ACCESS GRANTED?

Cyberbezpieczeństwo mikroinstalacji PV

ADVANT
systemy informatyczne

Aleksander Babś

Advant sp. z o.o.

20.05.2021

PTPiREE

Monitorowanie pracy instalacji PV

- Praktycznie wszystkie mikroinstalacje PV wyposażone są w urządzenia ("dongle/sticki") do monitorowania ich pracy
- Urządzenia te mogą być wpięte do sieci lokalnej (Ethernet, WiFi) lub posiadać modem komórkowy. Po podłączeniu i skonfigurowaniu, przesyłają na serwery producenta falownika szereg informacji związanych z działaniem mikroinstalacji. Typowo jest to określona paczka danych przesyłana co 1 min lub częściej 5 min.

```
"inverter_serial_number":
"inverter_temperature":
"dc_voltage_pv1":
"dc_current":
"ac_current_t_w_c":
"ac_voltage_t_w_c":
"ac_output_frequency":
"daily_active_generation":
"total_dc_input_power":
"total_active_generation":
```

- Oprócz funkcji związanych z monitorowaniem pracy instalacji, możliwa jest m.in zdalna aktualizacja firmware falownika oraz samego urządzenia

Urządzenia komunikacyjne

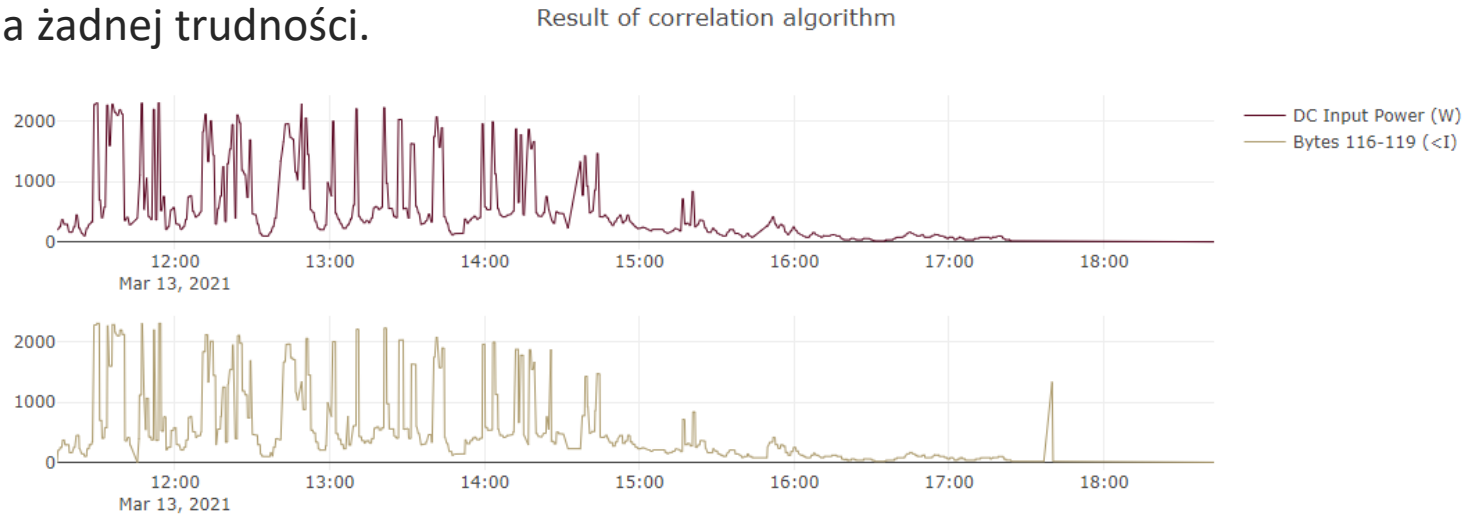
- "Sticki" wpinane są najczęściej do złącza RS485 i komunikują się z falownikiem w oparciu o własny protokół danego producenta ("proprietary"), mimo faktu iż na tym samym złączu często dostępny jest także protokół SunSpec - aktualnie wymagany przez IRiESD poszczególnych OSD. Jest to prawdopodobnie spowodowane chęcią zachowania wstecznej kompatybilności z wszystkimi modelami falowników danego producenta, gdzie nowsze modele są zgodne zarówno z protokołem producenckim jak też właśnie protokołem SunSpec, a starsze konstrukcje nie są zgodne z SunSpec.

- Niezależnie od zastosowanego protokołu sterującego falownikiem (własny producenta lub SunSpec), przesyłanie danych pomiędy urządzeniem a falownikiem odbywa się w sposób **całkowicie jawny** ("clear text"), bez żadnej identyfikacji, uwierzytelnienia ani autoryzacji użytkownika lub urządzenia. Jest to cecha protokołu Modbus, bo taki właśnie jest stosowany.

- Niektóre "sticki" podłączane do falowników posiadają określone podatności (https://www.secura.com/blog/iot-solar-inverters-trickle-down-vulnerabilities) lub "cechy funkcjonalne" takie jak login/hasło admin/admin do Web GUI, zapisane w pamięci flash statyczne i niezmienne hasło (np "HF-A11ASSISTHREAD") umożliwiające zdalnie sterowanie urządzeniem, i wiele innych "ciekawostek".

Łączność WAN - pełna kontrola

- Ponadto, komunikacja TCP/IP pomiędzy "stickiem" a serwerem producenta nie jest szyfrowana, możliwe jest jej podsłuchanie i analiza. Realizacja ataku Man-in-the-Middle nie przedstawia żadnej trudności.



- Fizyczny dostęp do złącza RS485 praktycznie gwarantuje **pełną kontrolę** nad falownikiem - w szczególności możliwe jest przesyłanie komend sterujących pracą falownika, takich jak:
  - wyłącz/załącz generację (SunSpec INV1)
  - zmiana mocy czynnej (INV2)
  - sterowanie mocą bierną (INV3)

...a zatem wszystko co podłączymy do złącza komunikacyjnego falownika (i co efektywnie łączy się poprzez WAN z serwerem producenta) pozwala na praktycznie nieograniczone kontrolowanie pracy mikroinstalacji.

A zatem - obce urządzenie w sieci lokalnej !?

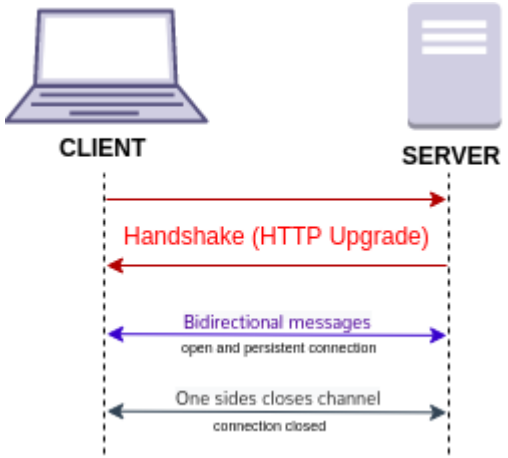
- Urządzenia dołączane do falowników nie posiadają żadnych certyfikatów bezpieczeństwa i nie zostały poddane audytowi bezpieczeństwa – a mimo to instalowane są bezpośrednio w sieciach lokalnych klientów, będąc de facto zupełnie obcym urządzeniem zainstalowanym za firewallem chroniącym taką sieć tj. wewnątrz sieci domowej lub firmowej.

- Urządzenia te są bezpośrednim punktem styku sieci energetycznej z siecią Internet - a zatem możemy za ich pomocą mieć określony i realizowany zdalnie wpływ na działanie tej pierwszej - sytuacja bez precedensu !!

Ale przecież mam firewall !?

Istnieją powszechnie stosowane techniki nawiązywania i utrzymywania dwukierunkowych połączeń sieciowych, w których jeden z węzłów wymiany danych - ten inicjujący połączenie - znajduje się za firewallem i posiada prywatny adres IP. Przykładowo:

- VPN - teoretycznie można zablokować IPSec, PPTP, ale zostają protokoły takie jak SSTP
- Websockets - czyli ruch de facto HTTP/HTTPS, "przeglądarkowy"



Producenci wykorzystują możliwość połączenia się z urządzeniem przy falowniku na przykład w celu zdalnej aktualizacji oprogramowania i zmiany ustawień.

Biorąc to pod uwagę, jest zatem możliwe zdalne wywołanie określonego działania na każdym falowniku wyposażonym w urządzenie komunikacyjne - co może przekładać się na funkcjonowanie lokalnej sieci elektroenergetycznej.

Nowa instalacja - co ujawniamy?

Podłączając producenckie urządzenie do monitorowania pracy falownika udostępniamy:

- SSID oraz hasło do WiFi,
- adresację IP sieci wewnętrznej, adres routera/firewalla
- dane o sieci elektroenergetycznej - napięcia fazowe w sieci, aktualną częstotliwość sieci
- informację o niezawodności sieci nn poprzez monitorowanie wyłączenia/załączenia zasilania AC - możliwe oszacowanie SAIDI i SAIFI
- dane pogodowe – profile natężenia promieniowanie słonecznego w miejscu instalacji poprzez przeliczenie prądów w łańcuchach (stringach) DC proporcjonalnych do natężenia tego promieniowania
- współrzędnie miejsca instalacji GPS (o ile użytkownik podał lub nastąpiło ‘podanie domyślne’) – można je także zgrubnie pozyskać za pomocą adresacji IP i serwisu typu IP2Geo

Dane z falowników - czy sensytywne / RODO?

W połowie lipca 2020 Trybunał Sprawiedliwości Unii Europejskiej (TSUE) wydał ważny wyrok w sprawie C-311/18 Data Protection Commissioner przeciwko Facebook Ireland Ltd. i Maximilian Schrems. TSUE stwierdził nieważność decyzji Komisji Europejskiej w sprawie Tarczy Prywatności, skutkiem czego USA uznane zostało za państwo niegwarantujące standardu równoważnego dla unijnego rozporządzenia o ochronie danych osobowych (RODO).

GeoTraceroute to:

47.88.8.200

#1 PL - **Warszawa** (0 km)
#2 PL - **Warsaw** (10 km)
#3 DE - **Frankfurt** (899 km)
#4 FR - **Roubaix** (388 km)
#5 GB - **London** (241 km)
#6 US - **New York** (5575 km)
#7 US - **Chicago** (1154 km)
#8 US - **Palo Alto** (2955 km)
#9 US - **San Mateo** (20 km)

Path via: Alibaba (China) Technology Co.
Path / real distance: 11242 / 9428 km
Countries involved: 5
View as: Google Maps - KML

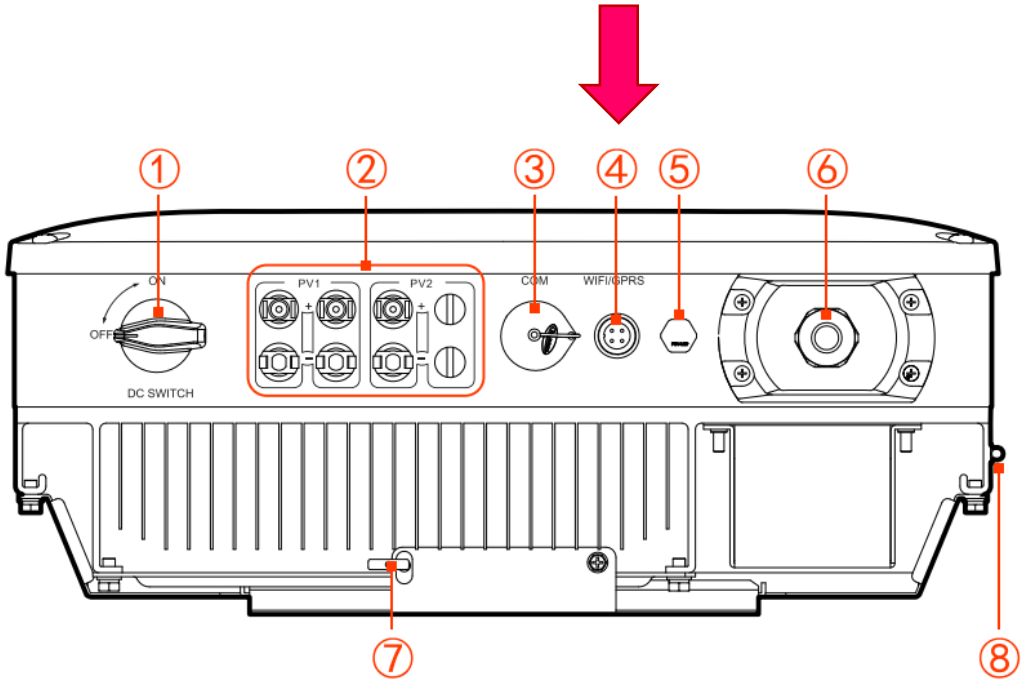
Co można wykonać zdalnie ?

Urządzenie może aktywnie nawiązać połączenie szyfrowane VPN na zaprogramowany adres – nawet zza firewalla prosumenta, stając się w pełni sterowalnym urządzeniem, które umożliwia poprzez tunelowanie pakietów między innymi:

- skanowanie sieci wewnętrznej
- przełamywanie zabezpieczeń urządzeń w sieci LAN – np switche, drukarki - typowo wykorzystujących hasła domyślne
- przełamywanie zabezpieczeń lokalnych komputerów, w tym serwerów – np. ekstrakcja plików z folderów sieciowych i wysłanie na zadany adres
- realizację ataków DDoS (ang. *distributed denial of service*)
- inne ataki w zależności od celu i poziomu wiedzy hakerów.

Jedno złącze - dużo możliwości

- Większość (wszystkie?) falowników realizuje komendę załącz/wyłącz (‘connect/disconnect’) poprzez interfejs RS485 (ew. Ethernet/Wifi/USB),
- Do tego samego interfejsu jest podłączone urządzenie monitorujące a zatem urządzenie to potencjalnie może zostać wykorzystane to ataku



Atak - dlaczego nie?

Scenariusz przykładowego ataku:

- Następuje włamanie do infrastruktury operatora agregującego działanie urządzeń monitorujących falowniki
- Haker ustala po adresach IP urządzeń interesującą go pulę/zasób falowników
- Sprawdza aktualnie generowaną moc czynną
- Tworzy listę falowników do wyłączenia - zaczynając od generujących aktualnie największą moc czynną
- Wysyłana jest masowo komenda INV1 z argumentem ‘disconnect’, lub INV2 z podaniem minimalnej wartości – np 1% wartości znamionowej, falownik dalej będzie dołączony do sieci – brak alarmu na wyświetlaczu, jednak ograniczy moc czynną o 99%
- W ciągu około 1 minuty – ubytek mocy rzędu na przykład 1 GW w KSE

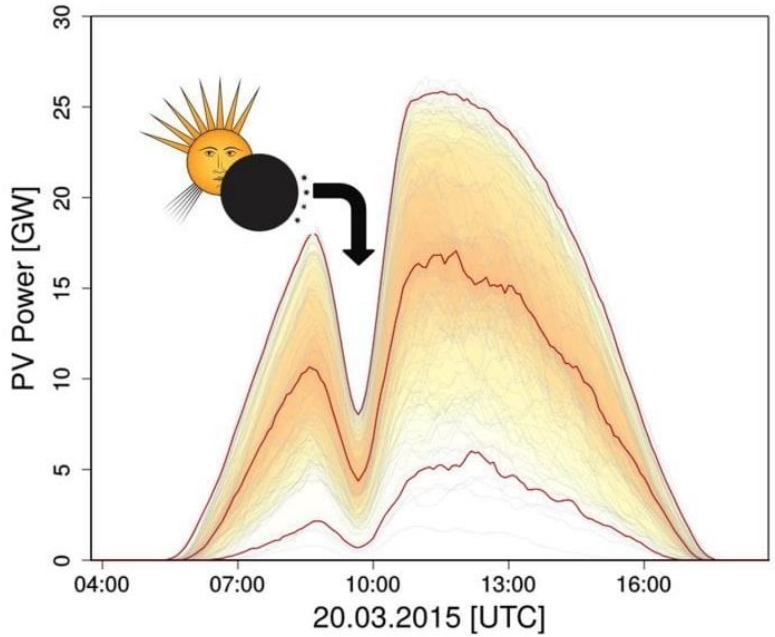
Ze względu na zróżnicowanie systemów monitorowania różnych producentów, jednoczesne wyłączenie wszystkich falowników jest **mało prawdopodobne**, należy jednak pamiętać o rosnącym potencjale mocy instalacji fotowoltaicznych i co za tym idzie - rosnący wpływ na funkcjonowanie KSE.

Nagłe wypadnięcie PV z KSE

Przyjmując obecne 4.5 GW mocy w instalacjach PV, z czego około 3 GW to instalacje prosumenckie, to nagły ubytek np połowy tej mocy - w wypadku skoordynowanego ataku - może będzie niebezpieczny dla KSE.

Prognozowany wzrost mocy prosumenckich instalacji PV będzie zwiększał **ryzyko zachwiania stabilnością** KSE w razie ich jednoczesnego "wypadnięcia" z systemu.

Do wypadnięcia "planowego" można się przygotować



ZAPOTRZEBOWANIE [MW]	21 230
GENERACJA [MW]	16 251
el. cieplne	14 176
el. wodne	501
el. wiatrowe	249
el. fotowoltaiczne	1 325
el. inne odnawialne	0
SALDO WYMIANY CAŁKOWITEJ [MW]	4 943 IMPORT
CZĘSTOTLIWOŚĆ [Hz]	49,877

https://www.advancedsciencenews.com/total-eclipse-sun-response-photovoltaics-germany/

Zmiana aktualnego stanu rzeczy - technicznie

Nie jest żadnym wyzwaniem technicznym opracowanie i wdrożenie całościowej architektury bezpieczeństwa, umożliwiającej kompleksowe zabezpieczenie falowników.

Elementami takiej architektury może być:

- wprowadzenie mechanizmów identyfikacji, uwierzytelnianie i autoryzacji, w tym na przykład metody challenge-response
- szyfrowanie przesyłanych danych
- wprowadzenie poziomów dostępu (np wyłącznie odczyt danych z falownika, odczyt + selektywny zapis, odczyt + pełny zapis)
- możliwość zdalnej deaktywacji złącza komunikacyjnego, w razie wykrycia prób naruszenia bezpieczeństwa falownika

Implementacja powyższych mechanizmów byłaby łatwiejsza w sytuacji w której falownik byłby wyposażony w zintegrowany port Ethernet/WiFi/modem komórkowy - a nie w postaci osobnego urządzenia, jak to najczęściej ma miejsce obecnie.

Zmiana aktualnego stanu rzeczy - prawnie

Rozważyć należy wprowadzenie odnośnych regulacji prawnych w celu zmiany obecnego stanu rzeczy. Dotyczyć to może:

- certyfikacji (licencjonowania) podmiotów uprawnianych do zbierania danych z urządzeń monitorujących pracę instalacji PV pod kątem cyberbezpieczeństwa oraz ochrony danych
- składowania i przetwarzania danych pochodzących z instalacji PV na terenie UE
- certyfikacji urządzeń monitorująco-sterujących, prowadzącej do ograniczenia dostępnego zakresu funkcji prowadzących do zdalnego odłączenia falownika oraz ograniczenia dostępu do istotnych danych o sieci elektroenergetycznej.

Czy jedynym uprawnionym do pełnego dostępu do mechanizmów sterowania falownikami jak i zbierania danych powinien być operator systemu energetycznego?


Dziękuję za uwagę