

AlticeLabs@UA – Innovation areas

1. Advanced Connectivity

Scope and focus

Advanced Connectivity focuses on the evolution of next-generation communication networks and infrastructures that enable high-capacity, low-latency and resilient digital services. This domain addresses the transformation and convergence of fixed, mobile, optical and satellite networks into unified, software-driven connectivity platforms. The scope extends beyond individual access technologies to include end-to-end architectures, network programmability and service orchestration.

Key research directions

- Evolution towards 5G Advanced and 6G architectures, including new spectrum usage, radio technologies and small/pico cell deployments;
- Optical access and transport networks (e.g. PON evolution, ultra-broadband optical systems);
- Fixed–mobile convergence, including Fixed Wireless Access (FWA), and multi-access integration;
- Network programmability, slicing, and exposure through open APIs
- Non-terrestrial networks, including satellite and hybrid connectivity scenarios;
- Deterministic, low-latency and high-availability networking for critical use cases;
- Application of AI for network optimization, automation and management.

2. AI-Driven Autonomous Systems

Scope and focus

AI-Driven Autonomous Systems explores AI as a transversal capability embedded into systems, networks and organizational processes, with the goal of enabling higher levels of automation, intelligence and autonomy. AI is treated as a foundational enabler for decision-making, optimization and adaptive behavior across complex, large-scale environments, spanning the full lifecycle of digital systems.

Key research directions

- Applied AI, Generative AI and Agentic AI for operational and business processes;
- Autonomous and intent-based network management and orchestration;
- AIOps and AI-driven service assurance;
- AI-assisted software engineering and AI-enabled SDLC transformation;
- Human-in-the-loop and human-on-the-loop control models;
- Metrics, validation and governance of autonomous behavior.

3. Secure & Trusted Systems

Scope and focus

Secure & Trusted Systems focuses on the integration of security, privacy and trust as key design principles of digital systems. The domain promotes holistic, by-design approaches covering

architecture, development, deployment and operation, ensuring that protection mechanisms are embedded throughout the system lifecycle rather than addressed reactively.

Key research directions

- Security-by-design and privacy-by-design methodologies;
- Zero-trust architectures and secure access models;
- Threat detection, incident response and cyber resilience;
- Secure software and system architectures;
- Trust frameworks, identity management and data integrity;
- Security assurance for distributed, cloud-native and AI-enabled systems;
- Application of AI for threat detection, prevention and adaptive security mechanisms.

4. Digital Experiences & Environments

Scope and focus

Digital Experiences & Environments addresses the design of intelligent, user-centric digital services and environments that integrate connectivity, devices, platforms and data. The domain emphasizes interaction, usability and contextual awareness within complex digital ecosystems, exploring how users perceive, interact with and benefit from connected environments. Research in this area focuses on the convergence of physical and digital spaces, enabling seamless, personalized and intuitive digital experiences.

Key research directions

- Smart home and smart environment platforms;
- User experience (UX) and user interface (UI) design for complex systems;
- Digital services, APIs and service composition;
- Ambient and context-aware computing;
- Spatial and immersive digital experiences;
- Application of AI for personalization, interaction and context-aware user experiences.

5. Defense & Dual-Use Systems

Scope and focus

Defense & Dual-Use Systems focuses on technologies applicable to both civilian and defense or security-critical contexts, characterized by stringent requirements for reliability, resilience and security. This domain addresses systems designed to operate in high-risk and mission-critical environments, while promoting dual-use innovation between defense and civilian applications.

Key research directions

- Mission-critical communications and systems;
- Secure and resilient communication infrastructures;
- Situational awareness and decision-support systems;
- Resilient networks for crisis and emergency scenarios;
- Dual-use technologies with civilian and defense applicability;
- Application of AI for situational awareness, decision support and autonomous operations in critical environments.