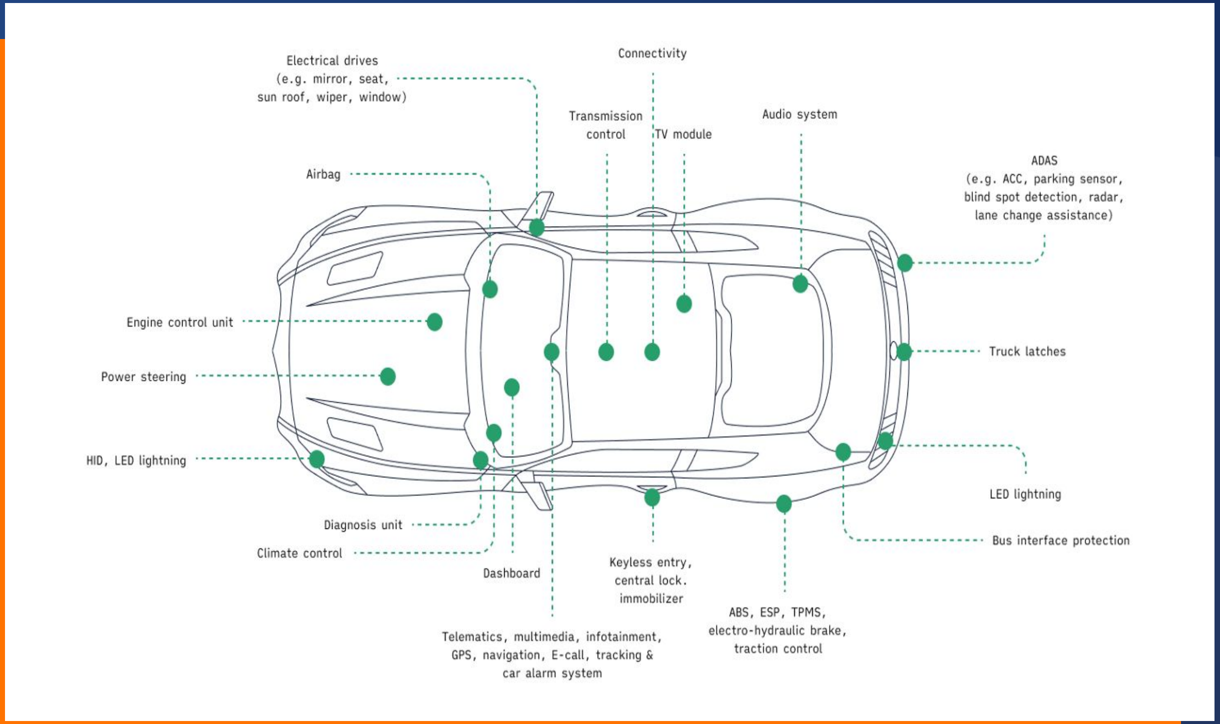
RUNSAFE SECURITY | Critical software | RUSTIC SECURITY LLC DESIGN, IMPLEMENT, VERIFY

ENSURING SAFETY AND SECURITY:

Navigating Cyber Challenges in Connected Cars and Autonomous Vehicles

2024 Automotive Attacks



- **92%** remotely executed
- **70%** could affect thousands or millions of devices
- **35%** involved car system manipulation

Source:
2025 Automotive & Smart Mobility Cybersecurity Report (Feb 13, 2025)

RUNSAFE SECURITY

RunSafe Security Platform

Automated software supply chain protection platform for embedded software

IDENTIFY RISK

in your software across your software supply chain leveraging build time SBOMs

PROTECT CODE

from memory-based attacks without rewriting a single line of code

MONITOR SOFTWARE

at runtime identifying code quality issues and indicators of compromise

Automated exploit prevention and 99% reduction in 0day risk.

Jose Rui Simoes
Automotive Solutions
Critical Software
jose.r.simoes@criticalsoftware.com

Scott Sheahan
Founder
Rustic Security
scott@rusticsecurity.com

Doug Britton
Executive Vice President
RunSafe Security
doug@runsafesecurity.com

Joe Saunders
Founder and CEO
RunSafe Security
(moderator)
joe@runsafesecurity.com

“The things that are now becoming the everyday parlance of cyber practitioners in automotive have their roots in problems that have been solved or addressed in other parts of the cybersecurity industry for the last 20 to 30 years.”

Doug Britton

Executive Vice President

RunSafe Security

RUNSAFE SECURITY

"I'd say some of the best practices and trends I've also seen are the OEMs are much more wanting to control their software. We're talking about this move to a software defined vehicle where there's value for the OEMs to push software updates across a vehicle architecture. … You can see across the board that this is going to be a future distinguisher amongst security quality for these OEMs."

Scott Sheahan

Founder

Rustic Security

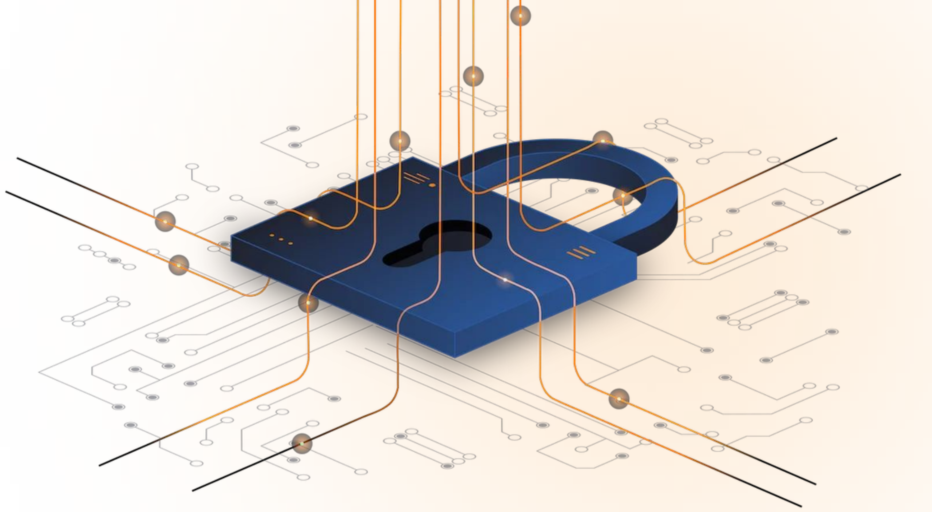
> “You have to plan for those 20 years of life cycle, but you also have to plan to continuously update... because if you decide to use version X or Z of operating system right now, that will be discontinued sometime in the future.”

Jose Rui Simoes

Automotive Solutions

Critical Software

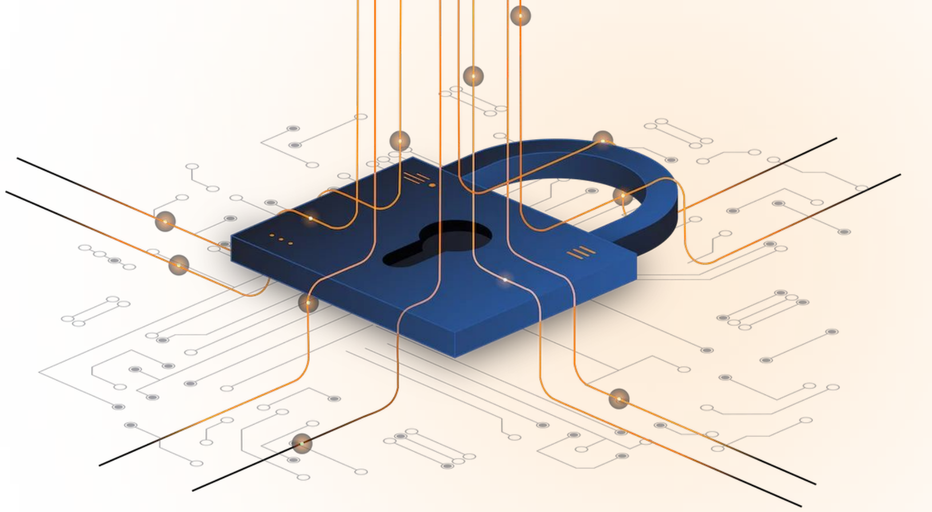
RUNSAFE SECURITY



Webinar Highlights

- **The scale of automotive cyber threats is significant:**
  - In 2024, 92% of attacks were remotely executed, 70% could affect thousands/millions of devices, and 35% involved car system manipulation.
- **The industry is moving from distributed ECUs to consolidated zonal architecture**, which reduces the number of components to secure but requires more robust security for each zone and the communication backbone.
- **Vehicle-to-vehicle and vehicle-to-infrastructure communications present new security challenges,** requiring careful consideration of authentication, privacy, and potential adversarial attacks.
- **Software supply chain security is becoming more complex as vehicles incorporate more open source software and multiple vendor components**, requiring comprehensive risk management strategies.
- **The industry is generally optimistic about autonomous vehicle security,** citing rigorous safety standards, redundant systems, and significant economic incentives to get it right.

RUNSAFE SECURITY



Additional Resources

- Securing Electronic Control Units (ECUs) in Autonomous Vehicles
- Defending Advanced Driver Assistance Systems (ADAS)
- Buckle Up: Addressing Embedded Systems Security in the Automotive Software Supply Chain
- Protecting the Automotive Industry at Every Turn: From RunSafe’s First Patent to Today
- Comprehensive Automotive Cybersecurity Protection

RUNSAFE SECURITY

GIVE RUNSAFE SECURITY PLATFORM A TRY

Receive a **FREE Risk Reduction Analysis** for your software

REQUEST A FREE ANALYSIS