Safer operations through modeling

by Kristin Rozier

*The **Intelligent Systems Technical Committee** works to advance the application of computational problem solving technologies and methods to aerospace systems.*

A major cause of failures in airplanes and spacecraft involves how humans interact with automated systems. The problem, known as HAI or **human-automation interaction**, has become a major safety concern.

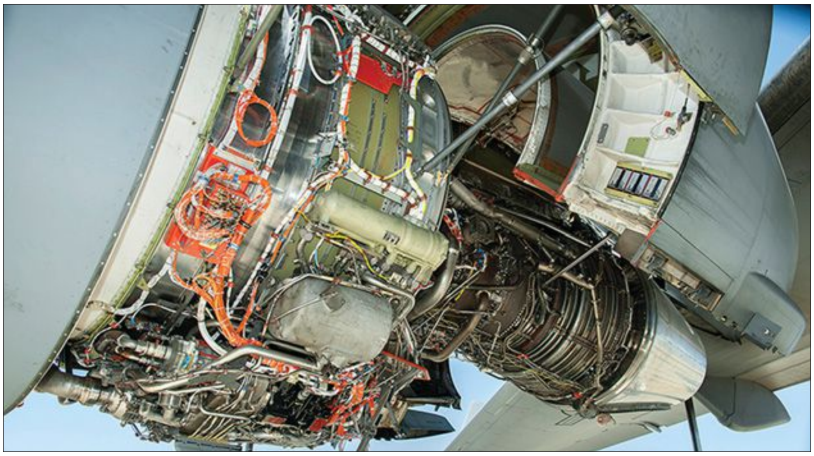
A team of analysts from **The University of Illinois at Chicago**, **Delft University of Technology**, the European Space Agency and IXION Industry and Aerospace has developed a new method that allows them to discover HAI problems automatically, using a process called formal verification.

The team used this method to evaluate a satellite tracking and control system and an unmanned aircraft ground control station. Their approach entails constructing formal models of human operator tasks, automation, and systems, and then integrating these models into a larger formal system model. A model checker enables verification that the system supports safe HAI.

In the analytical realm, a new toolset called **COMPASS** for correctness, modeling, and performance of aerospace systems has been used to study the software and **fault management** architectures of current European space missions. Developed by ESA, RWTH Aachen University, Fondazione Bruno Kessler, and Thales Alenia Space, COMPASS uses a model expressed in Architecture Analysis and Design Language. The model includes nominal, erroneous and degraded operations to enable rigorous, semi-automated analysis. Using model checking technology, COMPASS looks at the design's functional correctness, safety, fault management effectiveness, and other properties.

In aviation, the need for onboard **collision avoidance** systems increases as air traffic management reduces the spacing required between planes. Nonlinear flight trajectories create complexities that make these onboard systems impossible to analyze completely via testing or simulation. Researchers at Carnegie Mellon University pinpoint unexpected emergent behaviors using the theorem prover **KeYmaeraD**. This tool handles continuous and nonlinear flight trajectories and the infinite behaviors that can be generated by multiple maneuvering planes. The researchers proved **safe separation** for an arbitrary number of aircraft flying under a disc-based collision avoidance scheme. This level of verification has yet to be achieved for any other distributed and flyable collision avoidance protocol.

NASA Ames's System-wide Safety and Assurance project developed a framework for onboard uncertainty quantification and management in **automated** prognostics and **health monitoring**. The framework identifies sources of uncertainty and estimates systems' remaining useful life by analyzing possible failure scenarios and fault degradation modes. Decision-making for reducing these uncertainties then automatically enables fault recovery and mission replanning, which are vital for time- and safety-critical missions. Tests of this framework involved monitoring the power systems of mobile robots and unmanned aircraft.



Researchers demonstrated online wire chafing fault detection on C-17 engines at NASA Dryden. Credit: NASA Dryden.

Jet Propulsion Laboratory researchers created onboard real-time **cloud screening** for the AVIRIS-NG, or Next Generation Airborne Visible Infrared Imaging Spectrometer, demonstrating the highest execution speed yet for such screening. The spectrometers generate unprecedented volumes of data, requiring better storage and communications. Image screening could improve data volumes by a factor of two.

Hardware safety advances included a demonstration of online **wire chafing** fault detection technology on **C-17 jet engines** at NASA Dryden. Wiring is critical to aircraft safety–even minor issues can lead to serious problems including smoke, fire, and out-of-service time. A government-industry team developed advanced physics-based methods for automatically detecting sizes and locations of chafing faults in shielded and coaxial aircraft cables. The team included researchers from four NASA centers–Goddard, Dryden, Langley, and Ames–and the Air Force, Pratt & Whitney, Boeing, United Technologies Research Center, Makel Engineering, Auburn University and Kansas State.