CERIAS
The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Hardware/Software-in-the-loop Analysis of Cyberattacks on UASs

James Goppert, Andrew Shull, Nandagopal Sathyamoorthy, and Inseok Hwang

Abstract

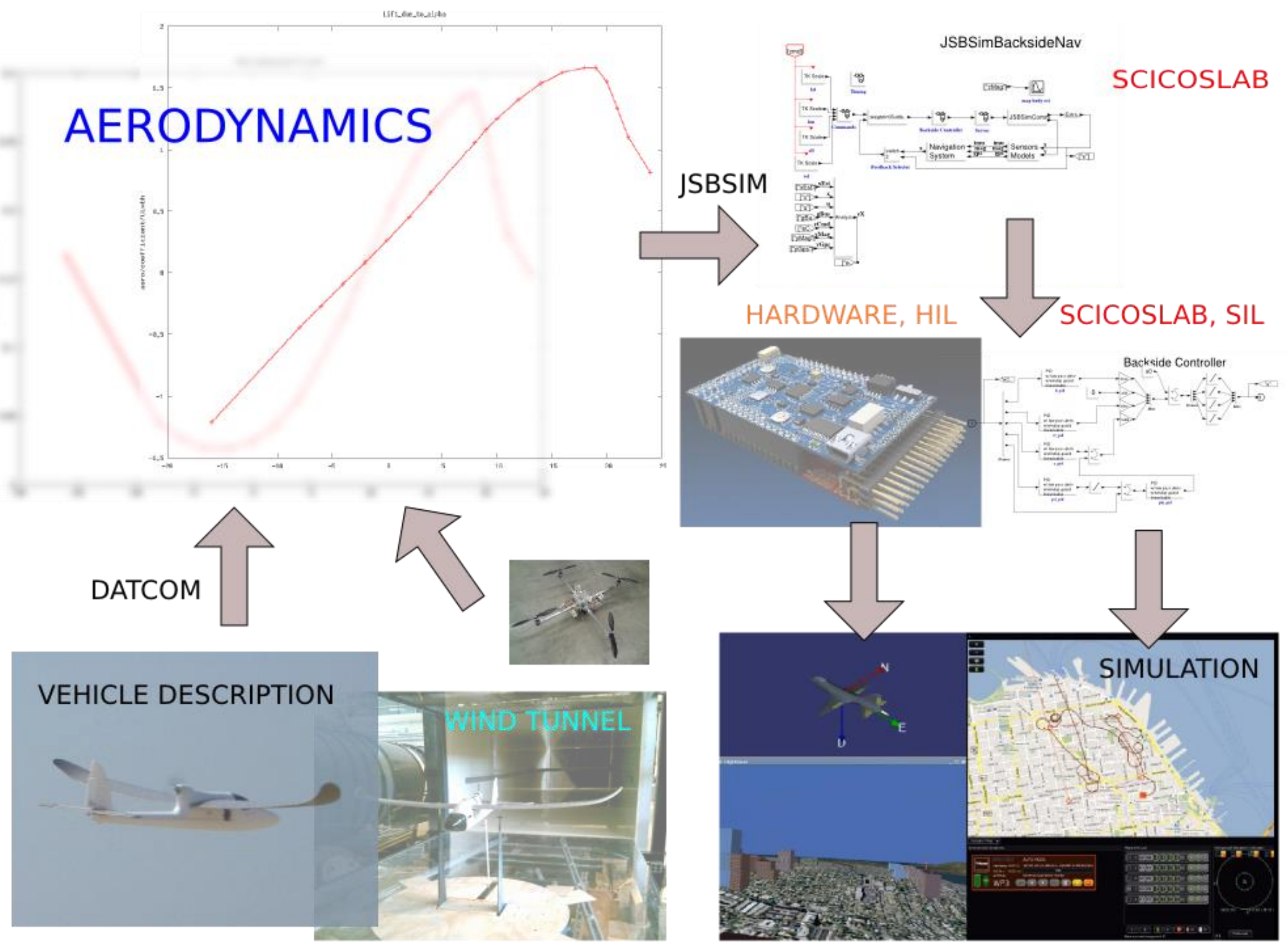
Unmanned aerial systems (UASs) have taken on a large role in military operations and there is considerable interest in expanding their use to commercial and scientific applications. Because of the dependence of these vehicles on computer systems, their high degree of autonomy, and the danger posed by a loss of vehicle control, it is critical that the proliferation of these vehicles be accompanied by a thorough analysis of their vulnerabilities to cyberattack.

Simulation

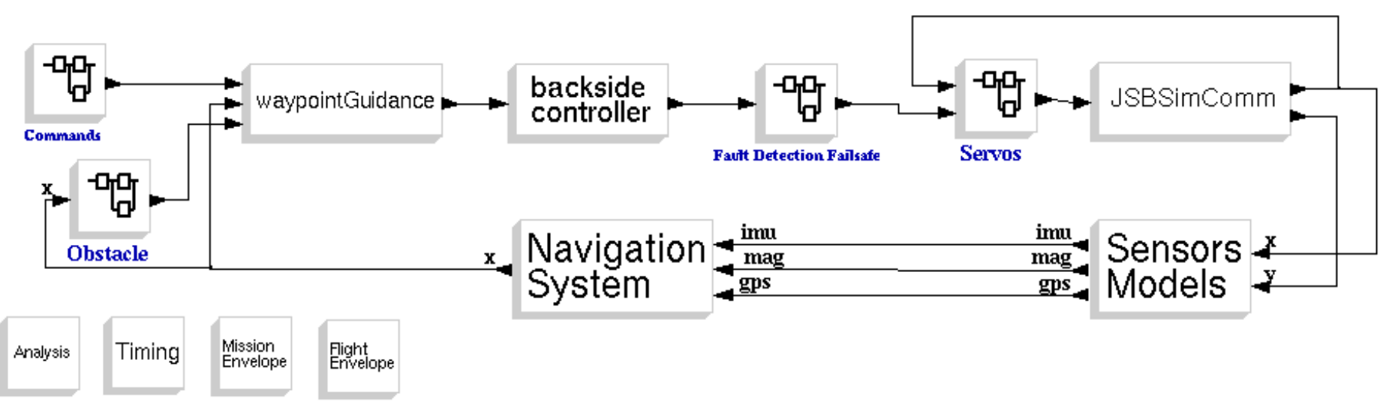
The Hybrid Systems Lab has created a simulation test bed that models UAS controls systems and flight operations. This test bed is capable of testing both software-in-the-loop and hardware-in-the-loop models. Using this test bed, UAS flight can be simulated in the presence of a cyber attack and attack success, severity, and detectability can be analyzed. The hardware-in-the-loop test bed enables testing at both the design and implementation levels.

An intelligent attack will likely need to use multiple attacks of small magnitude to avoid detection by monitoring and mitigation systems. These attacks would be chosen so that each individual attack is small enough that it can go unnoticed but that they will still be successful when coupled. Once these attacks are identified, countermeasures can be developed and the system can thus be hardened to such attacks.

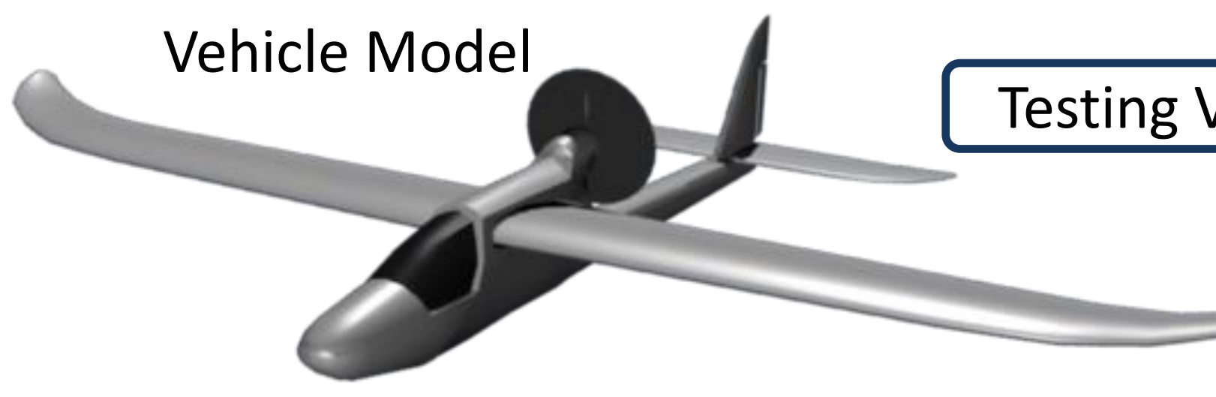
Test Bed

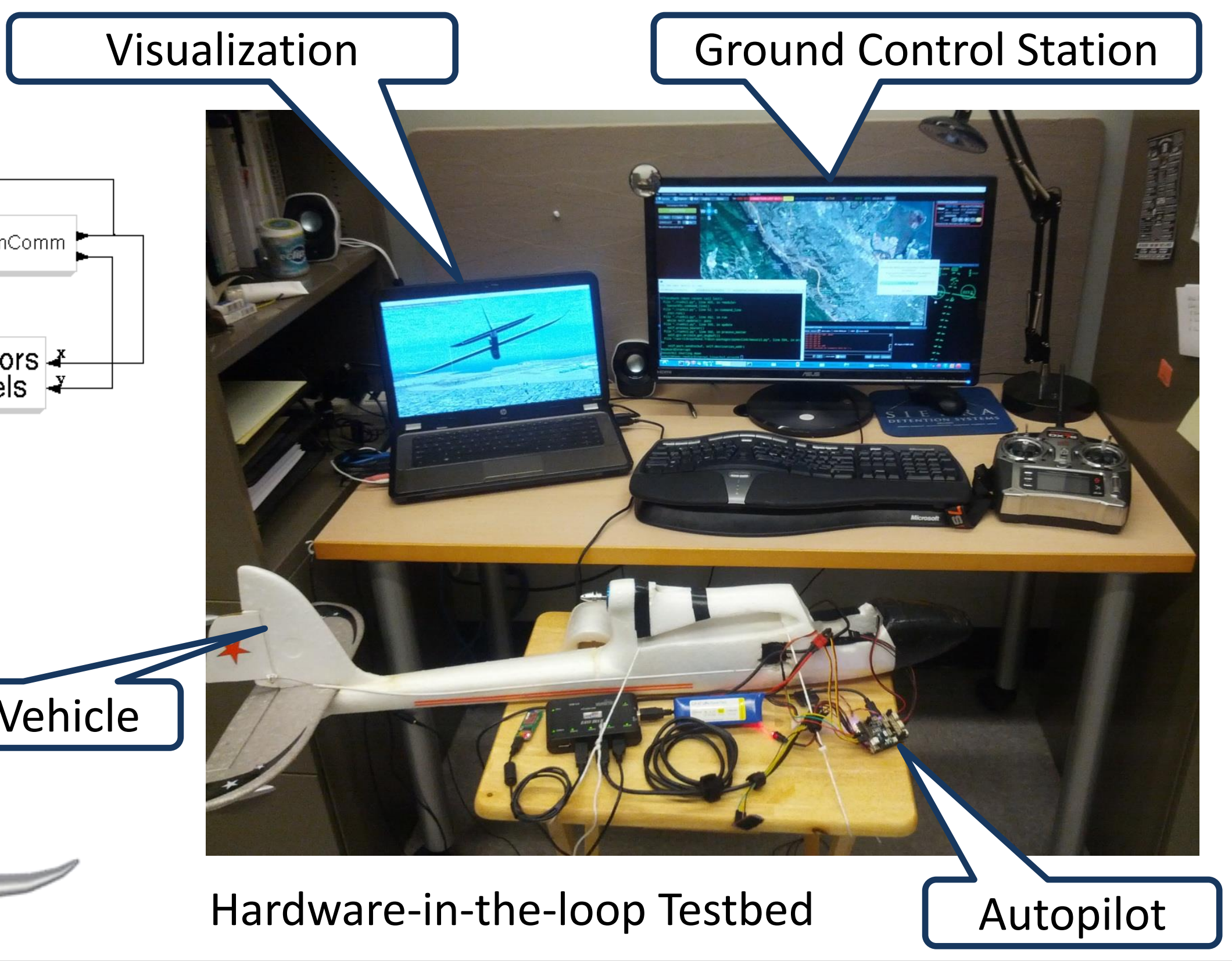


Software-in-the-loop Testbed



UAS Autopilot Model



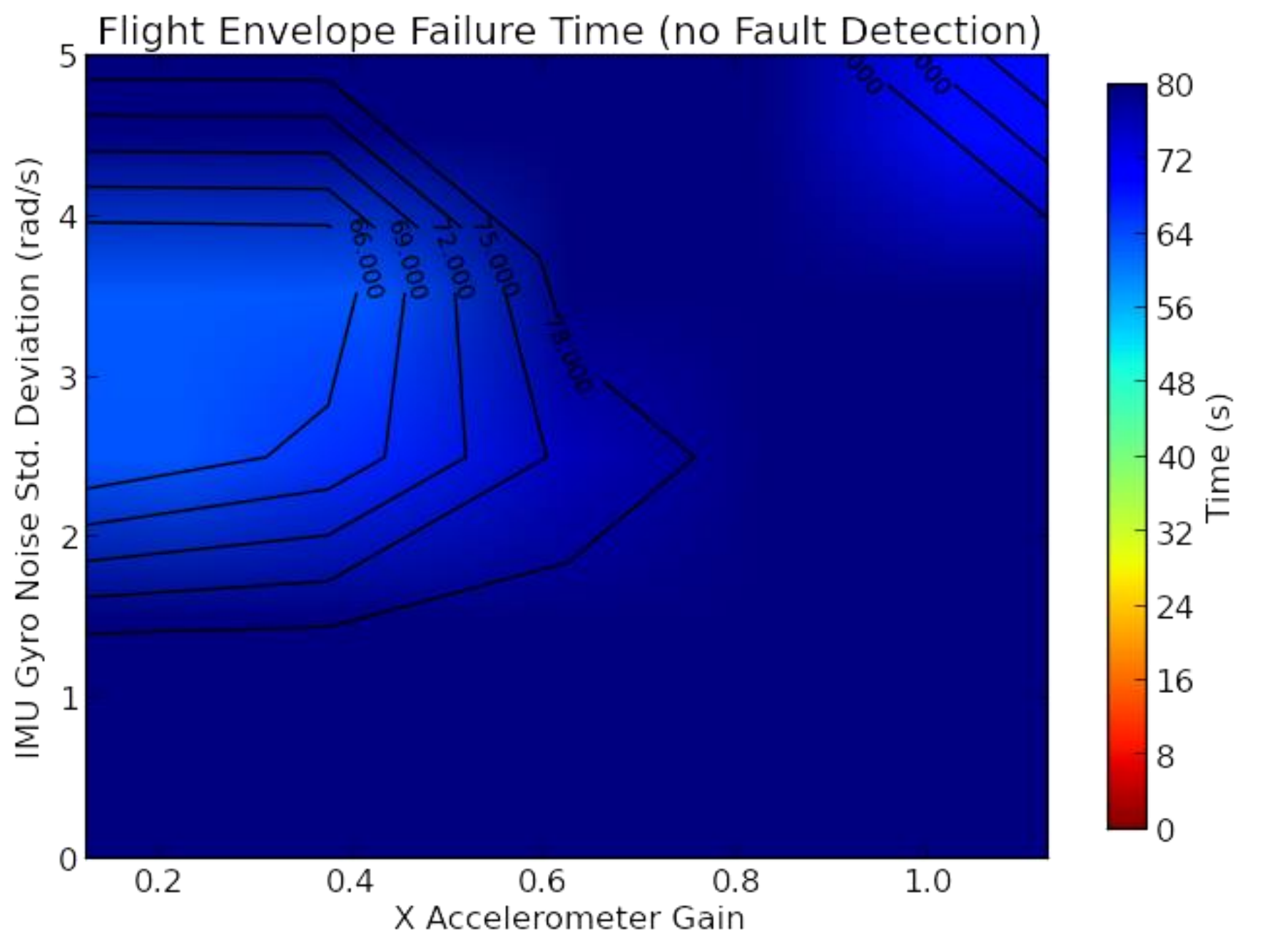


Hardware-in-the-loop Testbed

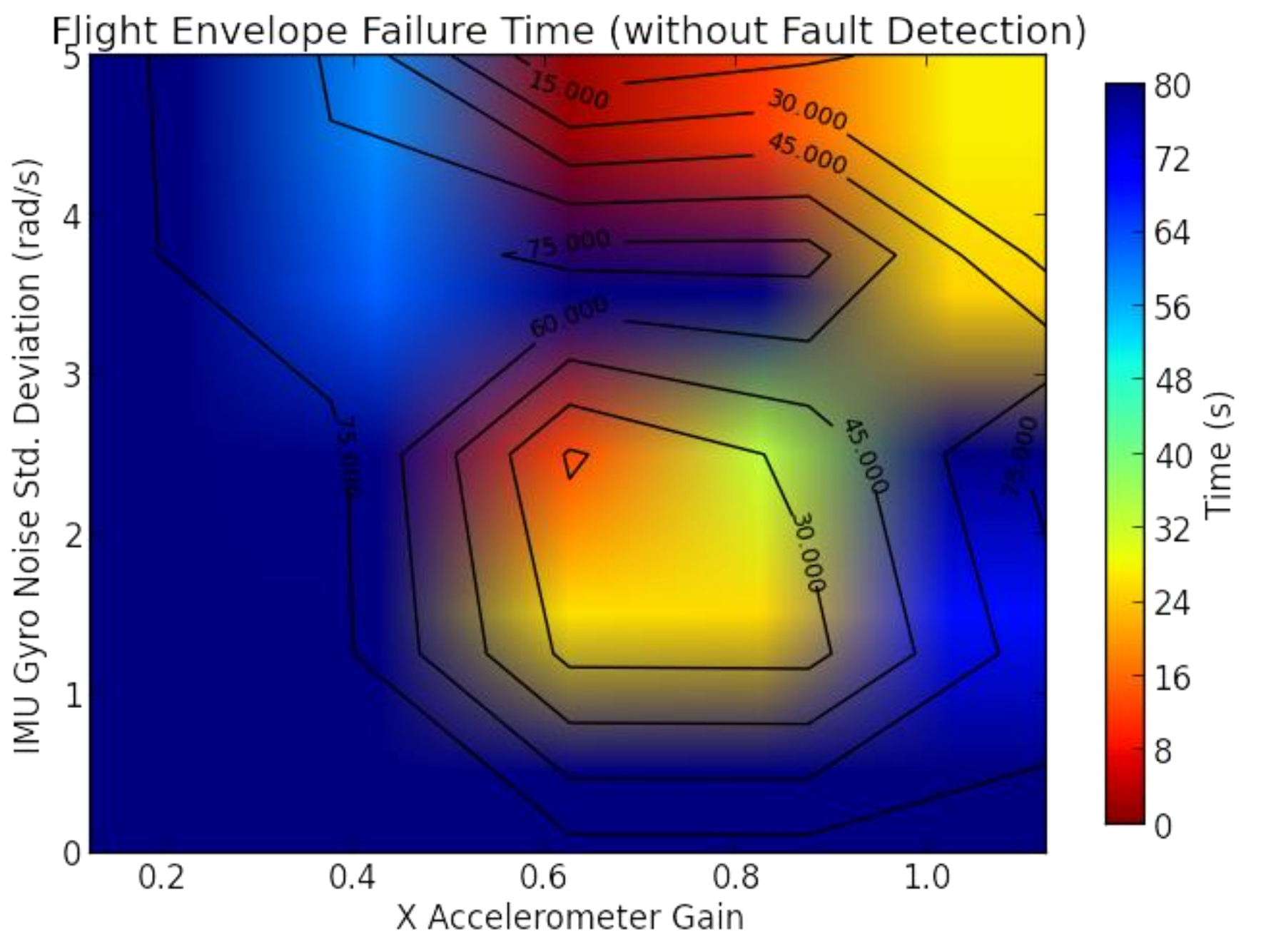
Motivating Examples

- Complete command and control capability of Landsat 7 and Terra AM-1, two Earth observation satellites operated by USGS and NASA, respectively, was obtained by unknown foreign agents for several minutes at a time in 2008.
- The US Air Force reported malware infections in UAS control system computers at Creech AFB in 2011. The infection was incidental and did not cause any reported damage, but demonstrates a vulnerability.

Results

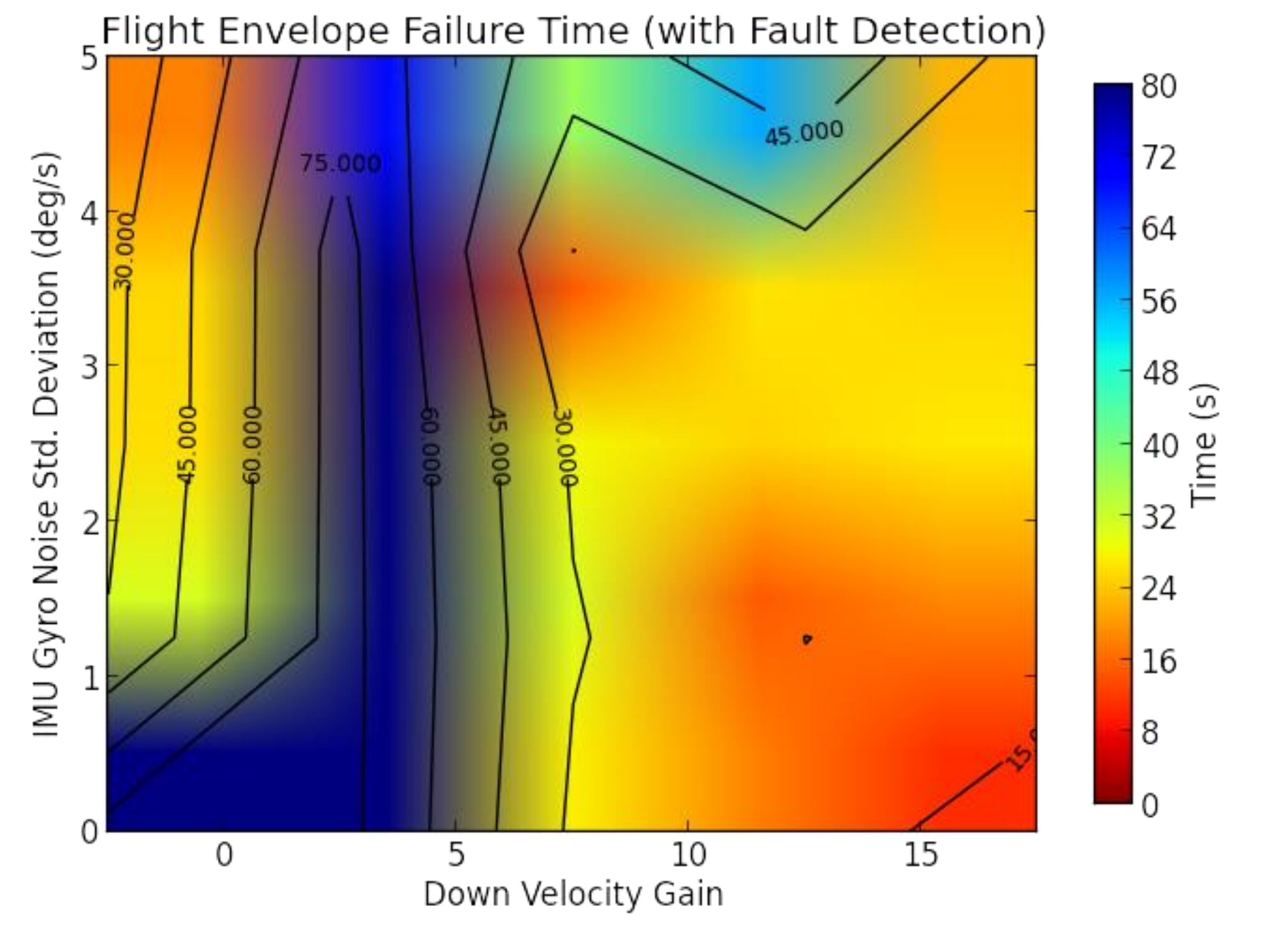


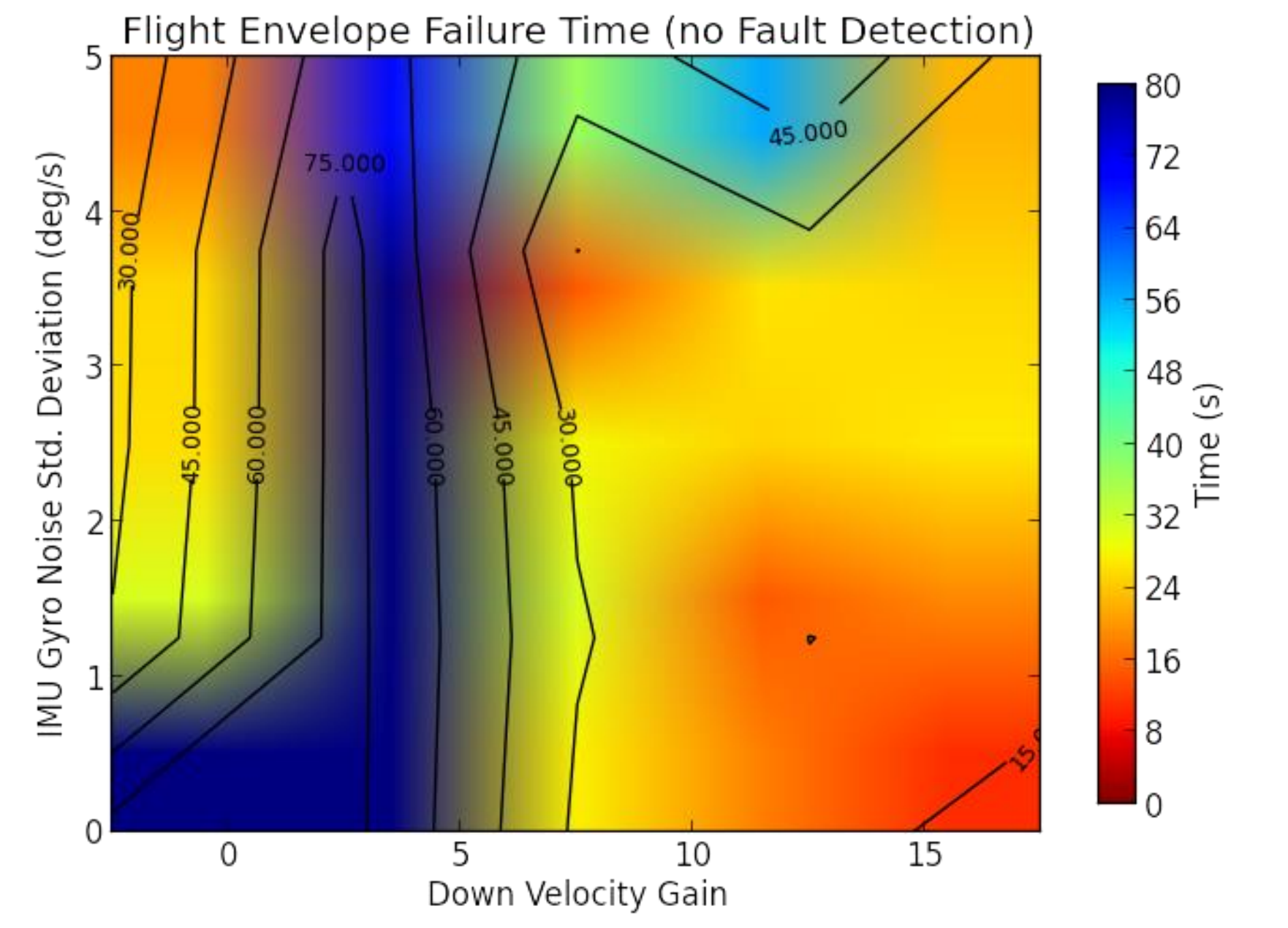
Software Simulation

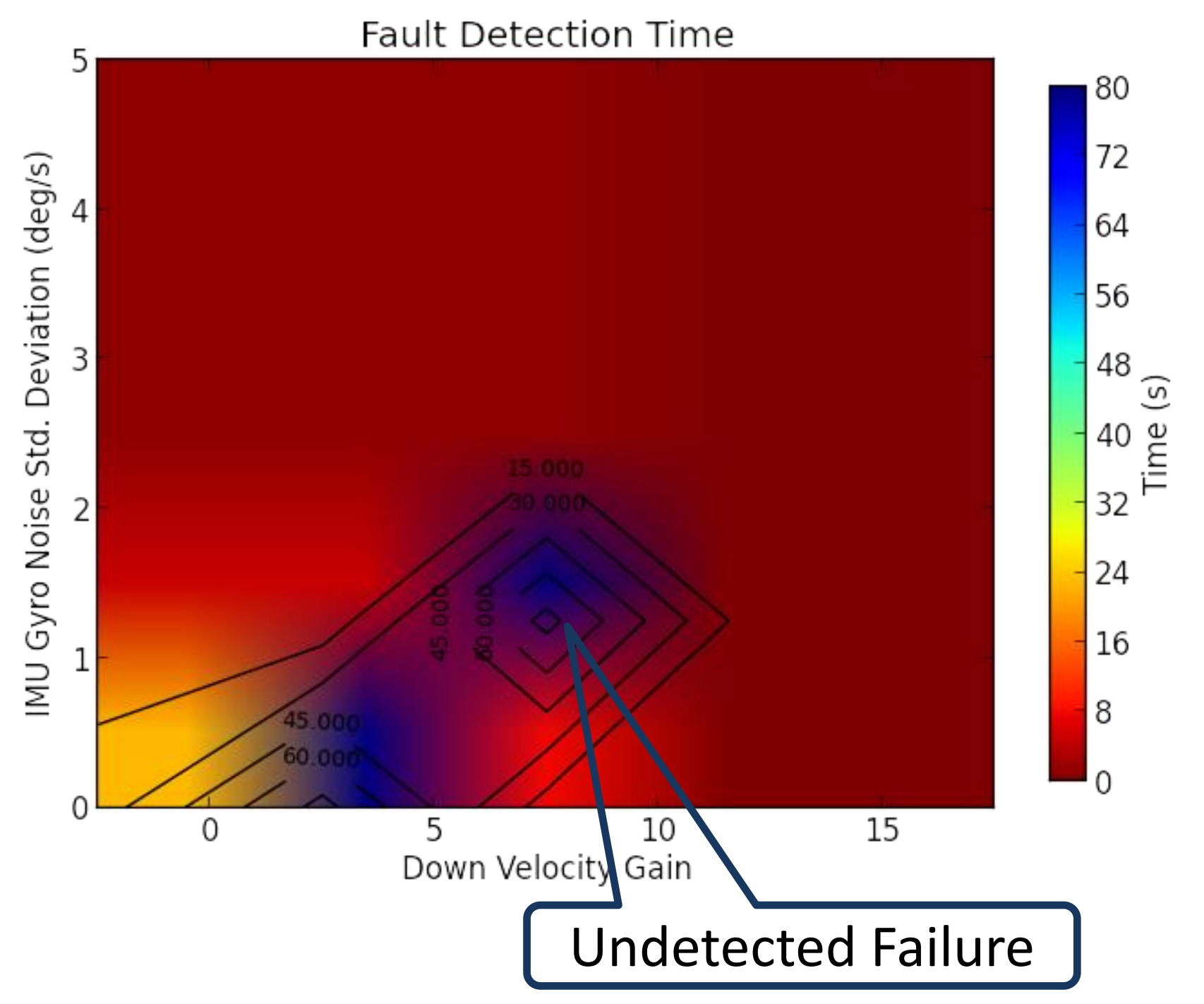


Hardware Simulation

The above figures show the flight envelope failure time for the software and hardware simulation of a cyberattack that inserts Gaussian noise into the IMU gyroscope measurements and adds a gain to the x accelerometer. The two simulations have some pronounced differences but share are some similarities as well such as the failure region near the top right corner of the plot and a separate failure region in the center of the plot. The notable differences however show the necessity of using a hardware based simulation that does not abstract away much of the system dynamics.







The above figures show the flight envelope failure time for the software simulation of a cyberattack that modifies the down velocity gain and varies the deviation of the gyroscope noise for the case when a fault detection system is used and when it is not. The results clearly show that the fault detection system is unable to mitigate the cyberattack in this case, as indicated by the identical system responses when the fault detection system is enabled and disabled. The figure to the left shows that the fault detection system is unable to detect these attacks with the failure region showing no fault detection before the flight envelope is violated.

We'd like to acknowledge that this project has been supported by Sypris Electronics and thank Dr. Hal Aldridge for his valuable discussions and support.