|  |  |  |  |
| --- | --- | --- | --- |
|  | UNIVERZITET U NIŠU ELEKTRONSKI FAKULTET |  |  |

**Сајбер безбедност соларних инвертера**

Дипломски рад

Студијски програ: Електротехника и рачунарство

Модул рачунарство и информатика

|  |  |
| --- | --- |
| Студент: | Ментор: |
| Вукашин Поповић, бр. инд. 17359 | Проф. др Леонид Стоименов |

Ниш, јул 2024. година

Univerzitet u Nišu Elektronski Fakultet

#### Сајбер беѕбедност соларних инвертера

**Solar inverter cyber security**

Дипломски рад

Студијски програ: Електротехника и рачунарство

Модул рачунарство и информатика

Студент: Вукшин Поповић, бр. инд. 17359

Ментор: Проф. др Леонид Стоименов

Задатак: *Представљање ризика при нападу на соларне инвертера, кроз анализа рањивости топ 10 произвоћача у последњих 5 година, протокола за комуникацију који су имплементирани OSGP, zibbee, modbus Omer TCP…, RS485, анализа контрола безбедности,* *анализа напада на број клонираних уређаја.*

Датум пријаве: 19.07.2024

Датум предаје рада:

Датум предаје рада:

|  |
| --- |
| Комисија за оцену и обраду: |
| 1. Председник Комисије |
| 2. Члан |
| 3. Члан |

Садржај

[**1.** **Увод** 4](#_Toc174397472)

[2. Соларни инвертери 6](#_Toc174397473)

[2.1. Зашто соларни инвертери представљају ризик сајбер безбедности 6](#_Toc174397474)

[2.2. Произвођачи соларних инвертера 7](#_Toc174397478)

[3. Анализа тржишта производње соларних инвертера 8](#_Toc174397479)

[3.1. Топ 10 произвођача соларних инвертера 2023. година 8](#_Toc174397483)

[3.2. Да ли кинески производи предстаљају проблем 8](#_Toc174397488)

[3. Комуникација, протоколи и интерфејс 9](#_Toc174397489)

[3.1. Типови инвертерске комуникације 9](#_Toc174397493)

[3.2. Комуникациони протоколи 11](#_Toc174397498)

[3.3. Интерфејси за комуникацију 13](#_Toc174397499)

[3.4. Примене инвертерске комуникације 15](#_Toc174397500)

[4. Препоруке решења 16](#_Toc174397501)

[5. Закључак 16](#_Toc174397502)

[6. Литература 16](#_Toc174397503)

# **Увод**

Са порастом популарности ИоТ (интернет ствари) технологија модерни свет се све више ослања на повезаност и дигиталне мреже. Преко 15 милијарди активних уређаја широм света, око 2 по особи, очекивано је повећање на 30 милијарди до 2030. године.

Термин интернет ствари описује уређаје који прикупљају податке из света, обрађују након чега су прослеђени даље у систем. Уређаји са сензорима, способношћу обраде података (софтвером), и другим технологијама које повезују и размењују податке са другим уређајима и системима преко интернета или других комуникационих мрежа. Интернет ствари уређаји не морају бити повезани са јавним интернетом, они само треба да буду повезани на мрежу и да буду појединачно адресабилни. Термин је додељен због конвергенције више технологија, укључујући свеприсутно рачунарство, робне сензоре и све моћније уграђене системе, као и машинско учење. Старија поља уграђених система, бежичне сензорске мреже, системи управљања, аутоматизација, самостално и колективно омогућавају Интернет ствари.

Интернет ствари уређаји доносе повезаност и велика побољшања у ефикасности свакодневног живота. Скоро све модерне популарне технологије као што су преносиви уређаји (паметни телефони, сатови...), уређаји унутар домаћинства као што су паметни фрижидери итд. такође спадају у ИоТ, ширина технологије је толика да чак има имплементације и у енергетским системима како у домацинству тако и у дистрибуираним системима што је конкретан фокус овог дипломског рада.

Током последње деценије електрични системи (ЕПС) су претрпели значајне иновације (децентрализација производње, дигитализација корисничких сервиса, паметне мреже, итд.) како би испунили повећану потрошњу електричне енергије, економичност и екологију. Обновљиви извори енергије (РЕС) искоришћење ветра, соларна и топлотна енергија се користе како би се повећала енергетска ефикасност као и испуњење строгих емисија гасова угљеника и других гасова са ефектом стаклене баште. Прелаз на све већу употребу обновљивих извора енергије такође утиче на развој и примену технологија за дистрибуиране изворе (електричне) енергије (ДЕР).

Практична интеграција ДЕР-а је доказ значења за ЕПС, не само у обнобљивим изворима енергије већ и у необновљивим изворима. ДЕР уређаји се категоришу у односу на основу операционих принципа, као што су производња, складиптење, или комбинација претходна два или чак контролна оптерећења. На пример фотонапонски панели и ветрогенератори спадају у генерациону категорију, батерије и електрична возила у категорију складиштења, а грејачи или клима уређаји у категорију подесивих оптерећења. Могућност генерисања електричне енергије јако близу до потрошача смањује губитке и оптерећење на мрежу. Флексибилност, скалабилност, аутономност су особине од јако великог значаја за критичну инфраструктуру ЕПС-а. Као најчешћи и најзасупљенији облик ДЕР-а су соларне електране, више домаћинстава са фото-напонским панелима (електрана) може чинити један систем. У соларним електранама најкритичнијеместо заузимају соларни инвертери, који претварају електричну енергију из панела у одговарајући облик потребан мрежи било то АЦ или ДЦ.

Међутим и з све предности интеграције ИоТ у ЕПС-у или конкретније ДЕР-у, ИоТ технологије доносе нови ниво претњи, отварају система предходно невиљиве сајбер нападима. Да би у будућности и била остварена комплетна итеграција у ЕПС и ипуњено постављање ДЕР-а као ослонца комплетног електричног снабдевања неопходно је дефинисати могуће претње, рањивости, у супротном би сваки отказ могао бити катастрофалан.

Пошто као што је већ наведено од свих ДЕР имплемтација соларних електрана има највећи број оне истовремено представљају и највећу рањивост за мрежу. Анализа могућих претњи и стандарда сигурности соларних инвертера ће и бити тема овог дипломског рада.

# Соларни инвертери

Соларни инвертери претварају енергију добијену из панема у прави облик потребан за употребу (АЦ/ДЦ). Повезани су у соларни енергетски систем, који интегрише паметну комуникацију и надгледање, ради лаког сагледавање производње и потрошње електричне енергије. Вишак електричне енергије је могуће преусмерити у батерије.

На основу глобалног истрживања, Аустралија тренутно има највећи проценат употребе соларне енергије, где је око 30% домаћинстава опремљено фотонапонским (ПВ) системима. Од Јануара 2022. године висе од 3 милиона домаћинстава користи ПВ системе, соларна енергија је тип обновљивих извора енегије са најбжим усвајањем и развијањем. Што се и огледа на примеру Аустралије где 10% укупног електроснабдевања долази из соларних панела.

### Зашто соларни инвертери представљају ризик сајбер безбедности

Традиционално ризик сајбер безбедности асоциран са соларним инвертерима је био јако мали највише из разлога што су то били уређаји који се уопште не повезују на интернет мрежу. Међутим, како је послење време са повећањем популарности ИоТ уређаја за надгледање и контролу, дошло је до интеграције интернета у контролерима (инвертерима), што је знатно повећало ризик, на велики опсег сајбер напада вируси, хаковање. Собзиром да се још увек повећава број корисника, тако се и повећава површина и ризик система.

САД владина канцеларија за енергетску ефикасност и обновљиве енергије (ОЕЕРЕ) истиче потенцијал сајбер ризика у соларним инвертерима. ОЕЕРЕ износи неколико круцијалних претњи које би биле последица неисправног софтвера, што значи да је могуће пресрести податке или манипулисати њима и потенцијал за уградњу малициозног кода у систем као и његово извршавање, што би такође могло утицати на његово пропагирање даље у систем. Штавише САД национална лабараторија за обновљиве енергије (НРЕЛ) открива да ДЕР уређаји шаљу своје податке нејчешће без икакве енкрипције или заштите, усуштини недостају им најосновнији сигурносни системи.

НРЕЛ напомиње да је "повећана сајбер-физичка зависност између електричне мреже и ДЕР-а омогућава нападачима више начина да се окрећу између дистрибутивних ресурса и пропагирања критичним ресурсима, што би могло довести до губитка података или потпуног отказа у раду. Ако рањивости на уређај, мрежи и нивоу примене ДЕР-а нису адресирани, ДЕР-ови би потенцијално могли служе као правци напада на дистрибутивну мрежу". Осим тога, "могуће је онемогућити и/или оштетити локалне мрежне променом фреквенције и/или дозвољеног напона мрежне онемогућавањем подфреквентног оптерећења или добијањем неовлашћеног приступа контролама регулатора помоћу прислушкивања, манипулације интерфејс човек-машина, анализа саобраћаја или других метода упада''.



### Произвођачи соларних инвертера

У последњој деценији идустрија производње ПВ опреме је прошло кроз знатне измене, са изменом центра производње са Европе, Јапана, САД доминантног тржишта на Кинеску монополизацију. Као велика инвестиција Кинеске владе у домаћу индутрију тј. произбођаче, еквиваленто отприлике 50 милијарди долара. Интернационална Енергетска Агенција (ИЕА) доноси у извештају чињеницу да 80% светксе произвозводње долази из Кине као и да свих топ 10 произвођача долази из Кине.

Што се тиче конкретно инвертера, тај број је тек нешто мањи, 76% укупне произво-дње чини Кина. Само инвертери прва два Кинеска произвођача Хуавеи и Сунгров укупно произведу више гигавати електричне енергије него сви остали европски заједно. ИЕА тврди да ће се комплетна светска производња ПВ опреме заснивати на Кини до 2025. године. Што још више ствара разлога за анализу рањивости и претњи.



Производња ПВ опреме по држави и региону, 2021. година

Извор: ИЕА

# Анализа тржишта производње соларних инвертера



### Топ 10 произвођача соларних инвертера 2023. година

Кина је постала гигант на тржишту соларне опреме, са великим бројем фирми које су специјализоване само за то, како је порасла популарност обновљивих извора енергије, тако је дошло до повећаних захтева за ефикасност и поузданост. Као последица тих захтева и њиховог испуњења дошло је до распоперада следећих произдођача на следећој светској листи тржишта.

1. Huawei Technologies Co. Ltd.
2. Sungrow Power Supply Co. Ltd.
3. SMA Solar Technology AG
4. Ginlong Technologies Co. Ltd.
5. TBEA Co. Ltd.
6. Omnik New Energy Co. Ltd.
7. Sineng Electric Co., Ltd.
8. Chint Group Corporation
9. Growatt New Energy Technology Co. Ltd.
10. Shenzhen KSTAR Science and Technology Co. Ltd.

### Да ли кинески производи предстаљају проблем

# Комуникација, протоколи и интерфејс

Инвертерска комуникације се односе на размену података (везу) између самог претварача (инвертера) и осталих система за надзор, контролу итд. како би омогућили лакше прикупљање података инвертерских система. Ово омогућава оператерима система оптимизацију, побљшање ефикасности, безбедности, као и решавање проблема у систему у реалном времену.



### Типови инвертерске комуникације

Инвертерска комуникација је начин комуникације између претварача и неког другог уређаја унутар систему, као што је систем за надгледање или контролу. Постоји их неколико сваки са својим предностима и недостацима у зависности од намене.

|  |  |  |  |
| --- | --- | --- | --- |
| Тип комуникације | Пример | Предности | Мане |
| Серијска комуникација | РС-232,  РС-485 | Поузданост и једноставност имплементације | Може бити спор и ограничена брзина преноса |
| Пралалена комуникација | Центроникс (Centronics), СЦСИ (SCSI) | Велика брзина и проток | Захтева велики број каблова и пинова, тешка синхронизација |
| Етернет  (Ethernet)  комуникација | Етернет  (Ethernet),  ТЦП(TCP) | Велика брзина и проток, велика дужина кабла | Захтева додатну опрему, свич, ру-тер. Подлежан мре-жним проблемима |
| Блутут  (Bluetooth)  комуникација | Блутут(Bluetooth Classic), (Bluetooth Low Energy) | Мали утрошак енергија и једноставна имплементација | Ограничен домат, може вити подле-жан сметњама од других бежизних уређаја |
| Зигби  (Zigbee)  комуникација | Зигби(Zigbee),  Тред(Thread) | Мала потрошња енергије, сигурност, (mesh networking) | Ограничен проток, домет, и број уређаја који могу бити на једној мрежи |
| Вај-фај  (Wi-Fi)  комуникација | Вај-фај  (Wi-Fi), ТЦП/ИП (TCP/IP) | Велика брзина, велики проток, велики домет и лакоћа употребе | Захтева додатну опрему, подлежан интерфернецији |

#### Серијска комуникација

Серијска комуникација је витална форма инвертерске комуникације са широком употребом у индустрији. Ова техника могућава пренос података узастопно бит по бит у један комуникациони канал. Популарни пример серијске комуникације укључује РС-232 интерфејс, примарно коршћен за рачунар-уређај комуникациу, и РС-485 интерфејс ког одликује већа издржљивост, најчешче коришћен у индустријској контроли и аутоматизационим системима.

Док серијска комуникација нуди разне бенефите као што су поузданост лакоћа имплементације, важно је имати на уму да ова метода може имати спорији пренос података када се упореди са другим техникама/технологијама.

Такође могуће је да постоје ограничења у количини податак који могу бити посла-ти одједном.

#### Паралелна комуникација

Пралелна комуникација, у поређењу са серијском комуникацију омогућава истовремени пренос података кроз већи број канала истовремено.

Овај приступ се често користи за велику брзину преноса података као што су апликације за обраду слиак и видео снимака.

Иако омогућава велику брзину преноса у односу на серијску комуникацију паралелна комуникација захтева вечи број ресурса као и компликованију поставку и имплементацију.

Самим тим, неопходно је сагледати ове елементе приликом избора технологије за комуникациију, треба изабрати прикладну за ту ситуацију.

#### Етернет (Ethernet) комуникација

Етернет комуникација има широку примену због своје лаке имплементације и велике брзине трансфера и комуникације између повезаних уређаја.

Видео надзор и идустријске контролне мреже су неки од примена ове технологије баш због брзог трансфера и велике поузданости.

#### Блутут (Bluetooth) комуникација

Блутут је бежична технологија којом се успоставља веза између два уређаја. Данас велики број преносивих уређаја има у себи блуту. Присутан је и у инвертерима (претварачима) како би се убрзао пренос података.

Једноставност блутута је једна од највећих предности које носи са собом, не захтева пуно техничког предзнања. Недостатак је што није могућ пренос података на великим даљинама.

#### Зигби (Zigbee) комуникација

Зигби комуникација је тип меш мрежног протокола који омогућава ниско енергетску комуникацију измећу уређаја у малој мрежи.

Једна од честих примена је у паметним кучним уређајима за аутоматизацију и управљање који захтевау поуздану комуникацију.

Ниска потрошња енергије и исплативост су две највеће предности Зигби протокола, није прикладан за преносе који захтевају брз пренос података.

#### Вај-фај (Wi-Fi) комуникација

Вај-фај је бежична технологија преноса података и умрежавања на брз и ефикасан начин.

Један од најкоришћенијих протокола у модерно вре, рачунари, паметни телефони .итд због сигурности које пружа део је и соларних инвертера.

Поставка је лака и интуитивна без захтева за специјалним вештинама или алатима. За све предности које доноси, један од највећих недостатака вај-фај технологије је ограничен домет.



### Комуникациони протоколи

Поред предходно наведених типова инвертерске везе у употреби су и разни протоколи зе успостављање комуникације између уређаја. Следе примери протокола који су употреби у индустрији данас.

#### Модбас (Modbus) протокол

Модбас је критичан протокол у омогућавању инвертерске комуникације, омогућава да више различитих уређаја размењује податке међусобно.

То укључује али не ограничава се на, сензорима, актуаторима, контролерима (PLC) и другим уређајима који имају улогу у индустријксој аутоматизацији.

Одликује га једноставност, добра поузданост, ефикасна комуникација пто га чини популарним избором за имплементирање инвертерске комуникације.

#### Кен (CAN) протокол

Кен магистрални (Controller Area Network) протокол игра суштинску улогу у инвертерској комуникацији.

То је комуникацијони систем који може да повеже раличите уређаје и сензоре омогућавајућ неспетану размену података између њих. Инвертери се посебно ослањају на овај протокол за размену критичних информација са другим уређајима као што су системи за праћење батерија, соларни пуњачи и друге опреме.

Са Кен магитралом инвертери могу брзо и ефикасно да преносе виталне податке, што је од критичног значаја обезбеђивању префроманси и стабилности електричне мреже.

Омогућавајући беспрекорну комуникацију између више система, Кен систем побољшава укупну ефикасност комуникационог система инвертера побољшавајући поузданост мреже и толеранцију грешака.

#### ОПЦ (OPC) протокол

ОПЦ (Object Linking and Embedding for Process Control) протокол има јако широку примену у индустриским контролиним системима, што укључује комуникацију соларних претварача.

Омогућава размену података између различитих уређаја, укључујући уређаје од различитих произвођача који нису направљени да буду међусобно компатибилни по хардверу или софтверу. ОПЦ протокол ради као гејтвеј (gateway) или интерфјес (interface), чиме омогућава мапирање података између уређаја и ИВР протокола.

Конкретно ОПЦ омогућава соларним претварачима да размењују податке у реалном времену са системима за надзор и прикупљање података (СЦАДА). Омпогућавањем једноставне комуникације између претварача и СЦАДА, ОПЦ протокол помаже побољшању перформанса и ефикасности индустријких система.

#### ДНП3 (DNP3) проткол

ДНП3 протокол је кључан за остваривање паметне електричне мреже јер олакшава комуникацију између инвертерских система и других уређаја у мрежи. Како је све випе дистрибуиранх енергетских ресурса интегрисано, тако је све важније да ови системи могу лако делити податке ради одржања стабилности и откривање грешака на мрежи односно спречавања хаварије.

Са ДНП3 протоколом претварач и контролни систем могу да деле податке у реалном времену, укључујући податке о призводњи енергије и потрошњи. Ово је неопходно за осигурање одређеног нивоас поузданости мреже.

Штавише ДНП3 протокол омогућава напредне мпрежне услуке као што су регулација напона и одзив на потражњу обезбеђујући стабилност и ефикасност чак и променљивом окружењу.

### Интерфејси за комуникацију

Постоји више интерфејса којис су у уотреби за остваривање инвертерске комуникације.

|  |  |  |  |
| --- | --- | --- | --- |
| Интерфејс | РС-232 | РС-485 | Етернет  (Ethernet) |
| Тип кабла | Серијски | Серијски | Упредене  парице |
| Максимална дистанца | 15м | 1219м | 100м |
| Максимална брзина | 115.2 kbps | 10 Mbps | 1 Gbps |
| Топологија | Поинт-то-поинт  (Point-to-point) | Мулти-дроп  (Multi-drop) | Поинт-то-поинт  или мрежа |
| Колуникација | Халф дуплекс  (Half duplex) | Халф дуплекс  (Half duplex) | Фул дуплекс  (Full duplex) |
| Детектовање грешке | Нема | ЦРЦ  (CRC) | Чексум  (Checksum) |
| Примена | Мала брзина,  мале дистанце | Средња брзина,  средње дистанце | Велика брзина,  велике дистанце  мрежни систем |
| Предности | Једностваност,  јефтино | Велике дистанце | Велика брзина,  упрежавање |
| Мане | Мале дистанце,  спор пренос | Подлежан интерференцији | Захтева додатну опрему, већа цена |

Битно је имати науму да специфичне предности и мане, ограничења сваког од типова интерфејса зависи од његове конкретне имлентације, конфигурације и цлучаја примене.

#### РС-232 интерфејс

РС-232 је серијски комуникациони протокол који се користи за повезивање уређаја, модема, индустријских контролних система, рачунарских периферија итд.

Протокол користи ДБ9 конектор и дозвољава један канал података са асинхроним слањем. Слање података се врши релативно споро до 19.2 kbps. Иако већина нових уређаја користи УСБ (USB) и друге протоколе, РС-232 и даље има велику употребу.

Све у свему, РС-232 је имао јако важну улогу у развоју модерних комуникацинох протокола, поред чега се и данас користи.

#### РС-485 интерфејс

РС-485 је серијски комуникациони протокол за велике дистанце. Могуће је повезивање више уређаја на једну магистралу и послати податке на раздаљине до 1219 метара.

РС-485 користи две жице са различитим сигналима због смањења интерференције за раслику од РС-232 који то нема. Индустријски контролни системи, аутмобили итд. користе овај протокол.

РС-485 је јако моћан протокол баш зато што омогућава повезивање више уређаја на једној магистрали и поузани трансфер података на великим дистанцама. Као и РС-485 служиао је као основа за развијање многих модерних протокола, а и данас има примена.

#### Етернет (Ethernet) интерфејс

Широко употребљиван комуникациони протокол за преношење података између претварача и других мпрежних уређаја.

Велика поутданост и ефикасност, омогућава достављање статистике у реалном времену о производњи и потрошњи електрилне енергије контролном систему и смарт мерачима.

Коришћење Етернета као комуникационог интерфејса омогућава интертерима слање великих података на великим дистанцама са најмањим губицима, што је и кључно за ефикасну комуникацију у памтеном систему.

### Примене инвертерске комуникације

#### Обновљиви извори енергије

Мониторинг и котрола система обновљивих извора енергије су критични за обезбеђивање њихових оптималних перформанси и поузданости.

Инвертери играју кључну улогу у томе тако што претварају једносмерну струју (ДЦ) коју добијају из фотонапонских панела, ветрогенератора или других извора енергије у употребљиву наизменичну струју (АЦ).

Инвертерске комуникације су такође битне јер омогућавају праћење, контролу, дијагностику у реалном времено што може помоћи у идентификовању проблема и побољшању перформанси.

Инвертерске комуникације могу помоћи у оптимизацији енергетске ефикасности система обновљивих извора енергије, обезбеђивањем тачних и благовремених података, смањење отпада и повећањем укупних перформанси.

#### Индустријска аутатизација

Инвертерски комуникациони системи су критични у разним индустријским применама као штоо су контрола мотора, транспортни системи и роботика.

Они омогућавају праћење и контрол у реалном времену омогућавају брзо откривање и решавање проблема и кваров, смањујући време застоја и повећавају укупну ефикасност система.

Инвертерски комуникацино системи могу побољшати продуктивност и безбедност омогућавајући размену података у реалном времену и пружају бољи увид у перформансе система.

Ово може помоћи у идентификацији потенцијалних проблема пре него постану критични, обезбеђујући максимално време рада и ефикасност система.

#### ХВАК (HVAC) системи

#### Медицинска опрема

# Препоруке решења

# Закључак

# Литература

<https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8498.ipd.pdf>

<https://solartechadvisor.com/inverter-communications/>

<https://www.hisenpower.com/Blogs/top-15-best-inverter-companies-in-china>

https://eepower.com/tech-insights/defending-the-smart-grid-against-inverter-attacks/