Automated Safety Analysis by Minimal Path Set Detection for Multi-Domain Object-Oriented Models

Christian Schallert

Institute of System Dynamics and Control, German Aerospace Centre (DLR),
Christian.Schallert@dlr.de

The presentation and corresponding paper describe a method called DMP that integrates safety or reliability analysis with multi-domain object-oriented modelling. In essence, the method automatically Detects the Minimal Path (DMP) set of any fault-tolerant technical system. DMP is based on the simulation of normal behaviour, degradation and failure of a system. Thus, modelling of failures has to be supplemented to component models from generic libraries, e.g. the Modelica Standard Library, that typically represent only normal, intact behaviour. Minimal path set analysis generally assumes that a system and its components are two-state, i.e. intact or failed.

The DMP method is a state space simulation. In this context, the state space denotes the set of all combinations of intact and failed components of a system to be examined for detection of its minimal path set. The object structure of the system model is represented as a graph, in which nodes correspond to components, and edges correspond to connections. Evaluation of the graph reduces the size of the state space and hence the number of simulations required.

DMP starts with all components (nodes) of a system being intact. Nodes are then successively removed from the system graph, which corresponds to component failures. The model is simulated to identify if the system still operates or fails. Articulations can occur in the graph that, if removed, cause disconnection of the graph into several subgraphs. Since only a coherent set of intact nodes can be a minimal path, splitting up the graph at articulations reduces the state space. The lower the density of a graph is, the more articulations occur within it and thus fewer simulations are required. For completeness, method DMP allows that articulations can also belong to a minimal path.

DMP enhances the scope of application of a model while permitting all other simulation studies that originally motivated implementation of the model to be conducted. The method can be employed throughout the system development process to keep the safety analysis up-to-date with design iterations.

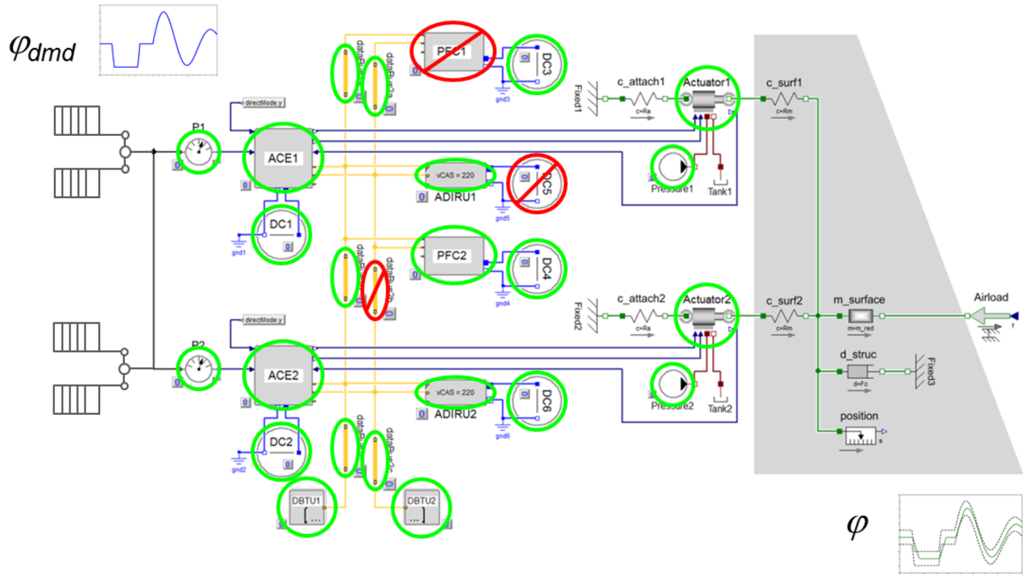

Figure 1. Safety analysis by state space simulation of an aircraft's rudder control system