Reliable Data Transport in Wireless Sensor Networks (WSN):
that assists in:
- Systematic identification and error propagation profiling framework
- Location of design and operational vulnerabilities, such as detection of enemies
- Dependable Embedded Wireless Sensor Systems
- Dependability assessment and enhancement of COTS Operating Systems
- Robustness improvement of COTS Operating Systems
- Developing a framework (see figure) which meticulously guides the integration
- Investigating the integration using multiple objectives
- Evaluating the goodness of a solution.

One of the current projects in this area is “COTS OS Fault Resilience: On Improving Robustness Testing of Drivers”. In this work we are investigating systematic testing strategies for device drivers.

Error and Threat Profiling of COTS Operating Systems

The Operating System (OS) constitutes a fundamental software component of a computing system. The robustness of its operations, or lack thereof, impacts the robustness of the entire system. Therefore our focus in this area is on:
- Dependability assessment and enhancement of COTS Operating Systems
- Robustness improvement of COTS operating systems and device drivers using wrappers
- Definition and specification of an error propagation profiling framework that assists in:
  a) Systematic identification and location of design and operational vulnerabilities,
  b) Quantification of their potential impact, and
  c) Providing quantifiable input to a systematic security threat modeling process.

Software-Hardware Integration

In this area our work focuses on design and evaluation of dependable embedded systems; specifically focusing on dependability driven software-hardware integration. Integration of mixed criticality systems covers the definition of a comprehensive FDIR (Fault Detection - Isolation - Recovery) diagnostic process, whose behavior is determined by some parameters that can be tuned, using stochastic evaluation, in order to efficiently address different issues in different system environments like handling transient faults, limited coverage of built-in tests and identifying the best recovery action after a fault is detected. One current project in this area is on “Exploiting Symmetries to Model Check Fault Tolerant Protocols”.

Diagnosis and Consensus Protocols in Distributed Systems

Our work in the area of Diagnosis Protocols in distributed systems covers the definition of a comprehensive FDIR (Fault Detection - Isolation - Recovery) diagnostic process, whose behavior is determined by some parameters that can be tuned, using stochastic evaluation, in order to efficiently address different issues in different system environments like handling transient faults, limited coverage of built-in tests and identifying the best recovery action after a fault is detected. One current project in this area is on “Exploiting Symmetries to Model Check Fault Tolerant Protocols”.

Consensus is at the heart of state machine replication, a powerful mechanism to enhance the reliability of distributed systems. Given identical input sequences and starting from identical initial states, replicas of the same deterministic state machine generate identical output sequences. If the correct replicas form a majority, then the “good” responses outvote the number of “wrong” responses generated by faulty replicas. Our work encompasses the development of highly efficient asynchronous consensus protocols for replica coordination despite failures both in the crash and more severe byzantine failure model.