Bezpieczeństwo i rozszerzony monitoring systemów fotowoltaicznych

Grzegorz Bardadyn

area account manager

Ustka, 26.05.2022

solaredge

Przykłady instalacji fotowoltaicznych

Solaredge informacje podstawowe

Poznaj SolarEdge

83.9M
Dostarczonych optymalizatorów

#1
Firma produkująca falowniki PV

405 Przyznanych patentów i **397** kolejnych zgłoszeń patentowych

34
Obecność krajów

$551.8M
Przychód w Q4 2021

>2.45M
Monitorowanych systemów w portalu monitorincu

3,800
pracowników

3.5M
Dostarczonych falowników

29.5GW
Dostarczonych systemów na świecie

solaredge

SolarEdge w liczbach

83.9M
Dostarczonych optymalizatorów

#1
Firma produkująca falowniki PV

405 Przyznanych Patentów i **397** kolejnych zgłoszeń patentowych

34
Obecność na rynkach

>2.45M
Monitorowanych systemów w Portalu Monitoringu

$655.1M
Przychody Q1 2022

3,800
pracowników

3.5M
Dostarczonych falowników

29.5GW
Dostarczonych systemów na całym świecie

solaredge

Globalny zasięg

- Ponad 45,000 instalatorów
- Obecność w 34 krajach
- Regionalne centra serwisowe
- Systemy zainstalowane w 133 krajach

R&D i linie produkcyjne

Centra badawczo-rozwojowe

- Izrael
- Bułgaria
- St. Zjednoczone (Kalifornia)
- Korea
- Włochy

Linie produkcyjne

- Chiny
- Wietnam
- Węgry
- Korea
- Izrael
- Meksyk

Bezpieczeństwo inwestycji

Miary zdolności bankowej

Preferencje ubezpieczeniowe

- Nowe standardy bezpieczeństwa PV opierają się na rozwiązaniach MLPE
  - Dokument FM Global „Property Loss Prevention Data Sheets" który zawiera wskazówki dotyczące zapobiegania utracie mienia związanego z pożarem i zagrożeniami naturalnymi w zakresie projektowania, instalacji i konserwacji wszystkich montowanych na dachu paneli fotowoltaicznych (PV) wykorzystywanych do wytwarzania energii elektrycznej
  - Rozdział 2.2 Elektryczna część sugeruje stosowanie MLPE

„Zapewnij układy elektroniczne na poziomie modułu MLPE (**takie jak optymalizatory** mocy i mikrofalownik), które wykrywają i izolują usterki oraz wyłączają zasilanie na poziomie modułu, a także alarmują o takich usterkach. System powinien raportować stan alarmowy do oprogramowania do zdalnego monitorowania sieci, umożliwiając szybkie wyłączenie systemów PV w budynkach zgodnie z definicją w NEC 2017. Patrz rysunek 2.2.2C."

2.2 Electrical

2.2.1 Install new PV electrical energy systems, including the array circuit(s), inverter(s), and controller(s) for these systems, in accordance with Article 690 of the 2017 version of NFPA 70, National Electrical Code (or equivalent international standard). Provide Module Level Power Electronics (such as DC optimizers and microinverters) that sense and isolate faults and deenergize the array at the module level, and alarm such faults. The system should report the alarm condition to remote network monitoring software, enabling rapid shutdown of PV systems on buildings as defined in NEC 2017. See Figure 2.2.2C.

For more information, see Section 3.3.

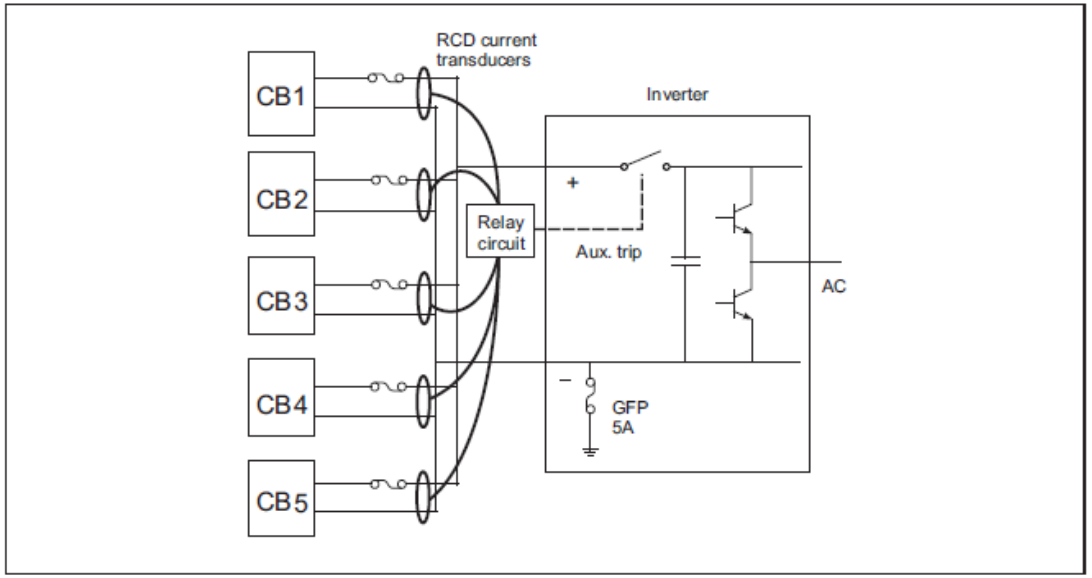
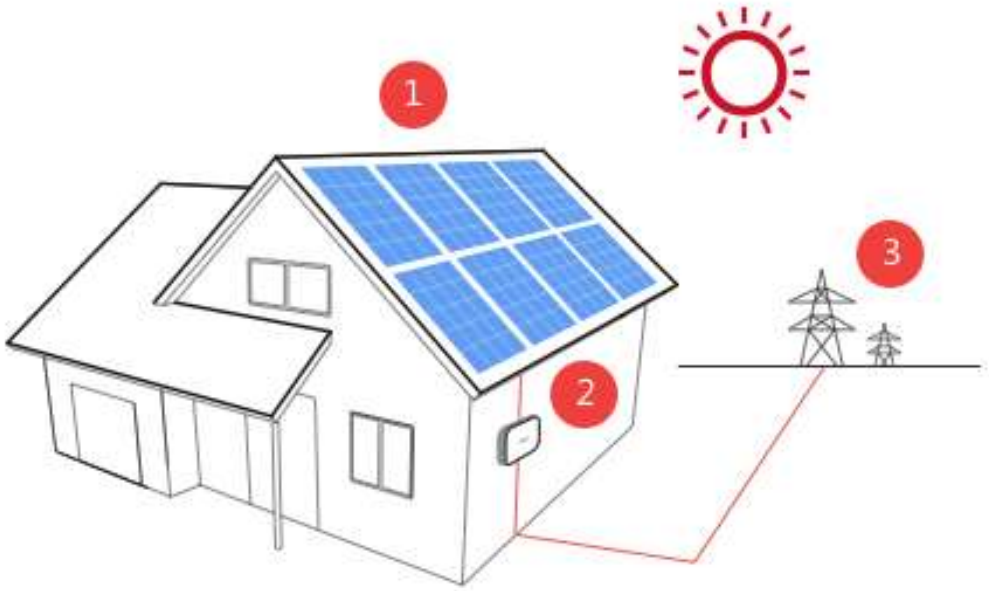


Fig. 2.2.2a. Example of residual current measurements with auxiliary trip (CB = combiner box, RCD = residual current disconnect, GFDI = ground fault detection and interruption)

Unikalna koncepcja

Tradycyjny system PV

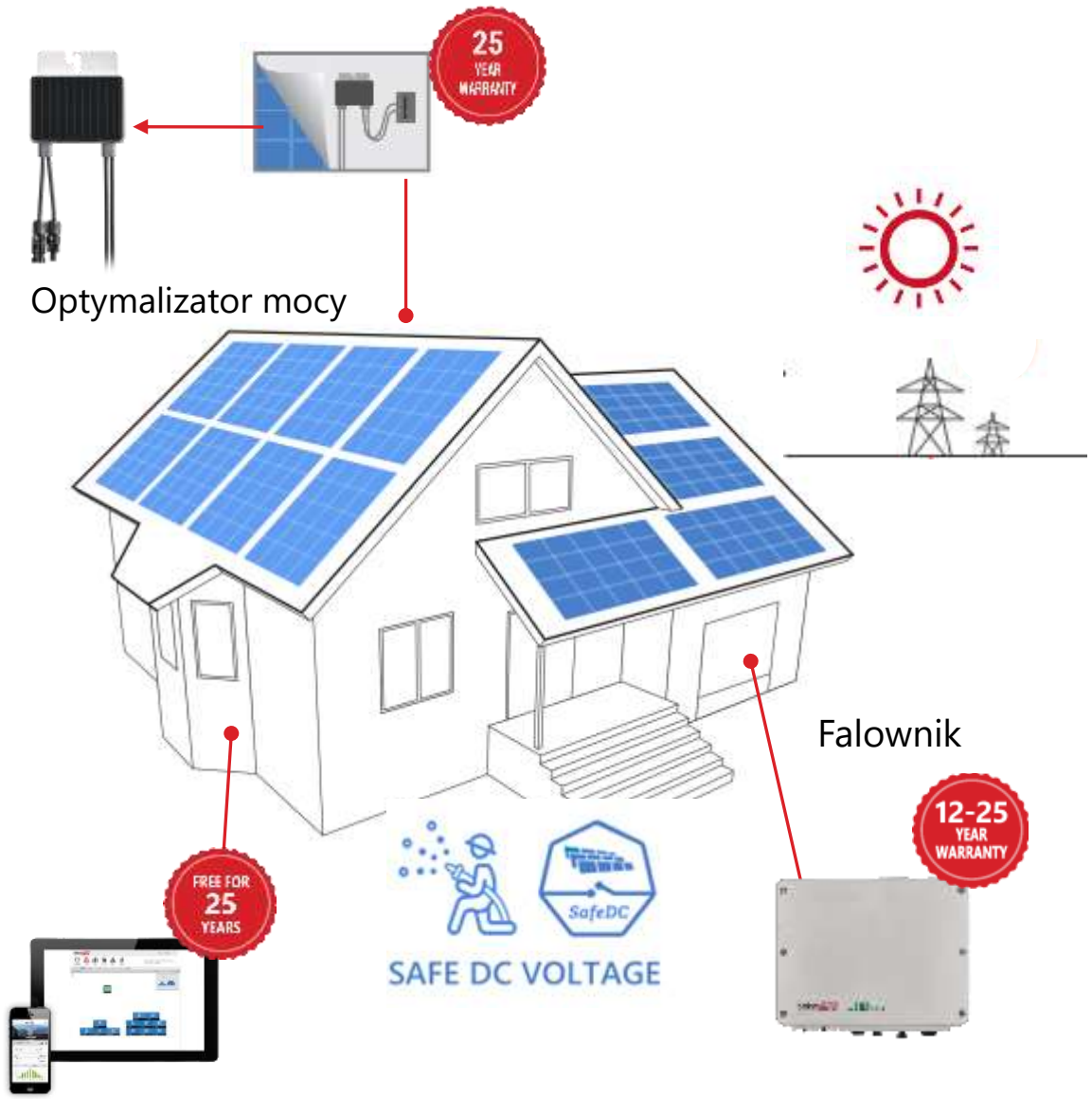
- Promieniowanie słoneczne padające na moduł fotowoltaiczny powoduje przemieszczenie ładunków elektrycznych w strukturze półprzewodnikowej modułu wywołując powstanie różnicy potencjałów, która umożliwia przepływ prądu stałego (DC) pomiędzy biegunami.
- Falownik solarny przekształca prąd stały z generatora fotowoltaicznego na prąd przemienny (AC) o stałej (wymaganej przez normy krajowe) częstotliwości
- Falownik optymalizuje również produkcję energii słonecznej na poziomie systemu i współdziała z siecią elektroenergetyczną.
- Falownik jest wyposażony w układ MPPT (śledzenia punktu mocy maksymalnej) na poziomie całego generatora – **nie rozróżniając poszczególnych modułów.**



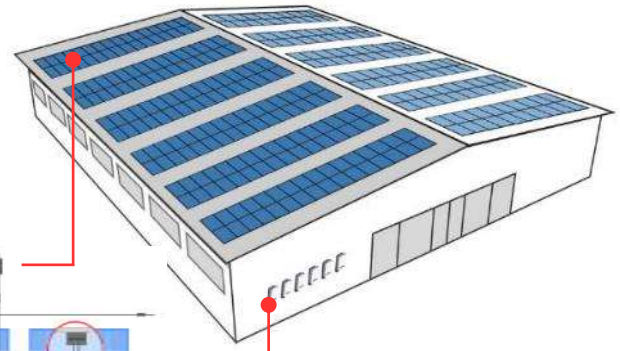
1. moduły PV 2. Falownik 3. Sieć elektryczna

Zoptymalizowany system PV - SolarEdge

- Każdy moduł jest podłączony do optymalizatora mocy
- Optymalizatory mocy to układy elektroniczne, które optymalizują produkcję energii słonecznej- każdy moduł jest zatem wyposażony w układ MPPT (śledzenia punktu mocy maksymalnej) – **indywidualnie dla każdego modułu**
- Optymalizator realizuje funkcje regulacyjne, pomiarowe i bezpieczeństwa (m.in.: ***Safe DC***) **na poziomie indywidualnego modułu PV**
- Falownik SolarEdge konwertuje tylko prąd stały na prąd przemienny zgodny z siecią i oddziałuje z siecią
- Platforma monitorowania wizualizuje wydajność każdego modułu w systemie



Ekosystem rozwiązań komercyjnych SolarEdge



25 LAT GWARANCJI

Optymalizatory mocy
P650–P1100

12-20 LAT GWARANCJI

Falowniki
16 kVA – 120 kVA

* 50 kVA i więcej

GOTOWE NA MAGAZYNY ENERGII

BEZPŁATNIE PRZEZ 25 LAT

Platforma Monitoringu

Licznik energii

Czujniki środowiskowe
i współczynnik wydajności
oparty na satelitach

Współpraca z siecią
BMS (Building Management System)
NC RfG
Rynek Mocy

Smart Grid Ready

Dostępne rozwiązania

Sterownik elektrowni (PPC)
Sterownik agregatu (APC)

Rozwiązania oferowane na żądanie

Niestandardowy interfejs monitorowania, kompleksowe integracje

4 kluczowe przewagi SolarEdge

Więcej energii

Zwiększony uzysk energii i szybszy zwrot z inwestycji dzięki MPPT na poziomie modułu

Niższe koszty eksploatacji i utrzymania

Pełna widoczność wydajności systemu i zdalne rozwiązywanie problemów

Zwiększone bezpieczeństwo

Bezpieczeństwo podczas instalacji, konserwacji, gaszenia pożaru i innych sytuacji awaryjnych

Elastyczne projektowanie

Maksymalne wykorzystanie przestrzeni przy minimalnym czasie projektowania

Ocena zwiększonej wydajności

- Uzysk energii zwiększony dzięki rozwiązaniom SolarEdge został potwierdzony w licznych testach i raportach, np:

Photon — Click for Report

PVEL ADVANCING SOLAR — Click for Report

NREL — Click for Report

- Badanie przeprowadzone przez LHW Partnership wykazało, że produkcja energii systemów SolarEdge jest wyższa we wszystkich rodzajach instalacji – domowych i komercyjnych, przy różnym stopniu zacienienia (od braku do dużego zacienienia)

LHW PARTNERSHIP

- Uzysk energii w systemach SolarEdge daje się w pełni modelować przy użyciu uznanych i wiarygodnych narzędzi symulacyjnych

PV PV*SOL

PVSYST PHOTOVOLTAIC SOFTWARE

solaredge

Niższe koszty O&M z monitoringiem na Poziomie Modułu

- Chroń swoje aktywa z pełnym dostępem do wydajności systemu oraz do narzędzia do zdalnego rozwiązywania problemów
- Monitoring SolarEdge jako narzędzie Serwisowe w dalszych usługach
  - Nieodpłatny przez 25 lat
  - Automatyczne wykrywanie błędów na wirtualnej mapie instalacji
  - Mniej wyjazdów na instalację

Zaawansowany monitoring systemu PV

solaredge

Wartość na każdym etapie (przepływ pracy – eliminacja błędów)

Planowanie → Instalacja → Eksploatacja i utrzymanie ruchu

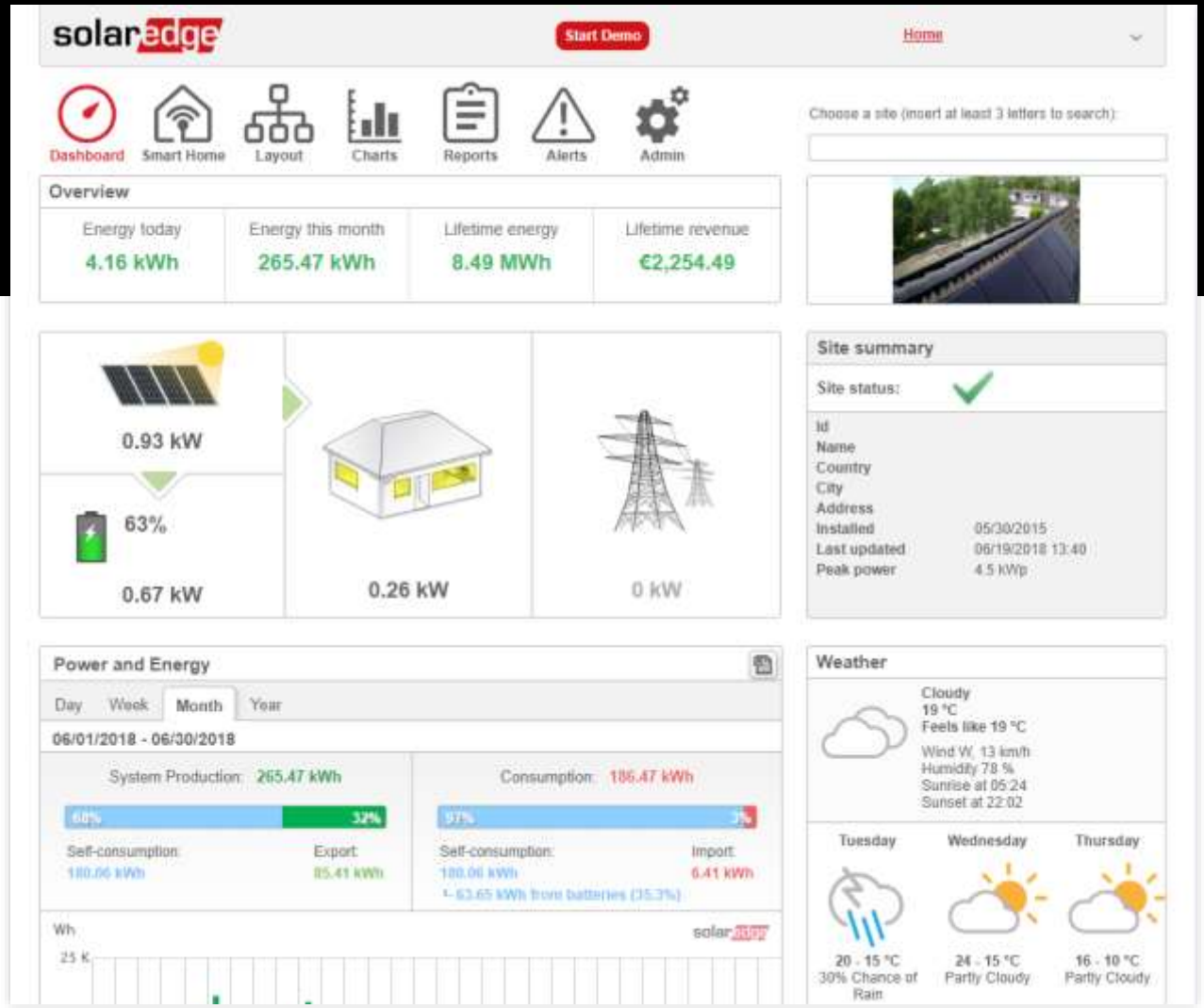
Designer	SetApp	Mapper App	Monitoring Platform	mySolarEdge
				

solaredge

Pełna przejrzystosć

Monitoring przepływu energii na żywo

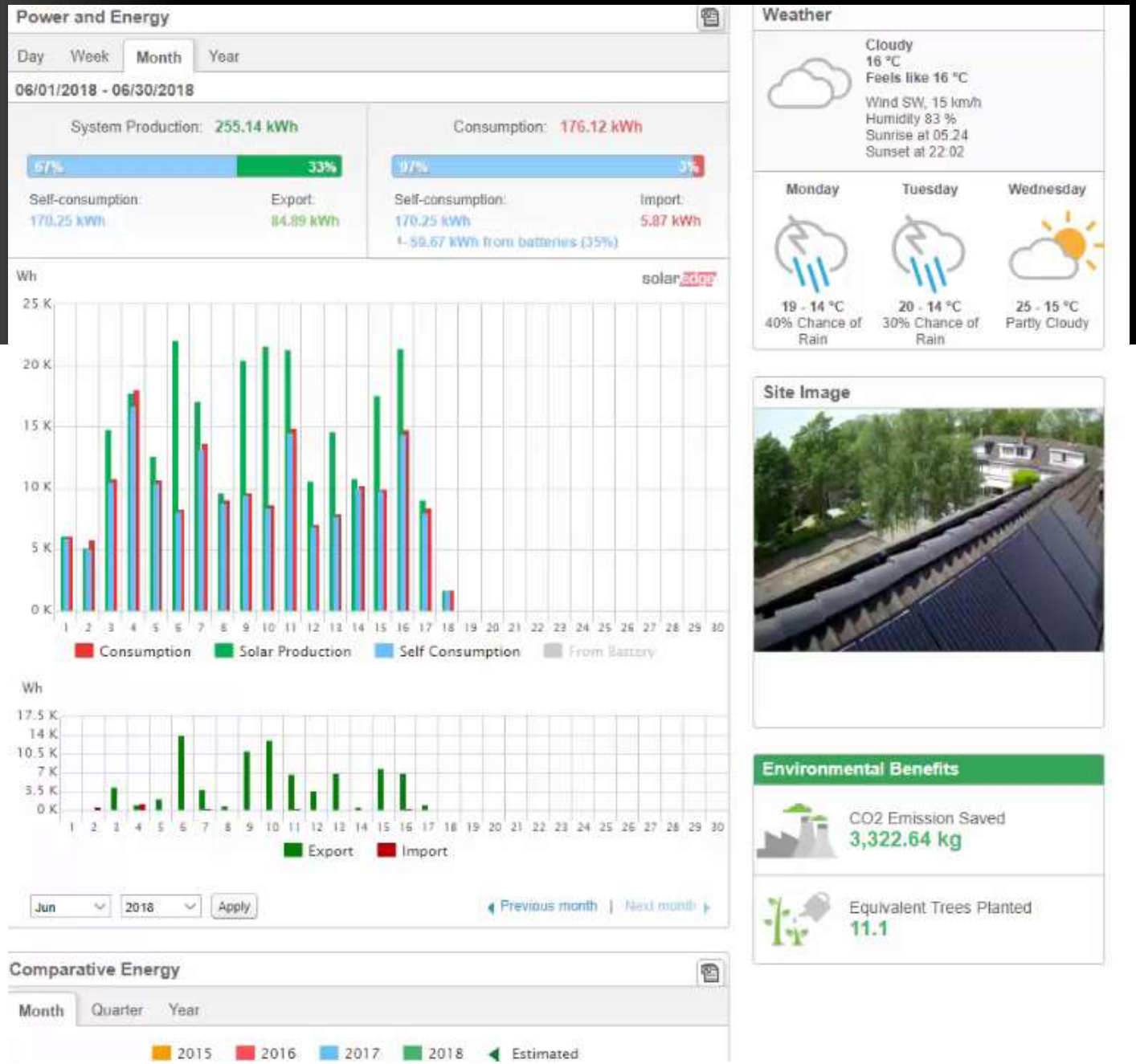
- Prezentacja przepływu energii międzu instalacją PV, baterią, siecią, obciążeniem w domu



Monitoring konsumpcji

Większa kontrola dla właściciela instalacji

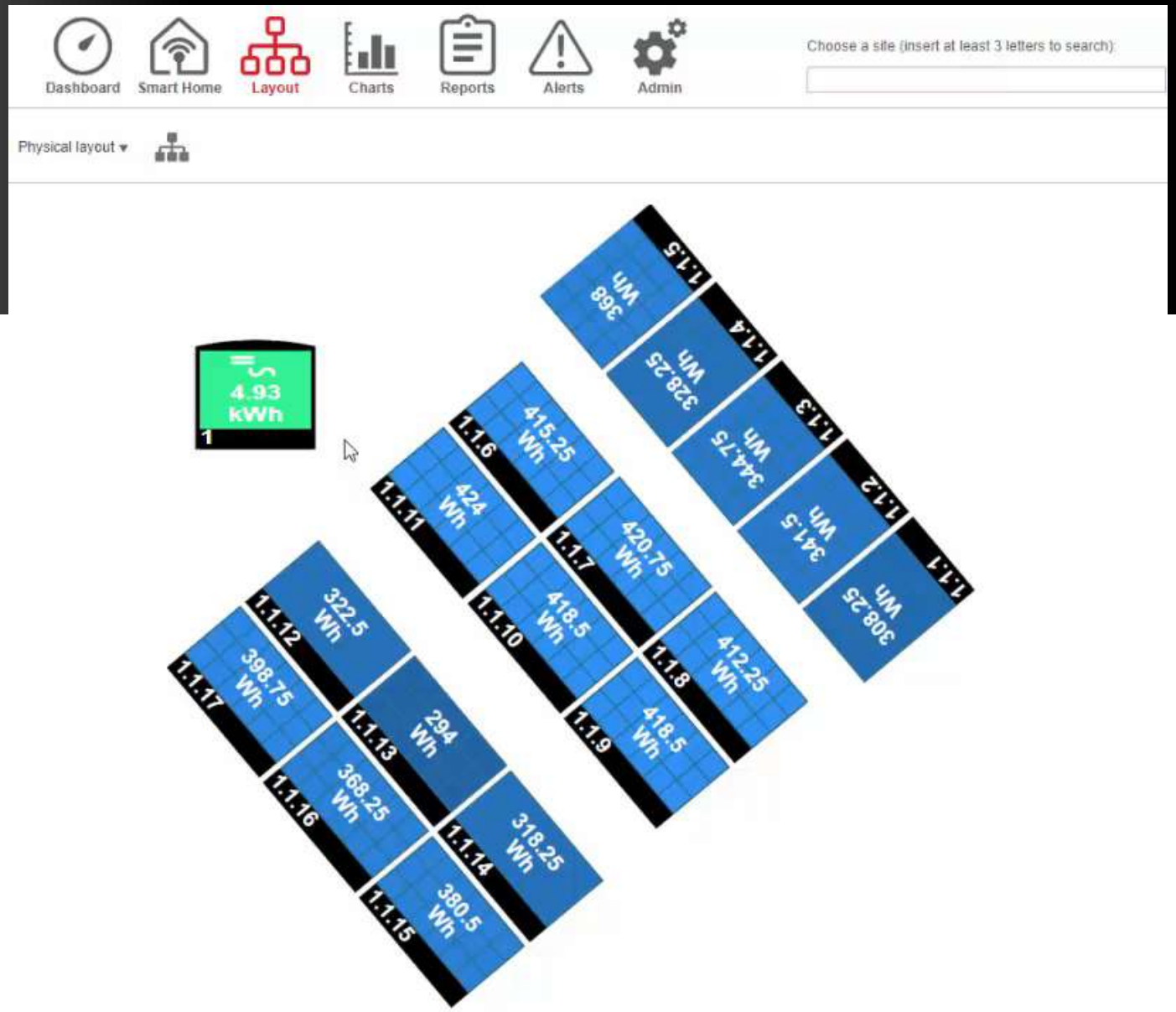
- Wysoka dokładność produkcji energii oraz konsumpcji energii pozwala właścicielowi lepiej zarządzać odbiornikami...



solaredge

Zdalne operacje

Redukcja liczby wizyt na instalacji



- Parowanie zdalne
- Włącz / czuwanie
- Zdalny wyświetlacz

solaredge

Redukcja kosztów utrzymania

- Błędy zarówno dla falownika jak i optymalizatorów
- Zdalna diagnoza – poprzedza akcję:
  - Identyfikacja słabej wydajności
  - Wykorzystanie wykresów to analizy wydajności
  - Mniej wyjazdów na instalację oraz mniej prac na niej

Większa dostępność systemu

- Dioda Bypass wydaje się być uszkodzona? Wadliwy moduł pokazuje 2/3 napięcia
- Problemy wyświetlane na poziomie modułu
- Instalator może świadczyć usługi proaktywnie
- Szybki i łatwy serwis będzie generować więcej energii dla właściciela systemu

Uszkodzona dioda Bypass

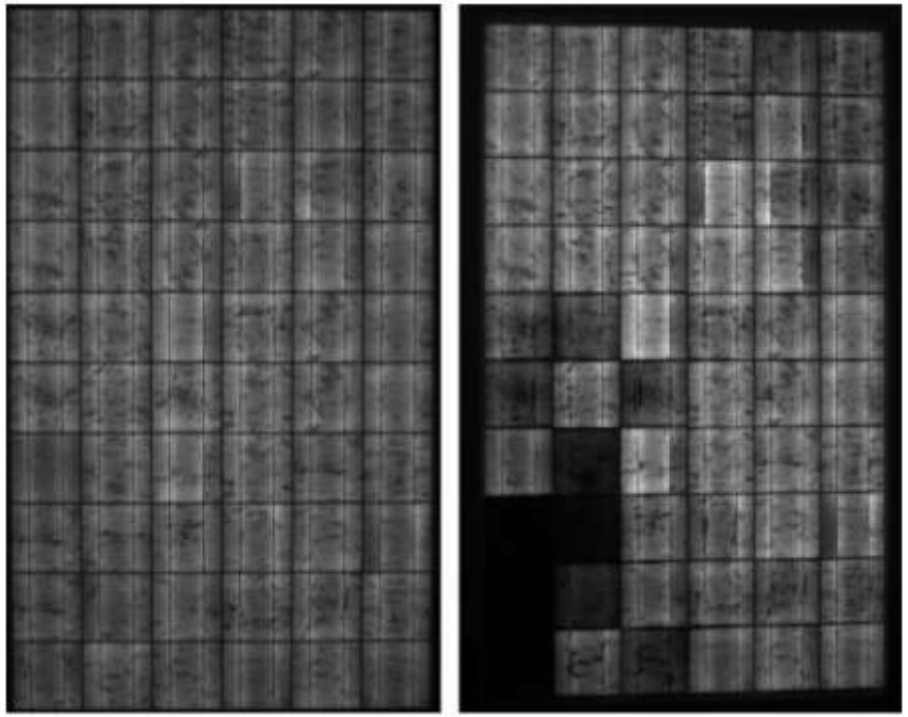
Moduł działający poprawnie, z pełnym napięciem

Źle działający moduł z niższym napięciem

solaredge

Przykład: wykrywanie PID

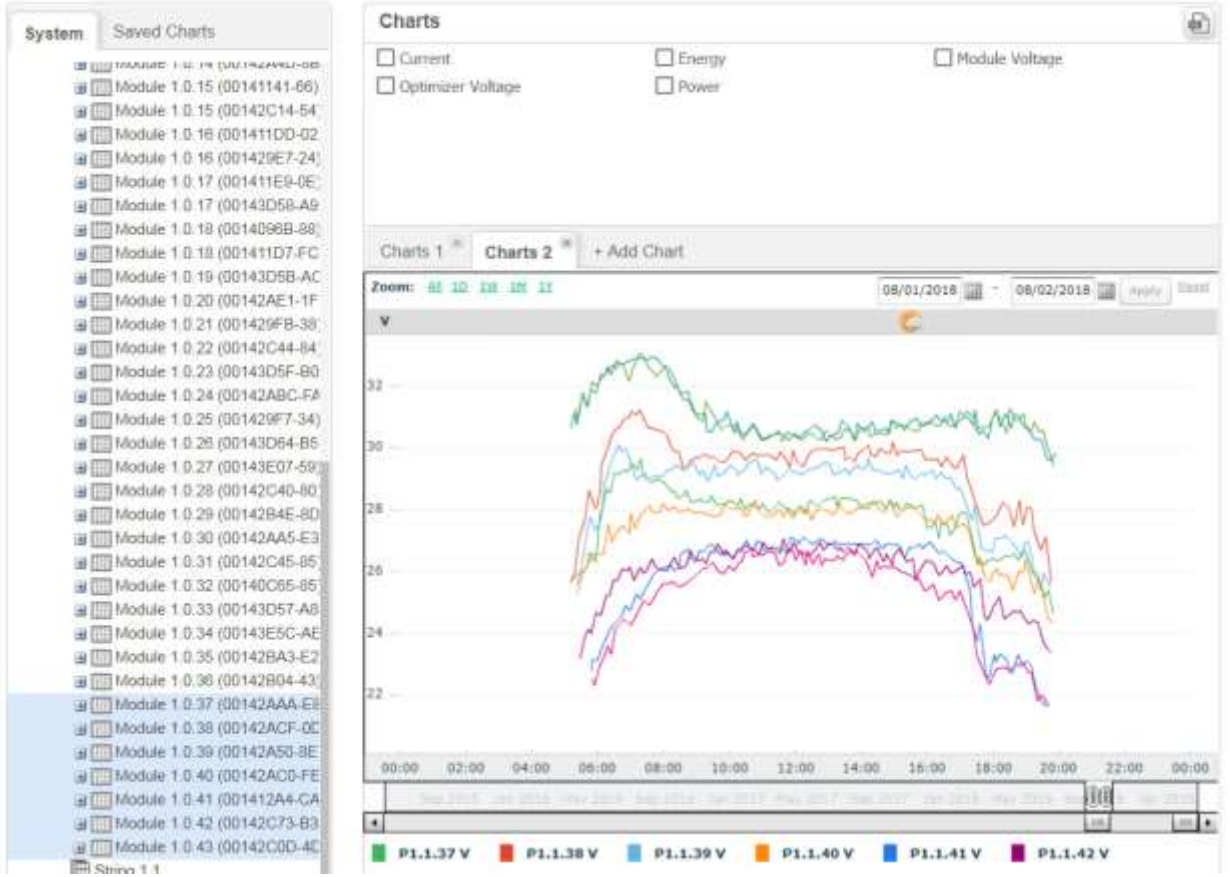
- Degradacja indukowanym napięciem jest zjawiskiem zmniejszającym moc modułu poprzez redukcję współczynnika wypełnienia (FF) i napięcia modułu
- Efekt PID jest najmocniej widoczny na modułach najbliższych ujemnego bieguna falownika
- Jeżeli podejrzewamy efekt PID na naszej instalacji, instalator musi zdemontować moduły i przeprowadzić pomiary



Obrazy elektroluminescencji modułu przed (po lewej) i po (po prawej) testowaniu PID. Źródło: PVTech Zdjęcie: © Fraunhofer CSE

Zdalne wykrywanie PID

- Instalator nie musi demontować modułów z dachu, aby sprawdzić napięcie.
  Robi to zdalnie przez portal



Satelitarny współczynnik wydajności

Współczynnik wydajności (PR) systemu fotowoltaicznego to stosunek bieżącej produkcji systemu PV do promieniowania słonecznego odebranego przez instalację. Służy on do oceny jakości systemu. Do pomiarów odebranego promieniowania słonecznego zwykle wykorzystuje się czujniki środowiskowe umieszczone w instalacji fotowoltaicznej. Wadą stosowania czujników do pomiarów odebranego promieniowania słonecznego jest fakt, że czujniki wymagają instalacji, kalibracji i konserwacji, a wszystko to na koszt właściciela systemu. Czujniki objęte są krótkim okresem gwarancyjnym i dlatego wymagają wymiany w trakcie użytkowania systemu PV.

SolarEdge połączyła siły z Solargis, świadczącą usługi z zakresu oceny energii słonecznej, dzięki czemu może zaoferować **satelitarny współczynnik PR** dla systemów fotowoltaicznych każdej wielkości, umożliwiający dostarczenie wiarygodnych, użytecznych danych za pomocą platformy monitoringu za kwotę 28 (* centów dziennie.

solaredge

Satelitarny współczynnik wydajności - korzyści

Eliminuje koszty nabycia, instalacji, konserwacji, czyszczenia i wymiany czujnika

Zapewnia dokładność porównywalną do czujników promieniowania*

Kompatybilny z różnymi kątami nachylenia i kierunkami, bez potrzeby instalowania różnych czujników w instalacji

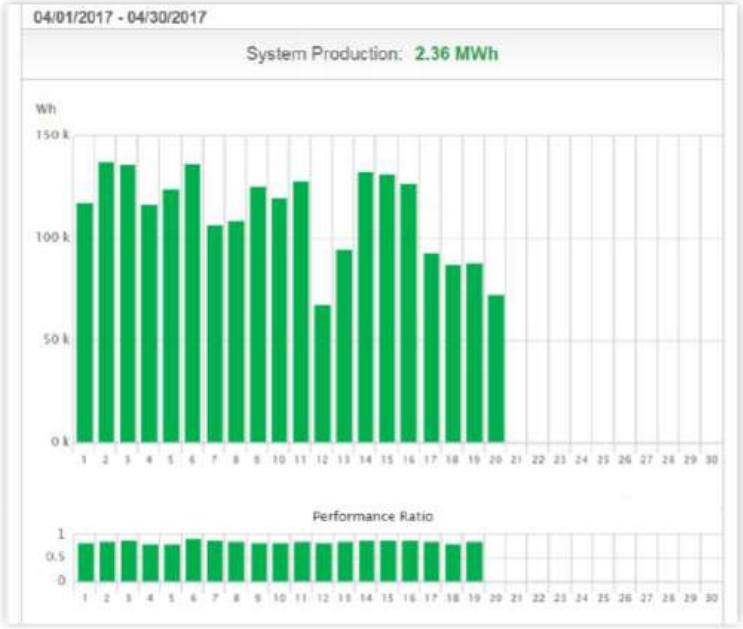
Zapobiega ewentualnym niedokładnościom wynikającym z zabrudzenia czujników

Oferuje dzienne i miesięczne kalkulacje PR

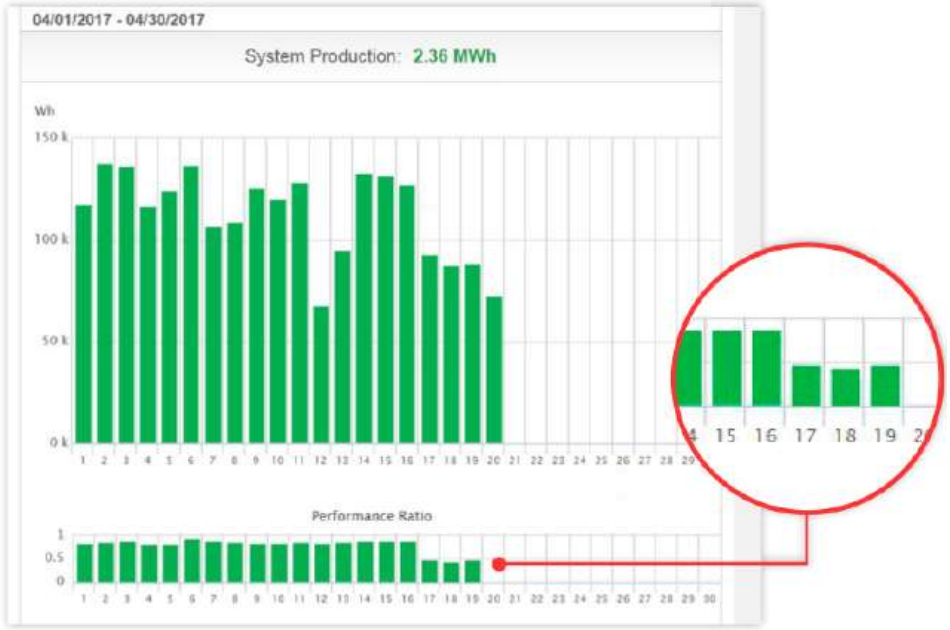
Dostarcza danych historycznych PR za okres do 12 miesięcy

solaredge

Bezproblemowa integracja z platformą monitorowania SolarEdge



Przykład normalnie działającej instalacji PV.



Przykład instalacji o niskim współczynniku PR, wskazującym na problem.

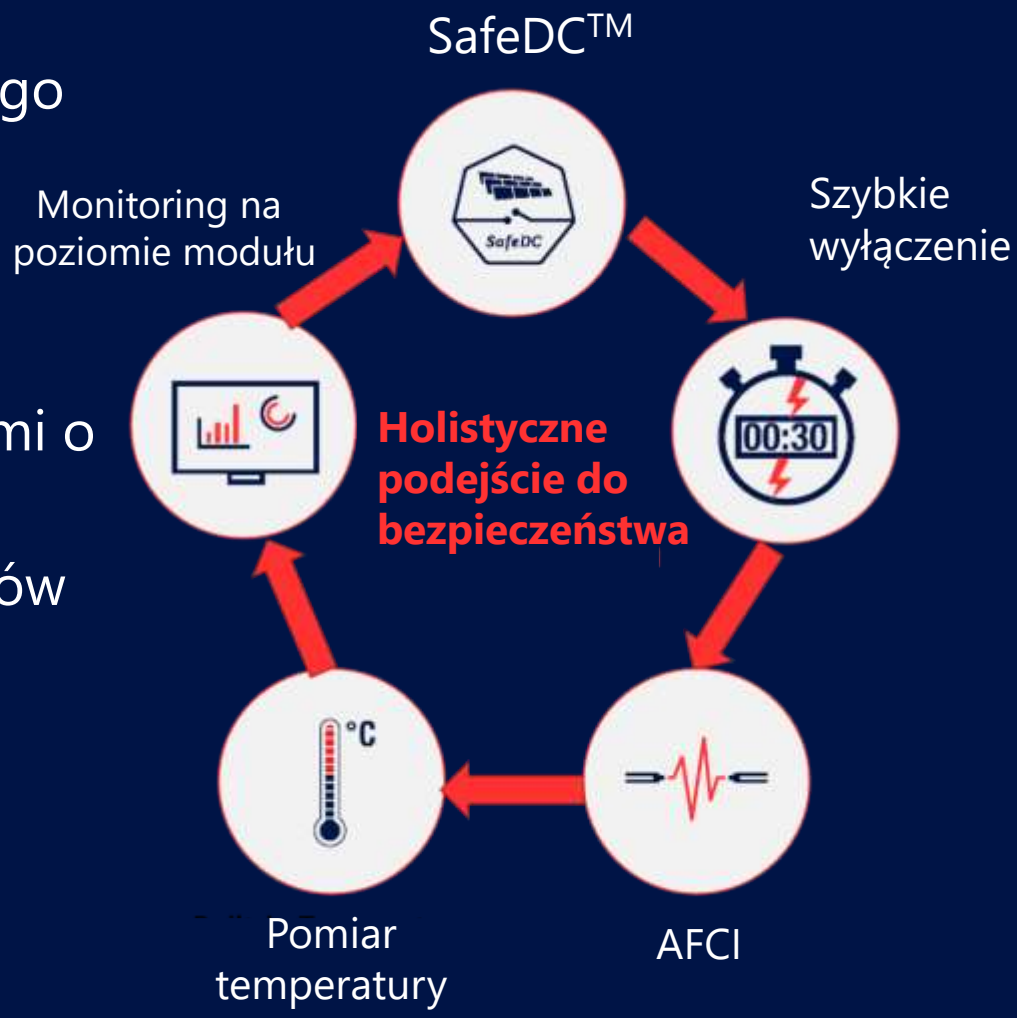
https://solargis.com/docs/accuracy-and-comparisons/combining-model-uncertainty-and-interannual-variability

https://www.solaredge.com/pl/satellite

Bezpieczeństwo mienia

SolarEdge = holistyczne bezpieczeństwo

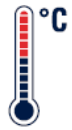
- Zapewnia obniżenie napięcia DC systemu do bezpiecznego poziomu, gdy system jest wyłączony
- Wczesne wykrywanie błędów i zapobieganie im
- Aktywna i ciągła ochrona instalacji
- Monitorowanie na poziomie modułu z aktywnymi alertami o błędach
- AFCI potwierdzone w praktyce przez ~ 1 milion falowników z włączoną funkcją AFCI



Bezpieczeństwo PV polega na kompleksowym podejściu do tematu

Zapewnia, że napięcie DC systemu jest obniżone do bezpiecznego poziomu po wyłączeniu systemu

Wczesne wykrywanie i zapobieganie zwarciom łukowym



Aktywna i ciągła ochrona falownika

Monitorowanie na poziomie modułu

W razie potrzeby umożliwiają szybkie rozładowanie przewodów do bezpiecznego poziomu / Obowiązkowe w USA zgodnie z NEC 2014, 2017 i 2020

Naprawdę bezpieczny system fotowoltaiczny powinien opierać się na kompleksowym rozwiązaniu, które spełnia różne wymagania bezpieczeństwa i jest potwierdzone w istniejących systemach

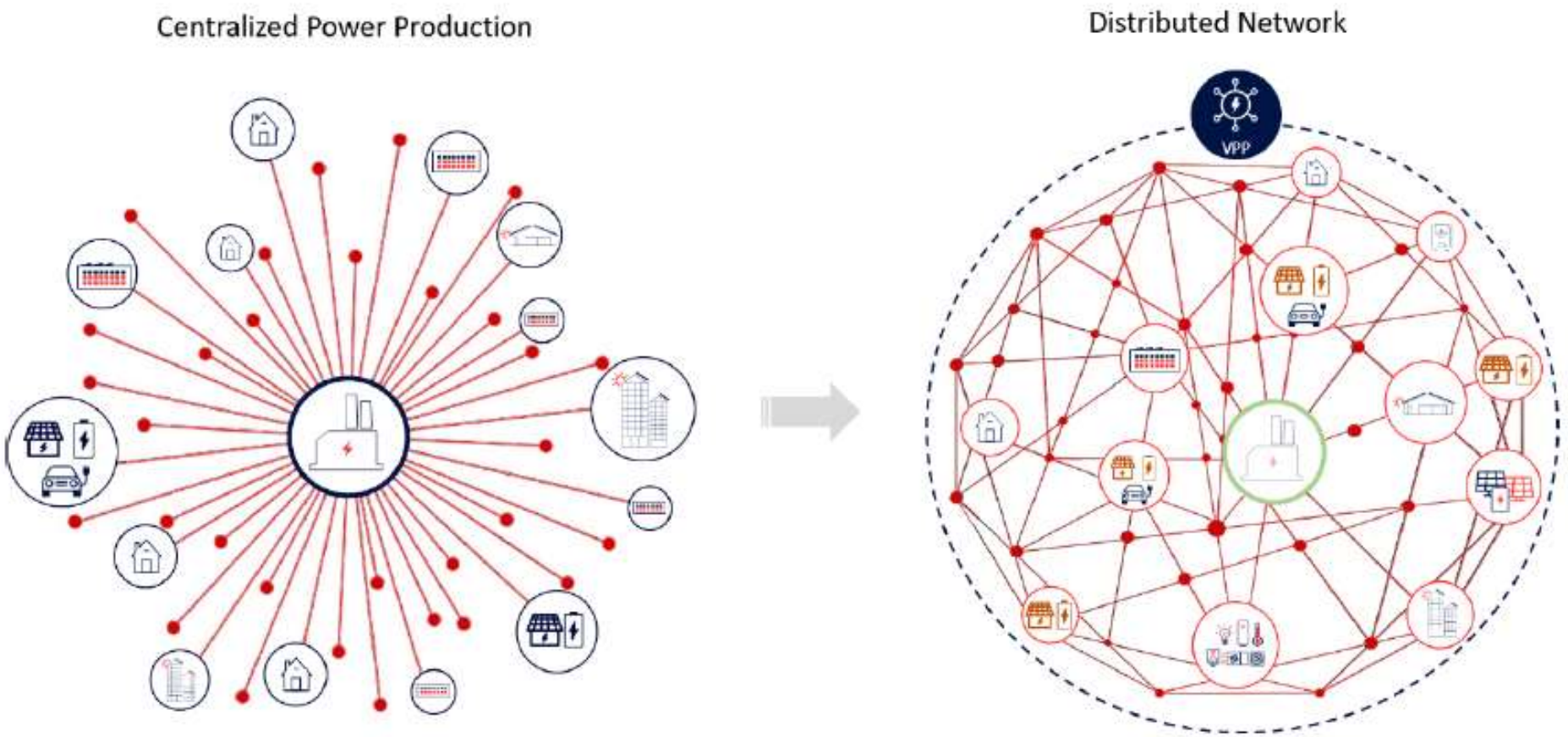
Naprawdę holistyczne rozwiązanie zapewniające bezpieczeństwo

solaredge

Bezpieczeństwo w cyberprzestrzeni

solaredge

Infrastruktura rozproszona – postęp i zagrożenia (IoT)



Rysunek 1 – Przejście od scentralizowanej produkcji energii do sieci rozproszonej

solaredge

- W ostatnich latach świat był świadkiem ataku cyberataków na urządzenia IoT.
  - *„Rzeczy, które kiedyś stanowiły fabułę filmu science fiction, takie jak włamania do urządzeń gospodarstwa domowego i obrócenie ich przeciwko ludzkości, stały się teraz rzeczywistością. Włamania do urządzeń IoT hacking mogą być niezwykle skuteczne, przyczyniając się do ataków typu DDoS, które mogą sparaliżować naszą infrastrukturę, systemy i sposób życia."* – twierdzi ***Daniel Markuson, ekspert ds. prywatności cyfrowej w NordVPN.*** *„Jeśli posiadasz wiele urządzeń podłączonych do tej samej sieci w domu lub w biurze, a haker uzyska dostęp do jednego urządzenia, może włamać się także do wszystkich pozostałych".*

    IT Reseller: Najgorsze i najdziwniejsze włamania wszechczasów do urządzeń Internetu rzeczy, firma NordVPN zebrała listę najbardziej zwariowanych włamań i naruszeń bezpieczeństwa urządzeń IoT. *Autor:**Mariusz Laurisz** 30 stycznia 2020*

  - *5 lutego 2021 r. stacja uzdatniania wody w Oldsmar (Floryda, USA) zgłosiła włamanie do swojej sieci zarządzania obiektem, w której nieznana osoba była w stanie na krótko zmodyfikować skład chemiczny przetwarzanej wody poprzez zwiększenie ilości wodorotlenku sodu (znanego również jako ług lub soda kaustyczna) do poziomu niebezpiecznego dla spożycia przez ludzi Według organów ścigania, około godziny 13:00, tego dnia, napastnik uzyskał dostęp do systemu kontroli poprzez preinstalowaną instancję oprogramowania zdalnego pulpitu TeamViewer4 - podczas 3-5 minutowego ataku, napastnik zmienił ilość wodorotlenku sodu ze 100 części na milion (ppm) do 11100 ppm.*

    Rekomendacje cyberbezpieczeństwa dla sektora wodno-kanalizacyjnego (R-CYBER-01/2021) (luty 2021 r.)

- *„Oczywiście, nie oznacza to, że jeśli coś można zhakować, to tak się właśnie stanie. Wiele z tych przypadków ma nadal charakter teoretyczny, ale niezachowywanie ostrożności może zaszkodzić. Jeśli posiadasz w domu lub w pracy inteligentne urządzenie, przeczytaj więcej na jego temat i skorzystaj z technologii bezpieczeństwa sieciowego. Silne hasła i metody uwierzytelniania również zmniejszają ryzyko." – twierdzi* ***Daniel Markuson, ekspert ds. ochrony prywatności w NordVPN.***

- ***Stuxnet*** *– działający w systemie Windows robak komputerowy, po raz pierwszy wykryty w czerwcu 2010[1]. Jest pierwszym znanym robakiem używanym do szpiegowania i przeprogramowywania instalacji przemysłowych[2]. Zawierał rootkit na system Windows[1], pierwszy w historii PLC rootkit[1]. Wykorzystywał też wiele luk 0-day[1]. Wirus miał zdolność aktualizacji metodą peer-to-peer[1].*

Po zainstalowaniu się w systemie operacyjnym Windows robak zaczyna przeszukiwać sieć lokalną w poszukiwaniu podłączonych sterowników PLC, które są często używane w różnego rodzaju fabrykach, rafineriach czy elektrowniach. W przypadku znalezienia ściśle określonej konfiguracji sterowników SIMATIC S7-300 oraz S7-400 firmy Siemens następuje aktywacja. Wirus wykorzystuje działające na zainfekowanym komputerze oprogramowanie Siemens SIMATIC WinCC/Step 7[6] (oprogramowanie łączące system SCADA[12] oraz programistyczną stację inżynierską) w celu zmian ustawień sterowników PLC. Robi to w sposób sugerujący, że jego twórcy mieli na celu tylko wybrane kontrolery[6]. Stuxnet atakował głównie konwertery częstotliwości zmieniając częstotliwość prądu, jaki one wysyłały, co doprowadzało do przyspieszenia pracy wirówek gazowych[13]. *[Wikipedia]*

- Obecny krajobraz cyberbezpieczeństwa wymaga od producentów inteligentnych systemów IoT zwiększenia skuteczności wbudowanych mechanizmów ochrony swoich produktów.

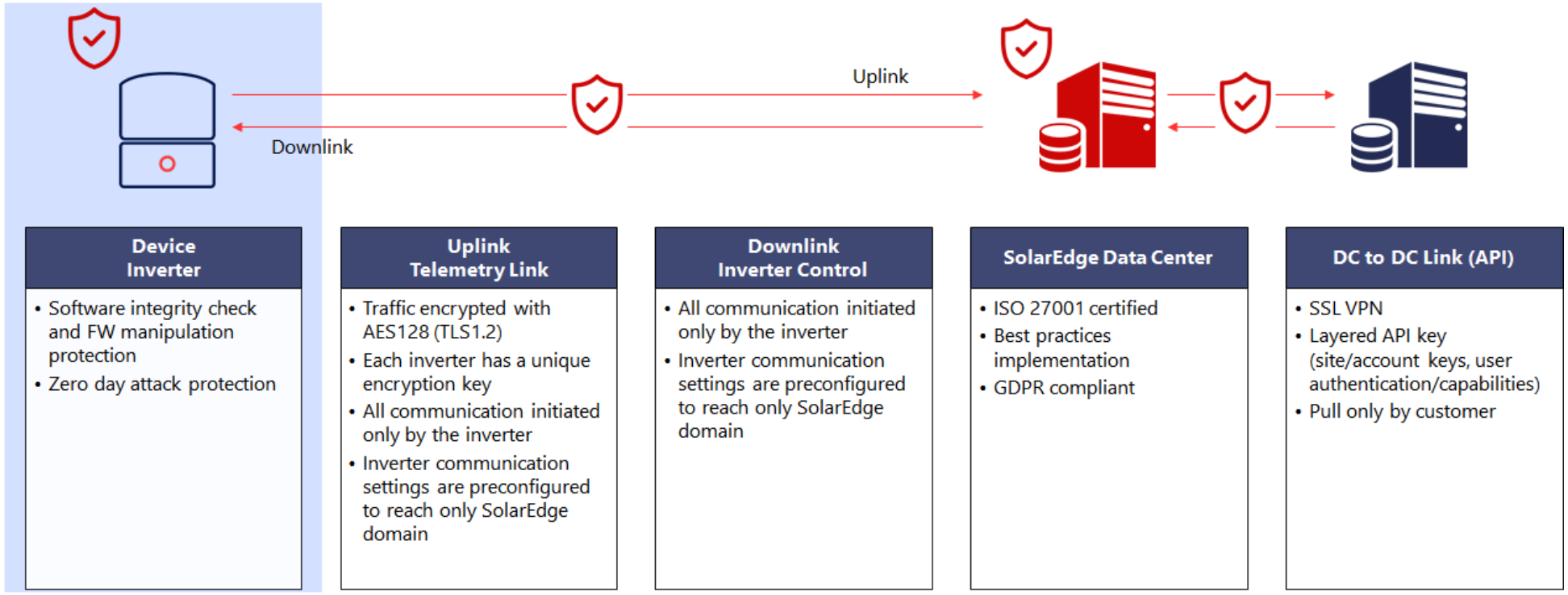
- SolarEdge angażuje się w promowanie cyberbezpieczeństwa w całej swojej linii inteligentnych falowników, światowej infrastrukturze danych i komunikacji oraz centrach danych.
- **Nasza holistyczna architektura bezpieczeństwa chroni przesyłane dane infrastruktury fotowoltaicznej (PV) i eliminuje potrzebę stosowania dodatkowych schematów ochrony ruchu, takich jak VPN.**
- SolarEdge regularnie przeprowadza zewnętrzne oceny ryzyka cybernetycznego i testy penetracyjne, aby zidentyfikować potencjalne naruszenia bezpieczeństwa i zwiększyć poziom cyberbezpieczeństwa
- Szczegółowo przestrzegamy najlepszych praktyk w zakresie bezpieczeństwa cybernetycznego we wszystkich naszych zasobach cyfrowych i dążymy do przestrzegania wszystkich odpowiednich przepisów branżowych, takich jak ISO27001 i RODO.

- Holistyczne, wielowarstwowe podejście do zagadnień bezpieczeństwa
  - SolarEdge wdrożył wielowarstwowe rozwiązanie, które zapewnia całościową ochronę przed nieautoryzowanymi próbami dostępu do systemu SolarEdge. Rozwiązanie zapewnia zdalną ochronę przed skalowalnymi atakami i nieautoryzowanym dostępem do pojedynczej jednostki. Został zaprojektowany w celu ochrony każdego składnika rozwiązania, łączności, funkcjonalności systemu i przechowywanych danych.
- Zakres rozwiązania
  - Przeglądowi podlegają następujące środki bezpieczeństwa:
    - Bezpieczeństwo punktów końcowych
    - Komunikacja między punktami końcowymi (falownikami) a centrami danych
    - Bezpieczeństwo serwera (sprzęt i oprogramowanie)
    - Bezpieczny hosting
    - Plan tworzenia kopii zapasowych i ciągłości działania (BCP)
    - Procedury i procesy organizacyjne

Bezpieczeństwo w każdym obszarze

Device Inverter	Uplink Telemetry Link	Downlink Inverter Control	SolarEdge Data Center	DC to DC Link (API)
• Software integrity check and FW manipulation protection • Zero day attack protection	• Traffic encrypted with AES128 (TLS1.2) • Each inverter has a unique encryption key • All communication initiated only by the inverter • Inverter communication settings are preconfigured to reach only SolarEdge domain	• All communication initiated only by the inverter • Inverter communication settings are preconfigured to reach only SolarEdge domain	• ISO 27001 certified • Best practices implementation • GDPR compliant	• SSL VPN • Layered API key (site/account keys, user authentication/capabilities) • Pull only by customer

Bezpieczeństwo punktów końcowych (inteligentny falownik)



Falowniki SolarEdge mają wiele warstw bezpieczeństwa – w tym zarówno mechanizmy wbudowane, jak i mechanizmy stron trzecich – które mają na celu ograniczenie narażenia na oportunistyczne i ukierunkowane cyberataki.

- Kontrola dostępu do urządzenia
  - Wzmocnienie ochrony dostępu - Wszystkie nieużywane interfejsy (usługi/porty) falownika są wyłączone. Tylko określone, chronione porty są otwarte na komunikację, umożliwiając dostęp do wcześniej określonych, zabezpieczonych usług.
  - Istnieją tylko zatwierdzone konta użytkowników/usług. Domyślnie usuwamy niepotrzebne konta, aby ograniczyć przestrzeń ataku niewykorzystanych i niezabezpieczonych kont użytkowników/usług.
  - Punkty końcowe nie obsługują funkcji automatycznego wykrywania i łączenia zapewnianych przez UPnP, co zapobiega nawiązywaniu nieautoryzowanych i nieznanych połączeń – należy je ręcznie sparować.
  - Komunikacja bezprzewodowa krótkiego zasięgu dla różnych urządzeń opiera się na protokole ZigBee i jego wymaganiach bezpieczeństwa (IEEE 802.15.4) – wymuszając bliskość falownika w celu zainicjowania dostępu i nawiązania połączenia.
  - Falownik działa jako router Wi-Fi do urządzeń peryferyjnych SolarEdge. Punkt dostępu Wi-Fi falownika nie publikuje swojego identyfikatora SSID (źródła) i można go włączyć tylko na bardzo krótki czas – konieczny jest fizyczny dostęp do falownika. Swobodne skanowanie Wi-Fi nie ujawni punktu dostępu falownika.
  - SolarEdge tworzy unikalny klucz szyfrowania dla każdego falownika podczas produkcji. W rezultacie:
    - Każdy falownik jest zaprojektowany tak, aby był jednoznacznie uwierzytelniany przez serwer sterowania i monitorowania.
    - Proces wymiany kluczy ogranicza narażenie na wektory ataków szyfrujących

- Oprogramowanie układowe SolarEdge zostało zaprojektowane w celu ochrony przed lokalnymi i zdalnymi eksploitami złośliwego kodu przy użyciu następujących mechanizmów:
  - Kod oprogramowania układowego falownika (FIRMWARE) jest zaszyfrowany tajnym kluczem mającym na celu zapewnienie, że aktualizacje oprogramowania FIRMWARE są autentyczne i nie zawierają tylnych drzwi ani niezatwierdzonego kodu.
  - Projekt zabezpieczeń jest osadzony na różnych etapach cyklu życia bezpiecznego programowania (SDLC) w celu ochrony przed różnego rodzaju lukami w kodzie.
  - Podczas przeprowadzania zdalnych, bezprzewodowych aktualizacji oprogramowania (OTA), SolarEdge zabezpiecza kanał transmisji i zapewnia weryfikację oprogramowania układowego. Procesem zarządza naszą platforma kontrolno-monitorująca (serwer zarządzający) w celu zapewnienia szybkich i jednolitych aktualizacji.

- W pierwszym kwartale 2020 r. SolarEdge nawiązał współpracę z firmą **Karamba Security** (We Protect the IoT) w celu zintegrowania w w swoich inteligentnych falownikach zaawansowanych agentów IoT chroniących przed złośliwym oprogramowaniem, zapewniając następujące ulepszenia bezpieczeństwa:
  - Mechanizm Karamba Security zapewnia ochronę Internetu Rzeczy przed atakami typu zero-day (które mają na celu nieznane luki w zabezpieczeniach kodu) oraz funkcje zapobiegania w czasie rzeczywistym.
  - Dodatkowa warstwa weryfikacji służąca do sprawdzania i zezwalania na legalne aktualizacje kodu.
  - Zaawansowana warstwa bezpieczeństwa o nazwie Control Flow Integrity (CFI). Kod falownika jest chroniony przed wrogimi próbami manipulacji na linii produkcyjnej i w terenie.
  - Rozwiązanie stale monitoruje zdarzenia związane z bezpieczeństwem i ostrzega zespół ds. bezpieczeństwa SolarEdge (powiadomienia o alertach są przesyłane w czasie zbliżonym do rzeczywistego do naszego centrum operacyjnego bezpieczeństwa).

- Dystrybucja i „wgrywanie” łatek
  - Poprawka (łatka, patch) to aktualizacja oprogramowania składająca się z poprawionego kodu wstawianego do kodu programu wykonywalnego. Zazwyczaj poprawka jest wdrażana w istniejącym programie. Poprawki mogą wykonywać dowolne z następujących czynności:
    - Naprawienie wykrytego błędu oprogramowania / Poprawa stabilności oprogramowania
    - Usunięcie luk w zabezpieczeniach
    - Aktualizacja oprogramowania (nowe lub usprawnione funkcjonalności)
  - SolarEdge stale monitoruje cyberzagrożenia dla swoich produktów i odpowiednio dostarcza poprawki bezpieczeństwa. Ich funkcjonowanie jest kontrolowane.

Działania zdalnego wsparcia dla falownika

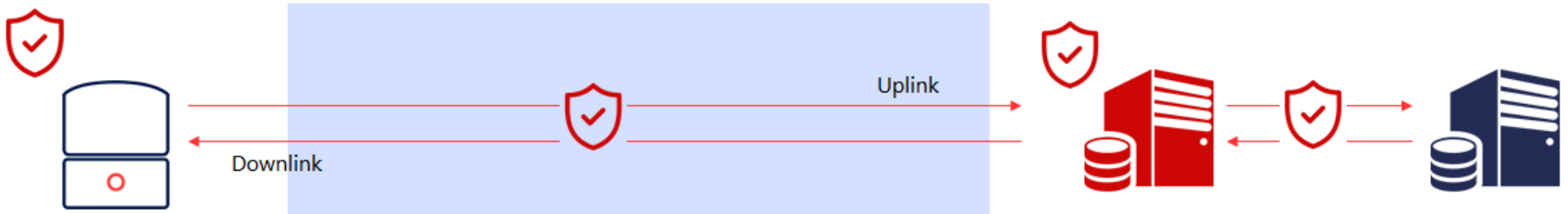
- Pomoc techniczna bywa wymagana w przypadku różnych awarii produktów, przerw w świadczeniu usług lub innych problemów. Grupa wsparcia technicznego składa się z certyfikowanych inżynierów wsparcia oraz akredytowanych partnerów wsparcia.
- Ze względu na wrażliwość operacyjną i bezpieczeństwo działań wsparcia, każda aktywność jest rejestrowana, a dostęp do kardynalnych działań wsparcia jest ograniczony i w pełni monitorowany.

Ochrona danych urządzenia (prywatność)

- Nasz sprzęt nie jest przystosowany do nagrywania dźwięku i obrazu, ani nie przechowuje żadnych danych osobowych, takich jak nazwiska czy adresy.

- Uruchomienie oraz normalna eksploatacja naszych urządzeń bez podłączania w jakikolwiek sposób do internetu czy innych środków komunikacji (w szczegołności bez nawiązywania komunikacji z nasza platforma monitoringu) – jest jak najbardziej mozliwa. (aczkolwiek użytkownik pozbawia się wielu cennych funkcjonalności)

Bezpieczeństwo komunikacji (między falownikiem a serwerami SolarEdge)



Device Inverter	Uplink Telemetry Link	Downlink Inverter Control	SolarEdge Data Center	DC to DC Link (API)
• Software integrity check and FW manipulation protection • Zero day attack protection	• Traffic encrypted with AES128 (TLS1.2) • Each inverter has a unique encryption key • All communication initiated only by the inverter • Inverter communication settings are preconfigured to reach only SolarEdge domain	• All communication initiated only by the inverter • Inverter communication settings are preconfigured to reach only SolarEdge domain	• ISO 27001 certified • Best practices implementation • GDPR compliant	• SSL VPN • Layered API key (site/account keys, user authentication/capabilities) • Pull only by customer

Szyfrowanie komunikacji

- Stosujemy wyłącznie szyfrowane łącza komunikacyjne w celu zwiększenia poufności i integralności danych.
- Rozwiązanie do sterowania i monitorowania SolarEdge wymusza szyfrowanie komunikacji między falownikiem a serwerem — w przypadku korzystania z sieci Ethernet, Wi-Fi lub modemu komórkowego — za pomocą 128-bitowego szyfrowania AES w standardzie Advanced Encryption Standard.
- Podejście SolarEdge do bezpieczeństwa zakłada, że użytkownik sprzętu zapewnia ochronę przed nieuprawnioną osobą, która może próbować fizycznie uzyskać dostęp do sprzętu lub przedostać się do sieci LAN.
- Komunikacja Wi-Fi LAN i WAN jest realizowana z najlepszymi praktykami bezpieczeństwa dotyczącymi silnego uwierzytelniania (802.1x) i algorytmów szyfrowania (WPA2-PSK ze 128-bitowymi kluczami AES).
- Inwertery SolarEdge komunikują się tylko w szyfrowanym trybie TCP (**SSL** over TCP).

Komunikacja asymetryczna

- Włączenie komunikacji sieciowej lub internetowej od falowników do serwerów w centrum danych może zagrozić systemowi.
- Otwarte kanały odbioru mogą być wykorzystywane przez cyberprzestępców, którzy wysyłają zapytania do urządzenia w poszukiwaniu otwartych portów i luk w zabezpieczeniach usług.

- **Aby złagodzić to ryzyko, falowniki SolarEdge zostały zaprojektowane z jednokierunkowym mechanizmem komunikacji,** w którym falowniki otrzymują wiadomości z serwerów tylko wtedy, gdy falownik inicjuje kontakt z serwerami, odpytując o nowe polecenia i przesyłając nowe dane.
- Zaimplementowane rozwiązanie maskuje falowniki przed potencjalnymi hakerami i skutecznie czyni je niewidocznymi dla ataków skanujących

Bezpieczeństwo centrum danych SolarEdge

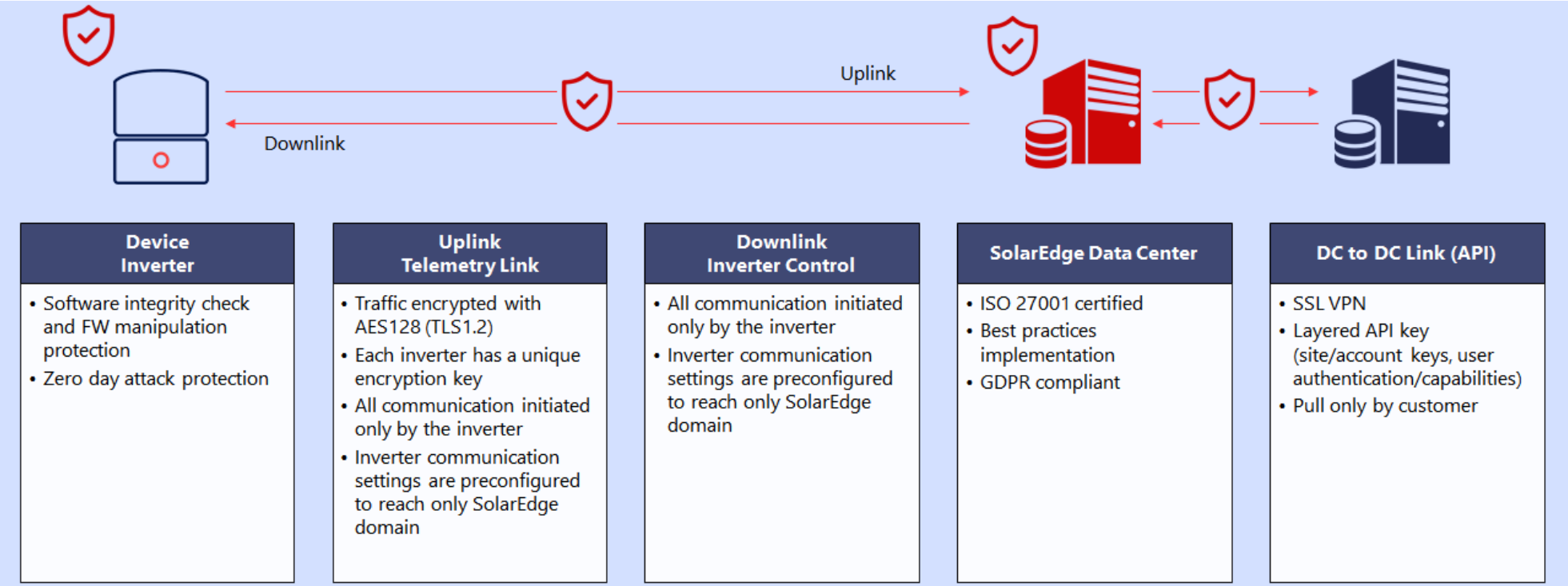
Device Inverter	Uplink Telemetry Link	Downlink Inverter Control	SolarEdge Data Center	DC to DC Link (API)
• Software integrity check and FW manipulation protection • Zero day attack protection	• Traffic encrypted with AES128 (TLS1.2) • Each inverter has a unique encryption key • All communication initiated only by the inverter • Inverter communication settings are preconfigured to reach only SolarEdge domain	• All communication initiated only by the inverter • Inverter communication settings are preconfigured to reach only SolarEdge domain	• ISO 27001 certified • Best practices implementation • GDPR compliant	• SSL VPN • Layered API key (site/account keys, user authentication/capabilities) • Pull only by customer

- Server Hardening
  - SolarEdge wdraża dokładny proces wzmacniania,w oparciu o wytyczne dostawców i najlepsze praktyki branżowe, aby poprawić stan bezpieczeństwa serwerów i wydajność operacyjną.
  - Dostęp do serwerów w celu zarządzania jest możliwy za pomocą dedykowanego SSL VPN, który wykorzystuje algorytmy szyfrowania 3DES/SHA256 i wymaga użycia uwierzytelniania dwuskładnikowego.
- Architektura klastrowa (serwery, firewalle, układy równoważnia obciążeń, dedykowane łącza dostępowe)
- Z punktu widzenia sieci bazy danych znajdują się w oddzielnej pod-sieci i są chronione zaporą sieciową. Ruch bazy danych jest otwarty tylko dla określonych aplikacji (segmentacja).
- łącze dostępowe z kopią zapasową zapewnianą przez wielu dostawców tier-1
- Bezpieczeństwo baz danych (ISO27000/xxx, NIST 800-123, pierwszorzzędni dostawcy usług)
- Kontrola przepływu. Przeglądanie stron internetowych na platformie monitorowania PV jest szyfrowane przy użyciu protokołu SSL z aktualnymi najlepszymi praktykami szyfrowania (odrzucamy podatne na ataki wersje TLS)
- Monitorowanie i aktualizacje serwerów

- SolarEdge przechowuje swoje dane i informacje w wielu dedykowanych ośrodkach hostingowych w Europie, obsługiwanych przez globalnego dostawcę usług hostingowych, który obsługuje ponad 140 centrów danych na pięciu kontynentach.
- Witryny spełniają następujące normy:(wszystkie zgodne z ISO 9001:2008, ISO / IEC 27001:2005 and 27001:2013, NIST 800-53/FISMA)

- Backup and Business Continuity Plan (BCP)
  - Backup Cycle
  - Restoration Tests
  - Backup Protection (Onsite and Offsite)
  - Alternate Site (Disaster Recovery Planning)

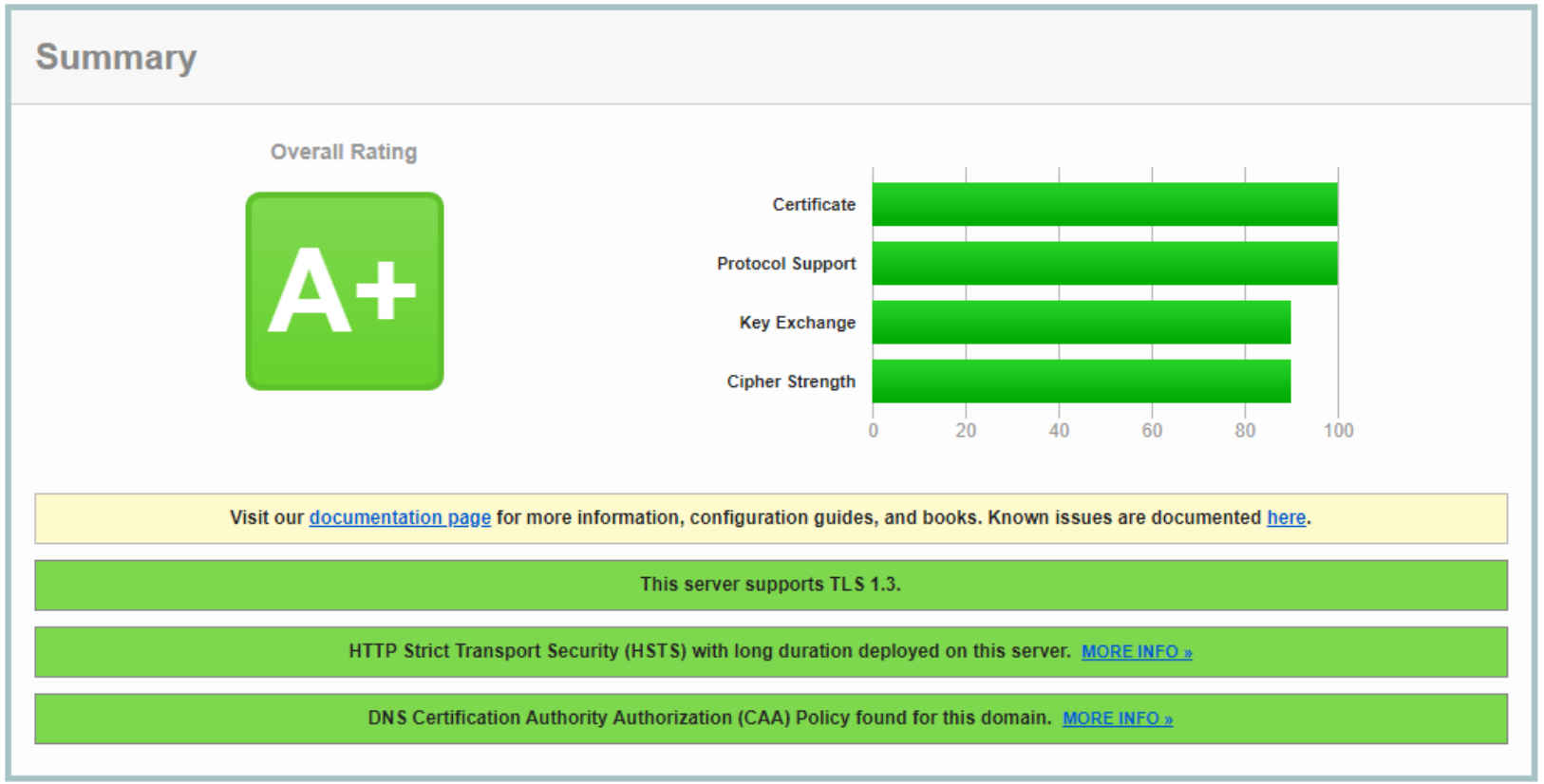
Procedury i procesy organizacyjne



Wewnętrzne procedury i procesy bezpieczeństwa SolarEdge mają na celu zapewnienie, że każdy komponent spełnia te same wysokie standardy, a cały przepływ od początku do końca nie ma słabego ogniwa.

- Zarządzanie kontami użytkowników
- SDLC (Secure Development Lifecycle) – metoda macierzowa, testy podatnosci
- Przydział uprawnień - „minimalne uprawnienia”,
- Rozdzielenie obowiązków
- Weryfikacja użytkowników i uprawnień
- Zarządzane umowy SLA ze stronami trzecimi – dostawcami usług IT
- „Bug Bounty” – wynagrodzenia dla ekspertów niezaleznie wynajdujących luki i podatności
- Rejestrowanie zdarzeń i incydentów
- Zlecane okresowo testy penetracyjne
- Reagowanie na incydenty
- Bezpieczeństwo łańcucha dostaw/podwykonawstwa
- RODO

- Qualys SSLabs Report
- To generate and view the report, visit the site: https://www.ssllabs.com/ssltest/analyze.html?d=monitoring.solaredge.com



Zastrzeżenie stwierdzeń dotyczących przyszłości

Niniejsza prezentacja zawiera stwierdzenia dotyczące przyszłości w rozumieniu ustawy o reformie sporów dotyczących papierów wartościowych z 1995 r. Te stwierdzenia dotyczące przyszłości zawierają między innymi informacje dotyczące naszych możliwych lub zakładanych przyszłych strategii biznesowych, rozwoju technologii oraz nowych produktów i usług.

Stwierdzenia dotyczące przyszłości są jedynie prognozami opartymi na naszych obecnych oczekiwaniach i są z natury narażone na ryzyko i niepewność. Nie należy ich traktować jako gwarancji przyszłych wyników, które mogą różnić się znacznie od wyników przedstawionych, rozważanych lub leżących u podstaw tej prezentacji.

Dziękujemy.

Uwaga ostrzegawcza dotycząca danych rynkowych i prognoz branżowych

Ta prezentacja Power Point zawiera dane rynkowe i prognozy branżowe z określonych źródeł zewnętrznych. Informacje te opierają się na badaniach branżowych oraz wiedzy specjalistycznej podmiotu sporządzającego sprawozdanie z danej branży i nie ma pewności, że takie dane rynkowe są dokładne lub że takie prognozy branżowe zostaną zrealizowane. Chociaż nie zweryfikowaliśmy niezależnie dokładności takich danych rynkowych i prognoz branżowych, uważamy, że dane rynkowe są wiarygodne, a prognozy branżowe uzasadnione.

Nr wersji: WER. 1.0