# A Unified Approach to Cyber-Physical Testing

## Federated Advanced Cyber physical Test range project (FACT)

**Project Coordinator**: **Jon Leistad**

Kongsberg Defence & Aerospace

Co-funded by the European Union

FACT

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them."

# Cyber-Physical Systems of Systems (CPS)

Characteristics of Systems of Systems (SoS), e.g. Smart Cities

- **Cyber-physical Systems**, incl. Automation
- **Autonomy of Subsystems** & System Components
- **Interconnected Subsystems** & Communication, even without human interaction
- **Diverse Goals among Subsystems**, and Collaboration to **Support Overarching Goal**
- **Emergent Behaviors** where the Capability of an SoS are greater than the Sum of its Part
- **Evolutionary Development** where an SoS Evolves over time with Subsystems being added, modified, or removed.

# CPS: Unmanned Vehicle

- **Autonomy & Remote Control**
  - Controlled remotely by human who may adjust actions in real time
  - Operate autonomously using AIML for tasks like navigation, object detection, decision making
- **Sensors & Detection Systems**
  - Cameras for visual navigation
  - Radar/LiDAR of object detection, 3D mapping etc
  - Proximity Sensors for nearby objects
- **Data Processing & AI**
  - Real-time Data Processing & Data fusion
  - Machine Learning for Continuous Improvement
  - Computer Vision of Situational Awareness
- **Communication Systems**
  - GPS & Satellite Communication
  - Radio & Wi-Fi Systems for control and data transmission
  - Telemetry for Monitoring & Diagnostics
- **Power Supply & Energy Efficiency**
  - Battery Powered
  - Alternative Energy Sources
  - Energy Management
- **Safety & Redundancy**
  - Fail-Safe Mechanisms
  - Obstacle Detection & Avoidance
  - Redundancy Systems

# Cyber Resilience for CPS

- Cyber Resilience of Subsystems & System Components
- Cyber Resilience of Integrated & Interconnected System of Systems
- Cyber-physical Resilience in Hazardous & Adverse Environments
- Possible Self-defense
  - Integrated Threat Detection
  - Autonomous Response & Recovery
  - Risk-based / Multi-layers Security Architecture
  - Self-Healing Capabilities, i.e. software patching
  - Redundancy & Robust Backup Systems
  - Threat Prediction & Adaptive Security
  - Physical Security & Hardware Security
  - Environmental Awareness

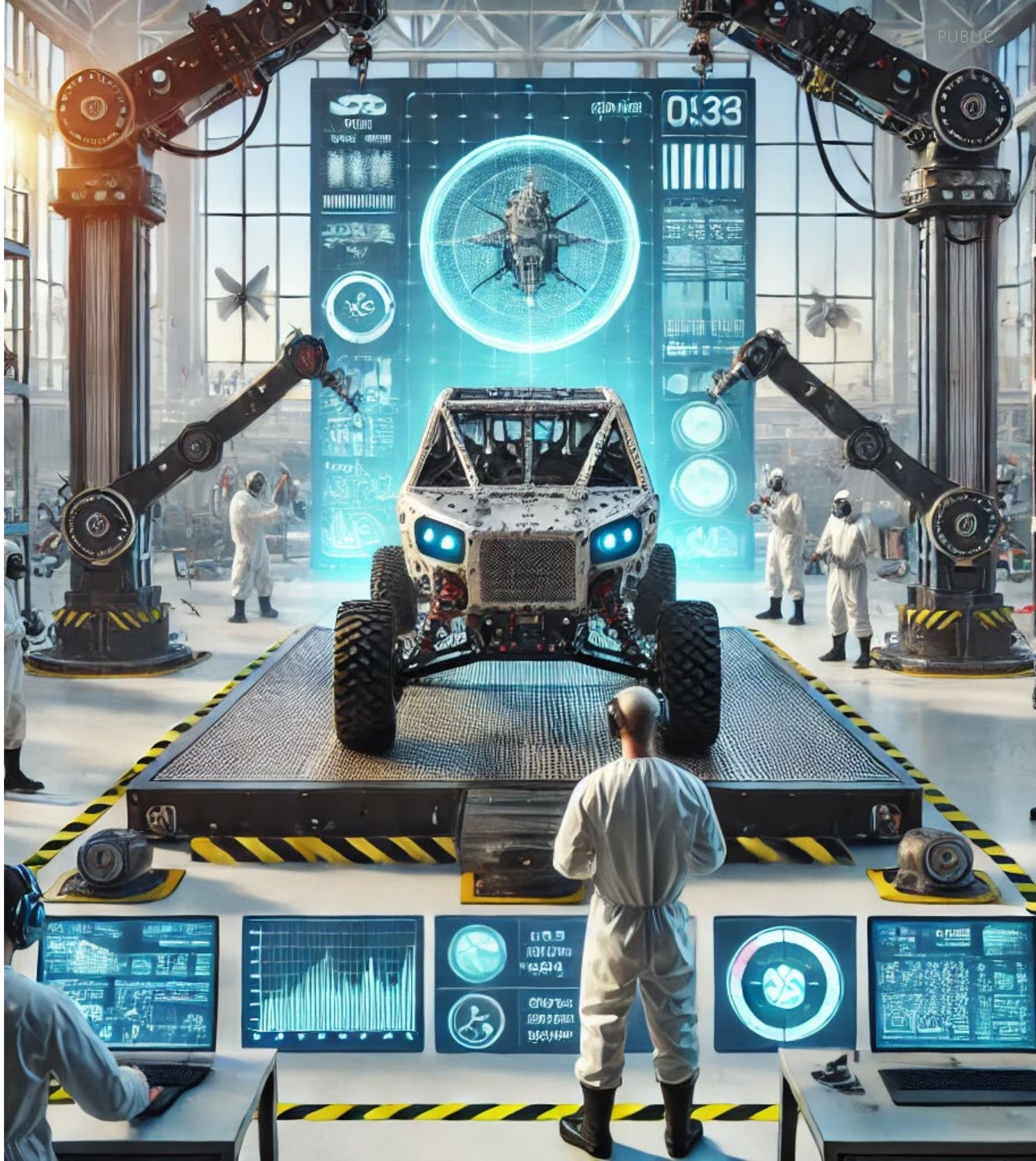
- Related EU Act & Directives
  - EU Cyber Resilience Act
  - EU Cybersecurity Certification framework
  - NIS2, and the EU Cyber Defence Policy.

# Cyber-Physical Testing

- Complex Cyber-physical Systems of Systems demand:
  - Prioritize & Mitigate Sub systems
  - Integration and End-to-end Testing

- Cyber-physical Test Range (CPTR)
  - Federated CPTR with Hardware & Software-based tools
  - Hybrid CPTR combined local & distributed components
  - Environment generates traffic, emulation & simulation in the network
  - Red team attacks CPS(s) dynamically, using AI/ML for ethical hacking
  - Blue team attacks CPS(s) dynamically, using AI/ML for cyber defense
  - Installed systems (OT) are subject to attack and are defended using hybrid intelligence
  - IT-system infrastructure are subject to attack and are defended
  - Federated service orchestration, and cyber-physical test-result aggregation using AI/ML

https://tinyurl.com/EDF-FACT-FactSheet



# What matters most?

- Assure **Cyber-Resilience** of equipment used
- Equipment is an arbitrary **Cyber-physical System**(-of-Systems)
- Perform **Cyber-Physical TESTING** *(semi-)automatic & manual*
- Overall **Testing Process** to validate cyber resilience
  - Testing Application (Purpose)
  - Testing Tools
  - Testing Methods
- Enabling **Federated** Testing

# FACT: A Solution through European Collaboration

The solutions lies in:

- A common European federated framework for cyber testing
- A common architecture
- A shared tool set for testing

Related PESCO Project:

- Cyber Threats and Incident Response Information Sharing Platform (CTIRISP)

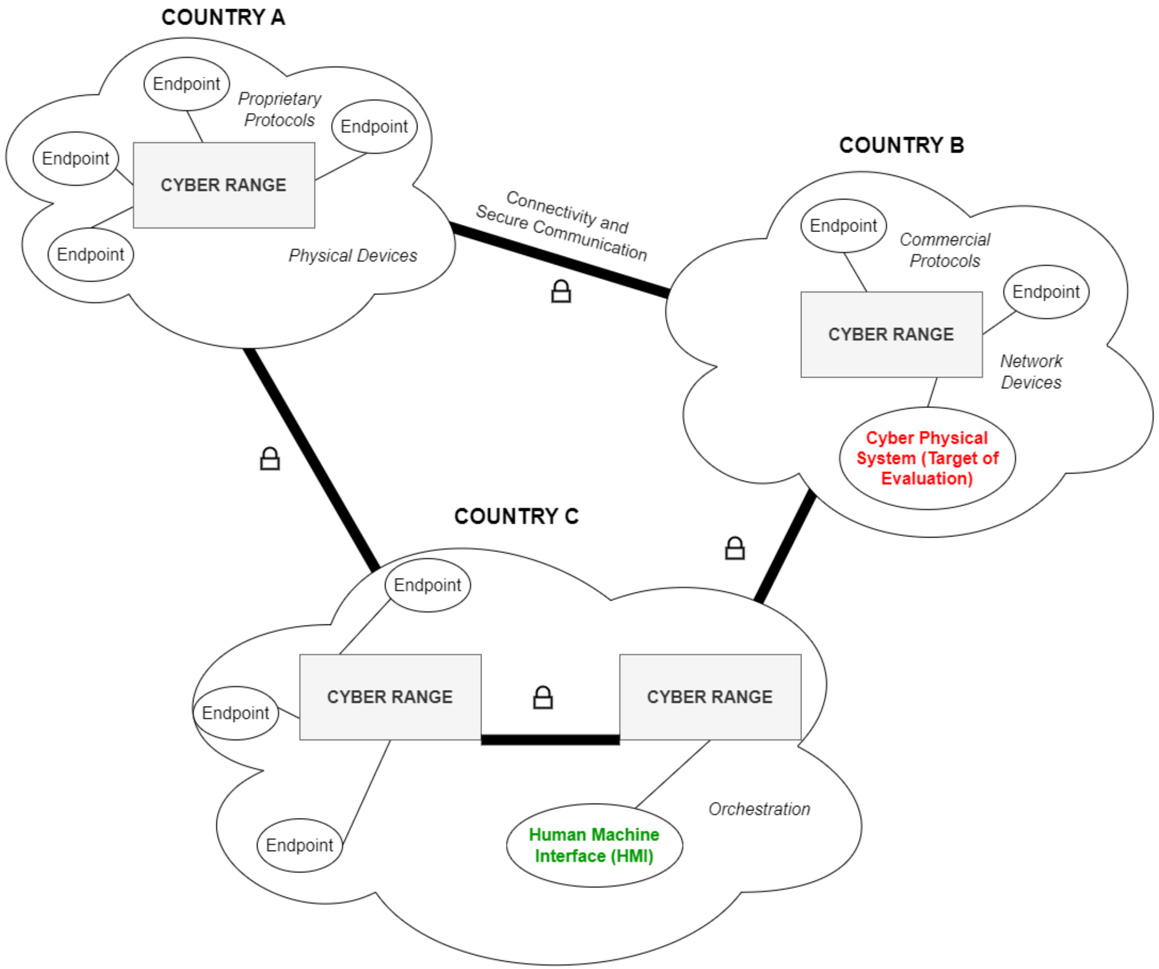
- Integrate “hardware-in-the-loop” approaches and test (including reverse-engineering) platforms and systems in very comprehensive conditions
- Increase the overall level of cyber-resilience of platforms and systems while fostering interoperability.
- a significant improvement, given the high number of platforms and systems in service with EU and Norway

*End User Conference, Oslo, March 2024*

FACT

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY
APPROACH CYBER
BPTI BALTIJOS PAŽANGIŲ TECHNOLOGIJŲ INSTITUTAS
bianor
C&V CONSULTING
certSIGN
crosshill SECURING EMBEDDED SYSTEMS
emproof embedded security
CR14
KONGSBERG
LEONARDO
lmt
NOKIA
NTNU Norwegian University of Science and Technology
RHEINMETALL
SPACE
TERMA
THALES
Università di Genova

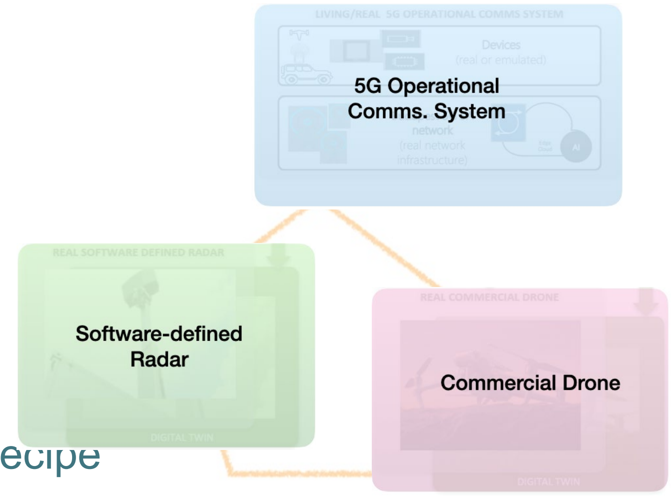
The Federated Advanced Cyber physical Test range (FACT) project will provide an unprecedented new European capability to test and verify the cyber vulnerability of equipment.


COUNTRY A
Endpoint
Proprietary Protocols
Endpoint
Endpoint
CYBER RANGE
Endpoint
Physical Devices
Connectivity and Secure Communication
COUNTRY B
Endpoint
Commercial Protocols
Endpoint
CYBER RANGE
Network Devices
Cyber Physical System (Target of Evaluation)
COUNTRY C
Endpoint
CYBER RANGE
CYBER RANGE
Endpoint
Endpoint
Human Machine Interface (HMI)
Orchestration

# FACT Deliverable & Demonstration

**Project Outcomes**

- Federated Test Range
- Adaptive on Demand
- Open API & Expandable
- Cyber Physical Testing
- Real-world Scenarios



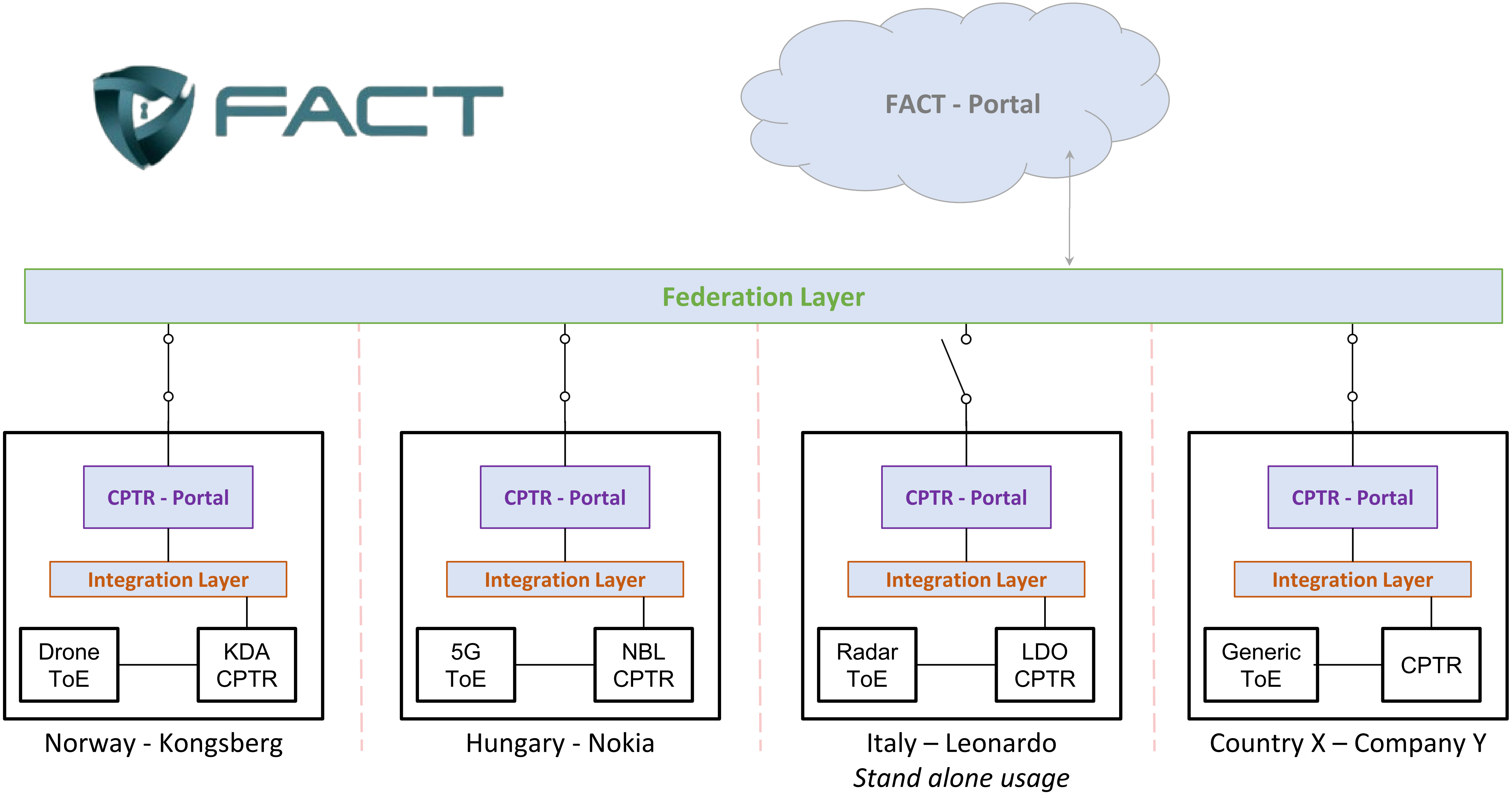
**FACT Blue print *(theory)*** - the cooking recipe

- Perform integrated cyber-resilience testing
- Design  the cyber-physical test range (military grade)
- Facilitate continuous update & extend testing

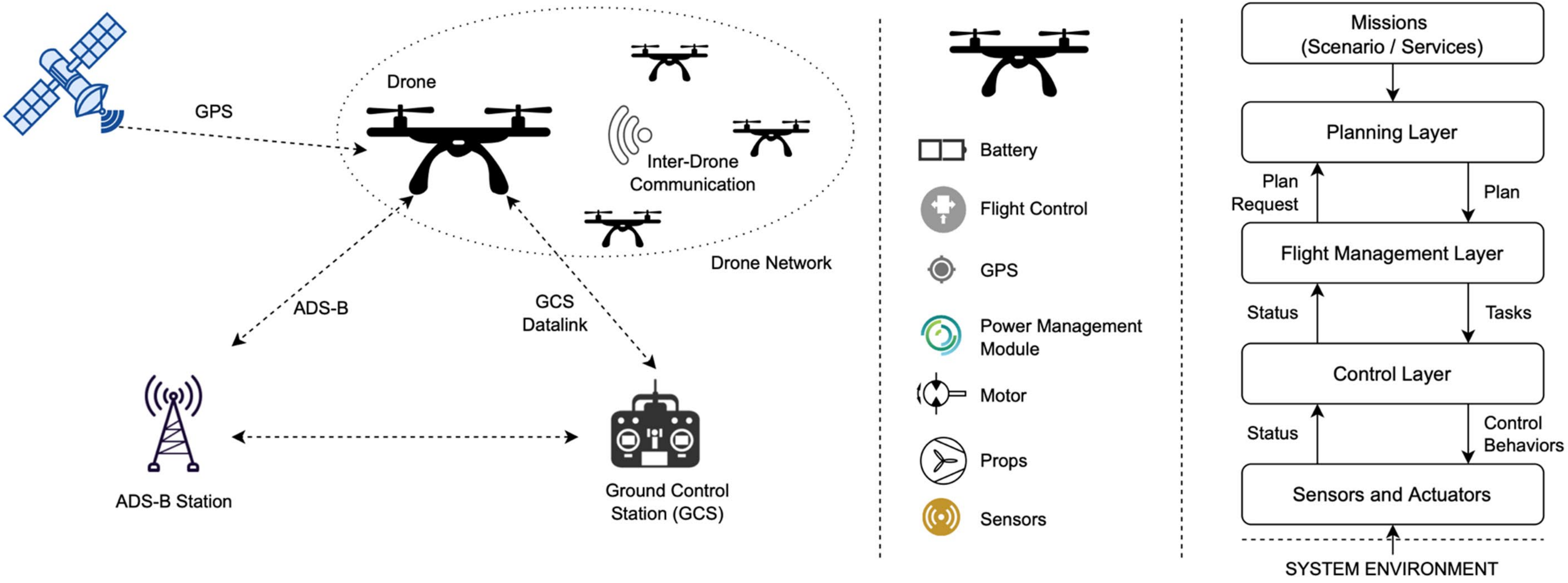
**Demonstrate the Testing *(practice)*** - three specific use cases

- Selected cyber-resilient testing
- Limit capability of the test infrastructure
- Technology-readiness level 6-8

Created with mapchart.net


FACT - Portal
Federation Layer
CPTR - Portal
Integration Layer
Drone ToE
KDA CPTR
Norway - Kongsberg
CPTR - Portal
Integration Layer
5G ToE
NBL CPTR
Hungary - Nokia
CPTR - Portal
Integration Layer
Radar ToE
LDO CPTR
Italy – Leonardo
*Stand alone usage*
CPTR - Portal
Integration Layer
Generic ToE
CPTR
Country X – Company Y

# Demonstration Use-Case: Drone



GPS

Drone

Inter-Drone Communication

Drone Network

ADS-B

GCS Datalink

ADS-B Station

Ground Control Station (GCS)

Battery

Flight Control

GPS

Power Management Module

Motor

Props

Sensors

Missions (Scenario / Services)

Planning Layer

Plan Request

Plan

Flight Management Layer

Status

Tasks

Control Layer

Status

Control Behaviors

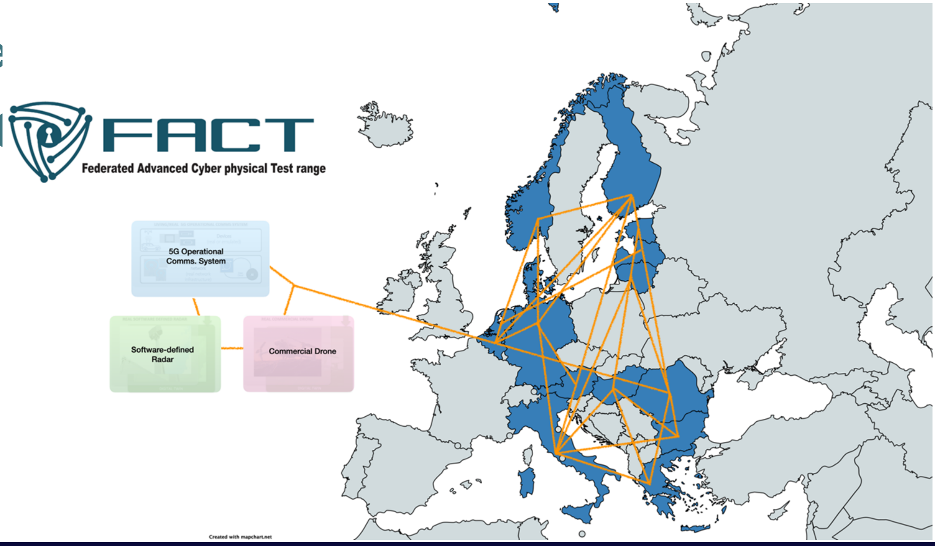
Sensors and Actuators

SYSTEM ENVIRONMENT

# Security Objectives

- Strategic Objective (overall) for Federated CPTR capability:
    - Advanced security resilience testing of Target of Evaluation (ToE) Cyber Physical Systems (CPS) – both military (and commercial)

- Security Objectives (overall) for Federated CPTR capability:
    - high level of security and trust - and be resilient against Cybe
    - able to handle and protect Information about ToE with discret and according to ToE System Owner security policy
    - able to handle and protect Classified Information (e.g. EUCI) military grade ToEs
    - comply with relevant Security Laws and Regulations


FACT
Federated Advanced Cyber physical Test range
5G Operational Comms. System
Software-defined Radar
Commercial Drone
Created with mapchart.net

# CPS Testing in NO

- FACT born in the SFI NORCICS realm
- Cooperation between KDA & NTNU
- CPS testing demanded everywhere

- Nordic Model of cooperation
- Cooperation & sharing across critical sectors
- Towards Norwegian Total Defence Approach

- From NORCICS to Europe & back again

# Contact information

## Project Coordinator

Jon Leistad
jon.leistad@kongsberg.com

## Technical Manager

Prof. Katrin Franke
katrin.franke@kongsberg.com

Co-funded by the European Union

Co-funded by the European Union under GA no. 101121335. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

FACT