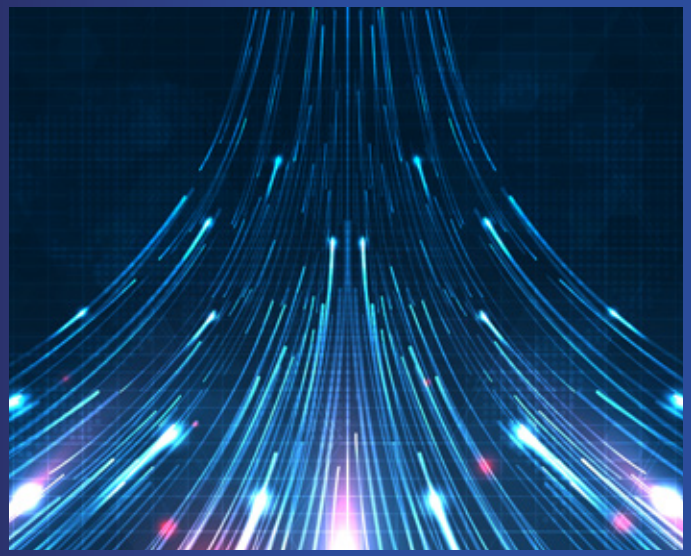
TrustEvaluation and IoT Management demo

WINGS ICT SOLUTIONS

The demo showcases how the **Trust Manager evaluates IoT devices in real time using trust metrics, updating each device's trust index dynamically.** Based on these values and resource availability, the Trust Manager Orchestrator assigns tasks to the most reliable and capable devices, ensuring secure and efficient operation.

CORE NEXT

The Trust Evaluation Function calculates a trust score (0 to 1) for each device class by normalising key metrics, applying weights based on importance, and adjusting for data age using exponential decay. This ensures recent data has greater influence, with the final score derived from a weighted average of the adjusted metrics.



EXPECTED RESULTS

- Calculated trust scores of devices
- A graph of trustworthiness vs number of tasks/workloads
- Evaluation of the execution time

WORKING TOWARDS END-TO-END TRUSTWORTHINESS

COREnext believes that trustworthiness needs to be a native part of 6G as anticipated applications will merge the digital and physical worlds.

The goal of the project is to strengthen the mobile communication ecosystem in Europe by addressing key challenges associated with beyond 5G use cases.

Activities stretch from radio hardware innovation to compute architectures – with trustworthiness in focus.

corenext.eu

@COREnext_EU

COREnext

COREnext project

@corenext.bsky.social

JOIN US

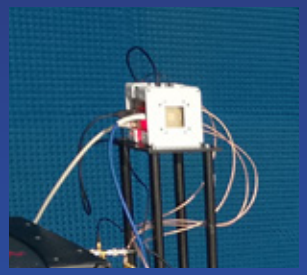
Funded by the European Union

European core technologies for the next generation communication-computing hardware

CORE NEXT

Eavesdropper avoidance

imec



This sub-THz demonstrator showcases **how beam-steering technology can be used to enhance link security.**
The system focuses on preventing eavesdropping by dynamically controlling signal direction. It offers an interactive experience for users to engage directly with the beam-steering process.

The system integrates MATLAB baseband signal processing with analogue beam-steering transceivers, featuring four independent RF front-ends and antennas for real-time beam control. An interactive interface enables live visual monitoring and operation.

Beam-steering at sub-THz frequencies enhances link security by lowering interception risks. Real-time user interaction demonstrates practical beam control, improving public understanding of physical-layer security and offering a scalable solution for future high-frequency wireless networks.

The demo shows how real-time beam-steering at sub-THz frequencies enhances link security, offering hands-on insight into practical physical-layer cybersecurity for future networks.

RF Fingerprint for Wireless Network Security

ERICSSON

The Radio Fingerprint demonstrator offers an interactive look at **how AI can use subtle hardware impairments in radio devices to enhance cellular communication security.** By learning these unique signatures, machine learning models can identify authorised transmitters and detect unauthorised access attempts.

The demo uses machine learning models trained on transmitter non-idealities to classify radio devices in real time. It employs real hardware to transmit authentication signals and identifies authorised devices based on physical signal characteristics, without decoding the data.

The system enables device identification using hardware-specific features, without cryptographic keys. It lowers the risk of unauthorised access from devices with identical chipsets and provides a low-complexity, efficient method to enhance physical-layer security.

The demonstration introduces RF fingerprinting and shows how machine learning can authenticate radio devices securely and efficiently. It highlights how physical-layer security can complement traditional cryptography to strengthen wireless network trustworthiness.

Secure Acceleration (FPGA)

NOKIA

The Secure Acceleration demonstrator showcases **FPGA-based hardware acceleration for improved digital platform efficiency.**
It allows multiple tenants to securely share resources, using cryptographic components and key exchange protocols to protect sensitive data, such as health information, during processing.

The FPGA acceleration board supports secure multi-tenant resource sharing, featuring cryptographic modules and secure key exchange protocols. It enables real-time, privacy-preserving data processing in sensitive areas such as healthcare.

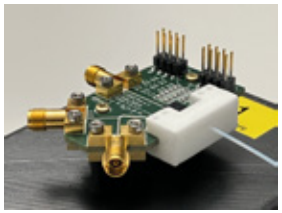
The demonstrator enables efficient and secure hardware acceleration for multiple users or applications, ensuring data confidentiality with robust cryptographic protection. It illustrates scalable, secure resource management for future digital infrastructures.

The goal of the demonstration is to show how sensitive data can be securely processed within shared hardware environments.
It highlights a crucial advancement towards secure, efficient computing for digital platforms requiring hardware acceleration in multi-tenant, high-security contexts.

High datarate interconnects over plastic fiber

Infineon

This demo is based on the concept of **high speed data link for communication via PMF in the H-Band, and PMF coupler in package at H-Band.**



- MMICs in eWLB package, assembled on PCB
- H-band PMF coupler realized in package
- H-band PMF fiber and holder

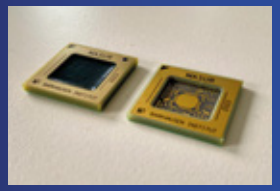
This is the first in-package PMF coupler demonstrated in the H-Band, offering a compact, low-loss, and cost-effective solution for high-speed data links. It enables faster communication with reduced energy consumption, supporting future applications such as next-generation data centres.

The goal of the demonstration is to prove the concept of communication via PMF in H-Band.

Trustworthy Computer Platform M³

barkhausen institut

M³, developed at Barkhausen Institut, is a **modular and secure operating system built on a tiled hardware architecture.** Each component runs on a separate, isolated tile, following a **security-by-design** approach that limits the impact of potential compromises. This architecture enhances containment of untrusted software and hardware, strengthening trust in connected systems.



The platform provides hardware-level isolation between processing components in heterogeneous systems, enabling secure execution environments that mitigate hardware-induced vulnerabilities. Its adaptable architecture supports diverse, multi-vendor system configurations.

The architecture enhances system resilience by containing faults within individual hardware modules and reducing the risk of system-wide compromise through trusted execution zones. It supports secure, scalable design essential for future digital infrastructure.

The objective of this demonstration is to illustrate how hardware isolation strengthens the trustworthiness of complex digital systems. The M³ platform demonstrates a practical method for securing next-generation platforms by compartmentalising potential risks at the hardware level.