Astronautics

VICE

Vulnerability Identification & Continuous Evaluation

Cybersecurity risks evolve over time, especially for long-lived aerospace products. Aerospace companies need the most advanced toolsets to assess and manage cybersecurity risks for their products.

Astronautics' VICE toolset can be leveraged to automatically process and manage all reported vulnerabilities across software, hardware, and firmware throughout the entire product lifecycle.

Aircraft and aircraft product cybersecurity risk assessment is most effective when treated as a continuous process.

VICE automates the risk-based approach of gathering and assorting vulnerabilities that account for operational use, criticality, safety, and mission impact, rather than relying on point-in-time or checklist-based assessments.

WHAT MAKES OUR CYBERSECURITY APPROACH DIFFERENT

Lifecycle-focused, not point-in-time

We continuously evaluate cybersecurity vulnerabilities during development, integration, production, and in-service operation.

Applies across the full product stack

The VICE tool covers software and firmware, hardware and electronic components, interfaces, integrations, and system architectures, and supply chain and supporting tools.

Risk evaluated in operational context

We assess not just whether a vulnerability exists, but how the product is configured and used, what functions it supports, and what the real-world impact would be.

Safety & mission impact are core considerations

Cyber findings are evaluated for potential effects on safety, reliability, and mission performance—not just data protection.

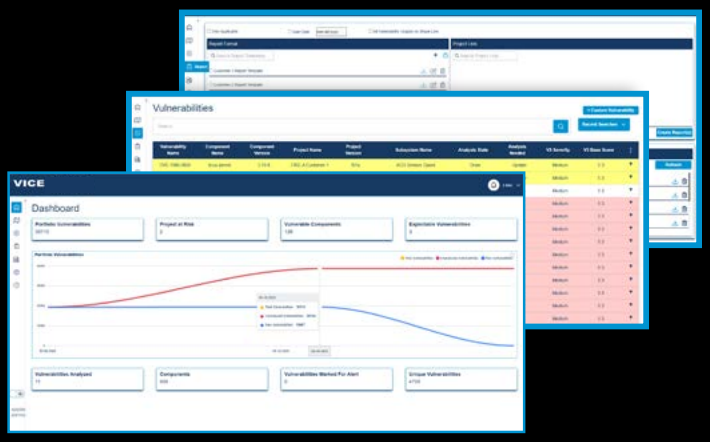
Advanced cybersecurity toolset

Our cybersecurity toolsets are implemented by engineers with deep experience in aerospace systems, safety-critical architectures, and regulated development environments.

This experience allows vulnerabilities to be evaluated in the context of real-world system behavior, certification constraints, and operational risk—not in isolation.

REGULATORY ALIGNMENT

Our VICE approach aligns with recognized cybersecurity and aerospace guidance, including NIST cybersecurity frameworks and airworthiness security practices such as DO-326A/ED-202A and DO-355A/ED-204A. This alignment supports both certification activities and continuing operational assurance without disrupting safety or availability.



For more information, contact: busdev@astronautics.com | +1.414.449.4000

HOW VICE WORKS

Astronautics' VICE toolset proactively identifies and mitigates cybersecurity risks through a streamlined process:

1. Identify

Vulnerabilities are continuously and automatically identified from public and private sources, manufacturer inputs, testing activities, and internal analysis.

2. Evaluate

Each vulnerability is evaluated to determine if applicable and exploitable, and then the degree of impact the vulnerability may have on the system.

3. Prioritize

Vulnerabilities are prioritized based on the evaluation process and their potential to create an unacceptable event that could compromise mission-critical systems.

4. Alert & Mitigate

The customer is alerted of vulnerabilities with the potential to create an unacceptable event, and a patch or procedure for mitigating the vulnerability is provided.

5. Verify & Monitor

A full vulnerability report is automatically generated for the avionics system, including all alerts, mitigations, and patches.

WHAT THIS MEANS FOR YOU

- Cybersecurity tightly integrated with safety and mission assurance
- Clear, risk-based decision making
- Reduced lifecycle risk for long-lived aerospace products
- Confidence that cybersecurity is actively managed—not static

VICE ensures cybersecurity risk is continuously understood, prioritized, and controlled—across systems, over time, and in real-world operation.

www.astronautics.com

Phone: +1.414.449.4000
busdev@astronautics.com

135 W Forest Hill Avenue
Oak Creek, WI 53154 USA

Astronautics

CYBERSECURITY