Cyber Secure Innovation
... an Oxymoron?

Method Park
Process Insights - October 2018

Meg Novacek
AGENDA

1. Product Development and Innovation
2. Embedded System Development
3. Automotive Cyber Security
4. Conflicts between Innovation & Cyber Security
Automotive Vehicle Development

Develop hardware and software *simultaneously*

Leverage sales revenue of new models to offset validation costs

2 - 3 year cycle
Executive & Investor **Expectations**

”Silicon Valley” speed of development

Almost **immediate** integration of consumer electronics technology into vehicles

(a year is too long)
Approach to Innovation Today

Quickest path to a minimum viable product “MVP”

Prototype / quickly code something to demonstrate the idea

Acquire funding for people and parts to make it to next milestone

Innovation is often “fueled” by start-up companies (or acquisitions of start-ups)

Little experience with, or appreciation for process discipline, product maintenance or liability
Typical Approach to Embedded Software Development

Distribute the coding across different teams globally
Develop functions simultaneously

Integrate new content and release bi-weekly
Embedded Software Validation

Software is tested:

- Model in the Loop
- Software in the Loop
- Hardware in the Loop
- Component Dynos
- Development Vehicles

Bugs are identified ✰
... but not all

Fixes developed and implemented
... asynchronously
and sometimes the fixes have bugs
Embedded Software Reality

Consumer Electronics Attitude
“There are always bugs in software”

My perspective:
Bugs can cause recalls
A component to break
A customer to be stranded
Embedded Software Update Strategy

Today, Automotive product differentiation relies on software

➢ Bring new / improved features to production quickly !!!!
➢ Fix quality issues and security vulnerabilities quickly !

Over 100M lines of code in highest-content vehicles

Over-the-Air software updates are being applied to more and more systems

➢ Infotainment
➢ EV functions
➢ Cybersecurity
➢ ADAS & Powertrain
Automotive Threat Surface

- Cellular
- Bluetooth
- V2X
- OBD II
- WiFi
- Infotainment
Potential Automotive Exploits

- Unlock doors
- Prevent ignition
- Turn radio to maximum volume
- Eavesdrop through microphones
- Track GPS location, alter navigation
- Turn off the engine
- Accelerate vehicle, disable brakes
- Control steering wheel
- Inflate airbags
Threat Scenarios

Warranty and Insurance Fraud owner **claims** hacking caused accident or vehicle theft

Theft of vehicle or personal property

Ransomware applied to vehicle owners – dealers – fleet owners - automaker

Brand Reputation Harm hacktivists sensationally disclosing vulnerabilities

hacker **claiming** that an accident was caused by a hack
Cyber Security Best Practices

1. A risk-based prioritized identification and protection process for safety-critical vehicle control systems;

2. Timely detection and rapid response to potential vehicle cybersecurity incidents on America’s roads;

3. Architectures, methods, and measures that design-in cyber resiliency and facilitate rapid recovery from incidents when they occur; and

4. Methods for effective intelligence and information sharing across the industry to facilitate quick adoption of industry-wide lessons learned (Auto ISAC).
Cyber Secure Embedded Software Development

Hackers (ethical and otherwise) like challenges
➢ They develop new *techniques* to get into systems and exploit them
➢ They identify vulnerabilities
   ➢ Coders *not following* best practices
   ➢ Weaknesses in *existing* coding practices

Product manufacturers are responsible to have a process to:
➢ review vulnerability lists
➢ be alerted for “Zero Day” vulnerabilities
➢ quickly mitigate them
➢ protect existing product in the market
Innovation & Cyber Conflicts

Code coming in from around the world
- Can’t “talk” to every coder involved on the team
- Significant amount of legacy code
- Open source code

Constantly evolving content
- add features
- abandon unused paths
- add branches to support product variants

Make it easy for developers to
- get system data for analysis
- make quick fixes and evaluate the effectiveness

**CYBER SECURITY MEASURES**

- How ensure everyone has cybersecurity training and knows the policies?
- Verify no known vulnerabilities
  - At key milestones prior to production
  - For every production release
- Remove unused code!
  - Who tests legacy features?
- Eliminate “back doors” in the code
  - Close ports when release for production!
Innovation & Cyber Conflicts

GO FAST!!

Lean teams

- Scan for vulnerabilities
- Perform Penetration Tests

Develop product enhancements

Fix quality problems

Address vulnerabilities

Secure Gateways block or control access.

Authentication required to request information and to run executables.

Leverage all info on vehicle for new feature innovation

Suppliers and Special Equipment manufacturers typically develop new features on their own

System integrators develop specialty vehicles

Cyber Secure Innovation
What can we do?

Recognize and appreciate the conflicting objectives

Develop policies and integrate into enterprise-wide processes

TRAIN Team members

Leverage tools that provide a framework for the whole team to follow the process
Questions?