

## Ampex Patches & Updates Your TuffServ / TuffCORD / miniRv2 Software

Ampex now offers a cybersecurity and software update service for our TuffServ, TuffCORD, and miniRv2 products. If you own one of these systems, Ampex will help you stay on top of cybersecurity enhancements, patches, interoperability issues, bugs, and latent vulnerabilities in the Ampex Common Compute Environment (ACCE), including Red Hat Enterprise Linux and other third-party software (drivers, etc.).

## Cyber Threats to Aerospace and Ground Vehicles are Growing

- Onboard data bus intrusion
- Malware injected via RF sensors
- Compromised vehicle datalinks
- Ground support computer attack vectors

## Keeping Your Ampex Systems Secure and Up-to-Date

Avoid the worry and hassle of ensuring your systems remain secure and up-to-date! The decision to install each update is up to you, but if you choose, Ampex will assume the responsibility of performing the updates or providing you with the requisite update files on a monthly or quarterly basis tailored to your mission needs. This includes working with you to assess the implications of applying or deferring each patch.

As a value-added feature, Ampex can test the updates in-house on a hardware / digital twin of your existing baseline prior to shipping. The periodic updates include comprehensive documentation for service history and security compliance.

- Hassle-free cyber & interoperability updates for your Ampex systems
- Patches, STIGS, vulnerabilities, bugs
- ACCE to include Red Hat Enterprise Linux OS
- In-house testing on hardware / digital twin
- Monthly or quarterly updates, compliance documentation

