Integrating Network Digital Twin into Future AI-based 6G Systems (6G-TWIN)

ETSI Security Conference 2024,
14-17 October, Sophia-Antipolis, France

6g-twin.eu | @6Gtwin | 6G-TWIN

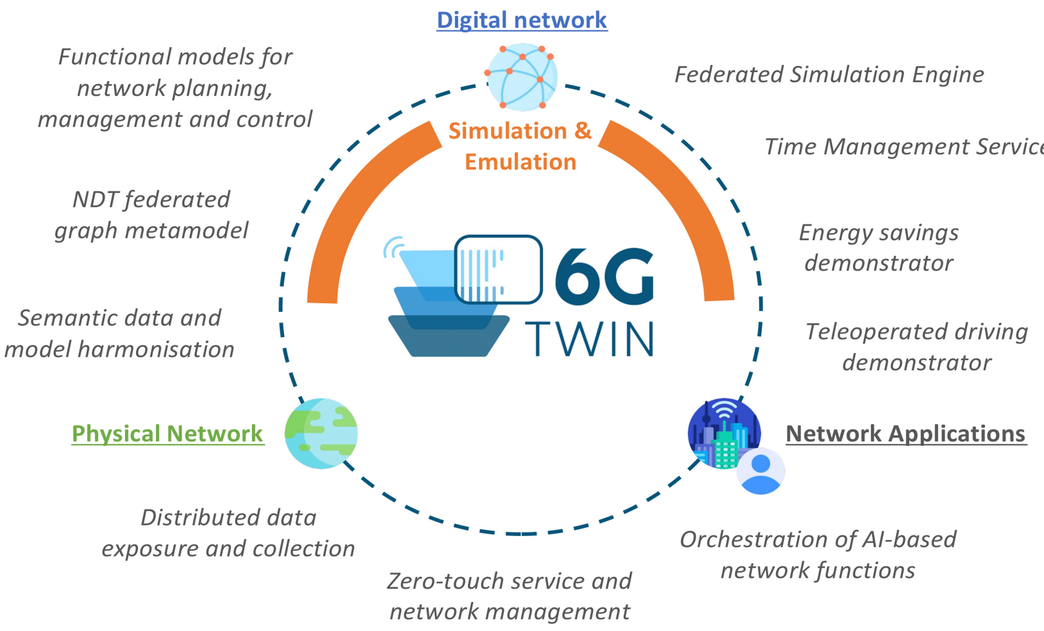
Co-funded by the European Union

Concept and objectives

Networks are becoming increasingly complex and distributed, requiring a large variety of technologies to operate. With 6G, which is now on the horizon for around 2030, it is essential to design, experiment and standardize new network architectures with more intelligence and automation.

6G-TWIN will provide the foundation for the design, implementation and validation of an **AI-native reference architecture** for 6G systems that incorporates **Network Digital Twins (NDT)** as a core mechanism for the end-to-end, real-time optimisation, management and control of highly dynamic and complex network scenarios.

Enabling a Cyber-Physical Continuum for Next-Generation 6G Systems

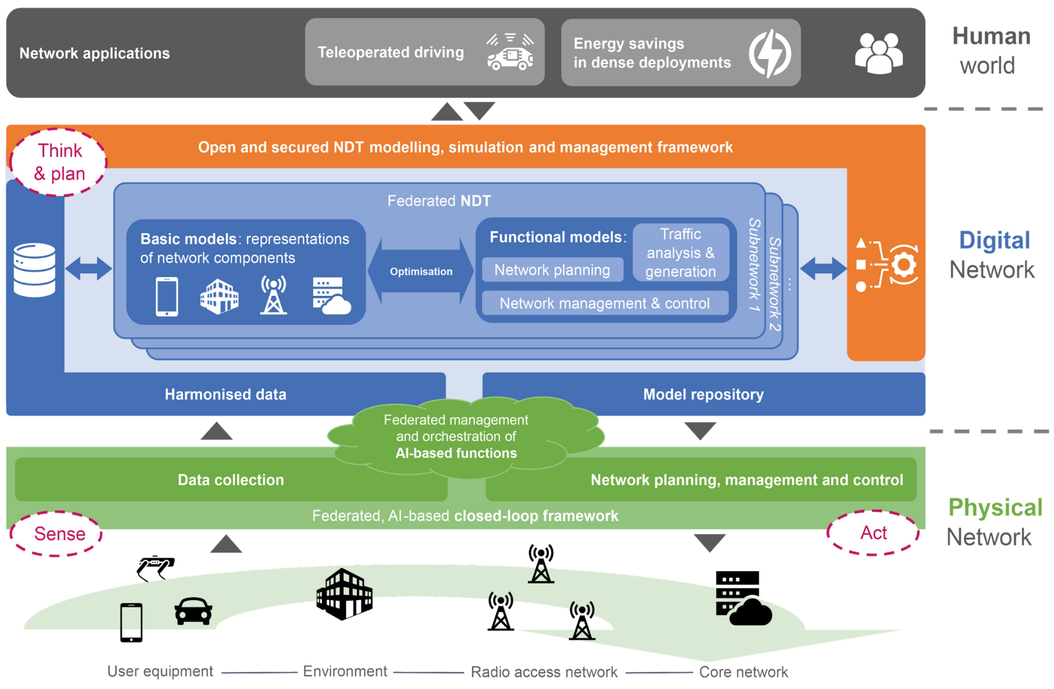


6G-TWIN will achieve its objectives through the integration of 10 technology components (TCs) over 4 dimensions.

Key expected results include a **Federated and AI-native network reference architecture that integrates multiple NDTs** for real-time data analytics and decision-making.

Creating a real-time digital replica of the physical network infrastructure (i.e., NDT) involves establishing a sandbox where models can be trained and various scenarios can be tested before deploying them on physical network controllers. While NDT can enhance the reliability of the system, integrating such tools into the network may lead to several breaches concerning data privacy and security:

- **Harmonization** As data is collected from heterogeneous networks with varying requirements related to data privacy, it must be harmonized prior to deployment via NDT to ensure compliance and consistency.
- **Adversarial Data** Data sourced from various vectors may contain poisoning elements that could undermine the integrity of AI/ML models trained within the NDT environment.
- **Threats to Data Privacy** The integration of NDT creates potential vulnerabilities, such as unauthorized access or data breaches, that can expose sensitive information. The dynamic nature of real-time data processing increases the risk of data interception and misuse, necessitating robust security measures to safeguard against these threats.
- **Regulatory Compliance** With respect to GDPR and U.S. data privacy regulations, including the California Consumer Privacy Act (CCPA), these concerns must be taken into serious consideration to mitigate risks and ensure compliance.



Demonstrators

Requirements analysis and architectural design

Threat landscape w.r.t data security & privacy

Identify potential threats for key components

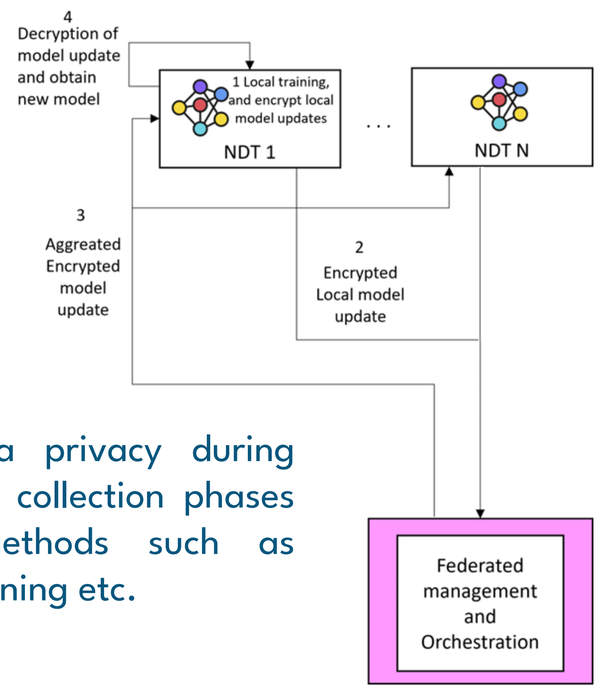
- Data collection and management
- Data exposure
- In distributed scenario

Requirements for ensuring data privacy & security

- Confidentiality, Integrity and Privacy

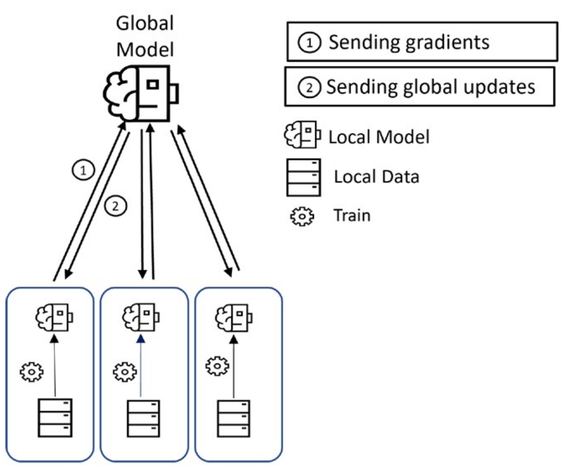
Secured, scalable and distributed data exposure and collection for network monitoring

- Data validation against attack such as data poisoning



- Ensuring data privacy during exposure and collection phases by using methods such as federated learning etc.

Federated management and orchestration of AI-based network functions and services



- Investigation of how federated learning can be used in federated management, by considering potential privacy and security requirements.

Partners

This work was supported by:
- the 6G-TWIN project which has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation program and Grant Agreement No 101136314.
- the Scientific and Technological Research Council of Turkey (TUBITAK) through the 1515 Frontier Research and Development Laboratories Support Program under Project 5169902

Contacts: Régis Decorme, R2M Solution, regis.decorme@r2msolution.com | Ayse Sayin, Ericsson, ayse.sayin@ericsson.com | Ramin Fuladi, Ericsson, ramin.fuladi@ericsson.com