УНИВЕРЗИТЕТ У НИШУ
ЕЛЕКТРОНСКИ ФАКУЛТЕТ

Сајбер безбедност соларних инвертера

Дипломски рад

Студијски програ: Електротехника и рачунарство

Модул рачунарство и информатика

Студент:

Вукашин Поповић, бр. инд. 17359

Ментор:

Проф. др Леонид Стоименов

Ниш, јул 2024. година

Univerzitet u Nišu
Elektronski Fakultet

Сајбер безбедност 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: *Проучити соларне инвертере и инвертерску комуникацију, са посебним освртом на сајбер безбедност контроле соларних инвертера. Проучити и приказати могућности заштите на мрежном нивоу и рањивости различитих соларних система, кроз анализу рањивости изабраних произвођача.*

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

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.

2. 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.

Слика 1. Соларна електрана

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.

2.1.Зашто соларни инвертери представљају сајбер безбедносни ризик

Традиционално сајбер безбедносни ризик 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

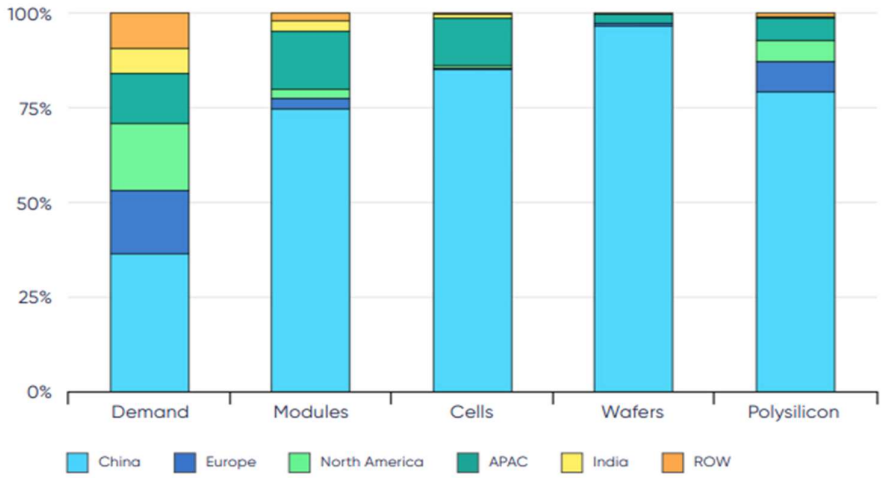
обновљиве енергије (НРЕЛ) открива да ДЕР уређаји шаљу своје податке нејчешће без икакве енкрипције или заштите, усуштини недостају им најосновнији сигурносни системи.

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".

2.2.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 производводње долази из Кине као и да свих топ 10 произвођача долази из Кине. Однос тржишта производње фотонапонске опреме на слици 2.

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.



Слика 2. Производња ПВ опреме по држави и региону, 2021. година
Извор: ИЕА

3. Анализа тржишта производње соларних инвертера

3.1.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.

3.2.Да ли кинески производи предстаљају проблем

Бриге око сајбер ризика у соларним инвертерима се доста стишала у последње време, 2023 године је дошло до нових запажања у Америчком комитету за енергију и трговину директно повезаних са претњом у соларним инвертерима кинеске производње. Сличне бриге су изнете и у Аустралији где је око 60% фотонапонске опреме кинеског порекла од поизвођача као што су Хаувеи и Сангроу.

Према члану 7 Кинеског закона о националног безбедности: "Свака организација и грађанин ће у складу са законом пружати подршку и сарадњу у националном обавештајном раду, и чувању тајности било ког националног обавештајног рада за који су свесни. Држава ће штитити појединце и организације које сарађују и пружају подршку у националном обавештајном раду."

За разлику од обичне робе и услуга које пружају кинеске компаније, а друге нације обезбеђују и уграђу повезаност са интернетом, овде је комплетан производ дело једне компаније. У најбољу руку ово је двосмислено значење, а у најгору је директно уплитање државе у друге нације.

3. Инвертерска комуникација

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 операторима система оптимизацију, побољшање ефикасности, безбедности, као и решавање проблема у систему у реалном времену.

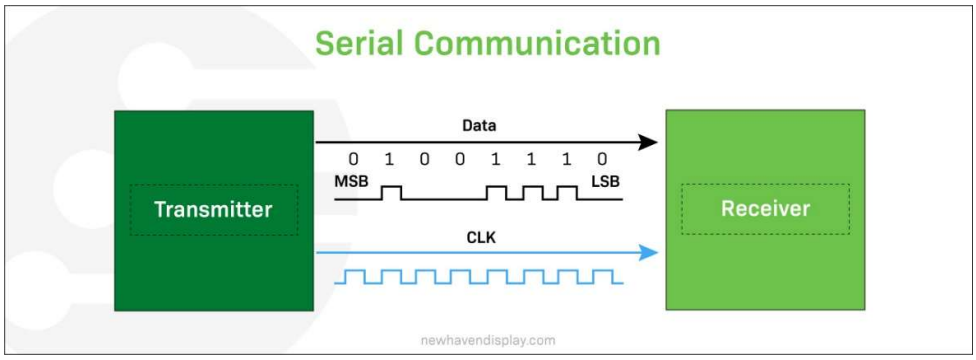
3.1. Типови инвертерске комуникације

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

3.1.1. 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 (Слика 3.). Популарни пример серијске комуникације укључује PC-232 интерфејс, примарно коршћен за рачунар-уређај комуникациу, и PC-485 интерфејс ког одликује већа издржљивост, најчешче коришћен у индустријској контроли и аутоматизационим системима.



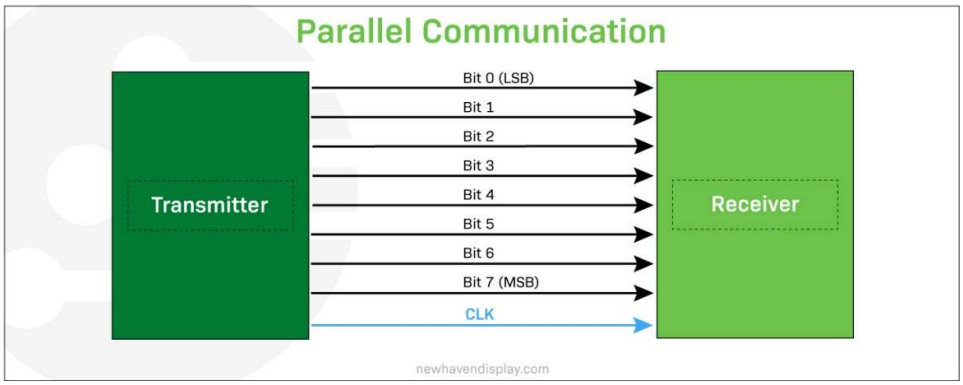
Слика 3. Серијска комуникација

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

Такође могуће је да постоје ограничења у количини податак који могу бити послати одједном.

3.1.2. Паралелна комуникација

Пралелна комуникација, у поређењу са серијском комуникацију омогућава истовремени пренос података кроз већи број канала истовремено (Слика 4.).



Слика 4. Пралелна комуникација

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

Иако омогућава велику брзину преноса у односу на серијску комуникацију паралелна комуникација захтева већи 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.

3.1.3. Етернет (Ethernet) комуникација

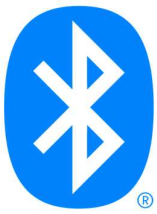
Етернет комуникација има широку примену због своје лаке имплементације и велике брзине трансфера и комуникације између повезаних уређаја.

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

3.1.4. 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.



Слика 5. Блутут лого

3.1.5. Зигби (Zigbee) комуникација

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

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

Слика 6. Зигви лого

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

3.1.6. 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.

3.2. Комуникациони протоколи

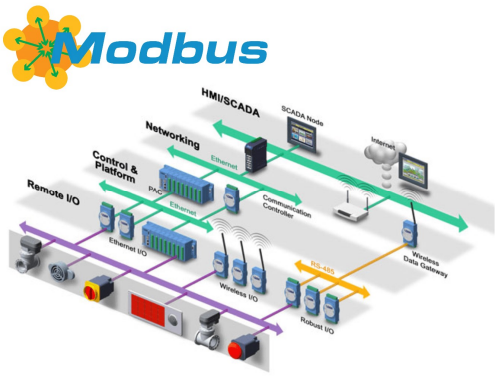
Поред предходно наведених типова инвертерске везе у употреби су и разни протоколи за успостављање комуникације између уређаја. Следе примери протокола који су употреби у индустрији данас.

3.2.1. Модбас (Modbus) протокол

Модбас је критичан протокол у омогућавању инвертерске комуникације, омогућава да више различитих уређаја размењује податке међусобно (Слика 7.).

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.



Слика 7. Модбус структура мреже

3.2.2. 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 несметану 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 магистралом инвертери могу брзо и ефикасно да преносе виталне податке, што је од критичног значаја обезбеђивању префромански и стабилности електричне мреже.

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

3.2.3. 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.

3.2.4. 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 хаваријe.

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.

3.3.Интерфејси за комуникацију

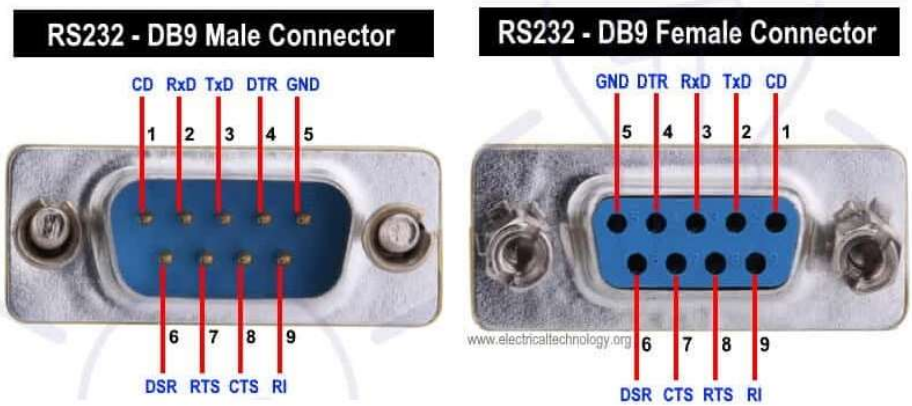
Постоји више интерфејса којис су у уотреби за остваривање инвертерске комуникације.

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	Једноставност, 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.

3.3.1. PC-232 интерфејс

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



Слика 8. PC232 конектори

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, PC-232 и даље има велику употребу.

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

3.3.2. PC-485 интерфејс

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

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

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

3.3.3. 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.

3.4.Примене инвертерске комуникације

3.4.1. Обновљиви извори енергије

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

Слика 9. Обновљиви извори енергије

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.

3.4.2. Индустријска аутоматизација

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

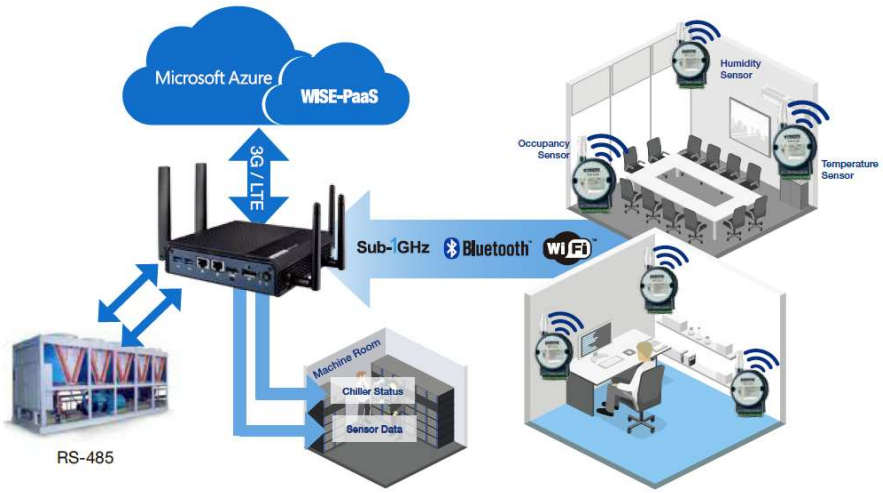
Они омогућавају праћење и контрол у реалном времену омогућавају брзо откривање и решавање проблема и кваров, смањујући време застоја и повећавају укупну ефикасност система.

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.

3.4.3. ХВАК (HVAC) системи

ХВАК (HVAC) системи дају најбоље перформансе и чувају највише енергије када претварачии и друге компоненте комуницирају добро. Претварачи се користе у ХВАК системима за контролу електромотора, компресора, итд. што је кључно за ефикасну контролу температуре.



Слика 10. Веза зензора са ХВАК системом

Инвертерске комуникације омогућавају праћење и контролу ХВАК система у реалном времену смањујући потрошњу енергије и трошкове.

Конкретније оптими-зација система се постиже усклађивањем рада компоненти условима у реалном времен (Слика 10.).

3.4.4. Медицинска опрема

Ефикасна комуникација између претварача и медицинских уређаја је од суштинсок значаја како би се обезбедила прецизна контрола и надгледање опреме што на крају повољшава негу пацијената.

Инвертери се користе у низу медицинске опреме као што су рендгенске машине. МРИ машине итд. и играју виталну улогу у обезбеђивању најбољег рада ових уређаја.

Инвертерске комуникације су кључне за постизање надзора и контроле медицинске опреме у реалном времену, омогућавајући здравственим радницима надгледање перформансама и откривање грешака.

Ово помаже да се максимално смањи време прекида рада и обезбеди непрекидна нега пацијента.

3.5.Предности и мане инвертерске комуникације

Следећа табела представља поређење предности и мана инвертерске комуникације.

Предности и мане инвертерске комуникације	Предности	Мане
1.Повећана ефикасност	Праћење система и контрола у реалном времену доносе оптимизацију перформанси ситема и уштеде енергије.	Комплексност: Интеграција инвертерских комуникационих система може бити комплексно, захтева посебно знање.
2.Даљинска контрола и надгледање система	Инвертерски комуникациони системи омогућавају даљински приступ, управљање и смањују захтеве за одржавање на локацији.	Компатибилност: Нису сви уређаји компатибилни са одређеним комуникационим протоколом или интерфејсом.
3.Смањењење потребних каблова	Бежична комникација смањује потребе за физичким повезивањем и смањује цену инсталације.	Безбедносни ризик: Бежична комуникација је подлежна хаковању и уноси рањивости у систем

4. Сајбер безбедност контроле соларних инвертера

Пошто је број претварача који су на мрежи све већи а самин тим и ослањање електроиндустрије на обновљиве изворе енергије као што је соларна постаје неопходна имплементација контрола сајбер безбедности. Постоје два генерална типа контрола (заштита), а то је контрола безбедности на самом претварачу (контрола на нивоу уређаја) и контрола безбедности на мрежном нивоу:

4.1.Заштита на нивоу инвертера

Заштита на самом уређају има за задатак одржање неколико важних аспеката сигурности и поузданости:

4.1.1. Спречавање неовлашћеног приступа – аутентификација корисника, правила за лозинке и сигурно покретање.

4.1.2. Одржање интегритета уређаја – енкрипција фирмвера, сигурно покретање и редовно ажурирање софтвера.

4.1.3. Спречавање физичког напада – физичке заштите као што је кућиште отпорно на природне појаве влагу, сунце, сензори за детекцију неовлашћеног приступа.

4.1.4. Осигурање поузданости рада – логовање активности уређаја, као и сигурносни протоколи за ажурирање софтвера.

4.1.5. Заштита података – енкрипција комуникације и фирмвера.

4.1.6. Превенција ширења напада – сигурно покретање, ИДС/ИПС (IDS/IPS) инте-грација и мрежне контроле.

Комбинацијом техника у циљу испуњавања претходних циљева постиже се већи ниво отпорности претварача (инвертера) на напад самим тим и целокупног соларног система. Приликом избора инвертера неопходна је анализа контрола безбедности који тај произвођач нуди.

4.1.1. Сигурно покретање (Secure Boot)

Технологија која осигурава приликом покретања учитавање само одобреног, валидног и потписаног софтвера. Ово спречава покретање маициозног, неовлашћеног софтвера.

Приликом покретања софтвера, систем проверава дигиталне потписе софтвера након чега се он покреће, уколико софтвере не испуњава услове тј. нема дигитални потвип који се тражи учитавање се обуставља или се покреће безбедни основни софтвер.

Пример: СМА (SMA) солар, један од водећих произвођача соларних претварача имплементира ову технологију како би се само проверени и овлашћени софтвер користио у њиховим уређајима, популаран модел са овом технологијом је Сани Бој (Sunny Boy).

4.2.1. Енкрипција фирмвера

Фирмвер је основни софтвер који контролише хардвер, енкрипцијом фирмвера се он закључава за прегледавање и измену од стране неовлашћених лица.

Фирмвер је енкриптован тако да је једини начин за његово прегледавање потрбан декрипциони кључ, чак и у случају да нападач добије физички приступ уређају без кључа је безбедност одржана.

Пример: Fronius International, познат по својим хибридним ивертерима Fronius Symo Hybrid, користи енкрипцију фирмвера како би заштитио софтвер својих уређаја.

4.2.2. Аутентификација корисника

Аутентификација осигурава да само овлашћени корисници могу приступити и извршавати операције на уређају, било то удаљено или локално.

Корисници морају унети валидне податке корисничко име, лозинка, биометријски подаци или други облици аутентификације, такође могуће је додатно осигурати овај процес коришћењем на пример двоструке аутентификације.

Пример: SolarEdge инвертори, користе јаку аутентификацију за приступ уређају, омогућавају операторима креирање јединсветног налога за заштиту поставки уређаја. Један од популарних серија са овом технологијом су SolarEdge HD-Wave Inverters.

4.2.3. Заштита од физичког напада

Заштита од физичког напада захтева физичке и електронске мере које спречавају неовлашћени приступ компонентама система.

Претварачи морају имати заштите кућишта, сензоре, браве који детектују отварање и аларме који покушају неовлашћеног приступа. Ту је могућа и употреба тембер-евидент технологија која детектује библо какво физичко нарушавање интегритета система.

Пример: Huawei у својој SUN2000 серији инвертера имплементира физичку заштиту, кућишта са сензорима који детектују покушаје отварања или манипулације.

4.2.4. Правила за лозинке

Лозинке су најосновнија али и најважнија мера одбране. Правилна процедура управљања лозинкама може знатно смањити ризик од неовшћеног приступа.

Инвертери могу захтевати комплексне лозинке које су дуге и садрже комбинацију слоба бројева и специјалних знакова. Такође уређаји могу бити конфигурисани да редовно захтевају мењање лозинке и се закључавају у потпуности након неколико погрешних лозинки.

Пример: АББ инвертери, као што је UNO-DM-PLUS серија омогућавају имплементацију сложених правила за лозинке, све преткодно наведено.

4.2.5. Даљинско ажурирање фирмвера (Firmware over-the-air)

Ова технологија омогућава ажурирање фирмвера без потребе за физичким приступом уређају.

Ажурирања се шаљу енкриптована преко мреже и примењују на уређају, процес ажурирања је вишеструко осигуран како би се спречило покретање невалидног кода.

Пример: Enphase у својој IQ Series микоинвертерима користи ФОТА (Firmware over-the-air) технологију сигурног, даљинског ажурирања фирмвера, што олакшава одржавање и побољшава сигнурност.

4.2.6. Мониторинг и логовање

Праћење активности уређаја и логовање помаже детекцији и анализи потенцијалних сигурностних инцидената.

Уређаји могу имати уграђене функције за логовање, бележење активности и критичних активности као што су покушаји логовања, неовлашћеног приступа у реалном времену.

Пример: Schneider Electric у својој серији Conext инвертера нуди напредне опције мониторинга и логовања догађаја, што омогућава праћење у реалном времену.

4.3.Заштита на мрежном нивоу

Заштита на мрежном нивоу је скуп мера, технологија за осигуравање комуникације, одржање интегритета података између инвертера и других мрежних система.Ово укључује заштитуподатака док су упреносу, контролу приступа мрежи, детекцију напда, обезбеђивање континуалног надзора над мрежним активностима.

4.3.1. Енкрипција комуникације (TLS/SSL)

ТЛС (TLS - Transport Layer Security) и ССЛ (SSL - Secure Sockets Layer) су протоколи енкрипције између инвертера и других мрежних уређаја, као што су контролни центри или сервери мониторинга.

Кад претварач комуницира са удаљеним сервером, подаци који се преносе су енкриптовани помоћу ТЛС/ССЛ протока чиме се осигурава интегритет података, спречава прислушкивање и манипулација над подацима у транспорту.

Примвер: SolarEdge инвертери користе ТЛС/ССЛ протоколе за енкрипцију података између претварача и назорних система.

4.3.2. ВПН (VPN) тунел

ВПН (Virtual Private Network) тунели се користе за безбедан даљински приступ инвертерима преко интернета (Слика 11.).

Слика 11. Принцип функционисања ВПН-а 1

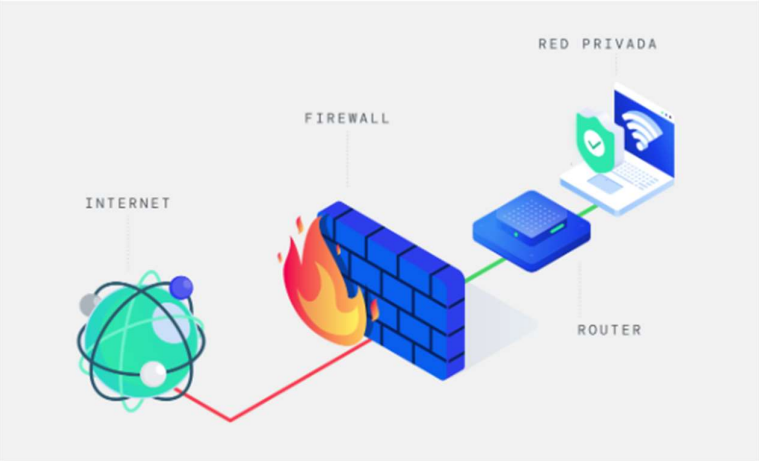
Кроз ВПН тунел комуникација између користника и инвертера иде прего сигурне, енкриптоване везе чиме се штити од пресретања и неовлашћеног приступа.

Пример:СМА инвертери, као што је Сани Бој серија омогућава безбедан даљински приступ путем ВПН тунела.

4.3.3. Фајервал (firewall)

Мрежна заштита која контролише улазни и излазни саобраћај између инвертера и мпреже, омогућавајући (филтрирањем) само дозвољени саобраћај (Слика 12.).

Фајервал може бити имплементиран као део инвертера или на мрежном нивоу како би се филтрирао саобраћај ка инветеру, како би се спречили напади као што су ДДоС (DDoS (Distributed Denial of Service)) или неовлашћени приступ. Конфигурацином фајервала може се блокирати непознати ИП или приступ преко одређеног порта.



Слика 12. Фајервал

Пример: Фрониус Симо серија долази са уграђеним фајервалом који филтрира улазни и излазни саобраћај.

4.3.4. ИДС (Intrusion Detection Systems) / ИПС (Intrusion Prevention Systems)

ИДС/ИПС су системи мрежне заштите који детектују покушаје напада на мрежу у којој се налази инвертер.

ИДС прати мрежни саобраћај и детектује сумњиве активности попут неовлашћеног приступа или злонамерног кода. ИПС мож аутоматски предусзеи мере кео

што је блокирање саобраћаја са сумњиве адресе или спречавање специфичних напада.

Пример: Хаувеи СУН2000 инвертери подржавају инвеграцију са ИДС/ИПС системима.

4.3.5. Сегментација мреже

Сегментација мреже подразумева одвајање мреже на мање, сегменте, како би се ограничио приступ.

Инвертери могу бити постављени на засебне мрежне сегменте одвојени од других критичних система, што помаже у случају ширења напада између сегмената, напад остаје изолован.

Пример: АББ Уно-Дм-Плус инвертери могу бити у сегментисаним мрежама, што омогућава изолацију уређаја од остатка система.

4.3.6. Редовно ажурирање софтвера и фирмвера

Редовно ажурирање софтвера и фирмвера је кључно за смањење рањивости уређаја и одржавање његове сигурности на дуже време.

Произвођач редовно шаље ажурирања која у себи имају сигурносне закрпе, она се могу радити аутоматски преко мреже или ручно на физичкој локацији.

Пример:Енфејз, IQ серија миктоинвертера подржава редовно ажурирање на даљину (over-the-air), омогућавајући корисницима да инсталирају најновије сигурностне закрпе.

4.3.7. Мониторинг и логовање мрежног саобраћаја

Праћење и логовање мрежног саобраћаја помаже у детекцији абнормалних активности и потенцијалних напада.

Инвертери могу бележити саобраћај усмерен њима или слати обавештења о потенцијалним нападима, приступима са недозвољених адреса на централизован систем у реалном времену.

Пример: Шнајдер Електриј Контекст серија нуди напреднде опције за мониторинг и логовање мрежног саобраћаја.

4.3.8. Сигурно управљање приступом (ИАМ - Identity and Access Management)

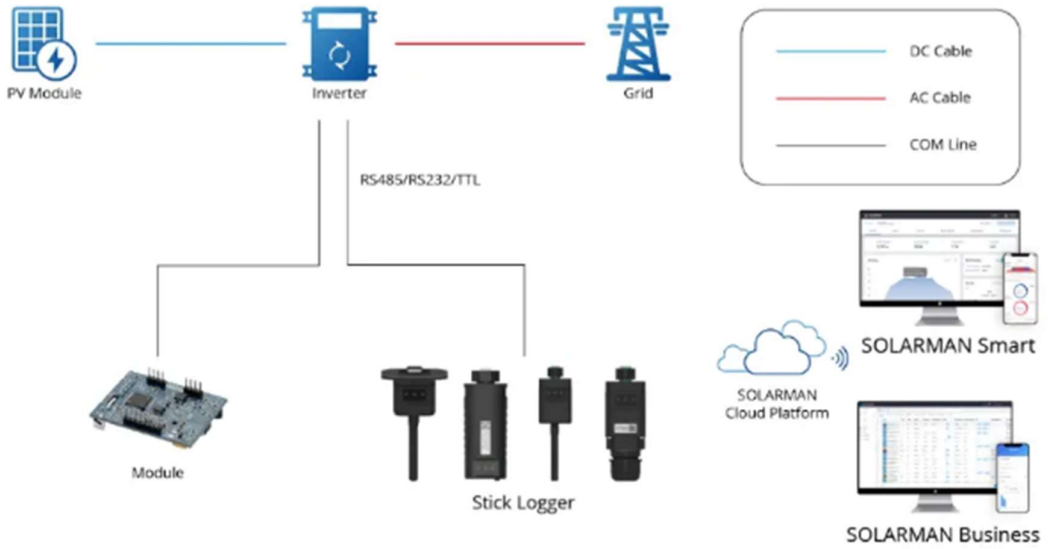
Управљање приступом кориснка и уређаја мрежним ресурсима осигурава да само овлашћени ентитети могу имати одговарајући ниво приступа.

Уређаји користе ИАМ системе за контролу ко може приступити мрежи на којем новоу, ово укључује улоге, дозволе за различите кориснике и аутентификацију и ауторизацију.

Пример: Сунгров (Sungrow) СГ серија инвертера користи ситеме за управљање приступом и идентитетима.

5. Рањивости соларних система

Серија рањивости соларних система утиче на милионе соларних система широм света, велике глобалне електричне мреже прожете брзо растућом соларном инфраструктуром и све заступљенијим Интернетом Ствари (Internet of Things), чини комплексан спој енергије и података.



Слика 13. Повезивање паметног инвертера

Произведена електрична енергија из инвертера ових произвођача Солармен и Дај (Solarman and Deye)) чини око 195 гигавати (gw) на глобалном нивоу што је око 20% укупне соларне енергије света, са серијом рањивости чини отворено малициозним нападима.

Електрична мрежа је сложен систем који чини производња енергије, пренос на даљину и локална дистрибуција. Традиционалне електране испоручују константу количину електричне енергије, након повећаног укључења соларне енергије то више није случај. Децентрализована природа соларних система ојачава стабилност система али истовремено уноси и нове проблеме и потешкоће у управљању мрежом, што повећава зависност соларне енергије од паметних, мрежних технологија, па самим тим и повећава захтеве сајбер сигурности.

Као најрањивија тачка а и најбитнија у овим системима су соларни инвертери, према најновијим анализама из БитДефендер-а (BitDefender) запажено је да низ рањивости у инвертерима произвођача Солармен и Дај (Solarman and Deye) може да утиче на милионе уређаја. Ово укључује компромитовање целих налога, дупликација токена на низу платформи, непотребно дељења података и интегрисане шифре у фирмвер инвертера.

У комбинацији са временом потребним (Слика 14.) са отклањање ових грешака, рањивости ово угрожава енергетске системе нападима, дестабилизацији електричне мреже и недозвољеном прикупљању података.

Solarman:

- May 22, 2024: Bitdefender reaches out to Solarman for a security contact
- May 23, 2024: Bitdefender gets in touch with Solarman security team and sends vulnerability information
- May 24, 2024: Vulnerabilities acknowledged; account takeover gets immediately fixed
- Jun 17, 2024: Vendor confirms that a fix for the API returning too much information is in place.
- Jul 17, 2024: Vendor confirms that the Deye token reuse issue is now fixed.

Deye:

- May 22, 2024: Bitdefender reaches out to Deye for a security contact
- Jun 03, 2024: Authorized security partner asks Bitdefender for details
- Jun 06, 2024: Bitdefender sends the vulnerability report
- Jun 17, 2024: Bitdefender asks for an update on the reported issues
- Jul 09, 2024: Deye sends an overview of the fixed issues
- Aug 07, 2024: This report becomes public as per the coordinated vulnerability disclosure protocols.

Слика 14. Слика приказује време потребно произвођачима Солармен и Дej да исправе проблеме на које им је указано из БитДефендера.

Истраживање је генерално обављено на Солармен опреми (даталогерима) који су популаран избор за употребу са Дej(Deye) инвертерима, такође је познато да је Дej користио основни систем Солармен инвертера и пратећих уређаја све до почетка 2024 године када је урађена имлементација за њихове инвертере и датацентре. Солармен као један од највећих произвођача не само да производи опрему под својим именом, већ и опрему коју лиценцирају другим произвођачима који се тренутно налазе међу најпопуларнијим, што значи да и сами имају исте рањивости, ту спадају: Дej(Deye), Афор(Afore), Канадиан Солар(Canadian Solar), Софар(Sofar), Интелбрас(Intelbras), Хавелс(Havells),Анфоуте(Anfuote), Бејндсун(Beyondsun), Фксповер(Fxpower) итд.

Солармен АПИ за дата логере представља приступну тачку за многим рањивостима које могу бити искорошћене за узнемиравање или комплетно обустављање рада фотонапонске опреме.

Дата логер (data logger) (Слика 15.) – уређај (може бити засебан или уграђен у претварач) који бележи и преноси податке о перформансама фотонапоснког система, омогућава праћење у реалном времену, логовање (бележење историје), даљинско управљање, омогућавајући да систем функционисе ефикасно и без проблема. Прикупљање метрике као што су излазна снага, напон, струка, даталогер помаже у оптимизацији производње

и коришћење енергије, олакшавајући одржавање путем нотификација и упозорења, интеграцију са рачунарством у облаку за даљинско управљање .

Слика 15. Солармен дата логери

Солармен платформа подржава креирање два типа налога, један је обичан кориснички налог који кориснику даје увид у доступне информације у реалном времену, а други је бизнис, сервисерски који има ауторизације за подешавање уређаја приликом инсталације, као што су напон, фреквенција итд.

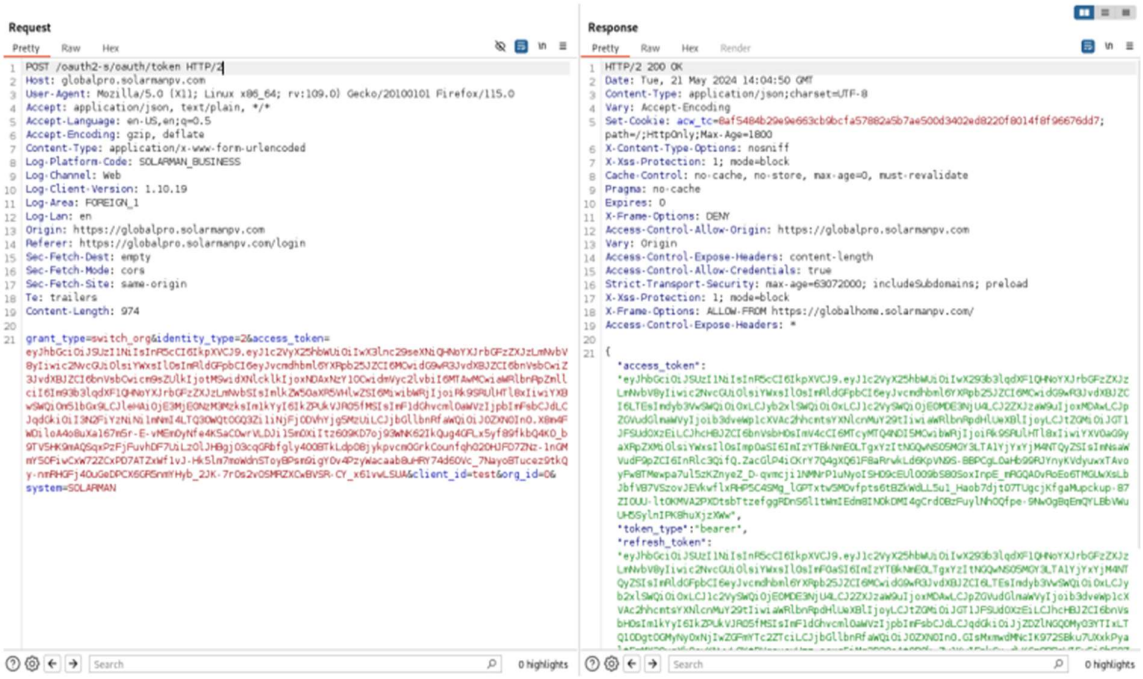
5.1.Рањивости Солармен (Solarman) соларне опреме

Пронађен је низ критичних безбедносних рањивости у Солармен платфори. Рањивости које обухватајо потпуно преузимање налога, преузимање Дej клауд токена и прикупљање података организације или корисника, што представља велики ризик за сигурност платформе и приватност корисника.

5.1.1. Преузимање контроле налога манипулацијом ауторизационих токена

Опис: АПИ ендпоинт /oauth2-s/oauth/token се користи за прибављање ауторизационог токена приликом промене организације за управљање, сервер не успева да верификује JBT(JWT) потпис, допуштајући нападачима да добију валидациони токен за било који налог модификовањем JBT(JWT) дела.

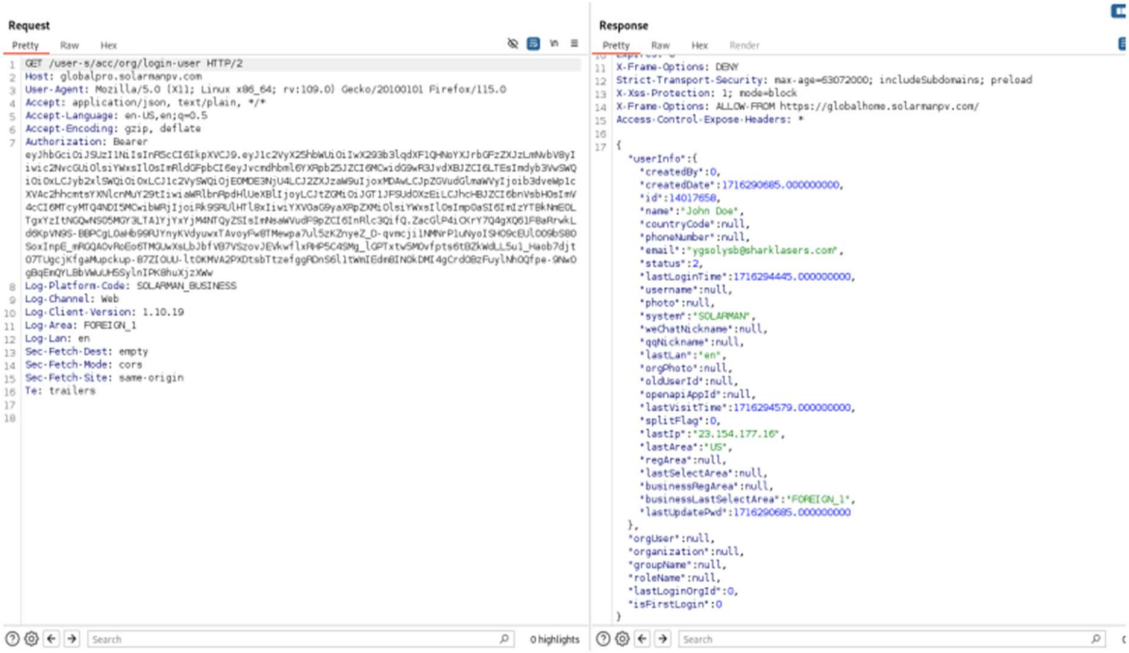
Утицај: Нападач може модификовати JBT(JWT) тако да садржи кориснички Ид (userId) произвољног корисника, што за резулат има недозвољени приступ и комплетну контролу над налогом.



Слика 16. Приказује прибављање JBT (JWT) токена

Техничка спецификација:
Ендпоинт(Endpoint): /oauth2-s/oauth/token
Рањивост: Недостатак верификације JBT(JWT) потписа.
Експлоит: Модификација JBT(JWT) токена да садржи кориснички Ид (userId) и имејл.

Након прибављања JBT(JWT) токена циљаног налога, добија се потпуна контрола над њим.



Слика 17. Приказује захтев и повратне информације о дему корисничком налогу

5.1.2. Поновна употреба Дај Клауд токена

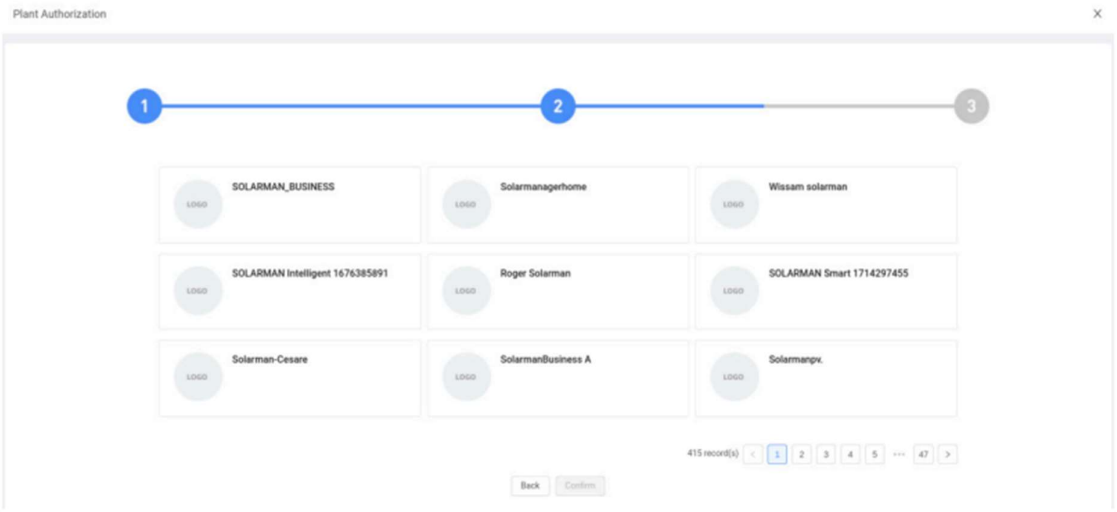
Опис: JBT(JWT) токен издат од стране Дај Клауд платформе има валидност у примени и на Солармен платформи, дозвољавајући потпун приступ налогу са специфичнм корисничким Ид-јем, иако овај Ид не одговара истом корстику на Солармен платформи, на пример корисник са Ид-јем 100 може бити на Дај платформи корисник А док на Солармен платформи може бити корисник Б.

Утицај: Рањивост дозвољава нападачима да прибаве JBT(JWT) токен са Дај Клауда и добију ауторизацију за приступ Солармен налозима.

Техничка спецификација:
Рањивост: Међу платформни JBT(JWT) токени.
Експлоит: Коришћење Дај Клауд JBT(JWT) токена за приступ Солармен налозима.

5.1.3. Прикупљање података кроз /group-s/acc/orgs АПИ ендпоинт

Опис: АПИ ендпоинт /group-s/acc/orgs враћа непотребне податкке о кориснику, организацију за приликом претраживања. Одговор укључује осетљиве податке као што је имејл, имена, бројеви телефона, државе и корисничке Ид-је.



Слика 18. Пример листе организација којој нападач може да добије приступ

Утицај: Нападач добија приватне информације свих регистрованих организација прављењем више АПИ позива.

Техничка спецификација:
Ендпоинт: /group-s/acc/orgs
Рањивост: Непотребно дељење приватних информација.
Експлоит: Добијање приватних информација АПИ позивима.


```
{
“total”: 415,
“data”: [
{
“org”: {
“createdDate”: 1716116429.000000000,
“id”: 10535375,
“type”: 2,
“businessType”: null,
“name”: “SOLARMAN_BUSINESS”,
“topGroupId”: 10336654,
“areaId”: 112,
“timezone”: “Europe/Amsterdam”,
“logo”: null,
“adminId”: 13669824,
“system”: “SOLARMAN”,
“category”: 1,
“originalLogo”: null,
“operateObject”: null,
“totalNames”: null,
“status”: null,
“splitFlag”: 0
},
“nameList”: [
{
“id”: 13656565,
“relateId”: 10535375,
“relateType”: 1,
“name”: “SOLARMAN_BUSINESS”,
“language”: “it”
}
],
“adminName”: “[redacted]”,
“adminPhoneNumber”: null,
“adminEmail”: “[redacted],
“entityRel”: null,
“adminCountryCode”: null,
“memberCount”: null,
“adminUsername”: “[redacted]”,
“adminLastVisitTime”: 1716457108.000000000
}
]
}
```


Слика 19. Пример одговора са осетљивим информацијама

5.1.4. Анализа утицаја рањивости

Установљења рањивост представља велике ризике који укључује:
- Недозвољен приступ корисничким налозима и осетљивим подацима.
- Малициозна употреба приватних информација.
- Нарушавање интегритета појединачних корисника и организација.

5.1.5. Процедура обавештења и поправљања рањивости

May 22, 2024: Bitdefender reaches out to Solarman for a security contact

May 23, 2024: Bitdefender gets in touch with Solarman security team and sends vulnerability information

May 24, 2024: Vulnerabilities acknowledged; account takeover gets immediately fixed

Jun 17, 2024: Vendor confirms that a fix for the API returning too much information is in place.

Jul 17, 2024: Vendor confirms that the Deye token reuse issue is now fixed.

Aug 7, 2024: This report becomes public as per the coordinated vulnerability disclosure protocols.

Слика 20. Процедура обавештења и поправљања рањивости

5.2.Рањивости Дej (Deye) соларне опреме

Дej(Deye) платформа нуди решење за управљање системима и уређајима у електричној мрежи, приликом провере сигурности пронађене су рањивости у систему које могу угрозити систем и или податке уређаја и корисника.

Уочено је неколико критичних рањивости у Дej(Deye) систему. Ове рањивости укључују хардкодиране налоге са неограниченим приступом уређају, непотребно дељење података кроз АПИ ендпоинте и генерисање недозвољених ауторизационих токена.

5.2.1. Хардкодирани профили

Опис: Дej(Deye) апликација користи хардкодиране профиле, на пример SmartConfigurator@solarmanpv.com са шифром 123456 за приступљање АПИ-ју у клауду и добијање ауторизационог токена са api4pro.solarmanpv.com АПИ сервера.

Утицај: Нападач може да искористи добијени токен за прибављње информација о било ком уређају, укључујући софтверске или хардверсе верзије, имена, ВајФај ССИД, шифре, безобзира на бласништво уређаја.

Техничка спецификација:
Налог SmartConfigurator@solarmanpv.com
Шифра: 123456
Рањивост: Хардкодирани подаци са неограниченим приступом.
Експлоит: Употреба хардкодираног профила за приступ било ком уређају.

Пример захтева за универзални токен:

```
GET /deviceConfig-s/mix/config/open/device/[DEVICE SERIAL NUMBER] HTTP/2
Host: api4pro.solarmanpv.com
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.
yJ1c2VyX25hbWUiOiIwN1NtYXJ0Q29guZmlndXJhdG9yQHNvbGFybWFucHYuY29tIiwiaW5zdG-
FudCI6ImV4YW1wbGVfdG9rZW4ifQ.2gtXZIuCJ2yZ9wZSt6IwYJhbGwiXSw1ZGVwL1slj7PT-
m9yZZFuA2FGhpdkvblkKIjJowLCbQb3BHcgm9LcElkIjpuWdXsLCJmcm9sLCElkIjpuWdXsLC-
Jyb2xlSWQiOiJcOiJ2c2VySWQiOjUwMzc1LCJmYW1sZXJvbGVzIjpmRWp2mLmclcj1lNTkYJ0X-
Q29uZmJndXJhdG9yQHNvbGFybWFucHYuY29tIiwiaW5zdGFudCI6ImV4YW1wbGVfdG9rZW4ifQ.
h2A1uEoVgex6yxH6Aex7ZITofXCeD3d7N3rJ1Sdzqr7nyCG6ugnvZ8trZJzo2Gp-Q8emOEmE34sEcwM-ttU0NCu-
UqHQ
Accept-Encoding: gzip, deflate
User-Agent: okhttp/4.9.3
```

Слика 21. Пример захтева за универзални токен

Пример одговора:


```
{
  "createdBy": null,
  "createdDate": null,
  "lastModifiedBy": [redacted],
  "lastModifiedDate": 1701922941,
  "deviceSn": "[redacted]",
  "devicePassword": "[redacted]",
  "brand": 1,
  "model": "LSW-3A5251-C",
  "hardwareVersion": "LSW-3DY1433T-VH1.0.0(2019-12-25)",
  "initFirmwareVersion": "MWXT-LPB100_RELOAD_V1.0.4(2018-05-25)lsw3",
  "communicationMode": "2",
  "networkingConfig": 1,
  "networkingJoin": 1,
  "deviceType": 18,
  "dataSource": 2,
  "companyId": 1,
  "batchId": "[redacted]",
  "localCommMode": 1,
  "wifiFrequency": "1",
  "gatewayKey": null,
  "shipperName": null
}
```


Слика 22. Пример одговора

5.2.2. Прибављање података кроз /user-s/acc/orgs АПИ ендпоинт

Опис: АПИ ендпоинт /user-s/acc/orgs на eu1.deyecloud.com враћа сувишне информације о кориснику током провере ауторизације. Одговор укључује битне информације као што су име, имејл, број телефона, државу, и корисничке Ид-јеве.

Контекст: Корисник може дозволити другим корисницима пристум његовом систему, Тако што се користи претраживање корисника, по именну, а претрага враћа број телефона или имејл адресу. Док АПИ позив враћа чак и приватне податке о корисницима.


```
"org":{
  "createdDate":1703824002.000000000,
  "id":1[redacted]6,
  "type":2,
  "businessType":"1,2,3,4,5,6",
  "name":"[redacted],
  "topGroupId":10236285,
  "areaId":70,
  "timezone":"Europe/Amsterdam",
  "logo":null,
  "adminId":[redacted],
  "system":"Deye",
  "category":1,
  "originalLogo":"",
  "operateObject":null,
  "totalNames":"[redacted]",
  "status":2,
  "splitFlag":0,
  "unifiedSocialCreditCode":null,
  "licenseNumber":null,
  "legalPersonName":null,
  "legalPersonPhone":null,
  "legalPersonEmail":null
},
"nameList":[
  {
    "id":1[redacted]7,
    "relateId":1[redacted]6,
    "relateType":1,
    "name":"[redacted],
    "language":"en"
  }
],
"adminName":null,
"adminPhoneNumber":"",
"adminEmail":"j[redacted]com",
"entityRel":null,
"adminCountryCode":"",
"memberCount":null,
"adminUsername":"",
"adminLastVisitTime":null
},
{
```

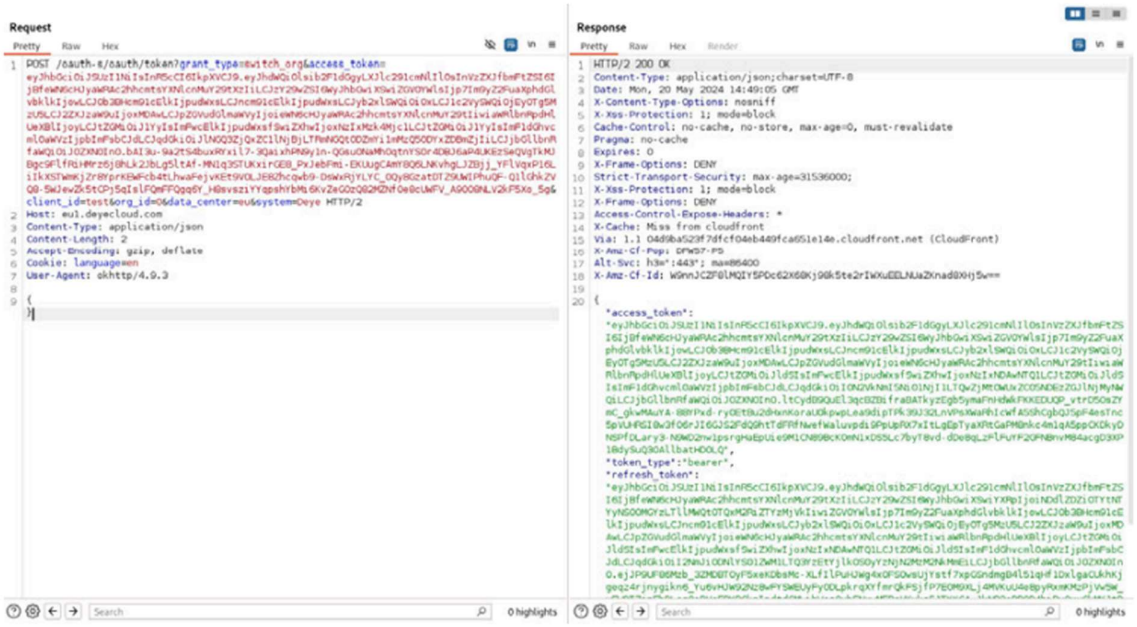

Слика 33. Пример одговора кроз АПИ позив

Последице: Нападач овим путем долази до приватних информација.

5.2.3. Генерисање недозвољених токена ауторизације

Опис: АПИ ендпоинт /oauth-s/oauth/token употребљава се за добијање ауторизацион токена у тренутку промене организација којим се управља. Сервер не успева да ферификује JBT(JWT) токен, дозвољавајући нападачима да генеришу валидациони токен.

Последице: Иако сервер враћа токен он поставља параметар верзије на нал(null) уместо на 1000, због тога сервер одбија овај токен као невалидан. Уколико је 1000 могуће је генерисање токена за било ког корисника на платформи.



Слика 34. Приказује захтев и повратне информације о дему корисничком налогу

Техничка спецификација:
Ендпоинт: /oauth-s/oauth/token
Рањивост: Непостојаност JBT(JWT) верификације потписа.
Експоит: Модификација JBT(JWT) токена да садржи кориснички Ид и имејл и постављање верзије.

5.2.4. Анализа утицаја рањивости

Идентификоване рањивости представљају велике ризике, који укључују:

- Недозвољен приступ уређајима и подацима
- Могућа злоупотреба података
- Компромитовање поверења корисника и интегритета платформе.

5.2.5. Процедура обавештења и поправљања рањивости

May 22, 2024: Bitdefender reaches out to Deye for a security contact

Jun 03, 2024: Authorized security partner asks Bitdefender for details

Jun 06, 2024: Bitdefender sends the vulnerability report

Jun 17, 2024: Bitdefender asks for an update on the reported issues

Jul 09, 2024: Deye sends an overview of the fixed issues

Aug 07, 2024: This report becomes public as per the coordinated vulnerability disclosure protocols.

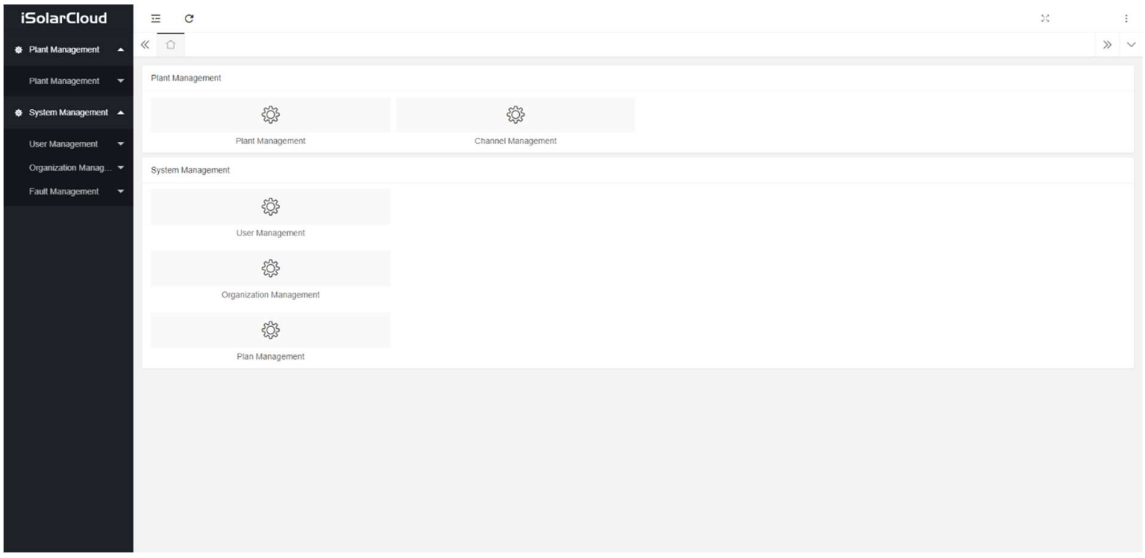
Слика 35. Процедура обавештења и поправљања рањивости

5.3.Рањивости Сангроу (Sungrow) соларне опреме

Истраживањем анонимног избора пронађене су рањивости и у Сунгроу систему, конкретно ајСоларКлауд (iSolarcloud (iSC)) систему за мониторинг и контролу свих фотонапонских претварача (инвертера) и решења за складиштење електричне енергије произвођача Сангроу (Sungrow). иСЦ омогућава контролу: конфигурацију уређаја на даљину, управљање конекцијама електране, ЛАН конфигурацију, аларме кроз нотификације, управљање гешкама, мониторинг. Логовање у систем корисник врши кроз веб интерфејс или мобилну апликацију.

Овај систем нуди више типова корисничких профила који су уређени у хијерархију од три нивоа:

- Супер администратор (SuperAdministrator)
- Администратор (Administrator)
- Корисник (User)



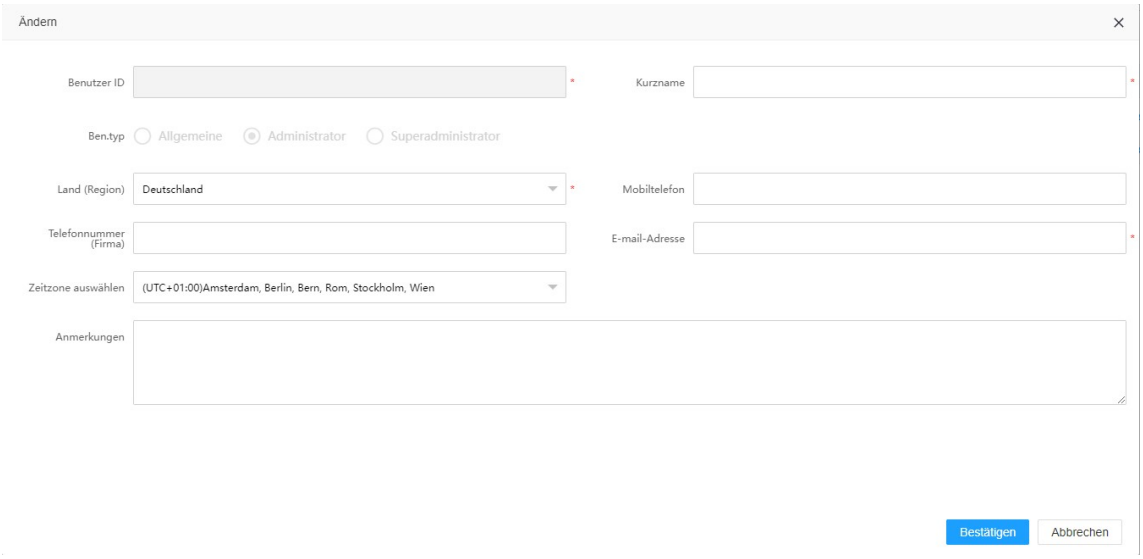
Слика 36. Администраторски профил

Администратор има могућност управљања позадином (backend) системима (Слика 36.) на највишем нивоу и управљање информацијама на том нивоу, управљање чворовима што укључује креирање нових региона и креирање чворова у тим регионима, креирање нових корисничких налога у управљање електранама.

Тип профила који има крајњи корисник се налази на најнижој позицији у хијерархији система, он нема увид у функционисање и управљање позадином система, већ може да користи крајње сервисе платформе. Такође функционалност сваког корисничког профила је ограничена додатно регионом у којем се налази - Кина, Европа, Аустралија итд.

5.3.1. Рањивост

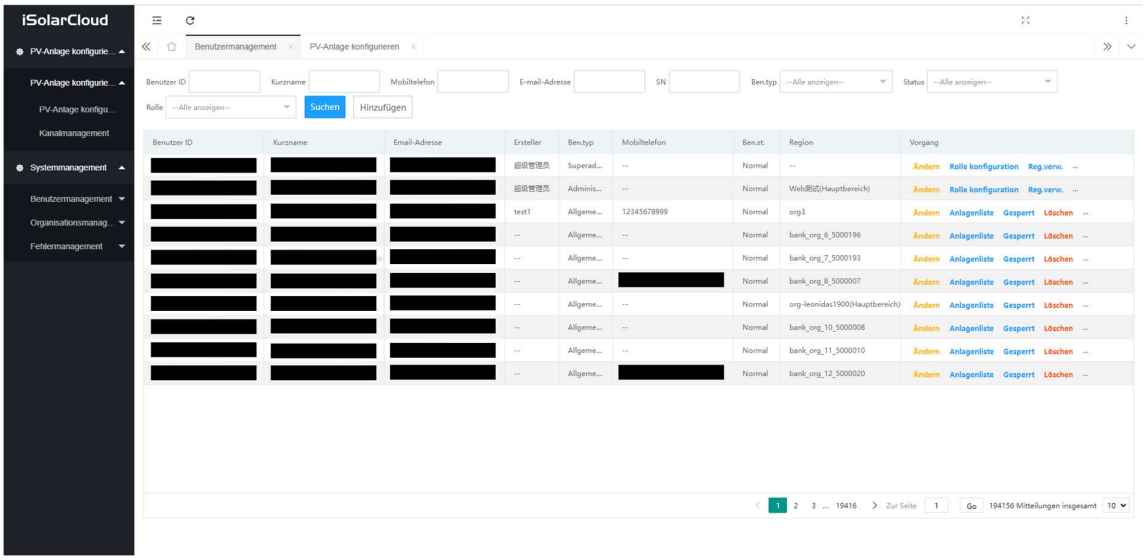
Систем за управљање омогућава додавање нових и уређивање постојећих кориснилких налога. У оквиру дијалога за подешавање профила (Слика 37.) могуће је променити детаље профила, имејл, временску зону, улоге. Баш у том дијалогу откривена је искључена радио контрола за уређивање нивоа корисника.



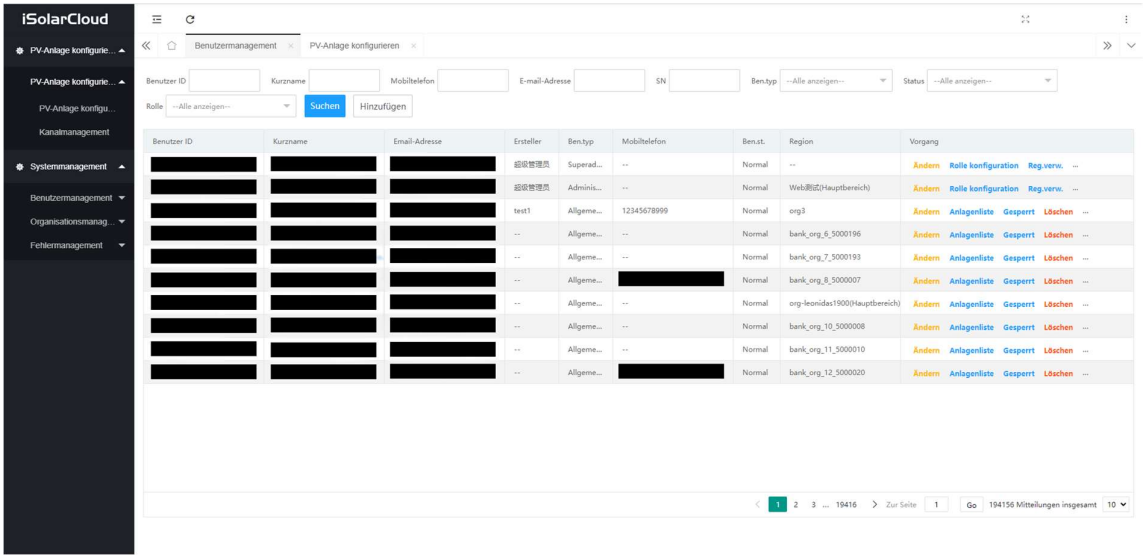
Слика 37. Форма за подешавање профила

Кроз ХТМЛ код веб сајта могуће је омогћити ту контролу и на овај начин нападач може да измени ниво било ког профила све до супер администратора. Клауд сервер не врши никакву проверу да ли је то дозвољено или не. У случају да нападач постави ниво свог профила на супер администратора он добија комплетно управљање свим системиа. Што представља велики ризик, собзиром да има контролу над свиме.

Привилегије супер администратора дозвољавају приступ свим ресурсима унутар региона налога, што укључује:



Слика 38. Читање, брисање или модификацију било ког корисничког профила унутар иСЦ система



Слика 39. Читање, брисање или модификација било које електране унутар иСЦ система

Овај тип привилегија ради у свим регионима иСЦ-еа. Нападач чак не мора да посадује Сангроу хардвер или да се налази у истом региону као циљ напада, пошто нови корисници могу бити креирани произвољно.

5.4.Рањивости Енфејз (Enphase) соларне опреме

Енфејз (Enphase) је Америчка компанија која производи производе за производњу, употребу електричне енергије, углавном су то инвертери и станице за пуњења, већину тржишта чине производи за појединачне кориснике.

Слика 40. Енфејз лого

Истраживањем неколико независних лабараторија ИНЛ, ДИВД, ЦИСА на Енфејз (Enphase) уређајима дошло је до откривања неколико типова рањивости, на основу чега су и груписане.

Рањивости су груписане:

- CVE-2023-32274 – на мобилна апликација за иницијализовање, конфигурацију и инсталацију Енфејз система (Енфејз алат за инсталацију (Enphase Installer Toolkit)). Апликација омогућава кориснику да повеже Енфејз Енвој претварач на гејтвеј (gateway) путем бежичне мреже и мониторинг система. Пронађено је да верзија 3.27.0 и касније верзије андроид апликације садрже хардкодиране креденцијале, који могу бити употребљени у сврху напада.

- CVE-2023-33869 – је рањивост која дозвољава убризгавање команди (command injection) у Енвој комуникационом гејтвеју верзије Д7.0.88, која дозвољава нападачу добијање роот приступа уређају, извшавање команди.

- CVE-2020-25754 – на Енфејз Енвој уређајима P3. и P.4 серије, постоји ПАМ модул за аутенфикацију корисника, не врши се класична аутентификација корисника. Овај модул користи шифру изведену из МД5 хеша корисничког имена и серијског броја. Проблем настаје зато што присуством ове рањивости неаутентификовани корисник може приступити серијском броју на даљину.

- CVE-2020-25753 – постојање уграђене администраторске шифре која је последњих шест цифара серијског броја за одређене верзије фирмевра, као и у прошлој рањивости могуће је бежично прибављање.

- CVE-2020-25752 – хардкодиране шифре за инсталер и Енфејз налог, немогућа промена.

- CVE-2019-7676 – могућност постављање слабе шифре.

5.5.Рањивости Контек (Contec) соларне опреме

Истраживањем ВулнЧек-а (VulnCheck) откривене су три нове рањивости које утишу на убризгавање команди (command injection) рањивост, што би могло довести у опасност стотине соларних система. Пошто се Контек бави производњом индустријске опреме, соларне електране, комерцијалне зграде, ове рањивости су од још већег значаја.

Слика 41. Контек лого

- CVE-2022-29303 – недозвољено, бежично (на даљину) убризгавање команди на conf_mail[dot]php ендпоинт, прво појављивање ове рањивости је забележено на верзији 4.0 фирмвера, а исправљено је у верзији 8.0.

- CVE-2023-23333 – рањивост убризгавања команди преко downloader[dot]php ендпоинта.

- CVE-2022-44354 – рањивост која дозвољава уплоудовање ПХП вебшела на Solar_Image[dot]php ендпоинт у систем, прво појављуивање је на верзији 4.0, исправљено је на верзији 7.0.

Забележене су и рањивости на мобилној апликацији која служи за управљање системом:

- Контек Солар Вју (2023):
    - Оверфлоу бафера у неким веб страницама дозвољава извршење кода
    - Пролаз кроз директоријуме дозвољава приступ приватним подацима

5.6.Рањивости Сименс (Siemens) соларне опреме

Сименс тим за испитивање сигурности (Siemens Energy ProductCERT) и објављује предлоге, безбедносне савете за рањивости које директно утичу на Сименс Енерџи призводе и захтевају акцију корисника.

Као део својих константих напора да помогне оператерима да управљају безбедносним ризицима, Сименс Енерџи (Siemens Energy ProductCERT) пружа информације потребне за процену безбедносних проблема.

Слика 42. Сименс лого

SSA-857368 – Низ рањивости у Омниверс Т3000 систему, најновији систем, све наведе рањивости су из 2024 године:

- CVE-2024-38876 – апликација са овим проблемом дозвољава извшавање кода обичног корисника као да има администраторске привилегије.

- CVE-2024-38877 – уређаји чувају креденцијале за логовање корисника без примене потребних заштита, нападач са даљинским приступом терминалу или физичким може да прибави све податке, што дозвољава несметано кретање кроз мррежу.

- CVE-2024-38878 – рањив ендпоинт АПИ-ја који дозвољава недозвољено скидање података са уређаја.

- CVE-2024-38879 – отворен порт интерне аплиакције на јавној мрежи, дозвољава нападачу да комплетно заобиђе логовање.

Сименс даје мапу типова рањивости као и њихов број у зависности од године (Слика 43.)

Year	Code Execution	Bypass	Privilege Escalation	Denial of Service	Information Leak
2014	3	0	0	13	2
2015	2	2	2	6	8
2016	2	9	9	11	10
2017	9	8	8	11	5
2018	15	11	13	21	3
2019	23	22	22	58	15
2020	9	4	4	21	7
2021	145	7	9	86	11
2022	104	17	18	48	7
2023	132	5	6	24	4
2024	80	4	3	19	1
Total	524	89	94	318	73

Слика 43. Типова рањивости рањивости

Сименс такође даје мапу најзаступљенијих рањивости као и њихов тип у зависности од године (Слика 44.).

Vulnerability Trends Over Time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2014	0	0	0	2	2	0	1	0	0	1	1
2015	1	0	0	1	1	0	1	0	0	1	6
2016	0	0	1	2	0	0	1	0	0	0	8
2017	4	4	0	4	1	0	2	1	0	0	8
2018	5	2	0	7	3	0	3	0	0	1	12
2019	44	38	1	10	3	0	3	0	0	0	5
2020	9	23	4	14	5	0	2	0	1	0	7
2021	66	118	8	4	25	1	3	5	0	0	40
2022	52	76	2	20	2	5	5	1	1	2	19
2023	27	66	4	7	8	1	2	2	0	0	4
2024	9	27	3	0	4	3	1	0	0	0	1
Total	217	354	23	71	54	10	24	9	2	5	111

Слика 44. Мапа најзаступљенијих рањивости

6. Степен отворености (Attack surface)

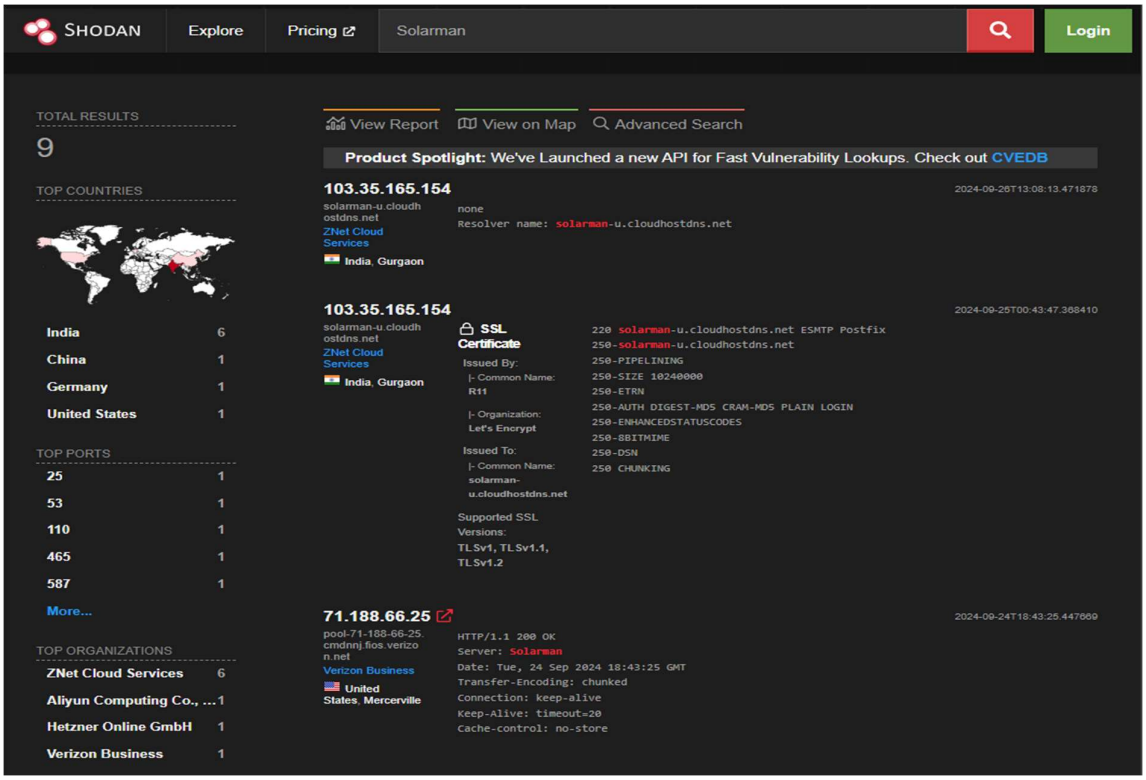
Степен отворености је број свих могућих тачака или вектора напада где неовлашћени корисник може приступити систему и прибавити податке. Што је мањи степен отворености већа је безбедности ситема. Организације морају стално настојати смањењу степена отворености како би смањиле ризик од успешних сајбер напада. Међутим, то постаје све теже како проширују своје дигитално присуство и прихватају нове технологије.

Степен отворености се дели на две категорије: дигиталну и физичку.

6.2.Дигитални степен рањивости

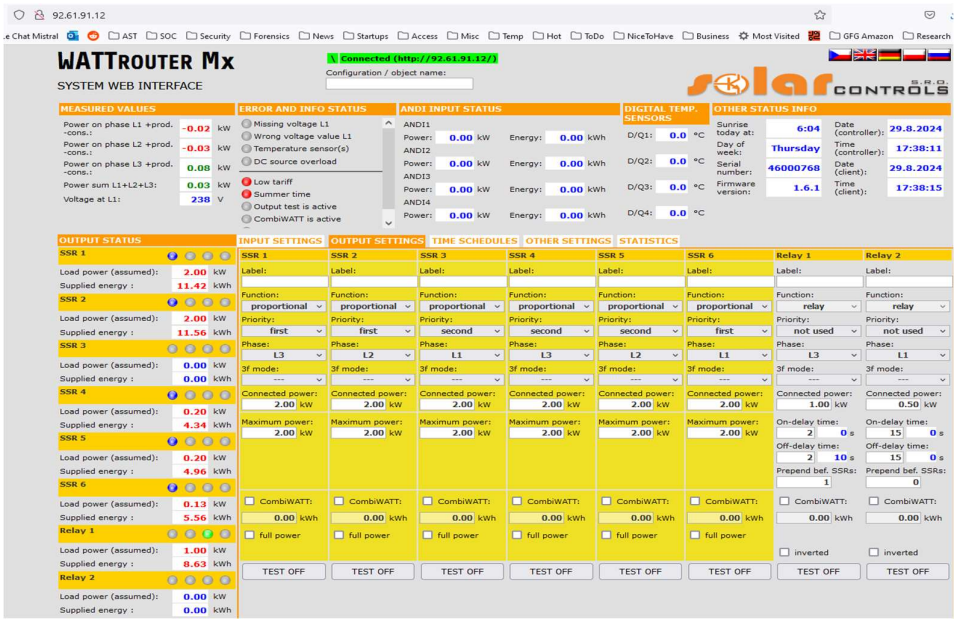
Дигитална степен рањивости обухвата сав хардвер и софтвер који се повезују на мрежу организације. Ово укључује апликације, код, портове, сервере и веб-сајтове, као и „shodan IT“ (неовлашћено коришћење апликација или уређаја од стране корисника који заобилазе ИТ оделење). Када се ради о оваквом типу уређаја као што су соларни претварачи, где мере сајбер безбедности нису прописане и саме имплементиације призвођача немају дефинисани стандард, могу постојати велике варијације.

Употребом алата за претрагу као што је "shodan.io" добијамо листу уређаја (Слика 45.) који у свом хедеру садрже претражени термин, то могу бити уређаји било ког типа.



Слика 45. приказ "shodan.io" претраге

Соларни претварачи су многобројни на овом списку, са као и претходно наведеним различитим степеном отворености, од уређаја који не дају никакав приступ са јавне мреже као на пример први на слици изнад до уређаја који су потпуно отворени за недозвољене кориснике (Слика 46.).



Слика 46. Пример приступа уређају

6.3.Физички степен рањивости

Физичка површина напада обухвата све крајње уређаје до којих нападач може физички доћи, као што су десктоп рачунари, хард дискови, лаптопови, мобилни телефони и USB меморије. Претње физичкој површини укључују неопрезно одложен хардвер који садржи корисничке податке и акредитиве за логовање, кориснике који записују лозинке на папир.

Организације могу заштитити физичку површину напада кроз контролу приступа и надзор око својих физичких локација.

7. Закључак

Интеграцијом Интернет ствари технологија у електроенергетске системе доноси велике погодности, побољшања, сигурности, ефикасности, али истовремено и отвара врата у комплетно нови свет претњи. Тренутно највећу примену Интернет ствари у електропривреди представљају соларни претварачи (инвертери). Интернет ствари технологија омогућава реализацију децентрализованих енергетских извора (ДЕР), као што су фотонапонски, ветар, вода, и других обновљивих извора. Ово је довело до већег ослањања на паметне технологије и мрежне системе. Са свим својим предностима Интернет ствари технологије доносе и мане, чине претходно затворени систем електропривреде изложен новим претњама, сајбер ризицима.

Један од значајних фактора који доприноси овом проблему је глобална доминација кинеских произвођача у сектору производње ПВ опреме, укључујући соларне инвертере. Према подацима Међународне енергетске агенције (IEA), Кина тренутно производи око 80% светске фотонапонске опреме, а овај тренд ће се наставити и у будућности. Ова доминација ствара одређене бриге у погледу сајбер безбедности, јер постоји могућност да кинески производи буду коришћени за сајбер шпијунажу или друге облике сајбер напада. Кинески закон о националној безбедности додатно придодаје на ове сумње, јер обавезује све кинеске компаније да сарађују са националним обавештајним службама, што изазива забринутост међу међународним купцима њихове опреме.

Како се све већи број домаћинстава и предузећа ослања на соларну енергију и друге обновљиве изворе енергије, рањивост соларних инвертера постаје све озбиљнији проблем. Иако соларни системи које користе појединци вероватно неће бити примарна мета сајбер напада ради уцене, они могу бити искоришћени као платформа за покретање контра и DDoS напада против трећих страна. Соларни системи представљају кључну компоненту глобалних напора за прелазак на обновљиве изворе енергије и одрживи развој, али, како се њихов значај повећава, тако се повећава и ризик од сајбер претњи. Самим тим сајбер претње које угрожавају соларне инвертере могу бити веома озбиљне, угрожавање ових уређаја може довести до прекида у снабдевању електричном енергијом па чак и до ширења напада на друге делове електроенергетске мреже. Рањивост соларних система указује на бројне и комплексне безбедносне претње које су се појавиле у овом брзо растућем енергетском сектору.

Различити произвођачи користе различите системе, различите технологије повезивања, комуникације, нивоа заштите ако их уопште има. Сва та разноврсност технологија и њихово комбиновање, као и пропусти приликом имплентације истих довело је до стварања ризика, рањивости. На шта ни један произвођач није имун.

Са циљем да се формира листа правила, прописа које морају испуњавати произвођачи, темељна анализа претњи и стандарда безбедности соларних инвертера је од кључне важности за очување стабилности и сигурности енергетских система. У будућности, континуирано унапређивање безбедносних мера и стандарда биће кључно за обезбеђивање стабилности енергетских система, а све ће бити последица формираних правила и прописа.

8. Литература

[1] Rachael Falk and Anne-Louise Brown, „POWER OUT? SOLAR INVERTERS AND THE SILENT CYBER THREAT“, Cyber Security Cooperative Research Centre, Доступно:https://cybersecuritycrc.org.au/sites/default/files/202311/3320_cscrc_powerout_art_web.pdf

[2] James McCarthy, Jeffrey Marron, Don Faatz, Daniel Rebori-Carretero, Johnathan Wiltberger, Nik Urlaub, „Cybersecurity for Smart Inverters“, NIST Technical Series Publications, Доступно: https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8498.ipd.pdf

[3] „Inverter Communications: Types, Applications, and Future Trends“, Solartechadvisor, Доступно: https://solartechadvisor.com/inverter-communications/

[4] „List: Top 15 Best Inverter Companies In China (Update 2023)“, Hisen Power, Доступно: https://www.hisenpower.com/Blogs/top-15-best-inverter-companies-in-china

[5] Darshil Patel, „Defending the Smart Grid Against Inverter Attacks“, EETech, Доступно: https://eepower.com/tech-insights/defending-the-smart-grid-against-inverter-attacks/

[6] „Powering Up Risk: Inverters Vulnerable to Cybersecurity Threats Through Software“, solar2power, Доступно: https://solar2power.pt/powering-up-risk-inverters-vulnerable-to-cybersecurity-threats-through-software/

[7] Ioan Alexandru MELNICIUC, Alexandru LAZĂR, George CABĂU, Radu Alexandru BASARABA, „60 Hurts per Second – How We Got Access to Enough Solar Power to Run the United States“, bitdefender, Доступно: https://www.bitdefender.com/blog/labs/60-hurts-per-second-how-we-got-access-to-enough-solar-power-to-run-the-united-states/

[8] Megan Jordan Culler, Megan Mincemoyer Egan, Remy Vanece Stolworthy, Jake P Gentle „Attack Surface of Renewable Energy Technologies“, inldigitllibrary, Доступно: https://inldigitallibrary.inl.gov/sites/STI/STI/Sort_90576.pdf

[9] Kelsey Misbrener, „Cyberattacks threaten smart inverters, but scientists have solutions“, solarpowerworldonline, Доступно: https://www.solarpowerworldonline.com/2019/04/cyberattacks-threaten-smart-inverters-but-scientists-have-solutions/

[10] „“ Доступно:https://mazumder.lab.uic.edu/wpcontent/uploads/sites/504/2024/02/T_An_Overview_of_Cyber-Resilient_Smart_Inverters_Based_on_Practical_Attack_Models.pdf

[11] „Cyber Emergency Response at Siemens Energy“, Siemens, Доступно: https://www.siemens-energy.com/global/en/home/company/cybersecurity/cert-services.html

[12] Ioannis Zografopoulos, Graduate Student Member, IEEE, Nikos D. Hatziargyriou, Life Fellow, IEEE, Charalambos Konstantinou, Senior Member „Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations“, arxiv, Доступно: https://arxiv.org/pdf/2205.11171

[13] „SMA Solar Technology AG Sunny WebBox Hard-Coded Account Vulnerability“, cisa, Доступно: https://www.cisa.gov/news-events/ics-advisories/icsa-15-181-02a