CELTIC-NEXT
∑eureka Cluster

Project Information

CYPRESS

Project ID: C2023/1-13

Start Date: 1 May 2024

Closure date: 30 April 2027

Partners:

Airbus Defence and Space Oy, Finland

Applio Tech AB, Sweden

Centria University of Applied Sciences Ltd, Finland

Elliot Cloud S.L., Spain

Ericsson AB, Sweden

Gebwell Oy, Finland

RISE Research Institutes of Sweden AB, Sweden

Sensative AB, Sweden

Co-ordinator:

Katarina Boustedt

RISE Research Institutes of Sweden AB

E-mail: katarina.boustedt@ri.se

Project Websites

www.celticnext.eu/project-cypress

https://www.celtic-cypress.eu/

Cyber-Physical Resilient and Secure Systems

The CYPRESS project focuses on developing advanced cybersecurity solutions for Cyber-Physical Systems (CPS) used in critical infrastructure, smart cities and smart buildings, and emergency networks. It aims to create lightweight, scalable protocols and methods for secure communication, fine-grained access control, key management, edge computing, and intrusion detection, by leveraging standards like CoAP, OSCORE, EDHOC, and ACE-OAuth. The project also emphasises AI-driven anomaly detection, adaptive defences against adversarial attacks, and machine learning techniques for IoT security. Additionally, it develops solutions for secure device management, automated onboarding, and trusted software updates. By promoting open standards and interoperability, CYPRESS enhances the resilience and commercial viability of CPS, ensuring strong authentication, privacy, and robust protection across network layers.

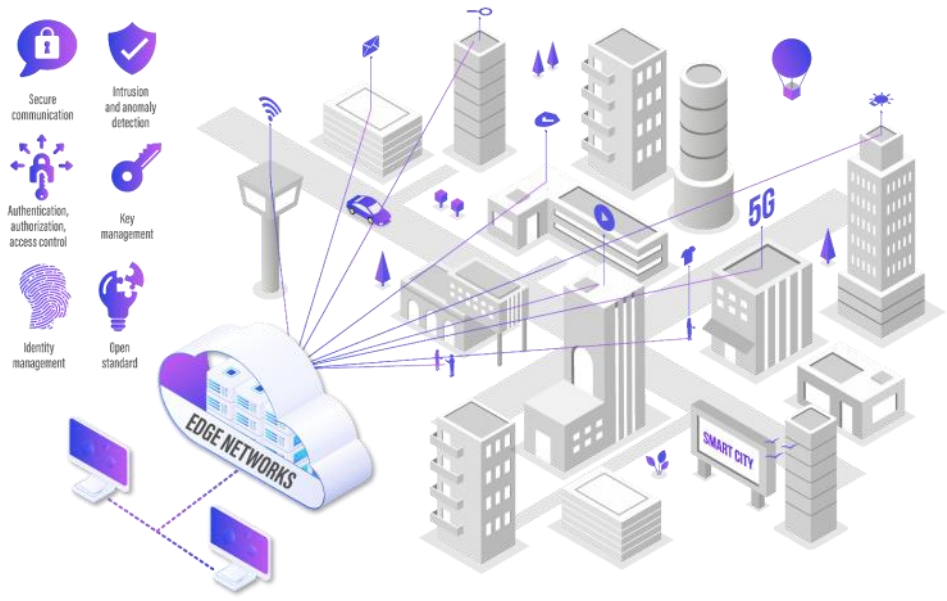
Main focus

The primary objective of the CYPRESS project is to develop innovative cybersecurity solutions for cyber-physical systems (CPS) that are both effective and lightweight, and feasible to run on resource-constrained devices. Cybersecurity solutions will focus on protocols and methods for ensuring both network and communication security, as well as for enabling the effective and efficient security management and security-driven development of CPS-based applications and services. The developed cybersecurity solutions constitute substantial input and contribution to standardisation activities, especially in the premier international body, the Internet Engineering Task Force (IETF).

Approach

The CYPRESS project focuses on developing advanced cybersecurity solutions for Cyber-Physical Systems (CPS), targeting critical domains such as energy production, smart cities, automated device management, 5G/satellite-based communications for Public Protection and Disaster Relief (PPDR), and environmental monitoring. The project will define detailed use cases and requirements to guide the design of modular, interoperable solutions that address specific functional and security needs.

Security solutions will be validated through



proof-of-concept software and integrated into demonstrators, paving the way for commercialisation by industrial partners. Key contributions will also support standardisation efforts, particularly within the Internet Engineering Task Force (IETF).

The work in CYPRESS includes project management, progress tracking, and partner coordination; identification of use cases, requirements, and technical challenges, establishing reusable workflows, APIs, and data formats; secure communication, intrusion detection, and edge computing, developing techniques such as end-to-end communication security, federated learning, anomaly detection, and secure routing in dynamic mesh networks; lifecycle security management, including key provisioning, access control, device enrolment, software/firmware updates, and privacy-preserving techniques; integrated demonstrators for each use case, validating cross-partner technologies in operational scenarios; and dissemination, standardisation, and exploitation, ensuring that results contribute to international standards (e.g., in the IETF) and supporting commercialisation through business models and IPR strategies.

Together, these efforts aim to deliver scalable, lightweight, secure, and standardised cybersecurity solutions for CPS that are widely applicable and ready for real-world deployment.

Main results

The CYPRESS project aims to enhance the security and resilience of Cyber-Physical Systems (CPS), particularly in critical infrastructure, smart environments and emergency networks, through the development of novel, lightweight, and standardised cybersecurity solutions. These include protocols for secure communication, access control and key management that build on standards such as CoAP, OSCORE, EDHOC and ACE-OAuth; intrusion and anomaly detection powered by AI; and secure edge computing architectures with multichannel routing and zero-knowledge-based approaches. Emphasis is placed on end-to-end security, including post-quantum adaptations, dynamic and fine-grained access control, secure device onboarding, and automated software updates. CYPRESS also targets secure identity and credential management across distributed systems. The project integrates these solutions into real-world use cases—such as energy production/distribution, smart cities and smart buildings, network device enrolment, public protection, and environmental monitoring—through proof-of-concept implementations and demonstrators. Standardisation plays a central role, with contributions largely directed toward the IETF to ensure interoperability and facilitate wide adoption. By promoting open, modular, and scalable security solutions and architectures, CYPRESS will reduce operational costs, improve system robustness, and accelerate market deployment of secure CPS-based services and applications.

Impact

The CYPRESS project focuses on developing standardised security solutions for Cyber-Physical Systems (CPS) to enhance trust, interoperability, and speed up commercialisation. Key deliverables include product versions of the Yggio IoT platform and the Applio Sense Platform, improved Edge Computing Security Modules (ECSM), multichannel router technology, and advanced cryptosystems. By promoting open standards, the project enables vendor interoperability, reduces development and operational costs, and simplifies system integration and maintenance. A common security framework also supports easier competence building and faster innovation. Collaboration among diverse partners ensures effective design, implementation, and demonstration of these solutions during the project. It also helps identify optimal integration methods and encourages broad industry and research consensus on new security protocols. This cooperation is expected to lead to widely accepted standards, increased market adoption, and long-term sustainability of solutions for secure CPS. Ultimately, CYPRESS aims to create a robust security ecosystem that fosters user trust and commercial success.

About CELTIC-NEXT

CELTIC-NEXT is the EUREKA Cluster for next-generation communications enabling the digital society. CELTIC-NEXT stimulates and orchestrates international collaborative projects in the Information and Communications Technology (ICT) domain.

The CELTIC-NEXT programme includes a wide scope of ICT topics based on new high-performance communications networks supporting data-rich applications and advanced services, both in the ICT sector and across all vertical sectors.

CELTIC-NEXT is an industry-driven initiative, involving all the major ICT industry players as well as many SMEs, service providers, and research institutions. The CELTIC-NEXT activities are open to all organisations that share the CELTIC-NEXT vision of an inclusive digital society and are willing to collaborate to their own benefit, aligned with their national priorities, to advance the development and uptake of advanced ICT solutions.

CELTIC Office

c/o Eurescom, Wieblinger Weg 19/4
69123 Heidelberg, Germany
Phone: +49 6221 989 0
E-mail: office@celticnext.eu
www.celticnext.eu

eureka