Embedded Fault Detection for Low-Cost, Safety-Critical Systems

Gary Balas, Jaideep Srivastava, Mats Heimdahl, Antonia Zhai, and Peter Seiler

Fault tolerance is vital to ensuring the integrity and availability of safety critical systems. Current solutions are based almost exclusively on physical redundancy at all levels of the design. The use of physical redundancy, however, dramatically increases system size, complexity, weight, and power consumption. Moreover, such systems are extremely expensive in terms of both the design and development, as well as the unit production costs. This research addresses the basic challenge of bringing high levels of reliability and integrity to other domains-domains that can afford neither the cost nor the extra power, weight, and size associated with physical redundancy. Our main research focus is on the development of algorithms and computing architectures which enable the detection of faults without relying on physical redundancy. In this context, we aim to address both detection of faults in the physical domain (sensor, actuator, and environment faults) as well as faults in the logical, cyber-domain (software and processor faults).

There is a significant opportunity to use *model-based* and *data-driven* monitoring techniques to reduce the reliance on physical redundancy. We are currently pursuing a three-pronged approach to fault detection. First, we are investigating the use of robust filters to estimate key signals using sensor measurements, actuator commands, and models of the physical system being controlled. We have developed a new algorithm to design optimal filters that are robust to model uncertainties. Faults in the physical (sensors, actuators, and environment) system can be detected by comparing the estimated quantities to the corresponding measured signals. Second, to detect faults in the cyber (software and hardware) domain, we are investigating the use of monitors derived from model-based software requirements. We have developed an efficient algorithm to non-intrusively measure structural coverage of an application during execution. The monitoring algorithm uses a bit set to describe the coverage obligations for an application to be monitored. Third, we are investigating the use data-driven anomaly detection methods to detect unexpected failure modes in the physical as well as cyber domains. We have constructed a hybrid algorithm capable of detecting many classes of faults by combining predicate logic satisfiability with existing statistical methods. Our algorithm detects contextual faults inaccessible to pure data-driven approaches using domain information to seed its knowledge base during training. We believe that these various fault detection methods are complementary schemes that are well-paired for reliably detecting a wide variety of faults. Implementing this three-prong approach to fault detection requires significant communication between the various software components. Naturally, this data sharing must not unduly affect the behavior of the application being monitored and must be high speed and low latency. This would be difficult, if not impossible, with existing software and computing architectures. We are currently developing extensions to multicore processor architectures that enable efficient and non-intrusive monitoring algorithms for control software.

An important component to our research is the formulation of realistic benchmark problems that span across the boundary between the physical and cyber domains. We have begun by formalizing many of the requirements for an inner loop flight controller. This example is of sufficiently complexity to highlight the interplay between dynamics and control, software, monitoring, and hardware. Initial flight tests have been performed using the Uninhabited Aerial Vehicle experimental facilities at the UMN Aerospace Engineering and Mechanics department. The flight test results are being used to investigate and compare the performance of the various fault detection methods.