Safety Supervisory Control for Risk-Informed Safety Interventions and Accident Prevention

Francesca M. Favarò
Georgia Institute of Technology, Atlanta, GA

Accident prevention and system safety are important considerations for many industries, especially large-scale hazardous ones such as the nuclear, the chemical, and the aerospace industries. Limitations in the current tools and approaches to risk assessment and accident prevention are broadly recognized in the risk research community. A safety gap is growing between the software-intensive technological capabilities of present systems and the still "too much hardware oriented" current approaches for handling risk assessment and safety issues.

To overcome these limitations, a novel framework and analytical tools for model-based system safety, or safety supervisory control, is developed to guide safety interventions and support a dynamic approach to risk assessment and accident prevention. This integrated approach rests on two basic pillars: (i) the use of state-space models and state variables (from Control Theory) to capture the dynamics of hazard escalation, and to both model and monitor "danger indices" in a system; and (ii) the adoption of Temporal Logic (TL, from Software Engineering) to model and verify system safety properties (or their violations, hence identify vulnerabilities in a system). The verification of whether the system satisfies or violates the TL safety properties along with the monitoring of emerging hazards provide an important feedback for designers and operators to recognize the need for, rank, and trigger safety interventions.

The integrated framework is implemented in Simulink and is capable of combining hardware, software, and operators' control actions and responses within a single analysis tool, as examined through its detailed application to runway overrun scenarios during rejected takeoffs (RTO). New insights are enabled by the use of temporal logic in conjunction with model-based system safety. For example, new metrics and diagnostic tools to support pilots' go/no-go decisions and to inform safety guidelines are derived.

By leveraging tools that are not traditionally employed in risk assessment, the framework and tools proposed offer novel capabilities, complementary to the traditional approaches to risk assessment, and rich possibilities for informing safety interventions (by design and in real-time during operations) and towards improved accident prevention.