Analyzing Interaction Paths to Evaluate Integrated Technical Risks and Plan Verification Tests

Jane T. Malin, *Johnson Space Center*
Land Fleming, *MEI Technologies*

System risk management, verification, and qualification are critical for engineering safe and successful aerospace systems. There are many methods for identifying, analyzing, and estimating technical risks in systems. Technical risks (or product risks) refer to problems in components or interactions that can result in failure or injury. Risk analysis drives plans for verifying and qualifying systems, by test and other methods. Despite best efforts, too many risks still slip through in early analyses and appear late in the system life cycle, when they can delay delivery or threaten safety or mission success. Risk identification methods are based on checklists and lessons from similar projects and equipment. Risk analyses work from the bottom (failure modes and effects analysis [FMEA]) or the top (fault trees) of a system, focusing on local causes and impacts and their probabilities. Problems can be missed if they are dependent on unusual or unexpected system configurations. To catch more risks, these methods need to more effectively consider risk dynamics as effects cascade across system interfaces and interaction paths.

A team of Johnson Space Center engineers has developed a risk analysis approach to identify more risk interactions and make better estimates of risk impact severity. The method uses early design information to extract abstract system connectivity models that can include external factors and interfaces among subsystems. These models are designed to be simpler and easier to maintain than risk models. The analysis method takes advantage of history and checklists by using standard nomenclature, ontologies, and libraries. These approaches can make risk analyses reusable and maintainable, as well as less time-consuming and more complete and focused. Model- and library-based approaches help achieve reusable and repeatable analyses and analysis products. They can indicate ways to control risk. Analysis models and results can also drive verification plans and design of systems from test, diagnosis, and impact analysis.

First, the risk analysis method identifies hazard-vulnerability pairs that should not reach each other. Impacted targets can be described as vulnerable to hazardous entities (e.g., materials, signals) that may be produced elsewhere in the system. A vulnerability is a sensitivity to local inputs that can contribute to losses or decreases in reliability (e.g., vulnerability to abrasive materials that may cause wear and early failure). Cross-subsystem interactions typically transmit "remote" hazards, which are not immediate, and local hazards to vulnerable entities. A hazard has a negative impact on a function, even though it may be a legitimate product or by-product of a subsystem function. For example, Freon may be a necessary resource for one process but could be detrimental to the functioning or physical integrity of another process. Likewise, effects need not be inherently hazardous, but they can depend on system configuration. System states and component modes can be reconfigured in the model to support finding configuration-dependent problems and analyzing effects of risk controls.

The analysis can pair up an "unexpected" remote hazard source with a target entity that is vulnerable to the hazard. This can be a useful starting point for discussion of subsystem interactions between development teams, even without further information about propagation paths. Figure 1 shows a simple spacecraft interaction model, where noise generated by a source in the thermal system (when it is operating) would affect transmitters that are vulnerable to noise.

Next, the method can analyze potential propagation paths across subsystems and analyze the integrated impact of risks. The current mode of each component in a system scenario is set when the model is initialized. Figure 1 shows a propagation path for noise from the thermal subsystem through electrical connections, which can affect both redundant transmitters in the model. Redundant transmitters protect against noise generated internally in a transmitter, but they do not protect against the external noise that is propagated to both redundant transmitters when the thermal system is operating.

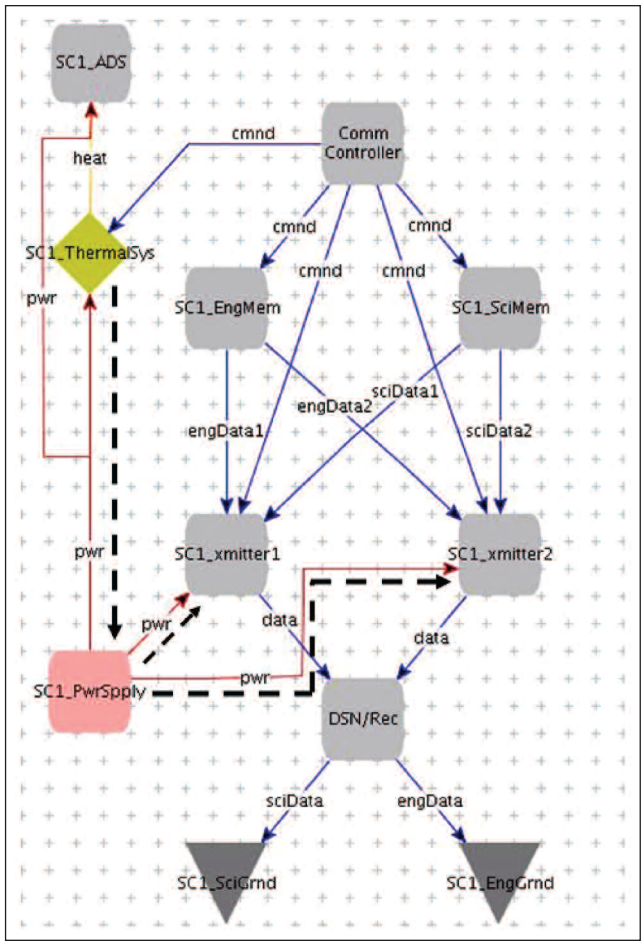

Fig. 1. *Model of spacecraft systems with connections and hazard paths (broken-line arrows) from the thermal system source of a noise hazard to two vulnerable transmitters.*

The analysis of potential propagation paths and integrated risk impacts includes:

(1) A path-finding procedure that identifies pairs of components in a connectivity model. An entity produced by a source component is considered to be hazardous if a path is found to a component function that is vulnerable to that disabling entity.

(2) A scheme for estimating the effectiveness of a source component at producing hazards and the degree of vulnerability of other components to hazards.

(3) A hazard impact analysis method using an And-Or tree of disablers and a search for the path with the maximum degree of hazard transmission effectiveness. This method accounts for the transmission effectiveness of components on the path.

If a path is found from a hazard source to the vulnerable component, an integrated numerical estimate of the impact of the hazard is calculated. There are two estimates of threat severity: 1) worst-case severity of threat influences on a vulnerable function; and 2) threat propagation effectiveness of connections in a configuration.

A search for propagation paths and estimates of "effectiveness" can start simply and be incrementally elaborated as design progresses. This approach should be applicable for hazard analysis and evaluation of fault trees and FMEAs. Work on interaction path analysis is continuing in a research project to adapt and extend this risk-based approach to planning tests for verification and qualification of software systems.