Real-time embedded systems (RTESs) have been widely used in modern society. And it is also very common to find them in safety and security critical applications, such as transportation and medical equipment. There are, usually, several constraints imposed on a RTES, for example, timing, resource, energy, and performance, which must be satisfied simultaneously. This makes the design of such systems a difficult problem.

More recently, the security of RTESs emerges as a major design concern, as more and more attacks have been reported. However, RTES security, as a parameter to be considered during the design process, has been overlooked in the past. This thesis approaches the design of secure RTESs focusing on aspects that are particularly important in the context of RTES, such as communication confidentiality and side-channel attack resistance.

Several techniques are presented in this thesis for designing secure RTESs, including hardware/software co-design techniques for communication confidentiality on distributed platforms, a global framework for secure multi-mode systems, and a scheduling policy for thwarting differential power analysis attacks.

All the proposed solutions have been extensively evaluated in a large amount of experiments, including two real-life case studies, which demonstrate the efficiency of the presented techniques.