., Srivastava, A.K.: A data-driven algorithm for enabling delay tolerance in resilient microgrid controls using dynamic mode decomposition. IEEE Transactions on Smart Grid, 13(4), 2500-2510, 2022, <https://doi.org/10.1109/TSG.2022.3167436>.
36. Mohamed, N., Al-Jaroodi, J., Jawhar, I.: Opportunities and challenges of data-driven cybersecurity for smart cities. In IEEE Systems Security

- Symposium (SSS), Crystal City, VA, USA, pp. 1-7, 2020, <https://doi.org/10.1109/SSS47320.2020.9174388>.
37. Mohammadi, E., Alizadeh, M., Asgarimoghaddam, M., Wang, X., Simoes, M.G.: A review on application of artificial intelligence techniques in microgrids. IEEE Journal of Emerging and Selected Topics in Industrial Electronics, 3(4), 878-890, 2022, <https://doi.org/10.1109/JESTIE.2022.3198504>.
38. Thanh, V.-V., Su, W.: Data-driven model predictive control-based proactive scheduling for commercial microgrid considering anomaly detection. IEEE Systems Journal, 17(1), 443-454, 2023, <https://doi.org/10.1109/JSYST.2022.3172397>.
39. Habibi, M.R., Baghaee, H.R., Blaabjerg, F., Dragičević, T.: Secure MPC/ANN-based false data injection cyber-attack detection and mitigation in DC microgrids. IEEE Systems Journal, 16(1), 1487-1498, 2022, <https://doi.org/10.1109/JSYST.2021.3086145>.
40. Alwi H, Edwards C, Tan CP. Fault detection and fault-tolerant control using sliding modes. Springer, 2011, <https://doi.org/10.1007/978-0-85729-650-4>.
41. Naseri, K., Vu, M.T., Mobayen, S., Najafi, A., Fekih, A.: Design of linear matrix inequality-based adaptive barrier global sliding mode fault tolerant control for uncertain systems with faulty actuators. Mathematics, 10, 2159, 2022, <https://doi.org/10.3390/math10132159>.
42. Zhang, L., Guo, G.: Observer-based adaptive event-triggered sliding mode control of saturated nonlinear networked systems with cyber-attacks. Information Sciences, 543, 180-201, 2021, <https://doi.org/10.1016/j.ins.2020.06.073>.
43. Nemati, A., Peimani, M., Mobayen, S., Sayyadfattahi, S.: Adaptive non-singular finite time control of nonlinear disturbed cyber-physical systems with actuator cyber-attacks and time-varying delays. Information Sciences, 612, 1111-1126, 2022, <https://doi.org/10.1016/j.ins.2022.09.018>.
44. Yu, Y., Yuan, Y.: Event-triggered active disturbance rejection control for nonlinear network control systems subject to DoS and physical attacks. ISA Transactions, 104, 73-83, 2020, <https://doi.org/10.1016/j.isatra.2019.05.004>.

Заклучение

Системите за разпределени енергийни ресурси, които могат да комбинират малки конвенционални енергийни източници с разнообразни опции за възобновяема енергия и съхранение, са идеални за задоволяване на нуждите от електрификация на малки общности, както и за проактивно смекчаване на отрицателно-то въздействие на изкопаемите енергийни източници върху околната среда. Преходът към възобновяема енергия е решаваща стъпка за справяне с изменението на климата и постигане на енергийна сигурност. Въпреки това, тъй като зависимостта от цифровите технологии нараства при управлението на системи за възобновяема енергия, рисковете от заплахи за киберсигурността също се увеличават. Кибератаките срещу енергийна инфраструктура могат да нарушат хранването, да причинят финансови загуби и дори да представляват заплаха за националната сигурност. Поради това ефективните микромрежи, които комбинират физически и киберсистеми, изискват надеждно и ефикасно наблюдение и администриране. Интегрирането на тези компоненти може да създаде слабости в системата, което налага специално внимание върху тези проблеми, за да се осигури успешно внедряване и работа на микромрежата. Интелигентните микромрежи са съставени от сложни механизми, включително разпределени сензори, задвижващи механизми, контролери и хранващи компоненти, всички от които изискват прецизна и бърза комуникационна координация. Интелигентните микромрежи трябва да се справят с предизвикателства като осигуряване на надеждна свързаност, подобряване на сигурността на данните и ефективно управление на широкомащабна обработка на данни.

Микромрежите са изложени на различни атаки, включително кибератаки, насочени към комуникационните мрежи, съхранението на данни и софтуера, както и физически саботаж, който

може да засегне оборудване, инфраструктура и персонал. Заплахите за киберсигурността също могат да компрометират поверителността, надеждността и достъпността както на ИТ, така и на системите за индустриална автоматизация. За щастие напредъкът в мрежовата сигурност подобри сигурността и оперативната ефективност на комуникационните протоколи в интелигентните микромрежови системи. Това позволява по-бързи и по-прецизни взаимодействия на устройствата, както и подобро наблюдение на неизправности и отстраняването им.

При проектирането и планирането на топологията на мрежата, маршрутизирането и управлението на информацията трябва да се вземат предвид следните два фактора:

- Ако кибератаки получат достъп до централния контрол, цялата система ще бъде изложена на прекъсване на тока;
- Централизираният контролер е изключително уязвим за фалшива кибератака и чрез заразяване на централизирания контролер нападателят може да зарази цялата система.

Следователно, добре е да се направи сегментиране на мрежата, използване на децентрализирани контролери за всеки сегмент, свързан с главния контролер (като йерархичен децентрализиран модел). Използването на защитни стени между сегментите и антивирусен софтуер, както и методи за двуфакторно удостоверяване (така че втората стъпка да е достъпна само за мениджърите по сигурността) трябва да са също приоритет при изграждане на комуникацията.

За контролиране на киберфизическите системи срещу кибератака могат да се приложат някои от следните подходи:

- Децентрализиране на взаимосвързаните стратегии за възстановяване на киберфизичната система, тъй като след атаката първоначално ще бъдат засегнати киберсъоръженията, а след и физическата структура на енергийните центрове. Основ-

ните предизвикателства се крият в точното управление на начините за кибервъзстановяването и вземането под внимание на тактиката на противника.

- Създаване на настройка за възстановяване при поискване, комбиниране на данни от киберфизичната система и създаване на техники за машинно обучение, които могат да постигнат устойчива конвергенция, дори когато информацията е подправена.
- Проучване на иновативни техники за предотвратяване, диагностика и ограничаване на кибератаки.
- Проектиране на иновативни методи за контрол с цел подобряване на устойчивостта на киберфизическите системи за подобрена устойчивост. Тези техники могат да бъдат придобити или от конвенционални подходи за контрол, или от съвременни системи за контрол, както и от нови технологии, които се основават на машинно обучение.
- Актуализиране на съществуващи устройства за интегриране на съвременни подобрения в системите. Прилагането на стратегии, които да включват модифициране на дизайна на микромрежите или използването на множество микромрежи за разпределяне на електроенергия помежду им, тъй като кибератаката може да използва преместване на натоварването, за да балансира производството на електроенергия в засегнатата зона.

За да се поддържа сигурността на киберфизичната система срещу различни кибератаки, трябва да се проектират подходящи защитни механизми като:

- *Механизъм за предотвратяване:* Алгоритмите за предотвратяване забавят времето за започване на атаката.

- *Повишаване на устойчивостта:* Алгоритмите за устойчивост намаляват ефекта от атака, т.е. увеличават толерантността срещу атака.
- *Откриване и изолиране:* Алгоритмите за откриване и изолиране смекчават ефекта от атаката след времето за изолация.

Следователно, наложително е търсенето на нови решения за подобряване сигурността на микромрежите свързани с: откриването на скрити кибератаки, насочени към качеството на захранването; възможност за реализиране на защитени протоколи, както и проектиране на стратегии за контрол, базирани на изкуствен интелект, за справяне с различни видове кибератаки.

Даниела Борисова
МИКРОМРЕЖИ И КИБЕРСИГУРНОСТ

Българска
Първо издание

Рецензенти:
Професор д.н. **Иван Гарванов**
Професор д-р **Радослав Йошинов**

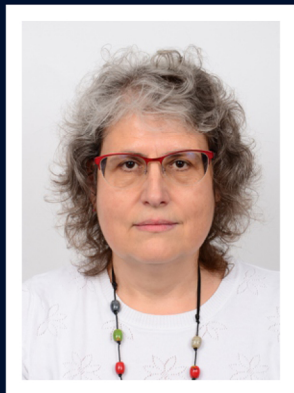
Редактор **Нина Керемедчиева**

Формат 142 x 197

Печатница

Спектър

ISBN 978-619-7515-57-2
eISBN 978-619-7515-61-9



Даниела Борисова е завършила висше образование в Софийския Университет Св. Климент Охридски. През 2006 защитава дисертационен труд за придобиване на ОНС „Доктор“, а през 2009 ѝ е присъдено научното звание „Доцент“. През 2015 защитава дисертационен труд за научната степен „Доктор на науките“, а през 2018 е избрана за „Професор“ в Института по информационни и комуникационни технологии при БАН, а през 2019 е избрана и за „Професор“ в УниБИТ.

От 1994 г. работи в Институт по информатионни технологии при БАН, който през 2010 се трансформира с още два института в Институт по информационни и комуникационни технологии при БАН. Основните научни интереси на проф. Д. Борисова са свързани с математическо моделиране, комбинаторна оптимизация, линейно и нелинейно програмиране, многокритериална оптимизация, многокритериален анализ, групово вземане на решения. Научно-приложните изследователски направления са в области като уеб приложения; електронно и дистанционно обучение; системи за подпомагане вземането на решения, уреди за нощно виждане, проектиране на ветрови паркове, както и в областта на кибербизурността и методите за откриване на зловреден софтуер.

ISBN: 978-619-7515-57-2

eISBN: 978-619-7515-61-9