Enabling FDIR design through diagnosability and recoverability analysis

This PhD research builds on the results of COMPASS and its follow-up projects AUTOGEF and FAME, and pushes the state-of-the-art in timed failure propagation analysis and diagnosability analysis with formal verification tools.

The first line of work is on Timed Failure Propagation Graphs (TFPGs), which represent possible sequences of faults and their consequences (including triggering of potential monitors), integrated with information on propagation delays and mode constraints. Several formal techniques based on model-checking have been developed to validate and also automatically generate TFPGs with respect to a system model of higher complexity.

The second line of work covers diagnosability analysis, which requires values observed by FDIR to carry enough information to allow diagnosis of faults or other anomalies. It is especially important when failure propagation analysis doesn't give enough insights on how to detect and precisely localize faults; diagnosability checks whether diagnosis is possible at all. Algorithms are developed to verify diagnosability under a given set of observables, possibly under a constrained operational context. The techniques are also extended to automatically select subsets of the observables that optimize a given cost function.

Experimental evaluation shows the feasibility of the developed techniques. Several case studies on an ESA mission under development show the high potential of the techniques in a project setting.