Modeling, analysis, and simulation methods and technology capture and integrate information from diverse sources into models and evaluate risks and countermeasures in early designs for systems of interacting hardware, software, and human subsystems. First, system requirements are used to automatically derive system architecture models (subsystems, components, and their interconnections). These models are used, in turn, to identify candidate risks and associated countermeasure options. Then, risks and countermeasures options are evaluated using a progressive sequence of analyses and simulations to assess dependencies, failure propagation paths, failure effects, and challenges to countermeasures. The feasibility of these methods and this technology has been demonstrated with a high-level spacecraft design case using an engineering support tool for hazard identification and architecture analysis and as abstract subsystem models in a hybrid simulation tool. Component-connection models of systems from the engineering support tool are mapped to system behavior models in the simulation tool.
Key to this approach is the use of ontology-based parsing of requirements and risk descriptions and ontology-based representations of design entities, functions, risks, and countermeasures for hardware, software, and humans. The standard vocabularies support text parsing and library-based assistance for considering potential problems and countermeasures for a broad set of types of functions and entities. Also important is the use of hybrid simulation technology that allows for a qualitative specification of system architecture behavior as well as numerical models and graph reachability analyses for finding failure propagation paths, including those that are due to interaction among subsystems. Models and simulations must be built progressively with content needed only for a particular phase of the life cycle. Thus, less detailed, “lightweight” models and simulations can support analysis of early design options. High-level models of system health management strategies and human system integration designs can be evaluated and included in early trades. In later design phases, more details can be added to support full-scale analysis. This technology can integrate concerns from multiple disciplines and enable a consistent level of design productivity throughout life-cycle phases.