|  |  |  |  |
| --- | --- | --- | --- |
|  | 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](#_Toc174192673)

[2. Соларни инвертери 6](#_Toc174192674)

[2.1. Зашто соларни инвертери представљају ризик сајбер безбедности 6](#_Toc174192675)

[2.2. Произвођачи соларних инвертера 7](#_Toc174192679)

[3. Анализа тржишта производње соларних инвертера 8](#_Toc174192680)

[3.1. Топ 10 произвођача соларних инвертера 2023. година 8](#_Toc174192684)

[3.2. Да ли кинески производи предстаљају проблем 8](#_Toc174192689)

[3. Проблем 9](#_Toc174192690)

[3.1. Анализа тржишта 9](#_Toc174192691)

[4. Соларни инвертери 9](#_Toc174192692)

[4.1. Анализа протокола за комуникацију 9](#_Toc174192693)

[4.2. Анализа контроле безбедности 9](#_Toc174192699)

[5. Препоруке решења 9](#_Toc174192700)

[6. Закључак 9](#_Toc174192701)

[7. Литература 9](#_Toc174192702)

# **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

# Проблем

### Анализа тржишта

# Соларни инвертери

### Анализа протокола за комуникацију

1. На уређају
2. На клијенту

### Анализа контроле безбедности

* 1. Анализа напада на број клонираних уређаја

# 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/