Road Vehicle Management
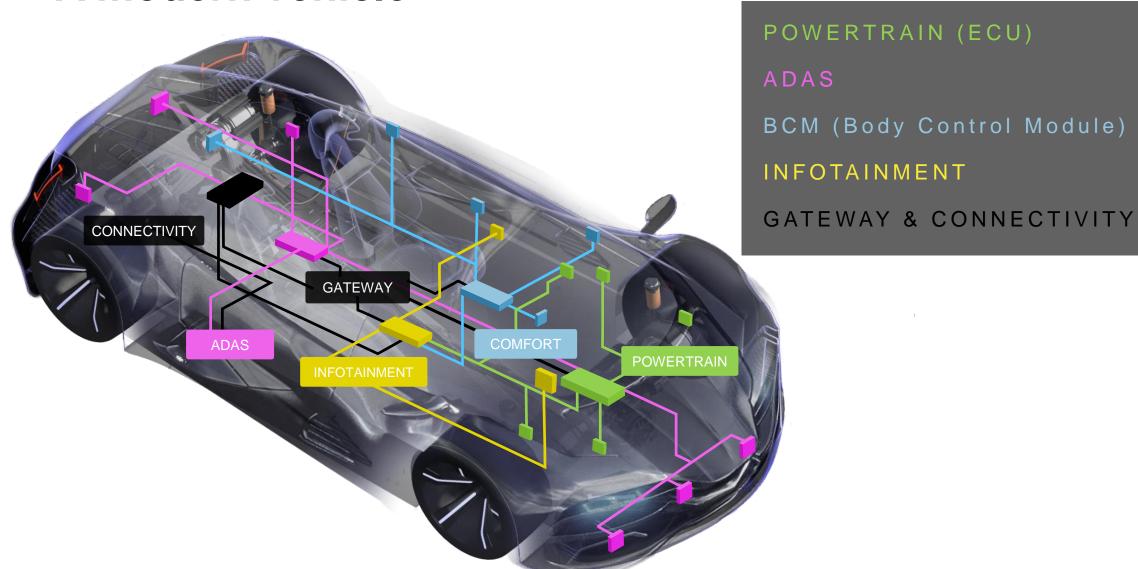
SIP ADUS 2019

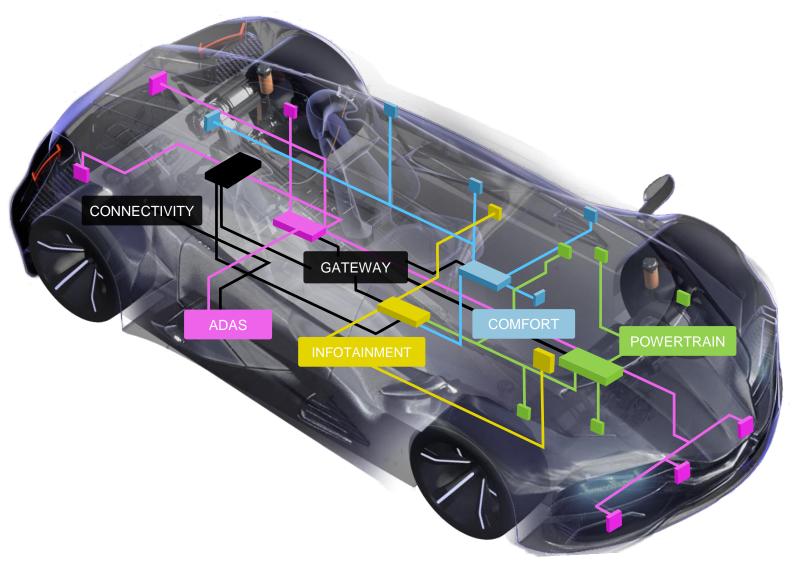Chris Clark

Embedded Systems Ecosystems

Synopsys Software Integrity Group

A modern vehicle

POWERTRAIN (ECU)

ADAS

BCM (Body Control Module)

INFOTAINMENT

GATEWAY & CONNECTIVITY

CONNECTIVITY

GATEWAY

ADAS

INFOTAINMENT

COMFORT

POWERTRAIN

CONFIDENTIAL

SYNOPSYS®

The future of vehicle computing

POWERTRAIN (ECU)

ADAS

BCM (Body Control Module)

INFOTAINMENT

GATEWAY & CONNECTIVITY

Centralized Computing

Virtualization

Containerization

Pervasive Connectivity

Distributed Computing

CONFIDENTIAL

SYNOPSYS®

What is the long term impact?

- Manufacturing
- Vehicle release
- Recalls
- Technical Debt
- COTS
- Reuse
- Safety
- Privacy

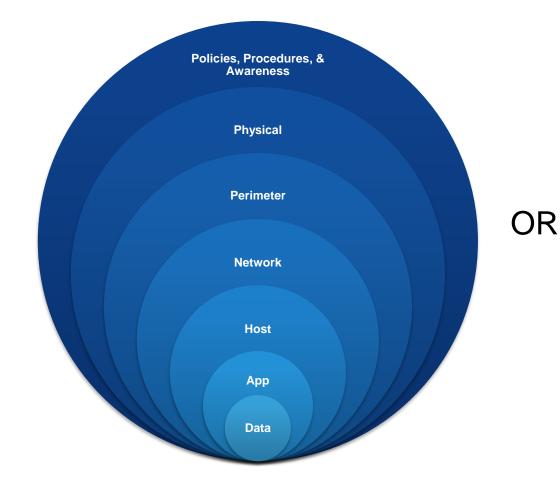How does this impact early vehicle development activities?
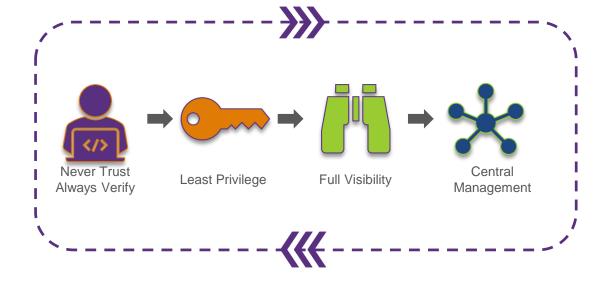
How will these systems be maintained?

CONNE

Codebases
Millions of lines of code
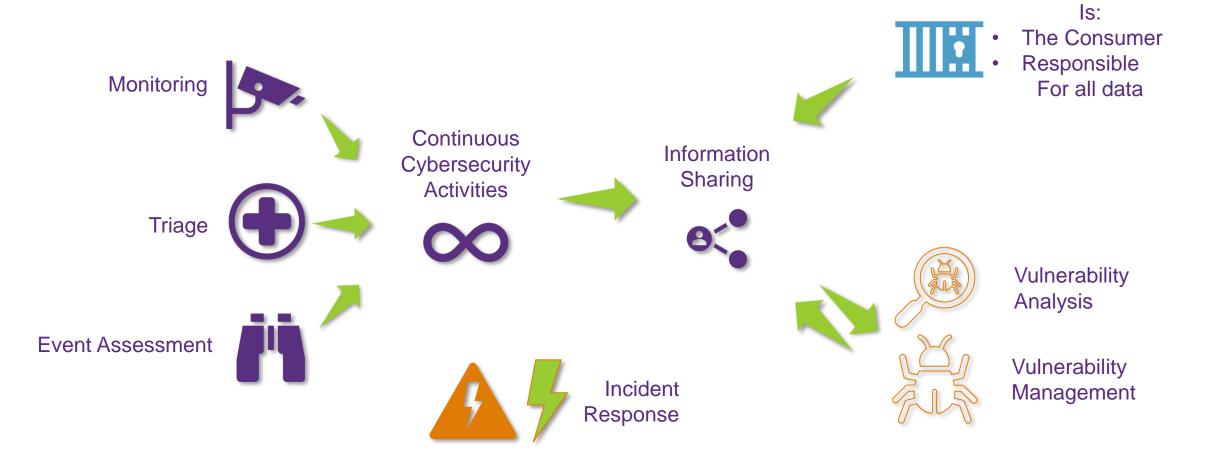
Microsoft Office 2013	
Large Hadron Collider total code	125%
Windows Vista 2007	
Microsoft Visual Studio 2012	
Facebook (including backend code)	
US Army Future Combat System fast battlefield network system (aborted)	
Debian 5.0 codebase free, open-source operating system	
Mac OS X "Tiger" v10.4	
Car software average modern high-end car	
Mouse* Total DNA basepairs in genome	
Google all internet services	

CONFIDENTIAL

SYNOPSYS®

Defense in Depth

Or something else…

Defense in Depth

Zero Trust Zones

OR

CONFIDENTIAL

synopsys

Information Sharing

Monitoring

Triage

Event Assessment

Continuous
Cybersecurity
Activities

Incident
Response

Information
Sharing

Is:
- The Consumer
- Responsible
  For all data

Vulnerability
Analysis

Vulnerability
Management

CONFIDENTIAL

SYNOPSYS®
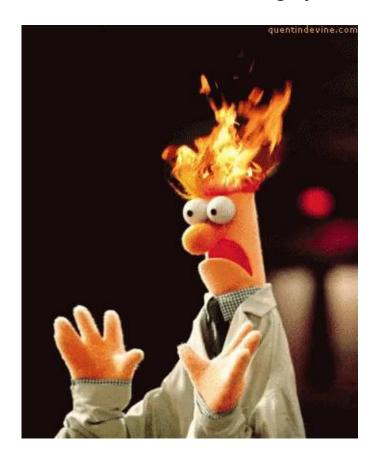
Conclusion

First off, don't be this guy!

1. Commit to making security a priority. Shift your focus from a reactive "we'll deal with it when the time comes" or "that is another team" mentality to one of proactivity so as to avoid the time from ever arriving.

2. Enable developers with the tools and training they need to build security into software they are coding.

3. To manage open source and software supply chain risk, you must include open source security considerations within your overall software security initiative.

4. Address the root cause. By building expertise and providing necessary information to prevent bugs from entering the code base in the first place.

5. Base the plan on a maturity model.

6. Be open to new ideas and ways of doing things.

7. Communicate!

CONFIDENTIAL

SYNOPSYS®

Thank You