Chapter 9

Avoidance of Functional Faults During Specification

9.1 INTRODUCTION

9.1.1 Specification Phase

The use of a product is fundamentally justified by the user's needs. The user possesses the initial motivation to buy or develop a product. In certain cases, this motivation corresponds to a necessity. For example, the fact that society does not accept accidents caused by the simultaneous presence of a train and a vehicle on a railroad crossing, justifies the creation of a system that avoids such accidents. Therefore, a product's life has to naturally start with the client's or future user's requirements (also called needs).

Then, this life cycle carries on with the product's specification stage in response to the previous needs. The previous example shows that one need could involve radically different specifications: a level crossing, or a bridge or a tunnel. The result of this stage is called specifications.

From the product's specifications, we obtain the system by a descending process known as design. This concerns a succession of stages, which are going to structure a system using the specifications expressed at an abstract level, to result in a system which is finally materialized as a physical (electronic) product or a software implemented on a physical support.

This chapter focuses on the requirement and specification stages which are at the origin of numerous faults. Their avoidance is fundamental, as their detection during the design or production stages is generally very costly.

In Chapter 6, we introduced two approaches which permit fault avoidance, that is to say fault prevention and fault removal. The objectives of such means have been presented concerning faults which can happen
during the creation stages. In this chapter, we present the practical techniques to reach the objectives assigned to these means during the requirement and specification stages. The integration of fault prevention and fault removal techniques in the same chapter is justified by their simultaneous use during the studied stages and their close correlations. Figure 9.1 shows the location of these techniques in the life cycle.

Fault avoidance techniques used during design are considered in Chapter 10. The mastering of faults associated with the technology used (electronic or software) to implement the product is discussed in Chapter 11 (fault prevention) and Chapter 12 (fault removal).

### Figure 9.1. Fault avoidance during the specification and the design

#### 9.1.2 Validation and Verification

The primary vocation of fault avoidance means is to prevent fault introduction during the considered stages of a system’s creation process (here the expression of the requirements and of the specifications). During creation stages, we have seen that the faults introduced were due to the