Obserwatorium Transformacji Energetycznej

AGH

NCBJ

Ministerstwo Rozwoju i Technologii

NCBR
Narodowe Centrum Badań i Rozwoju

Seminarium 2

Cyfryzacja energetyki rozproszonej

Cyberbezpieczeństwo – ochrona danych i systemów w energetyce

7 marca 2024 roku

Rafał Kozieł – SMA Solar Technology AG

Nota prawna

WAŻNA WSKAZÓWKA:

Wszystkie informacje tu zawarte zostały przygotowane z najwyższą starannością. Pomimo to nie gwarantujemy prawidłowości i kompletności danych i żadna z zawartych tu informacji nie powinna być interpretowana jako taka gwarancja. Przedsiębiorstwo nie ponosi odpowiedzialności za błędy zawarte w tym dokumencie, o ile szkoda nie została spowodowana umyślnie lub w wyniku rażącego zaniedbania ze strony Przedsiębiorstwa. Ponadto Przedsiębiorstwo nie ponosi odpowiedzialności za skutki działań wynikających
z danych i informacji udostępnionych w niniejszej prezentacji.

Informacje zawarte w tej prezentacji są wciąż uzupełniane, modyfikowane i aktualizowane, przy czym Przedsiębiorstwo nie musi o tym informować z wyprzedzeniem. Niektóre stwierdzenia zawarte w niniejszej prezentacji mogą być stwierdzeniami dotyczącymi oczekiwań co do przyszłości lub innymi stwierdzeniami wybiegającymi w przyszłość, na podstawie obecnych poglądów i założeń kierownictwa, które podlegają znanym i nieznanym ryzykom i niepewności. Rzeczywiste rezultaty, fakty i wyniki Przedsiębiorstwa mogą się w znacznym stopniu różnić od informacji zawartych w prezentacji, m.in. ze względu na określone czynniki, zmienione uwarunkowania handlowe i rynkowe oraz prognozowane przez kierownictwo koncernu możliwości wzrostu. Te oraz inne czynniki mogą mieć wpływ na wynik i konsekwencje finansowe opisanych w prezentacji planów i zdarzeń. Przedsiębiorstwo nie przejmuje żadnego zobowiązania do kontynuacji opisywania wypowiedzi zorientowanych na przyszłość i dostosowywania ich do przyszłych wyników lub projektów. Stwierdzeń dotyczących sytuacji w przyszłości, które dotyczą jedynie daty tej prezentacji, nie należy bezkrytycznie traktować jako pewnych.

Prezentacja ta służy jedynie do celów informacyjnych i jedynie po zezwoleniu udzielonym wcześniej przez Przedsiębiorstwo może być przekazana osobom trzecim lub tym, do których nie jest skierowana. Żadna część niniejszej prezentacji nie może być kopiowana, reprodukowana, cytowana ani wykorzystywana do celów innych niż te, dla których została udostępniona. Treści niniejszej prezentacji, tj. wszystkie teksty, obrazy i pliki dźwiękowe są chronione prawem autorskim. Informacje zawarte w prezentacji są własnością Przedsiębiorstwa.

Niniejszy dokument nie stanowi oferty sprzedaży papierów wartościowych w Stanach Zjednoczonych Ameryki Północnej. Papiery wartościowe nie mogą być oferowane ani sprzedawane w Stanach Zjednoczonych Ameryki Północnej bez rejestracji lub zwolnienia z obowiązku rejestracji na mocy zmienionego wydania US Securities Act z roku 1933.

SMA Solar Technology

Ponad 40 lat obecności na rynku

SMA jest jednym ze światowych liderów branży inwerterów fotowoltaicznych oraz rozwiązań do zarządzania i magazynowania energii. Wyróżnia nas jakość i innowacyjność.

>135 GW mocy zainstalowanej inwerterów PV

> 11 GW mocy zainstalowanej w inwerterach bateryjnych

1,700 patentów i wzorów użytkowych

4,100 pracowników

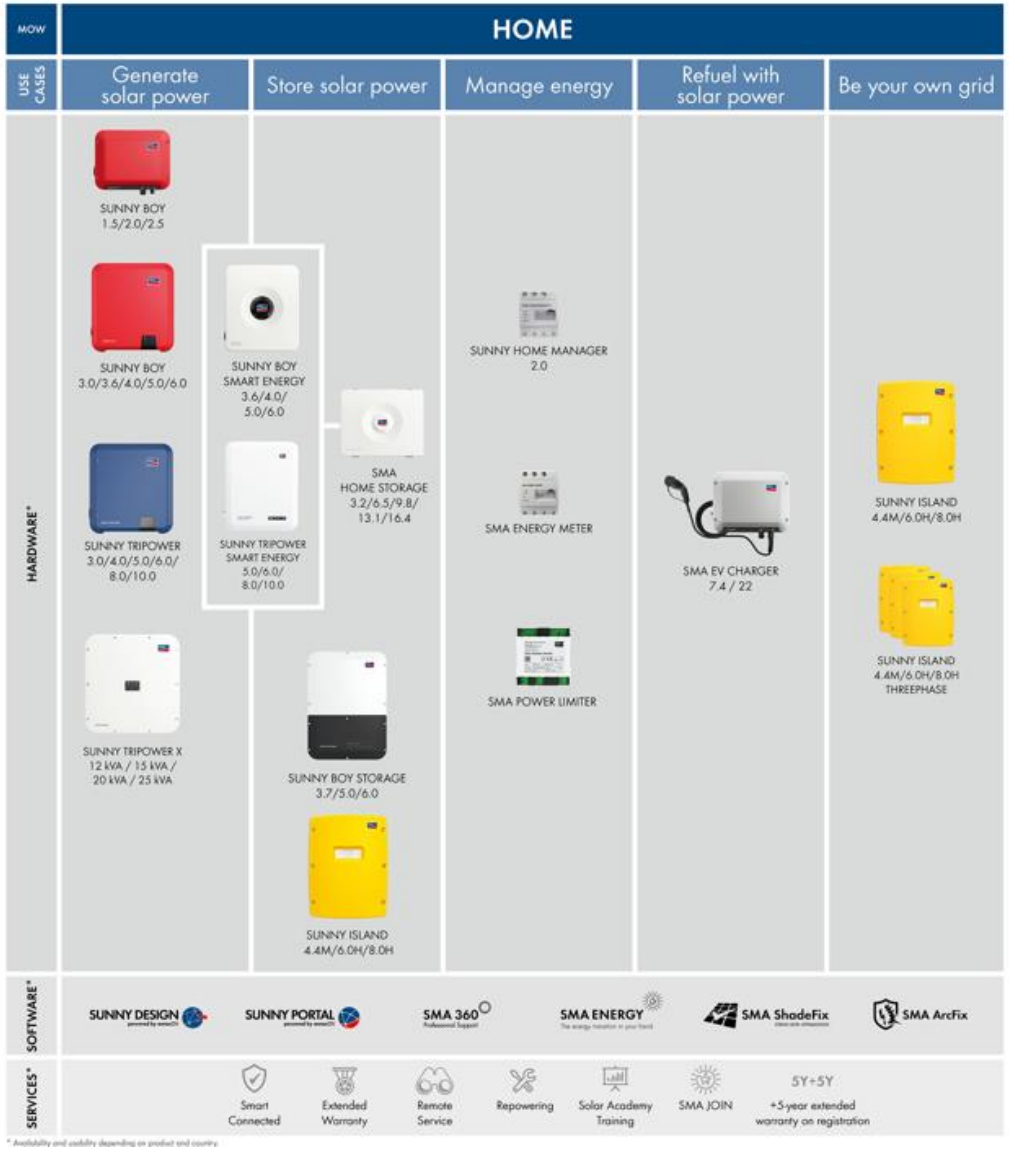
Kassel, Niemcy

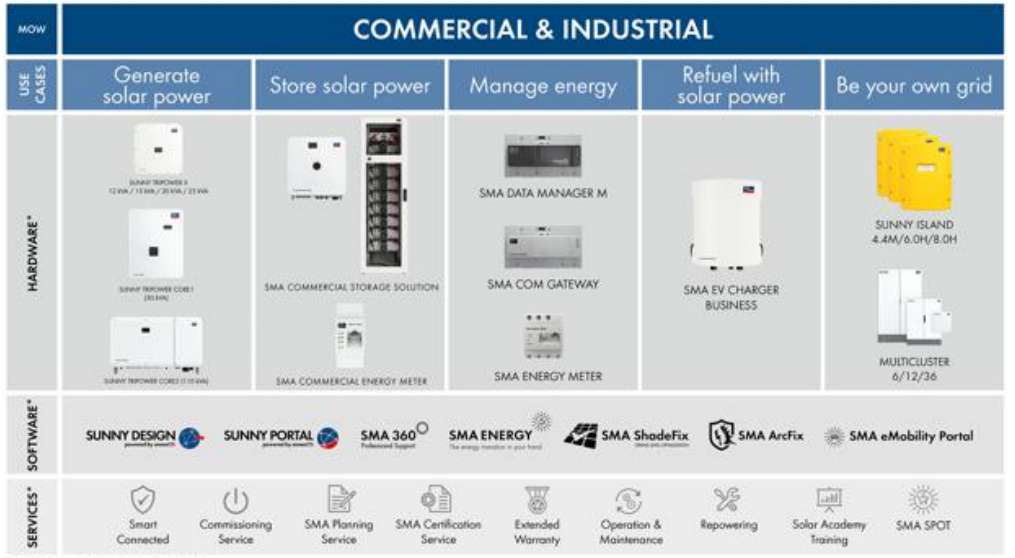
SMA Magnetics – polski oddział SMA Solar Technology AG

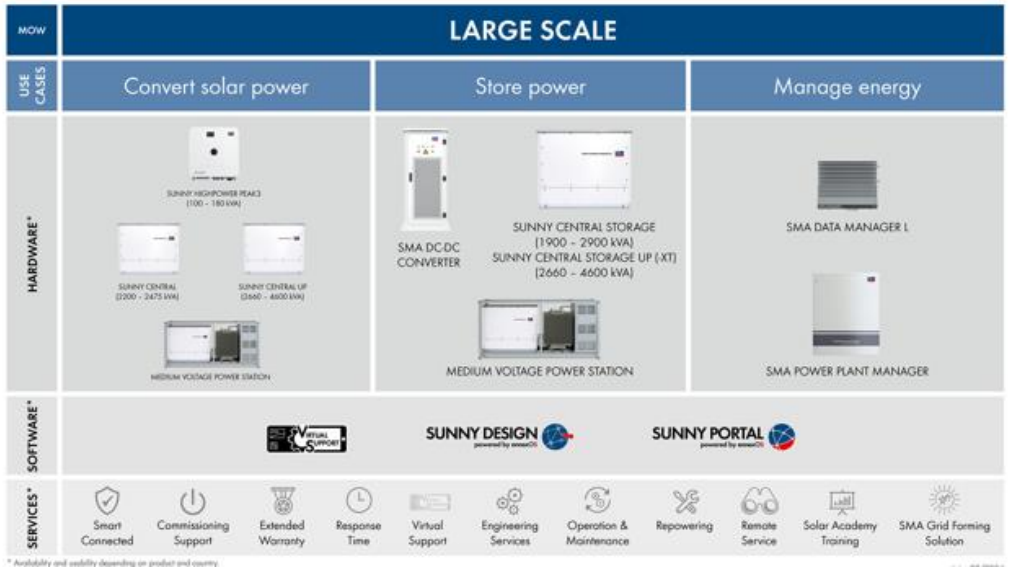
Kraków - Modlniczka

- ponad 800 pracowników
- Zautomatyzowana produkcja dławików, transformatorów i komponentów PCB
- Montaż falowników
- Duży dział R&D, działy wsparcia produkcji, zakupów, IT współpracujące z centralą

SMA Product Portfolio MOW 2024







Rzeczywistość transformacji energetycznej

Transformacja energetyczna = cybernetyzacja

Transformacja energetyczna / dekarbonizacja → zastosowanie rozproszonych, stosunkowo małych źródeł i magazynów energii.
Dla zapewnienia poprawnego współdziałania tych urządzeń, konieczne są zaawansowane technologie komunikacji pomiędzy nimi.
Dla celów rozliczeniowych i bilansowania energii elektrycznej, konieczne jest też zainstalowanie tysięcy liczników energii z możliwością zdalnego odczytu.....

Transformacja energetyczna = cybernetyzacja

Transformacja energetyczna / dekarbonizacja → zastosowanie rozproszonych, stosunkowo małych źródeł i magazynów energii.
Dla zapewnienia poprawnego współdziałania tych urządzeń, konieczne są zaawansowane technologie komunikacji pomiędzy nimi.
Dla celów rozliczeniowych i bilansowania energii elektrycznej, konieczne jest też zainstalowanie tysięcy liczników energii z możliwością zdalnego odczytu.....
Budowa ogromnego systemu informatycznego do komunikacji / wymiany danych

Cyberbezpieczeństwo

USA, 2003 rok

Wirus „Slammer" wprowadzony do sieci w elektrowni jądrowej David-Bess; atak typu DDoS zablokował system nadzorujący chłodzenie reaktora; konieczność wyłączenia awaryjnego na kilka godzin[1];

Ukraina, 2015 rok

Wprowadzenie złośliwego programu BlackEnergy do sieci operatora, wyłączenie stacji elektroenergetycznych, uruchomienie programu KillDisk opóźniającego możliwość zlokalizowania i usunięcia problemu; 230 tys odbiorców bez energii przez ponad 6h[2]

USA, 2021 rok

7 maja 2021 r. Colonial Pipeline, amerykański system rurociągów naftowych, padł ofiarą cyberataku ransomware, który wpłynął na skomputeryzowany sprzęt zarządzający rurociągiem. Kilka dni bez paliwa na stacjach benzynowych[3];

1. CIRE.PL – Cyberataki na energetykę są coraz częstsze
2. Energetyka.Plus - Cyberbezpieczeństwo infrastruktury krytycznej – energetyka na celowniku hakerów
3. Colonial Pipeline ransomware attack – Wikipedia

Cyberbezpieczeństwo

Niemcy, 2022 rok

W lutym 2022 r. cyberatak na dostawcę internetu satelitarnego Viasat sparaliżował komunikację z 11 GW niemieckich turbin wiatrowych, niejako „przy okazji" ataku wymierzonego w ukraiński wojskowy system łączności[4]

Europa i USA – codziennie!

Tylko przez pierwsze 4 miesiące wojny na Ukrainie, Microsoft wykrył próby włamania do ponad 130 organizacji rządowych i firm energetycznych (najwięcej w USA i Europie Zachodniej, w tym w Polsce); ich celem była m.in. próba destabilizacji infrastruktury technicznej[5]. Ogólny wzrost o 220% rok do roku

4. Satellite cyber attack paralyzes 11GW of German wind turbines – pv magazine International (pv-magazine.com)
5. „Defending Ukraine: Early Lessons from the Cyber War" Microsoft

Główne rodzaje ataków

Atak na protokół komunikacyjny

1. Wykrycie i wykorzystanie luk w oprogramowaniu („pozostawionych” nieświadomie przez autorów)
2. Metody socjotechniczne pozyskania danych / haseł dostępowych; phishing

Atak na łańcuch dostaw

1. Uruchomienie pozostawionego celowo na etapie produkcji oprogramowania, destabilizującego pracę urządzenia (bomba logiczna)
2. Użycie tzw. backdoora, „konia trojańskiego” przygotowanego znacznie wcześniej do przeprowadzenia ataku

Cyberbezpieczeństwo jednym z filarów stabilności SEE

Uwierzytelnienie

- Unikanie pozostawiania haseł domyślnych poprzez wymuszenie na użytkowniku jego zmiany w czasie pierwszego uruchomienia urządzenia
- Najnowocześniejsze technologie i algorytmy kryptograficzne
- Logowanie zabezpieczone weryfikacją typu „CAPTCHA"

Made in European Union

- Dane przechowywane w serwerowniach na terenie UE
- Niezależność producenta od wpływów politycznych / rządowych
- Jakość i zabezpieczenia zgodne z europejskimi wymaganiami

Edukacja

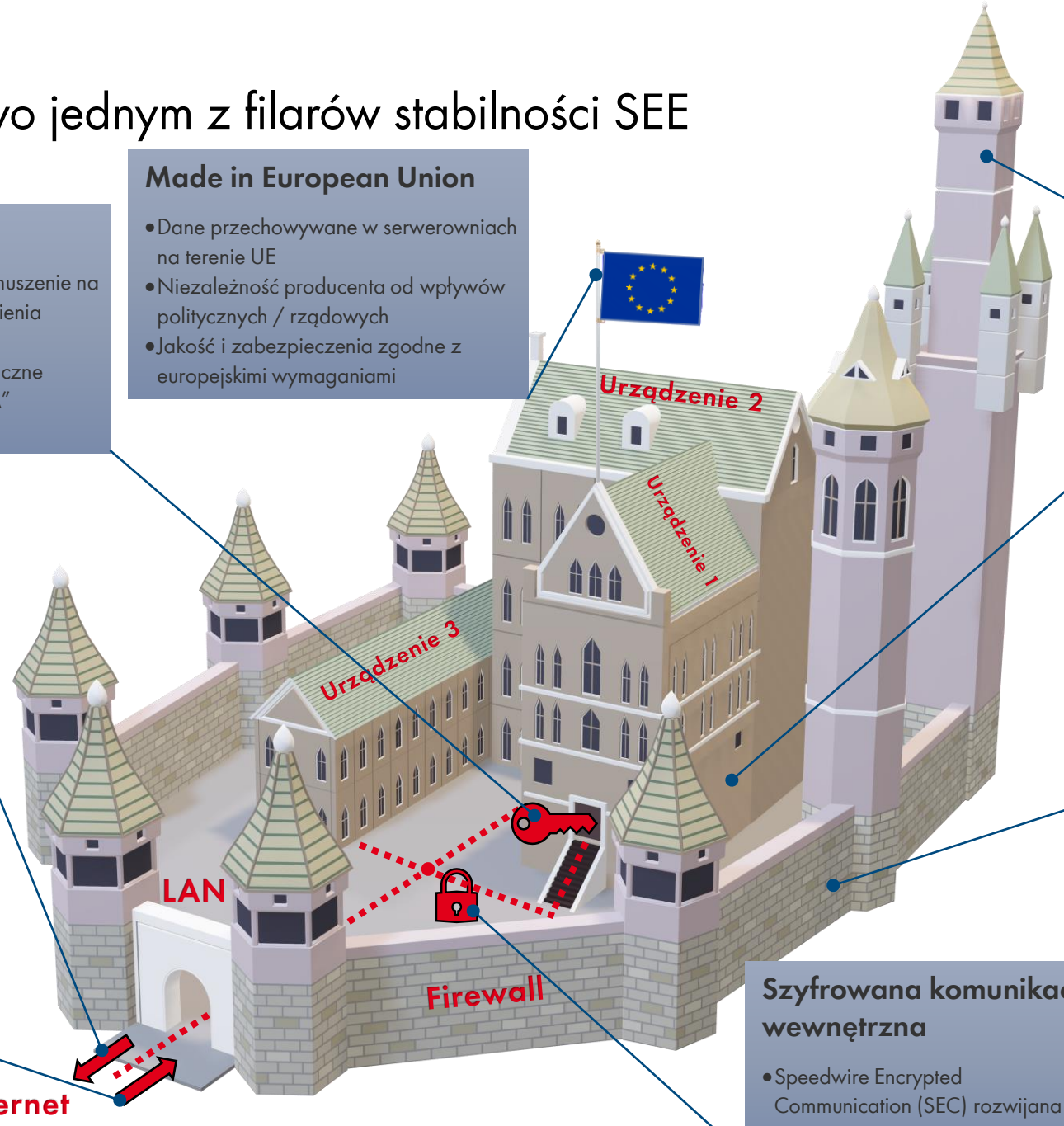
- Edukacja użytkowników na temat zagrożeń
- Szkolenia, biuletyny, manuale

Komunikacja zewn. (opcjonalnie)

- Nowoczesne technologie szyfrowania
- TLS/HTTPS, WebConnect

Minimalizacja liczby miejsc potencjalnego ataku

- Interfejsy i porty zewn. ograniczone do koniecznego minimum
- Bezpieczny system operacyjny i software
- Brak „tylnych drzwi" (back-door)



Zabezpieczony zewn. dostęp (opcjonalnie)

- WebConnect: uwierzytelnienie i szyfrowanie
- VPN

Transparentność i ciągłe doskonalenie

- Polityka informowania o zauważonych lukach w zabezpieczeniach celem uświadomienia o zagrożeniach
- Aktualizacje usuwające potencjalne „dziury w zabezpieczeniach"

Szyfrowana komunikacja wewnętrzna

- Speedwire Encrypted Communication (SEC) rozwijana przez SMA

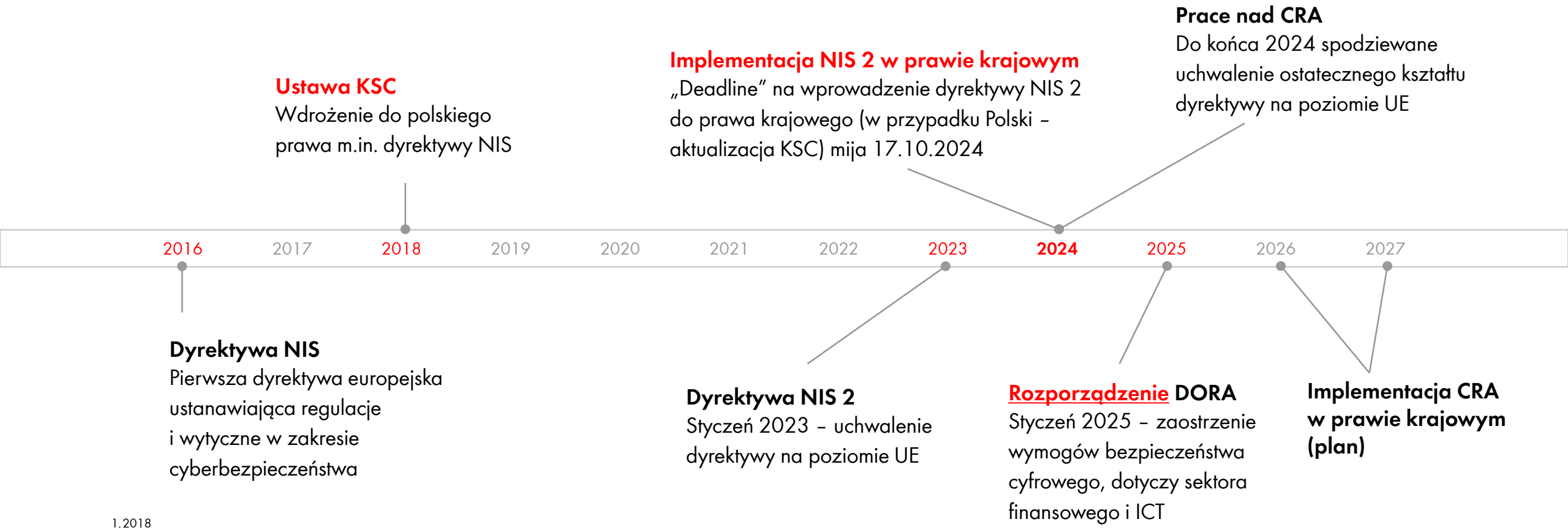
Najgorszy scenariusz...

Otoczenie regulacyjne

Regulacje prawne

Ustawa KSC - Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Główny dokument regulayjny w zakresie cyberbezpieczeństwa obowiązujący w Polsce



1.2018

Podstawowe wymagania NIS2

Strategia/polityka bezpieczeństwa informacji

Do zarządzania ryzykiem należy podejść proaktywnie, a nie reaktywnie, wprowadzając silne zasady bezpieczeństwa informacji, aby zapewnić systematyczną i dokładną analizę ryzyka.

Zapobieganie, wykrywanie i reagowanie na incydenty

Ustalenie planów tworzenia kopii zapasowych.

Projektowanie procedur i środków zapobiegających incydentom.

Przygotowanie planu / całego systemu obsługi incydentów.

Ciągłość działania i zarządzanie kryzysowe

Konieczność posiadania jasnego, weryfikowalnego planu działania podmiotu w przypadku wystąpienia ataku.

Harmonogram działań dla odzyskania pełnej sprawności po wystąpieniu incydentu.

Podstawowe wymagania NIS2

Ujawnianie luk w zabezpieczeniach

Transparentność, korekty i wyciąganie wniosków po zidentyfikowaniu luk

Zgłaszanie incydentów

Incydenty należy zgłaszać stronom zainteresowanym – władzom (do organów CSIRT)

Bezpieczeństwo łańcucha dostaw

Rzetelna ocena ryzyk stwarzanych przez luki w zabezpieczeniach w łańcuchu dostaw i zarządzanie nimi.

Dodatkowa kwalifikacja / certyfikacja poddostawców.

CRA (Cyber Resilence Act)

- **Księga zasad cyberbezpieczeństwa dla urządzeń IoT, wszystkich urządzeń łączących się z internetem**
- **Rozszerzenie dyrektywy NIS2 (procesy) na konkretne produkty**
- **Główne założenia:**
  - ewentualne podatności na zagrożenia będą skutecznie usuwane przez okres przewidywanego użytkowania produktu lub przez pięć lat od wprowadzenia go na rynek;
  - niezwłoczne zgłaszanie (w ciągu 24 godzin) zidentyfikowanych usterek produktów lub usługi Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) bądź jednostkom krajowym (podobnie jak w NIS2);
  - wdrożenia zasad cyberbezpieczeństwa na etapie projektowania towarów i usług.
- **Wszystkie produkty / urządzenia / oprogramowanie ujęte w zakresie CRA będą musiały spełnić te wymagania aby zostać dopuszczone do obrotu w Europie**
- **Wysokie kary za niedopełnienie obowiązków (do 15 MEUR / 2,5% obrotu)**

Podsumowanie

Wyzwania na przyszłość

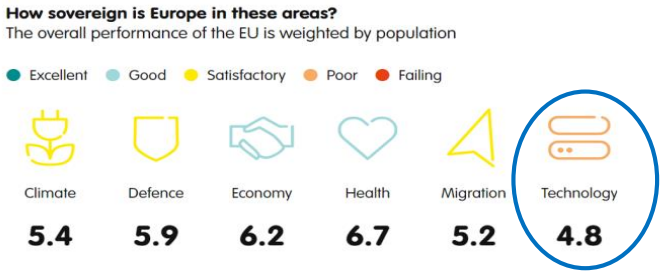
Dalsze możliwe kierunki:

1. Źródło: Europejska Rada Spraw Zagranicznych (ECFR) – European Sovereignty Report

Wyzwania na przyszłość

Dalsze możliwe kierunki:

1. Wzmocnienie suwerenności technologicznej Polski i Europy

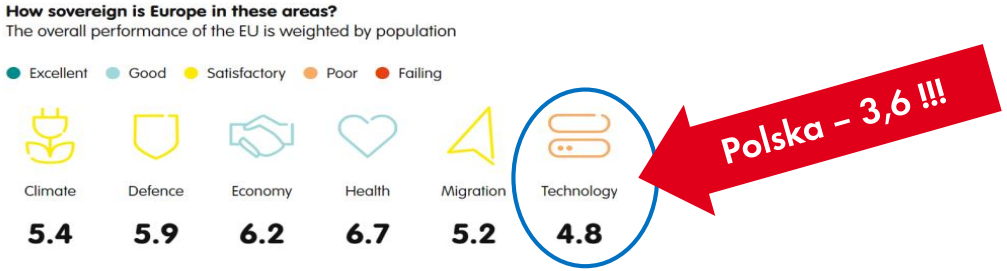


1. Źródło: Europejska Rada Spraw Zagranicznych (ECFR) – European Sovereignty Report

Wyzwania na przyszłość

Dalsze możliwe kierunki:

1. Wzmocnienie suwerenności technologicznej Polski i Europy

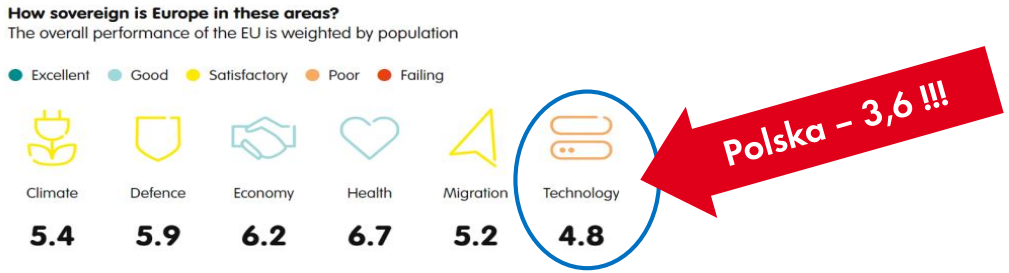


1. Źródło: Europejska Rada Spraw Zagranicznych (ECFR) – European Sovereignty Report
2. Źródło: Rezolucja Parlamentu Europejskiego z dnia 12 marca 2019 r. w sprawie zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia (2019/2575(RSP)

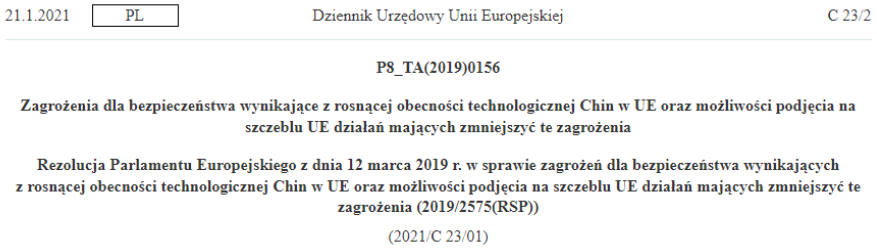
Wyzwania na przyszłość

Dalsze możliwe kierunki:

1. Wzmocnienie suwerenności technologicznej Polski i Europy



2. Ograniczenie stosowania w infrastrukturze krytycznej urządzeń pochodzących spoza EOG, szczególnie w przypadkach gdy zapisy ich przepisów krajowych mogą zagrażać bezpieczeństwu UE


21.1.2021 PL Dziennik Urzędowy Unii Europejskiej C 23/2

P8_TA(2019)0156

Zagrożenia dla bezpieczeństwa wynikające z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia

Rezolucja Parlamentu Europejskiego z dnia 12 marca 2019 r. w sprawie zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia (2019/2575(RSP))

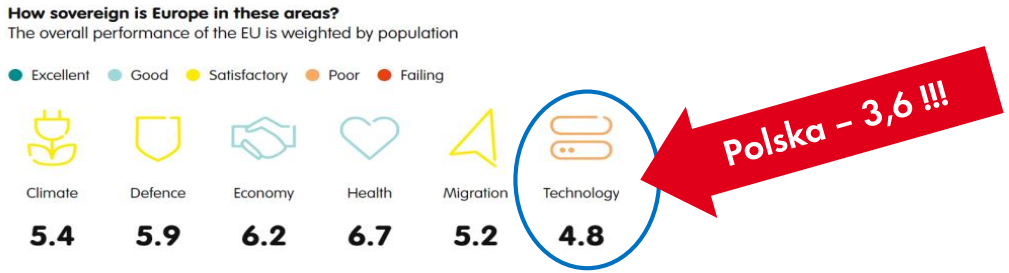
(2021/C 23/01)

1. Źródło: Europejska Rada Spraw Zagranicznych (ECFR) – European Sovereignty Report
2. Źródło: Rezolucja Parlamentu Europejskiego z dnia 12 marca 2019 r. w sprawie zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia (2019/2575(RSP)

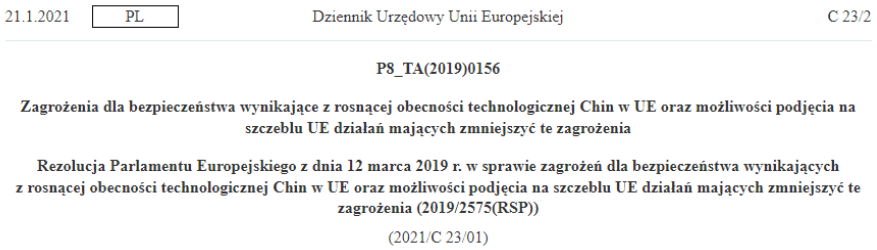
Wyzwania na przyszłość

Dalsze możliwe kierunki:

1. Wzmocnienie suwerenności technologicznej Polski i Europy



2. Ograniczenie stosowania w infrastrukturze krytycznej urządzeń pochodzących spoza EOG, szczególnie w przypadkach gdy zapisy ich przepisów krajowych mogą zagrażać bezpieczeństwu UE



21.1.2021 PL Dziennik Urzędowy Unii Europejskiej C 23/2

P8_TA(2019)0156

Zagrożenia dla bezpieczeństwa wynikające z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia

Rezolucja Parlamentu Europejskiego z dnia 12 marca 2019 r. w sprawie zagrożeń dla bezpieczeństwa wynikających z rosnącej obecności technologicznej Chin w UE oraz możliwości podjęcia na szczeblu UE działań mających zmniejszyć te zagrożenia (2019/2575(RSP))

(2021/C 23/01)

3. Rozpoczęcie dyskusji nad potencjalnymi zagrożeniami wynikającymi z zastosowaniem sztucznej inteligencji

Dziękuję !

SMA Solar Technology AG

mgr inż. Rafał Kozieł
Expert Photovoltaics & Standardization
rafal.koziel@sma-magnetics.com

SMA.de
info@SMA.de

Obserwatorium Transformacji Energetycznej

Projekt współfinansowany przez Narodowe Centrum Badań i Rozwoju w ramach programu badań naukowych i prac rozwojowych "Społeczny i gospodarczy rozwój Polski w warunkach globalizujących się rynków" GOSPOSTRATEG

Wniosek GOSPOSTRATEG.IX-000D_22
Wartość projektu: 7 881 705 PLN
Wartość dofinansowania: 7 719 705 PLN

Wykonawcy projektu

AGH

NCBJ

Ministerstwo Rozwoju i Technologii

Jednostka finansująca

NCBR
Narodowe Centrum Badań i Rozwoju

DOFINANSOWANO ZE ŚRODKÓW BUDŻETU PAŃSTWA

SPOŁECZNY I GOSPODARCZY ROZWÓJ POLSKI W WARUNKACH GLOBALIZUJĄCYCH SIĘ RYNKÓW GOSPOSTRATEG

Obserwatorium Transformacji Energetycznej jako instrument wspierania społeczno-gospodarczego rozwoju Polski (OTE)

DOFINANSOWANIE
7 719 705 PLN

CAŁKOWITA WARTOŚĆ
7 881 705 PLN