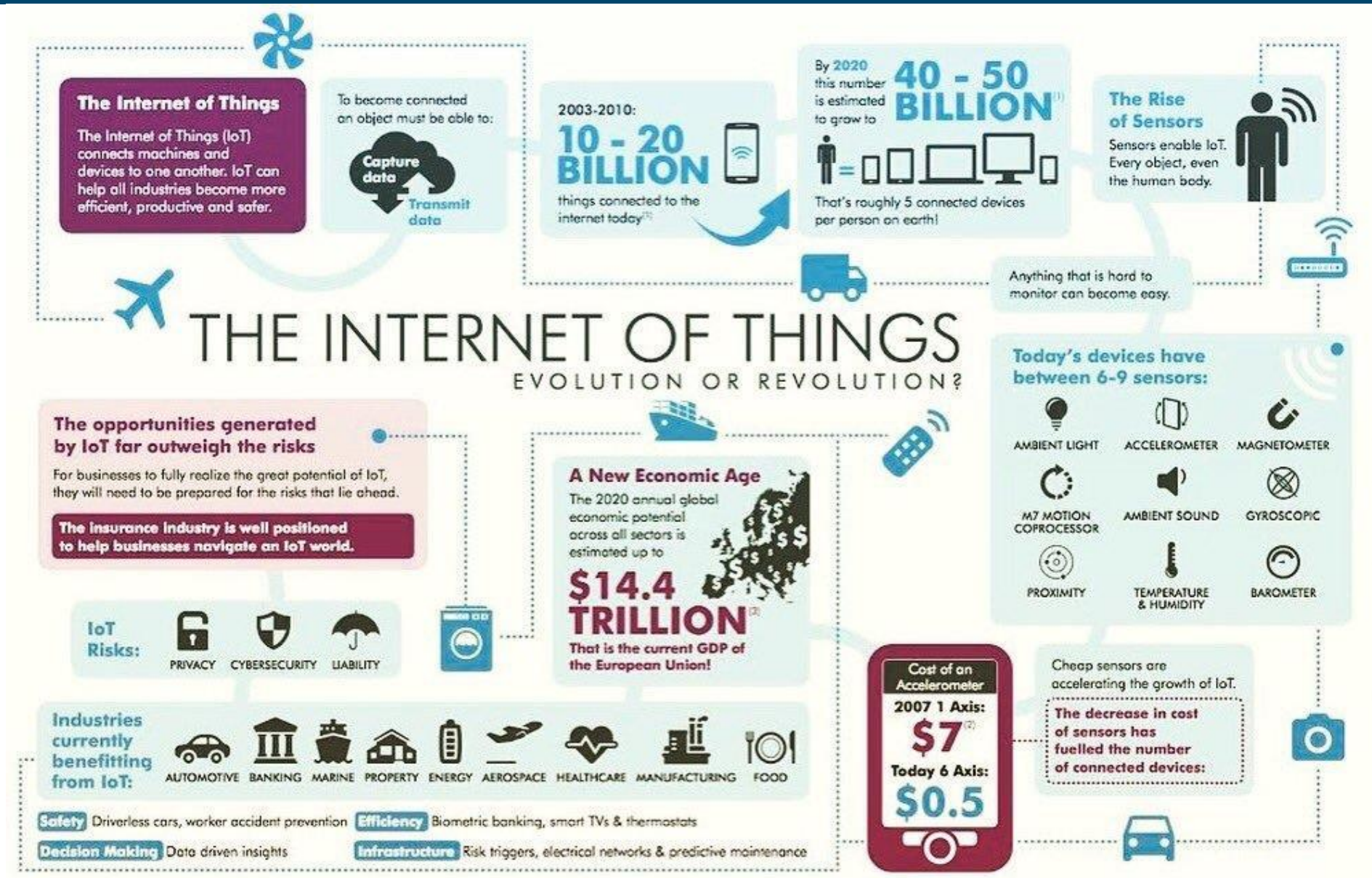
Secure Connected Trustable Things – możliwości technologii IoT

dr inż. Łukasz Kulas,
Wydział Elektroniki, Telekomunikacji i Informatyki, Politechnika Gdańska

secure connected trustable things

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

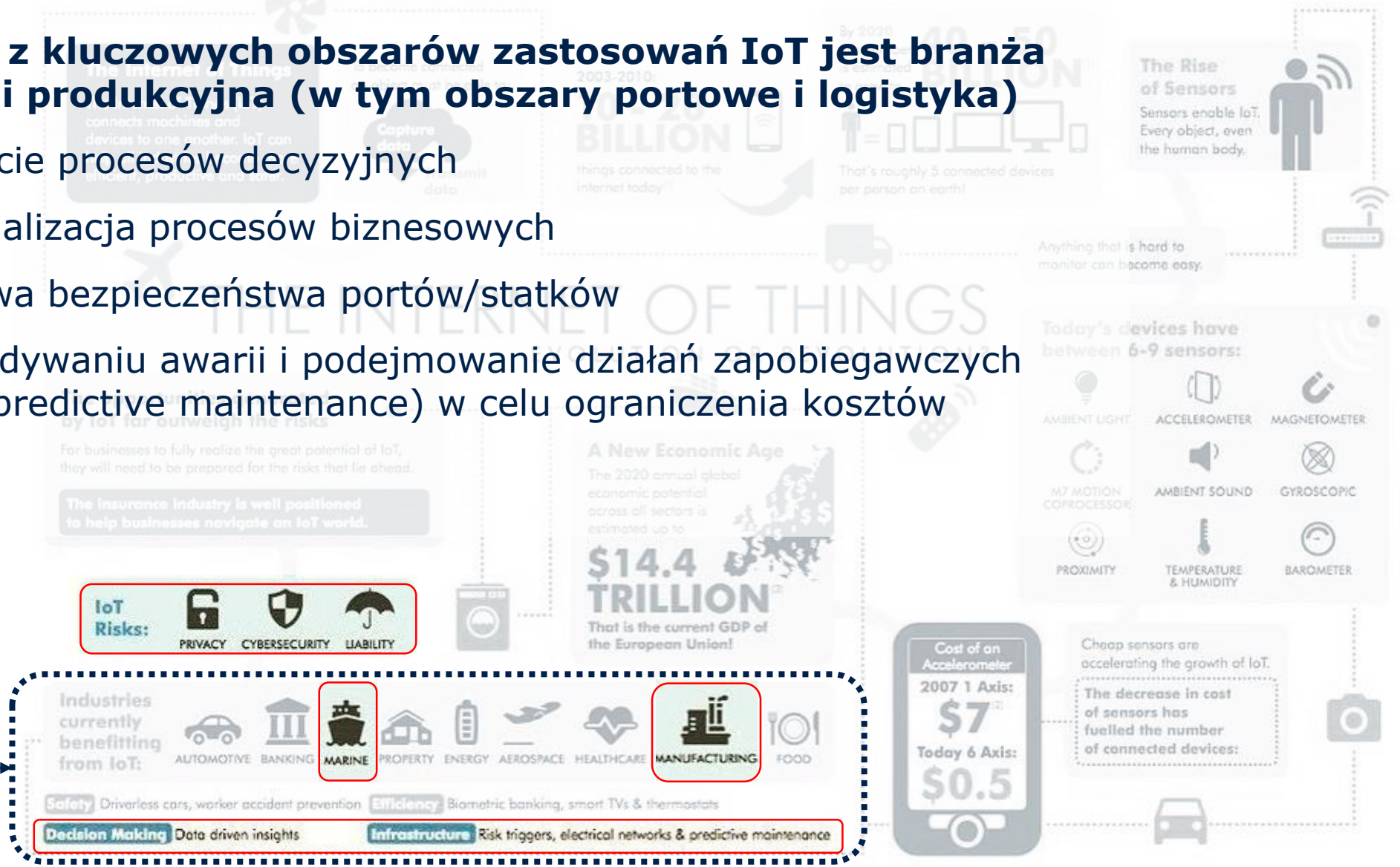
Internet rzeczy IoT (ang. Internet of Things) jako jeden ze światowych megatrendów



https://pbs.twimg.com/media/C_9wu1nVwAARLTl.jpg

Internet rzeczy IoT a produktywna (i bezpieczna) branża morska

- **Jednym z kluczowych obszarów zastosowań IoT jest branża morska i produkcyjna (w tym obszary portowe i logistyka)**
  - Wsparcie procesów decyzyjnych
  - Optymalizacja procesów biznesowych
  - Poprawa bezpieczeństwa portów/statków
  - Przewidywaniu awarii i podejmowanie działań zapobiegawczych (ang. predictive maintenance) w celu ograniczenia kosztów



https://pbs.twimg.com/media/C_9wu1nVwAARLTl.jpg

Internet rzeczy IoT a produktywna (i bezpieczna) branża morska

- **Główne wyzwania technologiczne projektu SCOTT**
  - Opracowanie nowych i bardziej zaawansowanych mechanizmów (cyber)bezpieczeństwa dla IoT
  - Stworzenie **wiarygodnych mechanizmów oceny bezpieczeństwa i prywatności** poprzez **„security classes”** oraz **„privacy labelling”**

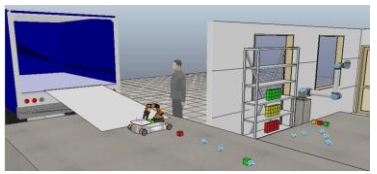
https://pbs.twimg.com/media/C_9wu1nVwAARLTl.jpg

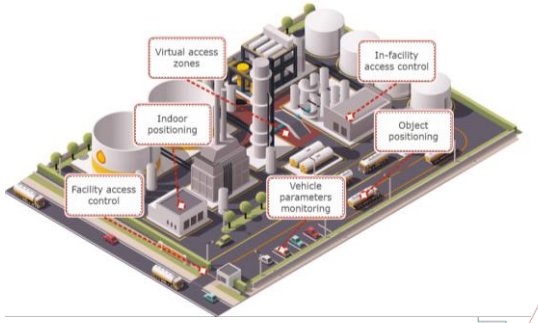
Projekt SCOTT – najważniejsze fakty

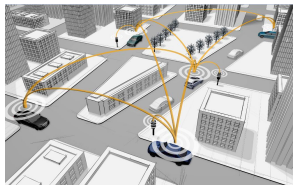
www.scottproject.eu

SCOTT Secure Connected Trustable Things

- **57 partnerów** z **12 krajów** (AT, BE, DE, FI, ES, IE, NL, NO, PL, PT, SE i Brazylia)
- Budżet projektu :**~40M€** – czyli ponad **120 osób** (głównie inżynierów) pracujących na pełen etat przez **3 lata**
- **5 obszarów zastosowań** (Automotive, Aeronautics, Home/Building, Rail, Healthcare) i „cross-domenowe”
  - ☐ **15 scenariuszy wdrożeniowych** (ang. use case)
  - ☐ **25 demonstratorów**
- **47 bloków technologii IoT** w 4 liniach technologicznych:
  - ☐ (cyber)zabezpieczenia i bezpieczeństwo
  - ☐ integracja rozproszonych systemów IoT w chmurze
  - ☐ autonomiczne i efektywne energetycznie węzły IoT
  - ☐ architektura referencyjna dla IoT i standaryzacja







Internet rzeczy IoT, branża morska w kontekście technologii kosmicznych i satelitarnych

- Planowanych jest <u>równolegle</u> co najmniej **kilka mega-konstelacji satelitów**
  - Szybka komunikacja pomiędzy satelitami
  - Wiarygodna i efektywna kosztowo komunikacja z Ziemią (m.in. dla IoT)
- Satelitarna łączność dla IoT obejmie cały świat – także morza i oceany
- Doświadczenia z obecnie realizowanych wdrożeń pilotażowych IoT:
  - Mogą przynieść szybko korzyści (zyski) …
  - … a w przyszłości będą mogły zintegrować także statki na pełnym morzu
  - Obszary, w których sygnał satelitarny będzie niedostępny (budynki, zadaszone parkingi, hale produkcyjne), będą miały własne sieci IoT

Możliwości technologii IoT w kontekście projektu SCOTT

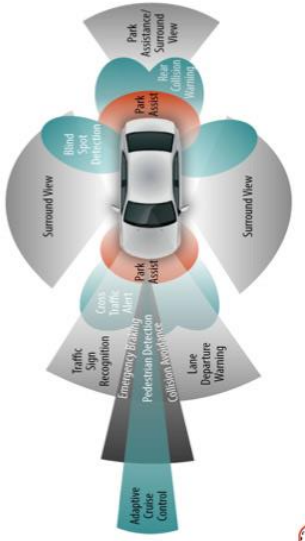
Kilka przykładów

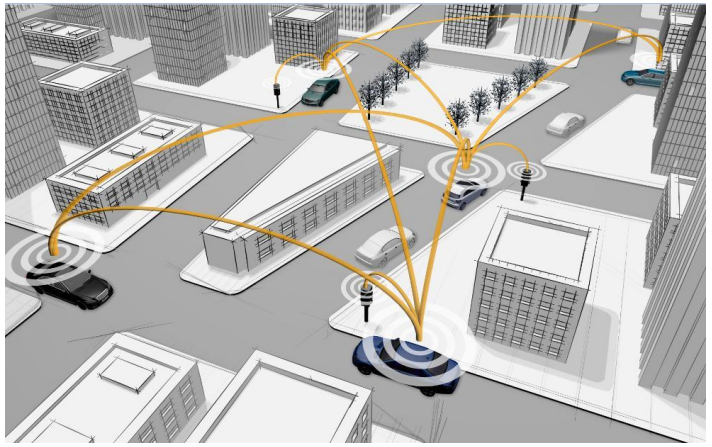
secure connected trustable things

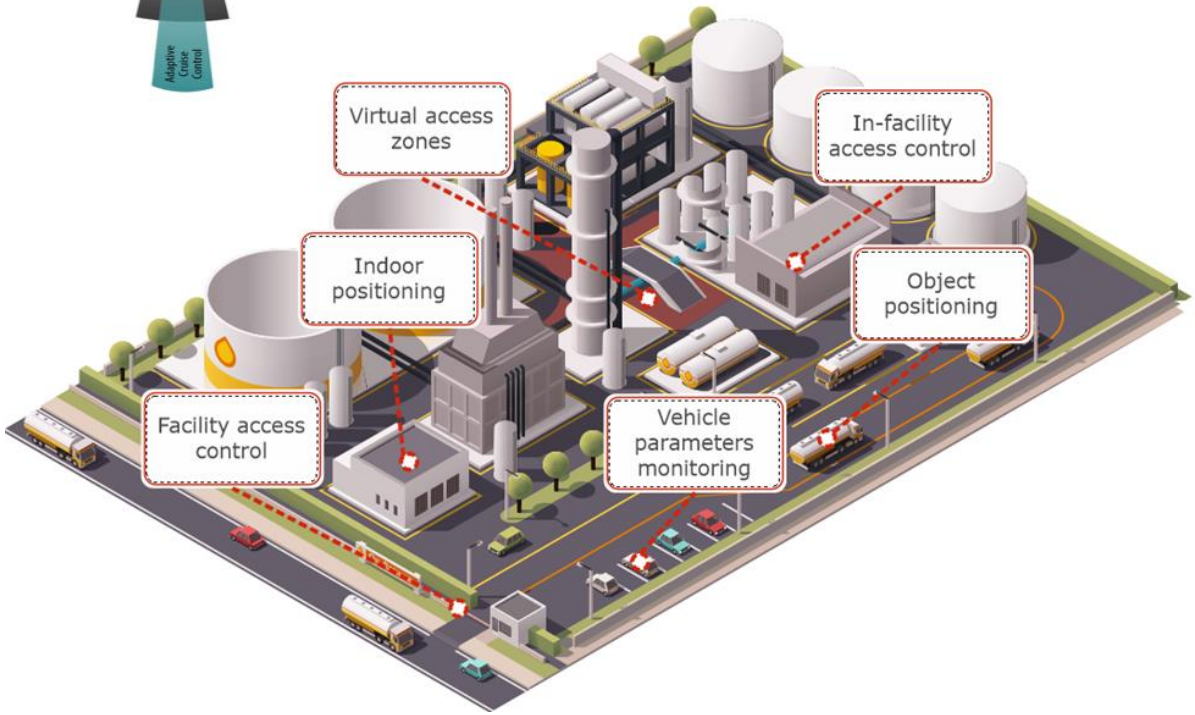
SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

Komunikacja pomiędzy pojazdami a inteligentną infrastrukturą (ang. Vehicle-as-a-sensor within Smart Infrastructure)

- Po dużych obszarach przemysłowych może poruszać się znaczna liczba pojazdów
- Bezpieczna komunikacja pomiędzy infrastrukturą a pojazdami (V2X – Vehicle-to-Everything):
  - Zbierać dodatkowe informacje o otoczeniu/obszarze w celu poprawienia procesów decyzyjnych i redukcji ryzyka
  - Poprawić bezpieczeństwo ruchu (m.in. poprzez monitorowanie zachowania pojazdów)
  - Zoptymalizować i zautomatyzować procesy produkcyjne (np. związane z wyznaczaniem tras czy dostępem do miejsc parkingowych)
- Planowane miejsca wdrożenia testowego – kampus Politechniki Gdańskiej
- Możliwe są rozszerzenia na potrzeby branży morskiej/portowej (pojazdy i infrastruktura)

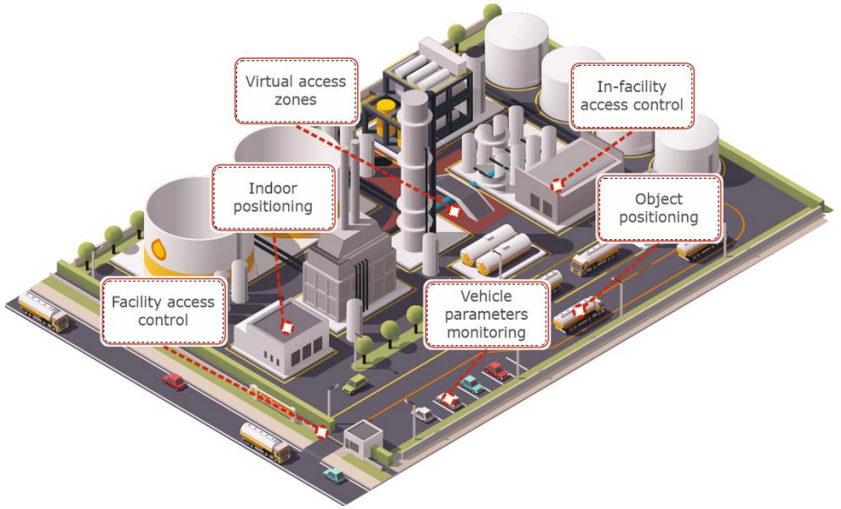




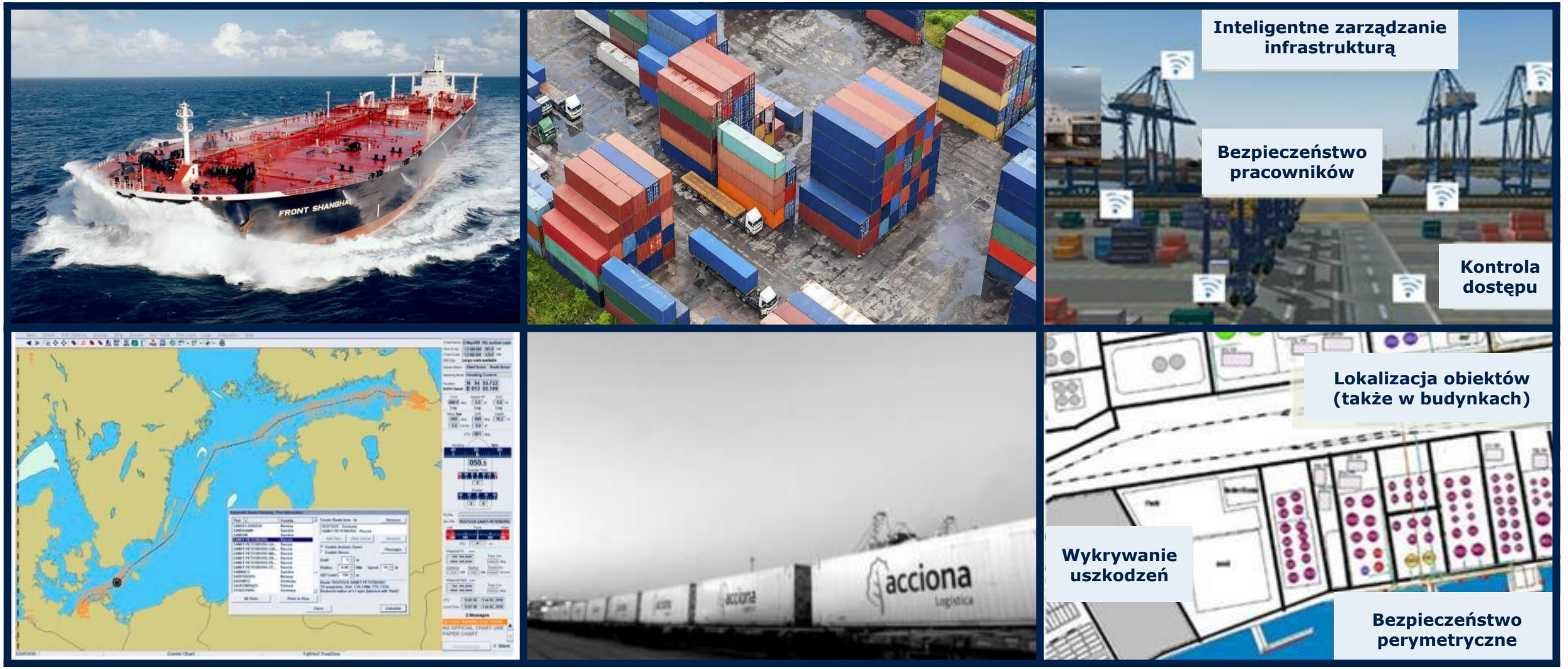


Zarządzanie inteligentną infrastrukturą opartą o bezpieczne IoT (ang. Secure Connected Facility Management)

- System zarządzania dużym obszarem przemysłowym
  - Detekcja, identyfikacja i lokalizacja obiektów (samochody, narzędzia, wyposażenie, itp.) oraz osób
  - Automatyczne wykrywanie zachowań niepożądanych/zagrożeń
  - Możliwość wydzielania wirtualnych stref i określania reguł (np. dla dostępu do stref i obiektów w strefach)
  - Praca w czasie rzeczywistym
  - System do pracy w trudnych warunkach przemysłowych (dużo metalowych elementów)
  - System dedykowany infrastrukturze krytycznej
- Planowane miejsca wdrożeń testowych:
  - Inteligentny budynek – TYCO (Cork, Irlandia)
  - Inteligentna infrastruktura – firma petrochemiczna (Polska)
  - Miejsce testowania technologii – kampus PG, (Gdańsk Polska)



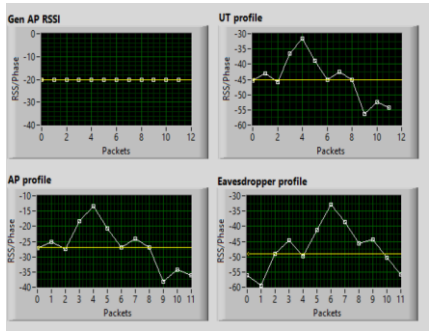
Zabezpieczanie ładunków w transporcie intermodalnym (ang. Cargo Security in Intermodal Transportation)

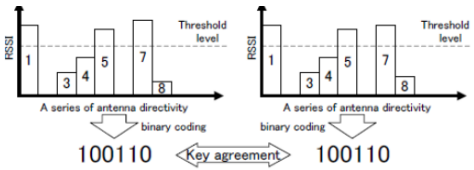


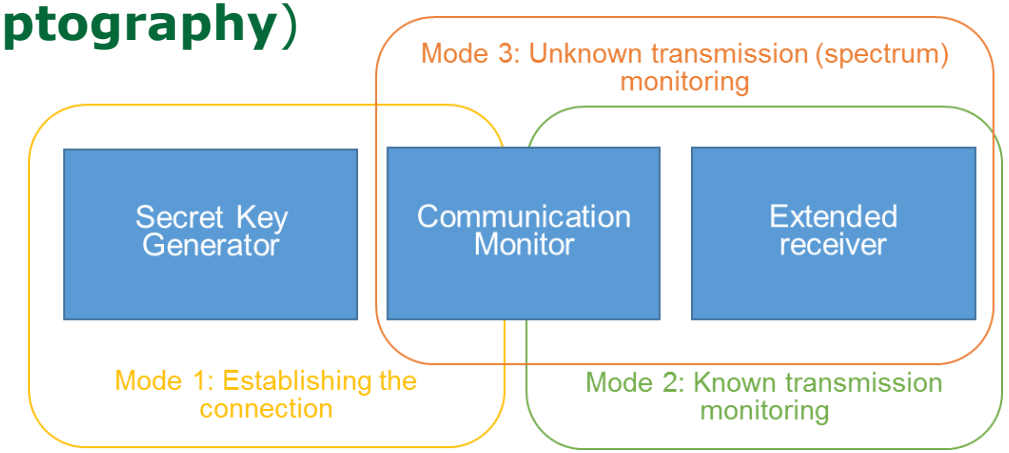
Zabezpieczanie komunikacji w przemysłowych rozwiązaniach IoT (ang. Industrial IoT Communication Security)

- W obszarach przemysłowych istnieje wiele źródeł zakłóceń elektromagnetycznych
- Systemy infrastruktury przemysłowej, a zwłaszcza infrastruktury krytycznej mogą stać się celem (cyber)ataków typu jamming lub spoofing
- Rozwiązania IoT dla zastosowań przemysłowych (ang. Industrial IoT) muszą wykazywać się zwiększona odpornością na zakłócenia i potencjalne ataki

1. Ekstrakcja kluczy prywatnych z parametrów kanałów komunikacyjnych (**post-quantum cryptography**)

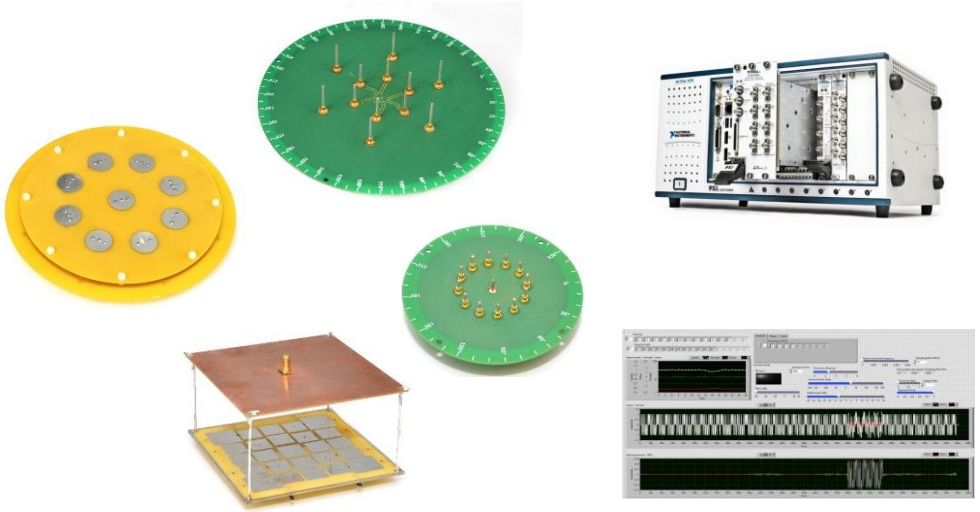






2. Detekcja i klasyfikacja różnych parametrów łączy komunikacyjnych oraz interferencji radiowych

3. Detekcja, identyfikacja i lokalizacja ataków typu jamming oraz aktywne zapobieganie atakom z wykorzystaniem nowej generacji anten inteligentnych

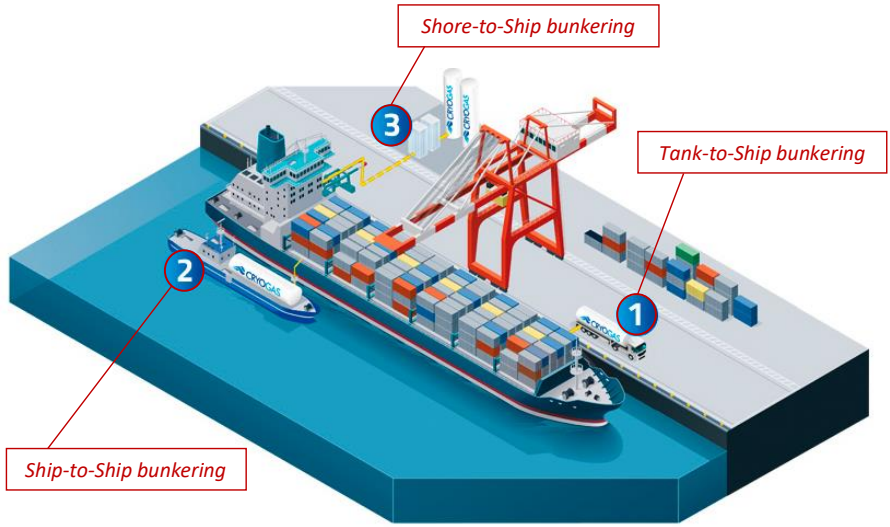


Smart port w oparciu o rozwiązania IoT?

Dziękuję za uwagę!

lukasz.kulas@eti.pg.gda.pl

www.scottproject.eu



An overview of possible LNG bunkering processeses.

secure connected trustable things

SCOTT has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 737422. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Spain, Finland, Ireland, Sweden, Germany, Poland, Portugal, Netherlands, Belgium, Norway.

Katedra Inżynierii Mikrofalowej i Antenowej (1)

- Katedra funkcjonuje jako część Wydziału ETI – nieprzerwanie od 1950 roku
- Obszar działalności Katedry:
  - Elektrodynamika obliczeniowa, CAD, teoria pola,
  - Projektowanie: filtrów, anten, obwodów oraz urządzeń RF
  - Bezprzewodowe systemy wbudowane dla IoT, M2M, RFID, Industry 4.0, …
- Wewnątrz Katedry działają:
  - WiComm Center of Excellence (od 2004 r.) – obszar bezprzewodowych systemów wbudowanych
  - GPU Research Center for Computational Electromagnetics and Photonics (od 2012 r.)
- Skład osobowy KIMiA to:
  - Prof. Michal Mrozowski – Kierownik Katedry/WiComm CoE/GPU RC, członek Polskiej Akademii Nauk, Fellow IEEE, ekspert IEEE
  - 3 profesorów, 5 adiunktów/wykładowców, 6 post-doc-ów,
  - 25 inżynierów (zatrudnionych w projektach B+R)

Katedra Inżynierii Mikrofalowej i Antenowej (2)

- Pracownicy Katedry:
  - Napisali ponad 250 artykułów w czasopismach naukowych z wysokim IF (ang. Impact Factor),
  - Są obecni na najważniejszych sympozjach i konferencjach branżowych,
  - Uzyskali wiele prestiżowych krajowych i międzynarodowych nagród,
  - Opracowali wiele patentów i rozwiązań innowacyjnych – wdrożonych w przemyśle,
  - Są rozpoznawani w Polsce na świecie,
- Projekty realizowane obecnie w Katedrze obejmują:
  - 4 projekty krajowe Narodowego Centrum Nauki (zaawansowane prace naukowe)
  - 1 projekt (EDISOn) ufundowany przez Fundację na rzecz Nauki Polskiej (zaawansowane prace naukowe i komercjalizacja wyników)
  - 5 projektów (ENABLE-S3, SCOTT, Productive 4.0, AFarCloud, SECREDAS) w mechanizmie Horyzont 2020 (tworzenie zaawansowanych technologicznie rozwiązań dla firm UE)
- **Całkowity budżet KIMiA/WiComm 2019-2021 to ok. 4M €**