

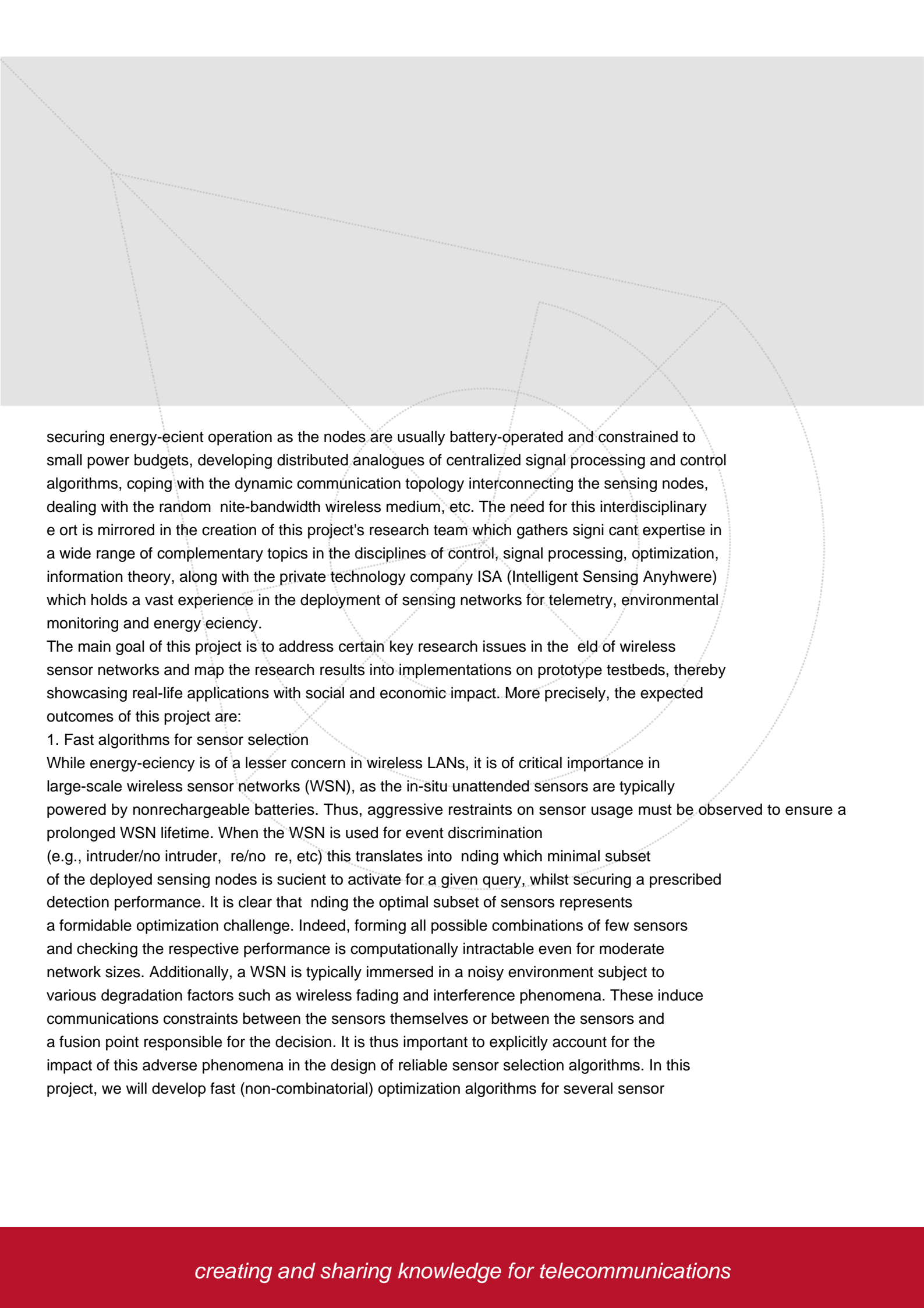
PROJECT / Novel information processing methodologies for intelligent sensor networks

Novel information processing methodologies for intelligent sensor networks

Main Objective:

Over the past few years, we have witnessed tremendous advances in the miniaturization of low cost electro-mechanical devices that exhibit several sensing capabilities (e.g. temperature, pressure, vision, etc) and possess significant embedded processing and low-range wireless communication. This triggered interest in wireless sensor networks (WSN) where large collections of such small wireless sensor nodes are scattered across critical geographical areas or infrastructures to execute a variety of monitoring and acting tasks. While the use of WSN is crucial to assess the state of a physical system, the ultimate engineering goal is to control such system to perform certain desired tasks. We refer to systems that close the loop around wireless sensor networks as cyber-physical systems (CPS). Cyber-physical systems are physical and engineered systems the operations of which are monitored, coordinated, controlled and integrated by a computing and communication infrastructure. Examples of CPS include medical devices and systems, aerospace systems, transportation vehicles and intelligent highways, defense systems, robotic systems, process control, factory automation, building and environmental control and smart spaces.

To realize the immense potential benefits of CPS in real-life applications, a plethora of novel problems lying at the intersection of statistical signal processing, control, communication theory, and distributed optimization, must be addressed. Indeed, it is clear that to achieve desired networkwide detection, estimation or control objectives, system designers should deal efficiently with simultaneous challenges, typically tackled in separate engineering disciplines. The challenges include

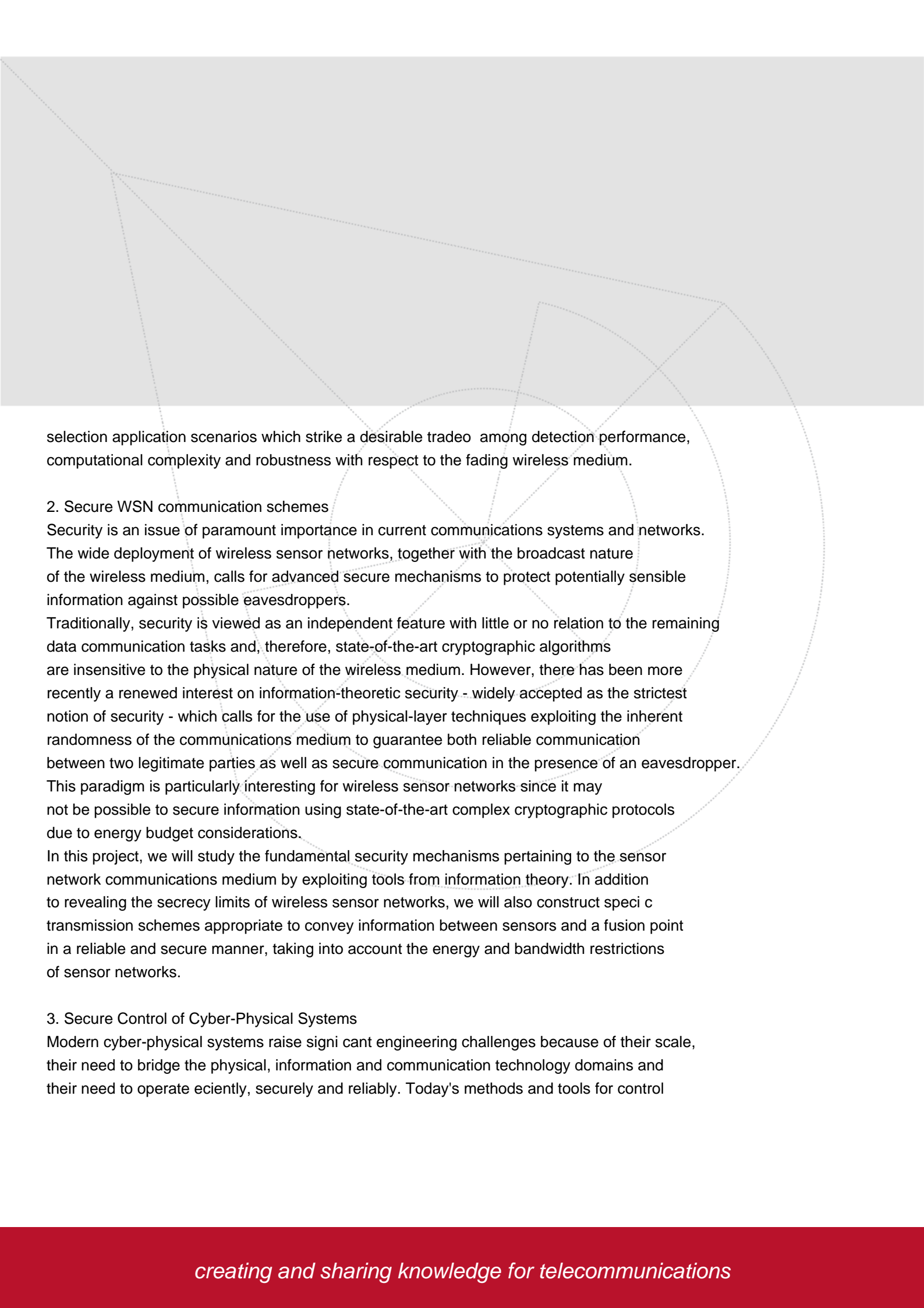


securing energy-efficient operation as the nodes are usually battery-operated and constrained to small power budgets, developing distributed analogues of centralized signal processing and control algorithms, coping with the dynamic communication topology interconnecting the sensing nodes, dealing with the random finite-bandwidth wireless medium, etc. The need for this interdisciplinary effort is mirrored in the creation of this project's research team which gathers significant expertise in a wide range of complementary topics in the disciplines of control, signal processing, optimization, information theory, along with the private technology company ISA (Intelligent Sensing Anywhere) which holds a vast experience in the deployment of sensing networks for telemetry, environmental monitoring and energy efficiency.

The main goal of this project is to address certain key research issues in the field of wireless sensor networks and map the research results into implementations on prototype testbeds, thereby showcasing real-life applications with social and economic impact. More precisely, the expected outcomes of this project are:

1. Fast algorithms for sensor selection

While energy-efficiency is of a lesser concern in wireless LANs, it is of critical importance in large-scale wireless sensor networks (WSN), as the in-situ unattended sensors are typically powered by nonrechargeable batteries. Thus, aggressive restraints on sensor usage must be observed to ensure a prolonged WSN lifetime. When the WSN is used for event discrimination (e.g., intruder/no intruder, fire/no fire, etc) this translates into finding which minimal subset of the deployed sensing nodes is sufficient to activate for a given query, whilst securing a prescribed detection performance. It is clear that finding the optimal subset of sensors represents a formidable optimization challenge. Indeed, forming all possible combinations of few sensors and checking the respective performance is computationally intractable even for moderate network sizes. Additionally, a WSN is typically immersed in a noisy environment subject to various degradation factors such as wireless fading and interference phenomena. These induce communications constraints between the sensors themselves or between the sensors and a fusion point responsible for the decision. It is thus important to explicitly account for the impact of this adverse phenomena in the design of reliable sensor selection algorithms. In this project, we will develop fast (non-combinatorial) optimization algorithms for several sensor



selection application scenarios which strike a desirable tradeo among detection performance, computational complexity and robustness with respect to the fading wireless medium.

2. Secure WSN communication schemes

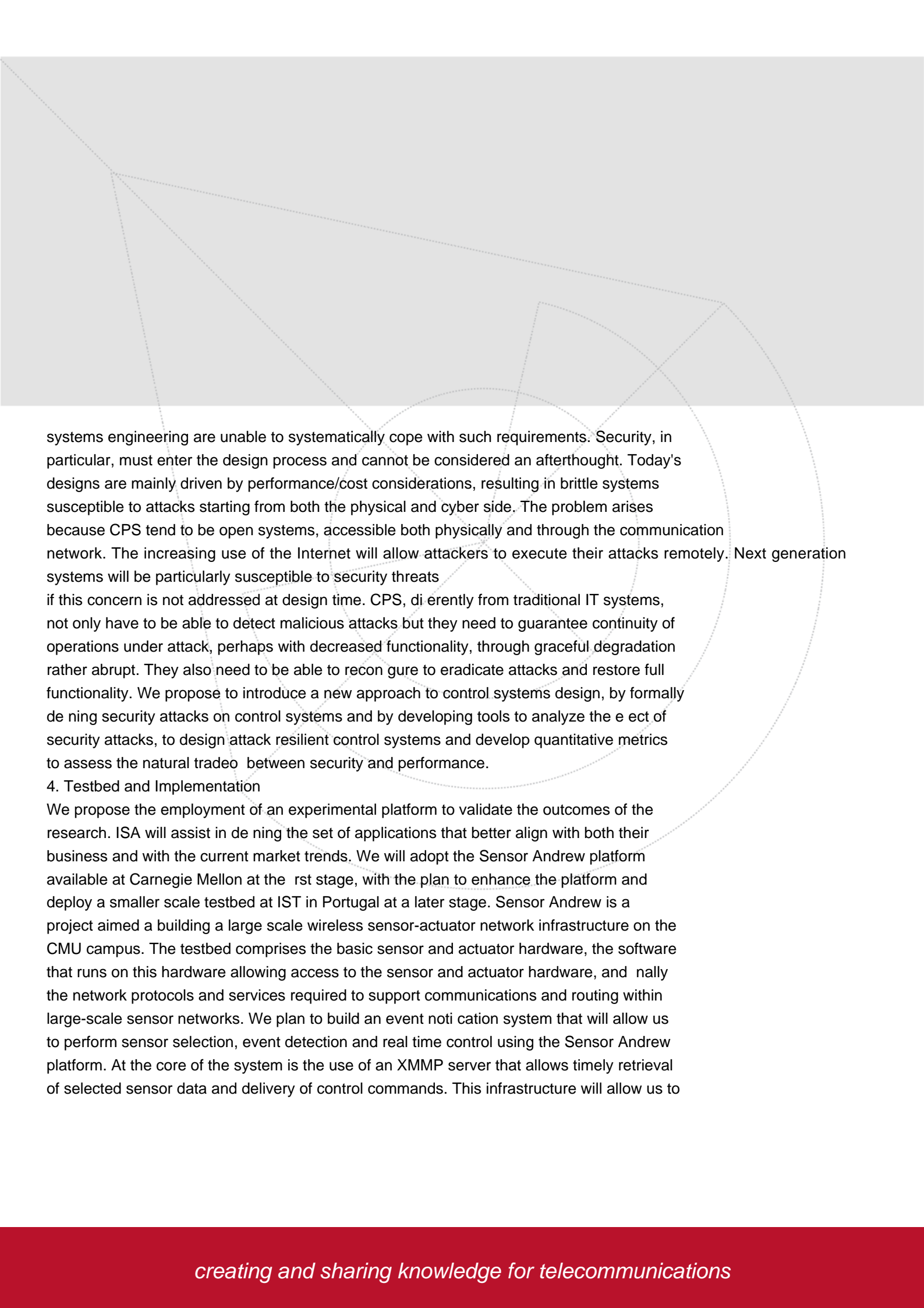
Security is an issue of paramount importance in current communications systems and networks. The wide deployment of wireless sensor networks, together with the broadcast nature of the wireless medium, calls for advanced secure mechanisms to protect potentially sensible information against possible eavesdroppers.

Traditionally, security is viewed as an independent feature with little or no relation to the remaining data communication tasks and, therefore, state-of-the-art cryptographic algorithms are insensitive to the physical nature of the wireless medium. However, there has been more recently a renewed interest on information-theoretic security - widely accepted as the strictest notion of security - which calls for the use of physical-layer techniques exploiting the inherent randomness of the communications medium to guarantee both reliable communication between two legitimate parties as well as secure communication in the presence of an eavesdropper. This paradigm is particularly interesting for wireless sensor networks since it may not be possible to secure information using state-of-the-art complex cryptographic protocols due to energy budget considerations.

In this project, we will study the fundamental security mechanisms pertaining to the sensor network communications medium by exploiting tools from information theory. In addition to revealing the secrecy limits of wireless sensor networks, we will also construct specific transmission schemes appropriate to convey information between sensors and a fusion point in a reliable and secure manner, taking into account the energy and bandwidth restrictions of sensor networks.

3. Secure Control of Cyber-Physical Systems

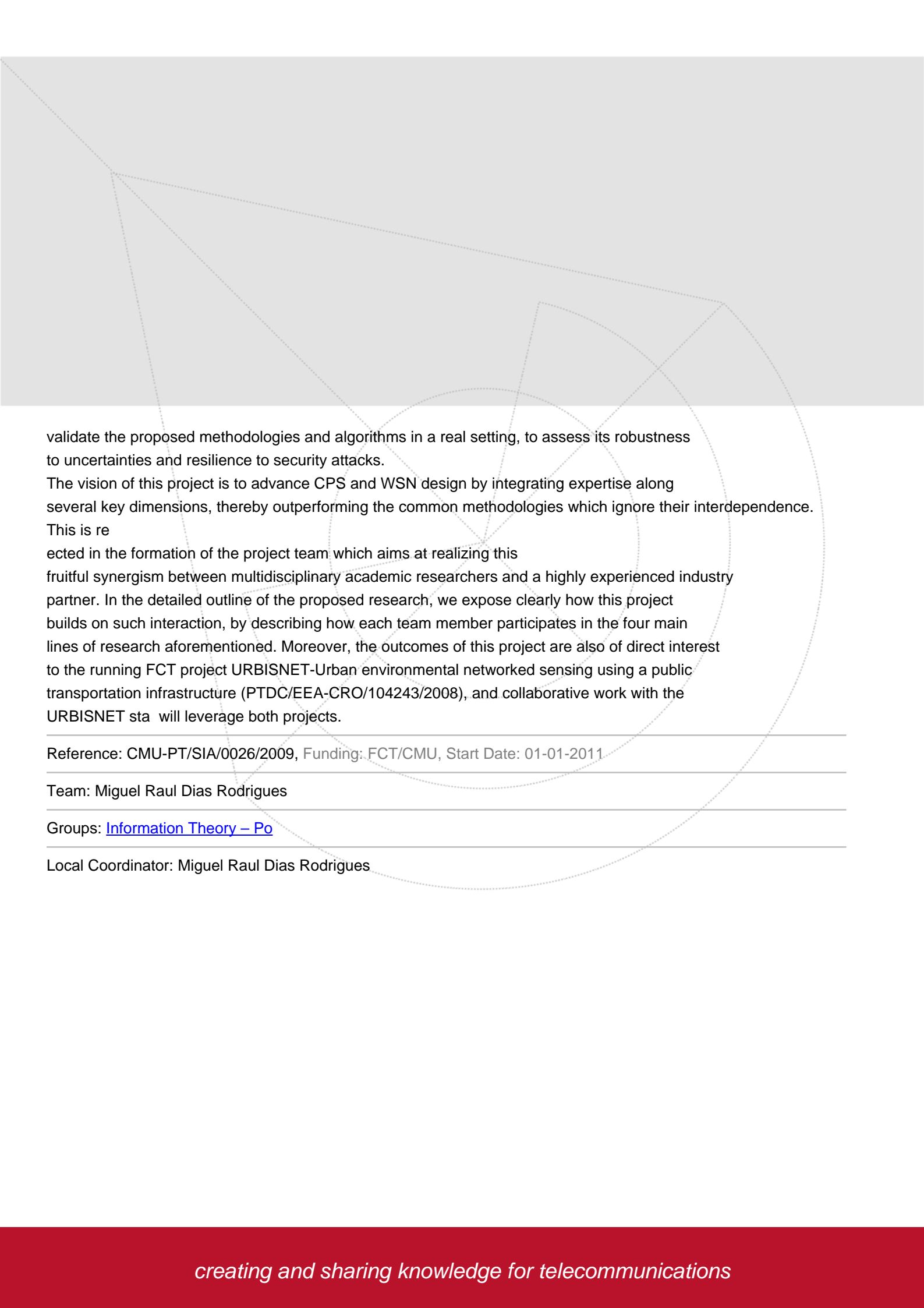
Modern cyber-physical systems raise significant engineering challenges because of their scale, their need to bridge the physical, information and communication technology domains and their need to operate efficiently, securely and reliably. Today's methods and tools for control



systems engineering are unable to systematically cope with such requirements. Security, in particular, must enter the design process and cannot be considered an afterthought. Today's designs are mainly driven by performance/cost considerations, resulting in brittle systems susceptible to attacks starting from both the physical and cyber side. The problem arises because CPS tend to be open systems, accessible both physically and through the communication network. The increasing use of the Internet will allow attackers to execute their attacks remotely. Next generation systems will be particularly susceptible to security threats if this concern is not addressed at design time. CPS, differently from traditional IT systems, not only have to be able to detect malicious attacks but they need to guarantee continuity of operations under attack, perhaps with decreased functionality, through graceful degradation rather abrupt. They also need to be able to reconfigure to eradicate attacks and restore full functionality. We propose to introduce a new approach to control systems design, by formally defining security attacks on control systems and by developing tools to analyze the effect of security attacks, to design attack resilient control systems and develop quantitative metrics to assess the natural tradeoff between security and performance.

4. Testbed and Implementation

We propose the employment of an experimental platform to validate the outcomes of the research. ISA will assist in defining the set of applications that better align with both their business and with the current market trends. We will adopt the Sensor Andrew platform available at Carnegie Mellon at the first stage, with the plan to enhance the platform and deploy a smaller scale testbed at IST in Portugal at a later stage. Sensor Andrew is a project aimed at building a large scale wireless sensor-actuator network infrastructure on the CMU campus. The testbed comprises the basic sensor and actuator hardware, the software that runs on this hardware allowing access to the sensor and actuator hardware, and finally the network protocols and services required to support communications and routing within large-scale sensor networks. We plan to build an event notification system that will allow us to perform sensor selection, event detection and real time control using the Sensor Andrew platform. At the core of the system is the use of an XMPP server that allows timely retrieval of selected sensor data and delivery of control commands. This infrastructure will allow us to



validate the proposed methodologies and algorithms in a real setting, to assess its robustness to uncertainties and resilience to security attacks.

The vision of this project is to advance CPS and WSN design by integrating expertise along several key dimensions, thereby outperforming the common methodologies which ignore their interdependence. This is re

ected in the formation of the project team which aims at realizing this fruitful synergism between multidisciplinary academic researchers and a highly experienced industry partner. In the detailed outline of the proposed research, we expose clearly how this project builds on such interaction, by describing how each team member participates in the four main lines of research aforementioned. Moreover, the outcomes of this project are also of direct interest to the running FCT project URBISNET-Urban environmental networked sensing using a public transportation infrastructure (PTDC/EEA-CRO/104243/2008), and collaborative work with the URBISNET sta will leverage both projects.

Reference: CMU-PT/SIA/0026/2009, Funding: FCT/CMU, Start Date: 01-01-2011

Team: Miguel Raul Dias Rodrigues

Groups: [Information Theory – Po](#)

Local Coordinator: Miguel Raul Dias Rodrigues