Abstract

Failure Modes and Effect analysis (FMEA) is a widely used technique for inductive safety analysis. FMEA provides the engineers with the valuable information about failure modes of system components as well as procedures for error detection and recovery. In this paper we propose an approach that facilitates representation of FMEA results in formal Event-B specifications of control systems. We define a number of patterns for representing the requirements derived from FMEA in formal system model in Event-B. These patterns facilitate traceability of requirements and allow us to increase automation of formal system development by refinement. Our approach is illustrated by an example - a sluice system.

Keywords: formal specification, Event-B, FMEA, patterns, safety, control systems

TUCS Laboratory
Distributed Systems Laboratory