Chapter 11

A Unified Modelling and Operational Framework for Fault Detection, Identification, and Recovery in Autonomous Spacecrafts

Andrea Bobbio
University of Piemonte Orientale, Italy

Daniele Codetta-Raiteri
University of Piemonte Orientale, Italy

Luigi Portinale
University of Piemonte Orientale, Italy

Andrea Guiotto
Thales Alenia Space, Italy

Yuri Yushtein
ESA-ESTEC, The Netherlands

ABSTRACT

Recent studies have focused on spacecraft autonomy. The traditional approach for FDIR (Fault Detection, Identification, Recovery) consists of the run-time observation of the operational status to detect faults; the initiation of recovery actions uses static pre-compiled tables. This approach is purely reactive, puts the spacecraft into a safe configuration, and transfers control to the ground. ARPHA is an FDIR engine based on probabilistic models. ARPHA integrates a high-level, a low-level, and an inference-oriented formalism (DFT, DBN, JT, respectively). The off-board process of ARPHA consists of the DFT construction by reliability engineers, the automatic transformation into DBN, the manual enrichment of the DBN, and the JT automatic generation. The JT is the on-board model undergoing analysis conditioned by sensor and plan data. The goal is the current and future state evaluation and the choice of the most suitable recovery policies according to their future effects without the assistance of the ground control.

DOI: 10.4018/978-1-4666-4659-9.ch011

INTRODUCTION

In autonomous spacecraft operations, both the system behavior and the environment can exhibit various degrees of uncertainty; control software must then provide the suitable and timely reaction of the system to changes in its operational environment, as well as in the operational status of the system. The operational status of the system depends on the internal system dependability factors (e.g. sub-system and component reliability models), on the external environment factors affecting the system reliability and safety (e.g. thermal, radiation, illumination conditions) and on system-environment interactions (e.g. stress factors, resource utilization profiles, degradation profiles, etc.). Combinations of these factors may cause mission execution anomalies, including mission degradations and system failures. To address possible system faults and failures, the system under examination must be provided with some form of health management procedures, usually relying on the *Fault Detection, Identification and Recovery* (FDIR) process.

The goal of the VERIFIM (*Verification of Failure Impact by Model-checking*) study is an innovative approach to on-board FDIR: the FDIR engine exploits an on-board probabilistic graphical model which must take into account the system architecture, the system environment, the system-environment interaction, and the dynamic evolution in presence of uncertainty and partial observability. Moreover, the on-board FDIR engine must provide the system with diagnosis (fault detection and identification) and prognosis (fault prediction) on the operational status to be taken into account for autonomous reactive or preventive recovery actions. To this aim, inside VERIFIM, we developed the software prototype called ARPHA (*Anomaly Resolution and Prognostic Health management for Autonomy*).

Before the execution of ARPHA (on-board process), the on-board model must be prepared. Since several aspects have to be represented by the on-board model, the modelling phase (off-board process) integrates a high level modeling formalism (*Dynamic Fault Tree* (DFT) (Dugan et al., 1992)), a low level modeling formalism (*Dynamic Bayesian Network* (DBN) (Murphy, 2002)) and an inference oriented formalism (*Junction Tree* (JT) (Huang & Darwiche, 1996)). Basic notions about these formalisms are reported in the next section. The on-board model (JT) is obtained through a sequence of model conversions and model enrichment. We present a case study concerning the power supply subsystem of a Mars rover. This case study provides a running example for the off-board process (modelling phase) and the on-board process (diagnosis, prognosis and recovery of the system, conditioned by sensor data and plan data).

BACKGROUND

Currently employed state-of-the-art of the FDIR is based on the design-time analysis of the faults and failure scenarios (e.g. *Failure Mode Effect Analysis* (FMEA), *Fault Tree Analysis* (FTA) (Schneeweiss, 1999)) and run-time observation of the system operational status (health monitoring). The goal is in general to detect faults in a timely manner and to start a predefined recovery procedure (by using look-up tables), having the goal of putting the spacecraft into a known safe configuration and transfer control to the ground operations for troubleshooting and planning actual recovery.

Standard FDIR approaches have multiple shortcomings which may significantly reduce effectiveness of the adopted procedures:

- The system, as well as its environment, is only partially observable by monitoring procedures; this introduces uncertainty in the interpretation of observations in terms of the actual system status, which is often disregarded in choosing the possible recovery.