

Securing Avionics Software for Safety & Certification

ACHIEVING DO-178A SOFTWARE ASSURANCE

Modern aircraft rely on highly integrated, software-driven avionics systems that must operate safely and reliably over decades. Although vulnerabilities can emerge, avionics software cannot be easily patched or updated with aircraft in service. Manufacturers must ensure software is resilient to conditions—including cybersecurity vulnerabilities—that impact the safe operation of aircraft. This makes software visibility, integrity, and lifecycle control critical to certification and ongoing safety.

Demonstrating compliance with DO-178C requires extensive, repeatable analysis and documentation across the software lifecycle. Automated tools—when qualified under DO-330—generate consistent software visibility, verification evidence, and traceability artifacts, helping accelerate certification while maintaining confidence in safety assurance.

DO-178C& 356A: WHAT MANUFACTURERS MUST DEMONSTRATE

Avionics manufacturers and suppliers must align with DO-178C to ensure airborne software is developed, verified, and maintained to the highest levels of safety assurance. This means OEMS are expected to demonstrate:

- A clear software baseline, including requirements, design, and all included components
- Verified software behavior through testing, validation, and verification
- Full traceability between requirements, code, and verification
- Controlled configuration and change management across the software lifecycle

For DO-356a, which is applicable when the manufacturer is looking to get a type certification:

- Each vulnerability, even in COTS, must be evaluated for its “exploitability” metrics (attack complexity, attack vector, scope - and our mitigations drastically reduces the risk
- It also has an objective to correct any vulnerabilities or justify them - and we can be a justification why memory vulnerabilities are not a risk to the system

HOW RUNSAFE SUPPORTS AVIATION REGULATIONS

RunSafe, as a DO-330 qualified tool, strengthens how manufacturers meet DO-178C by improving software visibility, integrity, and certification evidence—without requiring source code changes.

DEFINE TRUSTED SOFTWARE

Establish what the software is, what it does, and what is included

- SBOMs with full visibility into software components and dependencies
- Identifying vulnerabilities and software risk
- Understanding of software composition and attack surface

ASSURE SOFTWARE INTEGRITY

Build and rigorously verify that software behaves as expected

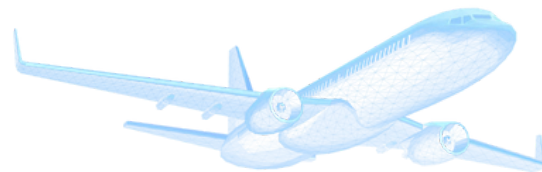
- Protects software by randomizing memory and reducing exploitability at runtime
- Verifies with analysis of a build-time SBOM and mapping to vulnerabilities and risk
- Validation and reporting for certification evidence

We also shine in DO-356A objective for Continued Security Effectiveness. This requirement asks for a vuln management system and a security incident response, which we can make easier.

MAINTAIN & PROVE TRUST

Ensure software remains controlled, traceable, and certifiable

- Tracking of software changes and dependencies across builds
- Tracing and reproducing software builds and their SBOMs
- On-demand reporting to support certification and compliance



A STRONGER CYBERSECURITY POSITION

RunSafe provides technical evidence and reporting that supports these elements, including artifacts supporting the Certification Evidence Package required for safety systems.

Component	Supported by RunSafe
Software Planning	**
Requirements Development	✓
Software Design	✓
Implementation	✓
Verification and Testing	✓
Structural Coverage Analysis	**
Configuration Management	✓
Certification Evidence Package	✓

** Subject to RunSafe customers' practice

WHY RUNSAFE?

Avionics software must remain safe and certifiable for decades—yet vulnerabilities can emerge at any time and cannot always be patched in-service. RunSafe helps manufacturers by making vulnerabilities non-exploitable through memory randomization and runtime protections, preventing them from impacting system behavior.

By combining this with full software visibility through SBOMs and trusted certification evidence, RunSafe strengthens both software safety assurance and in-service resilience under DO-178C, with the added benefit of tool-qualified outputs that support certification activities.

ABOUT RUNSAFE SECURITY, INC.

RunSafe Security proactively protects embedded software for both commercial and defense deployments across critical infrastructure, with comprehensive risk identification, protection, and monitoring, ensuring robust, continuous security without affecting performance. Headquartered in McLean, Virginia, with an office in Huntsville, Alabama, RunSafe Security's customers span the aerospace, defense, energy, industrial, and national security verticals. Learn more at: RunSafeSecurity.com.