Chapter 6

Conclusions and perspectives

The objective of this work was to specify and implements a component fault tolerance framework that can be adaptable to the particular characteristics of architecture, physical constraints, development platform, and real-time operation of embedded real-time systems.

The adopted methodology was:

- Analyze the ERTS fault focuses in order to define that the three layers of the fault tolerance framework are network, communication, and intra-node.

- Define the necessary policies for the framework instantiation on ERTS architectures being based on a component model.

- Implements the communication layer with a time-triggered bus with a component based programming model.

- Validate the communication layer implementing it on an electrical vehicle prototype.

6.1. Results

The main result of our work is a fault tolerant ERTS framework that focuses on the construction of fault tolerant ERTS. The framework defines a set of abstract classes that can be used by an ERTS designer in order to construct any of the three layers that the framework includes. It provides means for specifying fault tolerance properties on three layers: the network, the communication among their components, and their intra-nodes operation. Additionally:

- We defined a fault tolerant ERTS model that most be included inside an ERTS architecture in order to be able to implements the framework classes. Thus, fault tolerance ERTS framework can be adapted to any ERTS with the minimal characteristics of being composed by a set of nodes connected among them by a network bus cable.

- We defined the steps for the implementation of the ERTS components that include the framework classes, their interfaces, and their bindings. We implement the communication layer with a time-triggered bus of the fault tolerant ERTS framework. The implementation showed that using the fault tolerance ERTS framework it is possible to obtain a clear separation between the applicative and the functional code of an ERTS.

- The framework was validated through the construction of an electrical vehicle prototype that included the implementation of the communication layer of the fault tolerance ERTS framework.

6.2. Contributions

The contributions of our work were a state-of-the-art of the ERTS and the definition of a fault tolerance ERTS framework that can be used for the construction of ERTS. Another contribution is the demonstration that it is feasible to use a component model to implement any of the framework layers.

6.3. Future work

Our perspectives include design and implantation aspects:

- Design
  - Specify a service that allows the instantiation of the framework classes on an ERTS in an automatic way, according to its particular characteristics.
  - Analyze each framework layer in the search if it is possible to include fault tolerance techniques that consider components duplication.
  - Formalize the fault tolerant ERTS framework with mathematical tools [CRSS1999] [MR1989] [PR2003] [ST1993].
- Implementation
  - Realize the implementation of the network and the intra-node layers of the framework.
  - Implement the network and the intra-node layers in the electrical vehicle prototype and make a comparison of the resulting specification with the one of the electrical vehicle CyCab project.