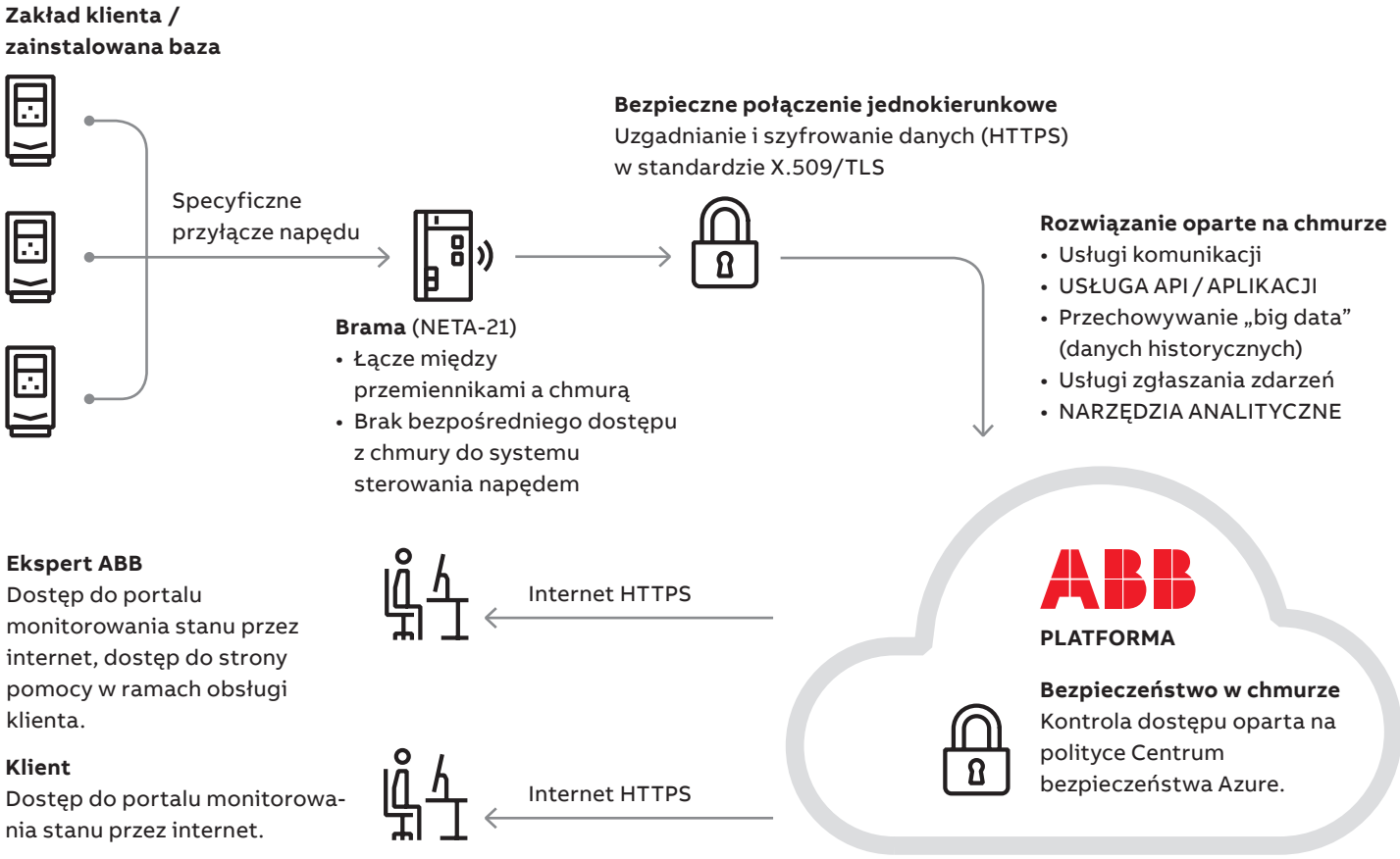
SERWIS NAPĘDÓW ABB

# Usługi cyfrowe ABB Ability™ dla napędów
## Cyberbezpieczeństwo w chmurze

Przesyłaniu danych z urządzeń przemysłowych poprzez sieć często towarzyszą obawy dotyczące cyberbezpieczeństwa. W niniejszym dokumencie omówiono przesyłanie scentralizowanych danych do chmury. ABB stosuje najnowocześniejsze procesy w celu zapewnienia bezpieczeństwa danych i urządzeń. Jednak sami klienci także muszą być świadomi zagrożeń i wiedzieć, czy ich systemy są objęte procesem monitorowania danych.



# Jak zadbać o cyberbezpieczeństwo?


## Procesy ABB zapewniające bezpieczeństwo

- Możliwość przeglądania i subskrybowania alertów i powiadomień ABB dotyczących cyberbezpieczeństwa pod adresem: https://new.abb.com/about/technology/cyber-security/alerts-and-notifications .
- Możliwość przesyłania raportów bezpośrednio do zespołu ekspertów ABB ds. cyberbezpieczeństwa, który jest oficjalną, certyfikowaną jednostką ABB, na adres: cybersecurity@ch.abb.com.
- Ciągłe zarządzanie poprawkami i monitorowanie podatności na zagrożenia dla poszczególnych wersji oprogramowania.
- Przestrzeganie zasad bezpieczeństwa SDL (ang. Secure Development Lifecycle).
- Sprawdzanie całego oprogramowania przez kilka programów antywirusowych przed jego opublikowaniem.
- Niezależne Centrum Zapewnienia Bezpieczeństwa Urządzeń (DSAC, ang. Device Security Assurance Center) jako kluczowy element oferty ABB — miejsce, w którym wszystkie produkty ABB przed wprowadzeniem na rynek są poddawane nowoczesnym testom bezpieczeństwa. Proces ten obejmuje ocenę odporności i integralność bezpieczeństwa, a także skanowanie portów, zalewanie sieci, skanowanie pod kątem podatności na zagrożenia oraz fuzzing protokołów.
- Szkolenie w zakresie cyberbezpieczeństwa jest obowiązkowe dla wszystkich użytkowników zaangażowanych w rozwój i świadczenie usług.
- ABB zobowiązuje swoich dostawców do przestrzegania zbioru zasad, a w strukturach wewnętrznych ABB stosowane są jeszcze bardziej rygorystyczne reguły.
- Więcej informacji na ten temat można znaleźć na stronie: https://new.abb.com/about/supplying/cyber-security.

## Zarządzanie danymi klientów

- Postanowienia ABB Ability™ Data Manifesto określają sposób wykorzystywania danych klientów.
- Dane klientów pozostają ich własnością.
- Klienci wiedzą, co robimy z ich danymi.
- Nie ujawniamy danych klientów bez ich zgody.
- Gwarantujemy, że dane/IP nie są udostępniane konkurencji ani wykorzystywane dla jej pożytku

**Specyficzne przyłącze przemienników**

- Przemienniki ABB można podłączyć z wykorzystaniem:
  - kabli światłowodowych
  - szyn panelowych (zamiast paneli)
  - łącza Ethernet przez moduł FENA-x1.
- Brama NETA-21 może pełnić funkcję lokalnej strony www do uzyskiwania dostępu do napędu.
- Domyślny poziom dostępu nie umożliwia konfiguracji napędu, ale funkcja ta może zostać włączona lokalnie.
- Należy ustalić bezpieczne hasło do interfejsu internetowego NETA 21, aby nie dopuścić do nieuprawnionego dostępu do sieci lokalnej.
- Do celów serwisowych interfejs NETA 21 nie wymaga żadnego połączenia przychodzącego ani VPN.
- Za bezpieczeństwo na terenie zakładu odpowiada klient. Lokalny dostęp do sieci Ethernet powinien być ograniczony, a zapory sieciowe powinny być skonfigurowane w taki sposób, aby umożliwiać tylko niezbędny ruch.
- Modem komórkowy zapewniający dostęp do internetu może pomóc w odizolowaniu przyłącza do monitorowania napędu od lokalnej sieci sterowniczej.

**Brama sieciowa**

- Urządzenie NETA 21 obsługuje funkcje konwersji protokołów, agregacji danych i kilka warstw bezpieczeństwa.
- Urządzenie NETA 21 obsługuje jedynie oryginalne obrazy oprogramowania ABB. Użytkownik nie może na nim zainstalować żadnego dodatkowego oprogramowania.
- Oprogramowanie bramy można aktualizować zarówno lokalnie, jak i centralnie z wykorzystaniem chmury.
- Urządzenie NETA 21 ma wewnętrzną zaporę sieciową, która blokuje niepotrzebne typy połączeń.
- Wszystkie działania są zapisywane na ścieżce kontrolnej w pamięci wewnętrznej i na karcie SD. Zdarzenia są ponadto wysyłane do chmury.
- W razie potrzeby lokalny interfejs sieciowy NETA 21 może zostać całkowicie wyłączony (po podłączeniu do chmury).
- Dane zapisywane na karcie SD mają sygnatury uniemożliwiające wprowadzanie niepożądanych zmian
- Dla zabezpieczenia przed usunięciem danych znajdujących się na karcie SD interfejsu niezbędne są również fizyczne środki bezpieczeństwa (np. szafka z zamykanymi drzwiczkami).

**Bezpieczne połączenie jednokierunkowe**

- Przesyłanie danych do chmury to procedura push z wykorzystaniem protokołu HTTPS, więc ich przepływ jest wyłącznie wyjściowy.
- Dodatkowy kanał WebSocket służy do wydawania ograniczonego zbioru poleceń dotyczących np. żądania niektórych plików dziennika, ponownego uruchomiania bramy (nie napędu) oraz wykorzystania najnowszych aktualizacji oprogramowania.
- Aktualizacje są pobierane wyłącznie z Biblioteki ABB i sprawdzane pod kątem ważności sygnatury.
- Użycie wewnętrznych kont użytkowników bramy uniemożliwia dokonywanie zapisu danych w napędzie przez użytkownika domyślnego i użytkownika w chmurze.
- W celu zapewnienia poufności danych podczas ich przesyłu stosowane są najnowsze metody szyfrowania, takie jak TLSv1.2 z certyfikatami X.509.
- Ważność certyfikatu gwarantuje, że dane są przesyłane wyłącznie do prawidłowej chmury ABB Ability™.
- Brama powinna znajdować się za zaporą sieciową. Port wyjściowy TCP:443 łączący interfejs NETA 21 z chmurą jest wystarczający. Porty wejściowe nie są potrzebne.
- Jeżeli klient nie może korzystać z własnej sieci, do udostępniania internetu można stosować routery komórkowe, takie jak eWON Cosy 131. Router komórkowy pełni funkcję zapory sieciowej i opcjonalnej warstwy VPN (VPN nie wchodzi w zakres standardowej oferty usług; należy ją aktywować tylko wtedy, gdy jest to absolutne konieczne).
- Alternatywą dla bezpośredniego połączenia z internetem jest przesyłanie danych masowych (tj. z karty SD do portalu w chmurze).

**Bezpieczeństwo portalu**

- Portale korzystają z bezpiecznych połączeń (HTTPS) i nowoczesnych interfejsów reaktywnych.
- Po zalogowaniu się do portalu MyABB użytkownik ma dostęp do wszystkich usług ABB.
- Konta użytkowników są obsługiwane w oparciu o centralne zasady w centralnej usłudze Active Directory.
- Dostępne jest uwierzytelnianie dwuskładnikowe.
- Wszystkie konta użytkowników są prywatne (nie występują żadne konta grupowe ani firmowe), które po upływie określonego czasu nieaktywności tracą ważność.
- O konieczności usunięcia konta klient informuje osobę kontaktową z ramienia ABB.
- W celu usunięcia konta osoba ta wprowadza do wewnętrznego systemu ABB (MyIS) zgłoszenie, które inicjuje proces powodujący (i procedurę zatwierdzającą) usunięcie konta.

**Bezpieczeństwo w chmurze**

- Wszystkie zapisywane dane są szyfrowane w chmurze.
- Do bezpiecznego przechowywania danych wykorzystywane są najlepsze praktyki, takie jak Azure Key Vault.
- W chmurze stosowane są funkcje zarządzania tożsamością i dostępem oraz uwierzytelniania wieloskładnikowego.
- Aktywa w chmurze są chronione przed zagrożeniami i monitorowane pod kątem zagrożeń.
- Usługi w chmurze zapisują ścieżkę kontrolną dla wszystkich działań.

—

Więcej informacji można uzyskać, kontaktując się z lokalnym przedstawicielem ABB lub na stronie:

**abb.pl/napedy**
**new.abb.com/drives/pl/autoryzowani-partnerzy-abb**
**abb.pl/silniki**

—

Dokumenty dotyczące innych produktów można znaleźć na stronie:

**www.abb.com/drives/documents**

—



9AKK106930A8297 REV D PL 6.11.2019