

ARTIFICIAL INTELLIGENCE AND CYBER PHYSICAL SYSTEMS

Supervisor Name: Prof. Dr. Francisco Javier González Castaño

Email: javier@det.uvigo.es

Research Group: Information Technologies Group

The Information Technologies Group comprises 5 full professors, 1 associate professor, 2 assistant professors, 2 postdoctoral researchers, and more than 20 research engineers. The group has demonstrated strong funding capacity: since January 1, 2010, it has been awarded over 30 publicly funded European and national R&D projects and has signed approximately 80 technology transfer contracts. Industry contracts include collaborations with major Spanish telecom operators (Telefónica, Orange, Vodafone, and Cellnex), leading Spanish multinationals (such as Indra), and other prominent technology companies and research centers, including Televés, Optare Networks, Centum Research, Marine Instruments, IMEC, and Gradiant.

The head of the group was a founding member of Gradiant, where he served as CTO for Networks and Applications from 2008 to 2013. Gradiant is currently one of the main agents of IT technology transfer to Spanish industry. The group has published over 200 papers in areas related to this project in international JCR-indexed journals, including Computer Networks, IEEE Transactions on Image Processing, IEEE Transactions on Communications, IEEE Transactions on Wireless Communications, IEEE Transactions on Systems, Man, and Cybernetics, IEEE Transactions on Vehicular Technology, IEEE Transactions on Industrial Electronics, IEEE Transactions on Industrial Informatics, IEEE Transactions on Consumer Electronics, and IEEE/ACM Transactions on Networking, among others. It has also presented numerous papers at leading international conferences such as IEEE ICC, IEEE GLOBECOM, IEEE HPSR, and IEEE MILCOM.

The group operates a unique infrastructure that enables full-campus coverage with a B5G network featuring programmable communications and computing resources. This infrastructure will be open to private-sector third parties, making it an ideal environment not only for basic research but also for technology transfer. It will allow to perform self-provisioning of SIMs and eSIMs, including configuring new SIM cards in the core network for new subscribers, covering both FR1 and FR2 frequency ranges.

Keywords: Networked intelligence services | Human-centric intelligent environments

Research Focus:

The rapid evolution of mobile networks is enabling a new generation of human-centric, dual-use autonomous systems integrated with advanced B5G/6G connectivity. This research line focuses on developing Zero-Trust, resilient frameworks to ensure secure, real-time collaboration between humans and autonomous agents across wide-area operations.

Achieving this vision requires pushing computing resources closer to where data is generated—namely, autonomous vehicles and edge infrastructure—rather than relying exclusively on centralized systems. This shift is driven by the stringent latency, bandwidth, and reliability constraints of real-time autonomous operations, where even minor delays can compromise safety or mission success. Edge computing enables local decision-making, reducing dependence on backhaul connectivity and improving robustness in intermittently connected environments. In this context, distributed algorithms become essential, as they allow multiple agents to coordinate, learn, and adapt without a single point of failure. Emerging paradigms such as federated learning further enhance this approach by enabling collaborative model training across distributed nodes while preserving data privacy and reducing communication overhead. Similarly, semantic communications introduce a paradigm shift by transmitting only task-relevant information rather than raw data, significantly improving communication efficiency and resilience under constrained network conditions—key requirements for scalable and adaptive intelligent systems in extreme environments.

By integrating ultra-low-latency capabilities and edge-to-cloud continuums, these systems support robust performance in mission-critical scenarios such as emergency response, strategic infrastructure protection, and tactical networks. These scenarios are inherently complex cyber-physical systems, where tightly coupled interactions between physical processes, sensing, communication, and decision-making must be continuously maintained under dynamic and often unpredictable conditions. For example, multi-robot coordination in disaster response requires real-time sharing of situational data, decentralized planning, and adaptive task allocation in partially observable environments. Situational awareness systems must fuse heterogeneous data sources—such as sensor networks, aerial imagery, and communication signals—to provide a consistent operational picture. In such contexts, quantum-ready networking technologies and enhanced network resilience mechanisms offer forward-looking solutions to address emerging security and performance challenges, including resistance to future cryptographic threats and improved robustness against network disruptions.

This line also explores the mitigation of hostile agentic AI threats and adversarial autonomous agents through dynamic security mechanisms and intelligent fail-safe protocols, ensuring a high degree of trust and operational reliability in degraded environments. This mitigation is particularly relevant in the aforementioned scenarios, where systems operate in contested or adversarial conditions, such as disaster zones with compromised infrastructure or tactical environments subject to cyber and physical attacks. In these settings, malicious agents may attempt to manipulate data, disrupt coordination, or degrade system performance. Therefore, incorporating adaptive threat detection, robust consensus mechanisms, and fail-safe operational modes is critical to maintaining system integrity and ensuring that autonomous agents can continue to operate safely and effectively even under partial system compromise or hostile interference.