# Designing for Security: A Cybersecurity Introduction for Aerospace Education

Karl Roush[1]

*Aerospace Systems Design Laboratory, Georgia Institute of Technology, Atlanta, GA 30332*

**The world is becoming increasingly digital-- the integration of communications, sensors, and data collection is becoming more and more prevalent in the Aerospace sector. Furthermore, the Aerospace sector plays a large role in connecting the world through air transportation networks, navigation satellites, information services, weather/environmental monitoring, and much more. Preventing disruptions to said networks is of utmost concern, with stability being a key factor in their construction. Recently, there has been a shift in computer science to push for security at a fundamental design level rather than a late-stage development consideration. In contrast, the Aerospace industry is only just now seeing a push to translate existing standards and implementing various cybersecurity practices. Even more troubling, many students' first exposure to aerospace concepts in their undergraduate studies neglects to mention cybersecurity as a consideration. This paper serves as a cursory introduction of topics with the purpose of exposing the next generation of aerospace engineers to key areas where cybersecurity concepts will prove essential.**

## I. Nomenclature

| | | |
|---|---|---|
| *AI/ML* | = | Artificial Intelligence/Machine Learning |
| *KFC* | = | Kentucky Fried Chicken, a restaurant chain |
| *MITM* | = | Man in The Middle |
| *DDoS* | = | Distributed Denial of Service |

## II. Introduction

The world is becoming increasingly connected. Within the Aerospace sector, the integration of communications, sensors, and data collection (often referred to as "Digital Enterprise" or "Digital Engineering") is starting to become widespread. However, such progress is not without its challenges [1]. As the number of connected systems grows, so too does the potential for a cyber-attack [2], as evidenced by a leak of the Boeing 787 source code [3].

Currently, much of the focus in the aerospace literature is on porting existing standards, recommendations, and practices from other fields to aerospace. There is simply a vacuum in the space regarding core cybersecurity principles [4]. That is not to say that members of the field are ignorant of the threat-- indeed, there has been a growing push for cyber risk management processes [5] as well as in the field risk assessments [6].

Although there are mitigations and protections for systems after development, the best way to protect a system is to consider the cybersecurity aspects early in the design phase [7]. As such, aerospace engineers should be exposed to these concepts early on in their career as they learn to implement development processes.

Undergraduate education in aerospace engineering often does not touch on these cybersecurity-related concepts. Often, these topics are relegated to a graduate level in computer science-- in fact, the undergraduate CS degree in "Information Internetworks" at the Georgia Institute of Technology only makes a passing mention of cybersecurity [8]. Given the growing importance of cybersecurity, it is paramount that students have some knowledge of it. This paper serves as a cursory introduction of topics, with the purpose of exposing the next generation of aerospace engineers to key areas where cybersecurity concepts will prove essential.

[1] Graduate Research Assistant, Aerospace Systems Design Lab, Georgia Tech, AIAA Student Member

## III. Autonomous Navigation

### A. Definition

Autonomous navigation simply refers to the process by which a vehicle navigates with minimal or no human intervention. The most common instance of this is self-driving cars. Often these systems operate using cameras assisted by machine learning models to “understand” the environment and act accordingly.

### B. Potential Attacks

Because these autonomous navigation systems often rely on cameras for sensory input, attacks often focus on the visual medium with the purpose of disrupting image recognition. Furthermore, the decisions made by the system often utilize a machine learning model. It has been documented that these models can be deliberately misled in several methods, but for the sake of brevity this paper will only discuss two:

1. Adversarial objects- e.g., printing a logo that looks like a stop sign, modifying the object at an interpretation level.
2. Environmental modification- e.g., modifying a sign via stickers or graffiti, modifying the object at a physical level.

Both attacks present threats to the system since they modify the input to the navigation system, in turn modifying the system’s behavior beyond that which is expected.

#### *1. Adversarial Objects*

Consider the first case of adversarial objects- a KFC logo which looks vaguely like a stop sign. A human can clearly tell that it is merely a logo with some distortions. However, to the machine learning system driving the navigation, it appears as a stop sign. Clearly this is detrimental since the vehicle would stop when it should not.

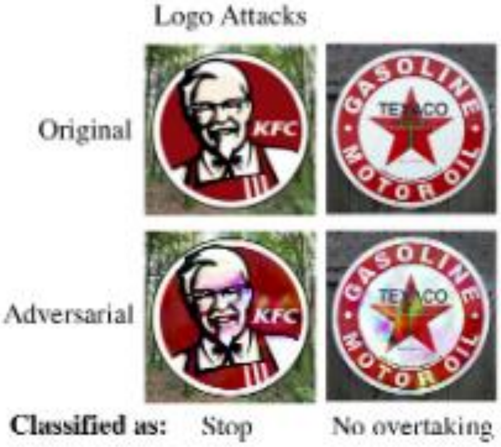

**Fig. 1 Out-of-distribution attack using adversarial objects [9]**

Although humans can distinguish the difference between the original and adversarial images, machine learning algorithms cannot.

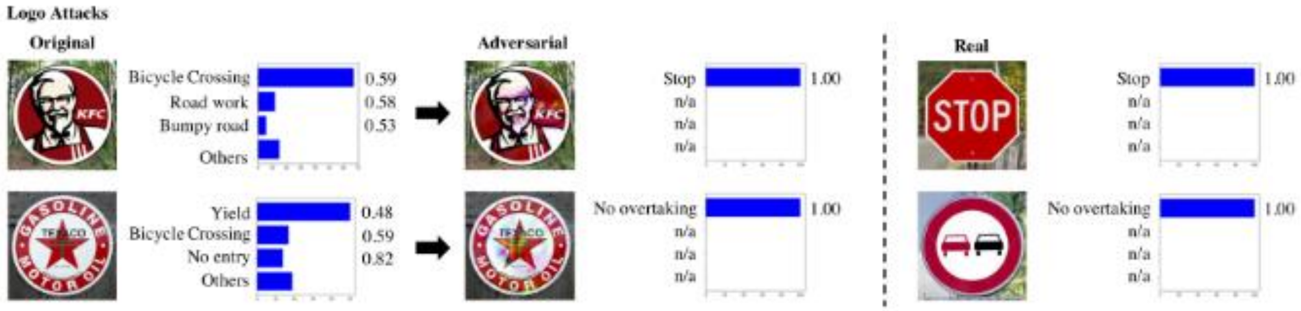

**Fig. 2 Adversarial signs are misclassified with high confidence [9]**

Abstracting this attack to aerospace is relatively simple. Many entry, descent, and landing (EDL) systems support computer assistance. An adversary could modify runway indicators, throwing off the landing. Currently, the pilot could simply override the autonomous navigation system, but as automation increases, one could see this attack as an area for concern.

### ***2.*** *Environment Modifications*

Now consider the second attack: environmental modification. In our everyday lives, we are used to environmental variability. Even with graffiti on it, we can clearly recognize a stop sign. In contrast, a machine learning model is looking for a specific type of stop sign (clean, clearly marked, bright red, etc.). By adding trivial modifications to the stop sign (tape in the below image, right), the model no longer recognizes the sign. The danger of this attack is subsequently obvious- if the underlying machine learning model cannot recognize environment cues, then the autonomous navigation system will not behave accordingly in said environment.

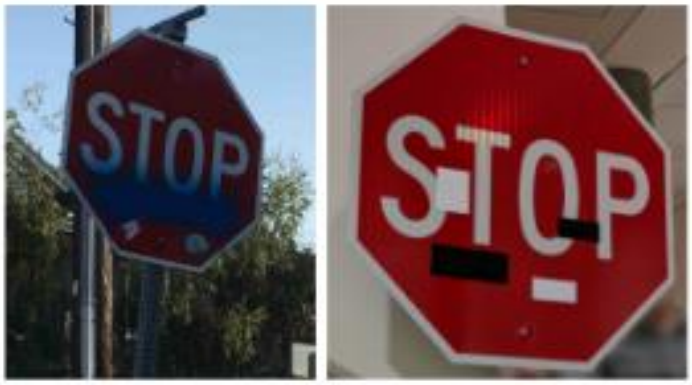

**Fig. 3 Physical environment modification on a stop sign [10]**

Abstracting this attack to aerospace is relatively simple. The same concept of fooling automated systems as in the first attack still applies. However, this second attack is simpler in that it requires minimal setup and almost no knowledge of the target system. Additionally, the attack itself is not as noticeable to a human user, whereas the adversarial object attack is more apparent.

## C. Mitigation and Counters

Since these attacks are limited to physical modifications, their effects are less so when compared to direct attacks, e.g., hijacking the navigation system itself. Technically, both the adversarial object and environment modification attacks exploit the underlying machine learning model’s susceptibility to noise. As such, this implies future defenses should not rely on physical sources of noise as protection against physical adversarial examples [10].

At a fundamental level, these attacks are exploiting the visual aspect of autonomous navigation systems. Therefore, aerospace engineers should not only seek to protect that specific avenue of attack, but also consider integrating a wider range of sensors into their design (i.e., sensor fusion). Of course, every additional sensor and integration adds further risk, so additional exploration and consideration is encouraged.

# IV. Communications

## A. Definition

Communications are the lifeblood of any interconnected system. The simplest definition of such is simply the process of relaying information from one place to another. For example, consider the case of a connected space system below. Each line represents a communications path and therefore a place for an attacker to exploit.

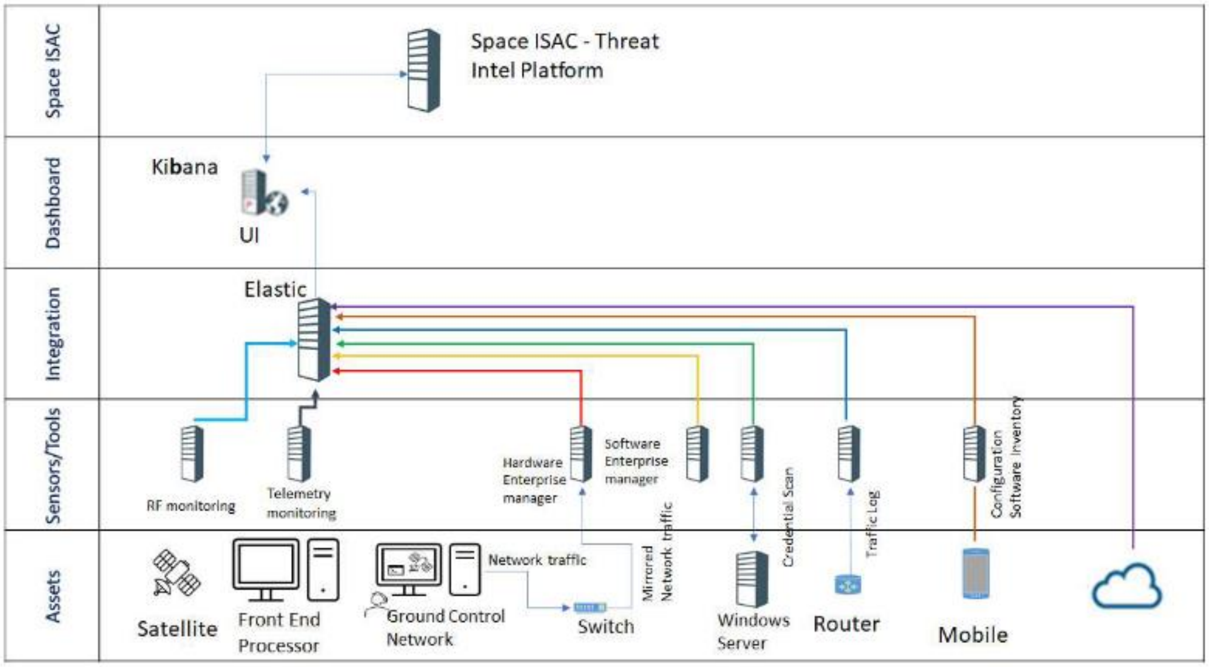

**Fig. 4 Monitoring architecture for notional space operator organization [11]**

## B. Potential Attacks

Although there are many possible attacks against communication systems and protocols, the goal of this paper is just to serve as a "tasting menu" of sorts, acting as a first exposure for students. For the sake of only three attacks are discussed, listed below.

1. Eavesdropping
2. Man in the middle (MITM)
3. Distributed Denial of Service (DDoS)

Each of the attacks is described in detail below.

### *1. Eavesdropping*

Data integrity of the information transmitted between components requires data confidentiality, availability, and integrity. The first attack, eavesdropping, is the unauthorized interception or sniffing of a conversation, communication, or data transmission [12]. The risk of this attack to aerospace applications should therefore be apparent. For example, consider a fighter aircraft transmitting target coordinates. Should that communication be intercepted, it could have disastrous consequences.

### *2. Man in the Middle (MITM)*

The second attack is an extension of eavesdropping. However, in this case, the attacker sits between the communicating parties. In this position, they are privy to all sides of the conversation. Similar to the previous fighter example, this attack could prove even worse as the attacker could feed parties incorrect information or simply block communications.

#### 3. *Distributed Denial of Service (DDoS)*

On the note of blocking communications, the last attack does exactly that. Essentially, a DDoS attack stays true to its name-- it blocks service using a distributed network. The purpose of the attack is to degrade or block the availability of services to users. Botnets (a large number of often hacked devices, united for a single purpose) are commonly used to conduct DDoS attacks against networks and services [12]. Given the connected nature of airports, one could imagine a situation where the flight scheduling software gets DDoS'd and air traffic controllers are no longer able to coordinate flights.

### C. Mitigation and Counters

The first two attacks rely on obtaining access to the communications. Therefore, the best defense is to secure the network. This is done through the usage of virtual private networks (VPNs), monitoring network traffic, and extensive filtering.

In contrast, DDoS attacks are harder to counter and are much more prevalent. Just earlier this year (February 2021), a report from FS-ISAC, a cyber intelligence sharing community focused on financial services, indicated that over 100 financial services were targeted by DDoS attacks conducted by a single threat actor in just 2020 [13]. The best counter to this kind of attack is to leverage services provided by Content Delivery Networks (CDNs) or specific filtering services like Cloudflare.

By far, attacks against communications systems and protocols are the most common simply due to the sheer number of them. There are a great many possible types of attacks against these systems and, given the interconnectivity of aerospace systems, it is paramount that aerospace engineers consider how to secure those communications. Given the massive size of this area of attacks, it is encouraged that the reader explores Freeman & Garcia's "A Survey of Cyber Threats and Security Controls Analysis for Urban Air Mobility Environments" listed in reference [12].

## V. Control Systems

### A. Definition

Control systems broadly refer to systems related to regulating the behavior of the parent system. As an example, the flaps on an airplane are part of the control system. Often there is an overlap between control systems and communications systems, with the latter conveying information to the former. With this in mind, only control-specific attacks will be discussed in this paper.

### B. Potential Attacks

Although control systems are of critical importance, the attacks against them are relatively simple. Again, there are many possible attacks. The ones below are but a small sample of the possibilities [14].

1. Sensor modification
2. Fake command data

Each of the attacks is described in detail below.

#### 1. *Sensor Modifications*

The first attack involves modifying the output of a sensor. As an aerospace example, consider an attacker that has control over the angle of attack sensor. The attacker could output sensor data saying the aircraft was at an angle of 15 degrees instead of the actual angle of -15 degrees. Such a result could cause the plane to pitch downwards to "fix" the angle of attack reading but would instead put the plane into a dive.

#### 2. *Fake Command Data*

Fake command data is even more straightforward. Instead of the operator's commands, the attacker inputs their own commands (similar to a MITM attack). Consider the case of a commercial quadcopter. The user wants to take a photo of a tree, so they command the drone to fly up. However, the attacker commands the drone to fly forward into the tree, crashing the aircraft. While a rather trivial example, one could see the potential danger, especially around high traffic areas like an airport.

### C. Mitigation and Counters

Because attacks against control systems often involve the attacker gaining access to a system, the best counter is to protect said systems, whether it be through firewalls, restricting access, or some other method. However, assuming an attacker manages to gain control of a control system, there are two main techniques to reduce their effects: sandboxing and redundancy.

Sandboxing refers to the concept where certain systems are limited in what they can access. Translating this to an aerospace case, consider the gimbal system of a satellite controlling its orientation. The gimbal system does not need access to the main power controls of the satellite, so it is "sandboxed" such that the gimbal system does not interact with the power supply controls.

Redundancy refers to the duplication of critical components or functions of a system with the intention of increasing its reliability. For example, consider a sensor on a helicopter measuring the main shaft speed, compromised by an attacker. If there was only one such sensor, then the attacker could easily make modifications. However, if there were three shaft speed sensors and the attacker controlled one, the result would be overridden by the other two, making their efforts moot.

## VI. Conclusion

Cybersecurity is a fast-growing field, with the US Bureau of Labor Statistics predicting a 39% growth between 2019 and 2029 (much higher than the average of 4%) [15]. Such growth is unsurprising when considered against the growing connected nature of today's modern world. However, much of the focus in the aerospace sector is on porting existing standards, recommendations, and practices from other fields to aerospace applications. Although there are mitigations and protects for systems after development, the best way to protect a system is to consider the cybersecurity aspects early in the design phase [7]. As such, aerospace engineers should be exposed to these concepts early on in their career as they learn to implement development processes.

The overarching goal of this paper is to serve as a cursory introduction of topics for the next generation of aerospace engineers to key areas where cybersecurity concepts will prove essential. There is a vast area of cybersecurity of concepts, far beyond what can be covered in a short paper-- readers are encouraged to explore this topic in further detail. AIAA themselves have also advocated for additional progress in several aspects of cybersecurity for aerospace applications-- this is detailed in "Aerospace Cybersecurity and Safety" [16]. For the more technical-minded reader, there are more detailed analyses of the threat landscape in the report "Cyber Threats to The Aerospace and Defense Industries" from FireEye [17]. Additionally, the Open Web Application Security Project (OWASP) provides a great starting place for any reader interested in cybersecurity, regardless of their experience level.

## Acknowledgments

The author would like to thank the fellow students Ian Marks and Mollie Johnson for helping proofread this paper, effectively translating incoherent thoughts into concise, human readable concepts.

## References

[1] Yusuf Ogun Kargin, Ashley A. Barnes, O D. Uysal, Olivia J. Pinon-Fischer, Michael G. Balchanos, Dimitri N. Mavris, Melissa Hughes, Jason LaJeunesse, Alexander Karl, and John F. Matlik. "Digital Enterprise Across the Lifecycle," AIAA 2021-0240. AIAA Scitech 2021 Forum. January 2021. doi.org/10.2514/6.2021-0240

[2] Sheema Mirchandani and Sam Adhikari. "Aerospace cybersecurity threat vector assessment," AIAA 2020-4116. ASCEND 2020. November 2020. doi.org/10.2514/6.2020-4116

[3] HackersOnBoard. (2019, October 5). Black Hat USA 2018 - Last Call for SATCOM Security [Video]. YouTube. https://www.youtube.com/watch?v=CvlCt6a17ho

[4] Gregory Falco. "The Vacuum of Space Cyber Security," AIAA 2018-5275. 2018 AIAA SPACE and Astronautics Forum and Exposition. September 2018. doi.org/10.2514/6.2018-5275

[5] Jeremy L. Pecharich, Kendra Cook, Wesley Walker, Michel D. Ingham, Kymie Tan and Stephen Watson. "Cyber Risk Management Process for Space Missions," AIAA 2020-4114. ASCEND 2020. November 2020. doi.org/10.2514/6.2020-4114

[6] Krishna Sampigethaya. "Aircraft Cyber Security Risk Assessment: Bringing Air Traffic Control and Cyber-Physical Security to the Forefront," AIAA 2019-0061. AIAA Scitech 2019 Forum. January 2019. doi.org/10.2514/6.2019-0061

[7] Thomas Llanso and Dallas Pearson. "Achieving Space Mission Resilience to Cyber Attack: Architectural Implications," AIAA 2016-5604. AIAA SPACE 2016. September 2016. doi.org/10.2514/6.2016-5604

[8] Information Internetworks Degree Program. College of Computing, Georgia Institute of Technology (2021). Retrieved 18 February 2021, from https://www.cc.gatech.edu/information-internetworks

[9] Sitawarin, C., Bhagoji, A. N., Mosenia, A., Chiang, M., & Mittal, P. (2018). Darts: Deceiving autonomous cars with toxic signs. arXiv preprint arXiv:1802.06430.

[10] Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., ... & Song, D. (2018). Robust physical-world attacks on deep learning visual classification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 1625-1634). DOI: 10.1109/CVPR.2018.00175

[11] Theresa Suloway, Scott Kordella and Samuel S. Visner . "An attack-centric viewpoint of the exploitation of commercial space and the steps that need to be taken by space operators to mitigate each stage of a cyber-attack," AIAA 2020-4015. ASCEND 2020. November 2020. doi.org/10.2514/6.2020-4015

[12] Kenneth Freeman and Steve Garcia. "A Survey of Cyber Threats and Security Controls Analysis for Urban Air Mobility Environments," AIAA 2021-0660. AIAA Scitech 2021 Forum. January 2021. doi.org/10.2514/6.2021-0660

[13] Fs-Isac. (2021, February 09). More than 100 financial services firms hit with ddos extortion attacks. Retrieved February 18, 2021, from https://www.fsisac.com/newsroom/globalleaders

[14] Kevin Yang, Jeremy Price, Robert H. Klenke and Matthew Leccadito. "Implementation of a Hierarchical Embedded Cyber Attack Detection system for sUAS Flight Control Systems," AIAA 2021-0038. AIAA Scitech 2021 Forum. January 2021. doi.org/10.2514/6.2021-0038

[15] Information Security Analysts. (2021). Retrieved 18 February 2021, from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[16] AEROSPACE CYBERSECURITY AND SAFETY. (2021). Retrieved 18 February 2021, from https://www.aiaa.org/docs/default-source/uploadedfiles/issues-and-advocacy/key-issues/aerospace-cybersecurity-and-safety.pdf?sfvrsn=818c1784_0

[17] CYBER THREATS TO THE AEROSPACE AND DEFENSE INDUSTRIES. (2021). Retrieved 18 February 2021, from https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-aerospace.pdf