Chapter 5

Development of Safety-Critical Control Systems in Event-B Using FMEA

Yuliya Prokhorova
Åbo Akademi University, Finland

Elena Troubitsyna
Åbo Akademi University, Finland

Linas Laibinis
Åbo Akademi University, Finland

Vyacheslav Kharchenko
National Aerospace University KhAI, Ukraine

ABSTRACT

Application of formal methods, in particular Event-B, helps us to verify the correctness of controlling software. However, to guarantee the dependability of software-intensive control systems, we also need to ensure that safety and fault tolerance requirements are adequately represented in a system specification. In this chapter we demonstrate how to integrate the results of safety analysis, in particular failure mode and effect analysis (FMEA), into formal system development in Event-B. The proposed methodology is exemplified by a case study.

INTRODUCTION

A widespread use of software for controlling critical applications necessitates development of techniques for ensuring its correctness. In other words, these techniques should guarantee that software behaves according to its specification. However, to achieve a high degree of system dependability, we should address not only software correctness but also ensure that safety requirements are adequately represented in a software specification.

Safety (Storey, 1996) is property of the system requiring that it will not harm its environment or users. It is a system-level property that can be achieved via a combination of various techniques.
Development of Safety-Critical Control Systems in Event-B Using FMEA

for safety analysis. The aim of safety analysis is to uncover possible ways in which system might breach safety and then devise the means to avoid these situations or mitigate their consequences. There is a wide spectrum of techniques that facilitate the analysis of possible hazards associated with the system, the means for introducing fault tolerance to prevent occurrence of dangerous faults, as well as the techniques for deriving functional requirements from the conducted safety analysis.

In this chapter we focus on the use of Failure Modes and Effect Analysis (FMEA) – a widely-used inductive technique for safety analysis (FMEA Info Centre, 2009; Storey, 1996). We propose a methodology that allows us to incorporate the results of FMEA into a formal system specification. FMEA aims at a systematic study of the causes of components faults, their global and local effects, and the means to cope with these faults. Since the fault tolerance mechanisms are often implemented as a part of the developed software, this information constitutes the necessary requirements that the controlling software should fulfil.

Since safety is a system-level property, it requires modelling techniques that are scalable to analyse the entire system. Scalability in the system analysis is achieved via abstraction, proof and decomposition. The Event-B formalism (Abrial, 2010) provides a suitable framework that satisfies all these requirements. Event-B is a state-based formalism for development of highly-dependable systems. The main development technique of Event-B is refinement. In Event-B, we start system modelling at a highly-abstract level and, by a number of correctness-preserving transformations called refinement steps, arrive at a system specification that is close to the eventual implementation. Correctness of each refinement step is verified by proofs.

In this chapter we show how to incorporate the results of FMEA into the formal Event-B development. Our approach enables elicitation and traceability of the safety requirements that thus potentially enhance system dependability. The proposed methodology is illustrated by a small case study.

The chapter is structured as follows. Section “Related work” gives an overview of the related work. In Section “Modelling control systems in Event-B” we briefly present the Event-B method and also describe modelling of control systems in Event-B. In Section “Incorporation of fault analysis results in Event-B” we propose a methodology for integrating the results of FMEA into the Event-B development. Section “Case study” illustrates the proposed approach by a case study – a heater controller. In Sections “Future research directions” and “Conclusion” we give concluding remarks and discuss our future work.

RELATED WORK

Integration of the safety analysis techniques with formal system modelling has attracted a significant research attention over the last few years. There are a number of approaches that aim at direct integration of the safety analysis techniques into formal system development. For instance, the work of Ortmeier et al. (Ortmeier, Guedemann, & Reif, 2007) focuses on using statecharts to formally represent the system behaviour. It aims at combining the results of FMEA and FTA to model the system behaviour and reason about component failures as well as overall system safety. Moreover, the approach specifically addresses formal modelling of the system failure modes. In our approach we define general guidelines for integrating results of FMEA into a formal Event-B specification and the Event-B refinement process. The available automatic tool support for the top-down Event-B modelling ensures better scalability of our approach.

In our previous work, we have proposed an approach to integrating safety analysis into formal system development within the Action System formalism (Sere & Troubitsyna, 1999), (Troubit-