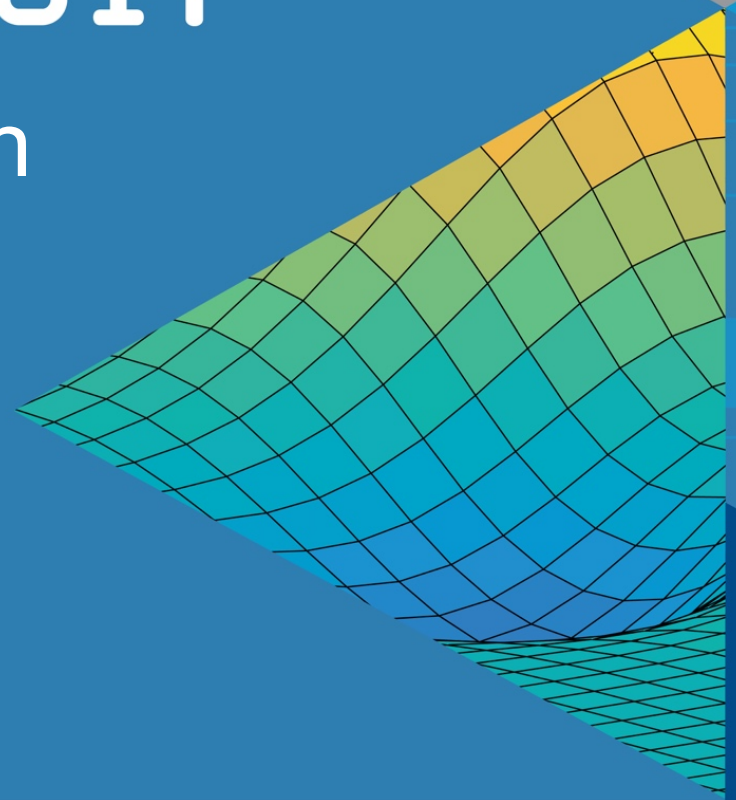
MATLAB EXPO 2017

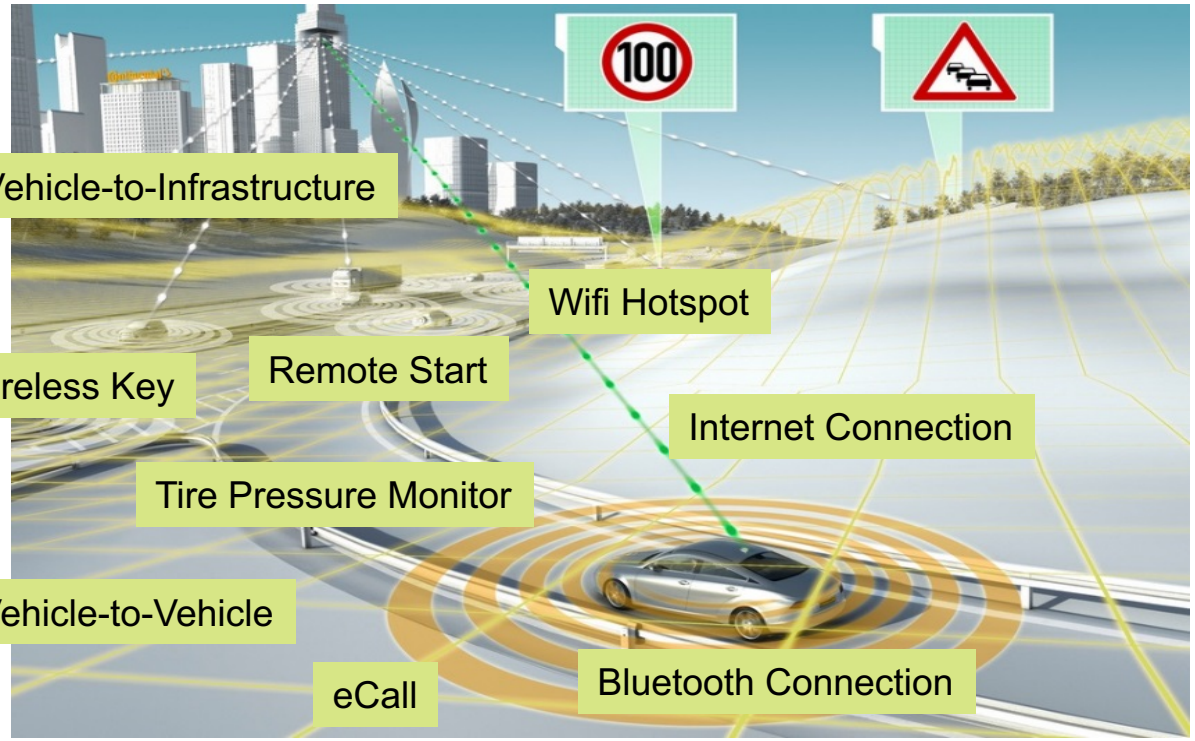
Automatisches Erkennen von Sicherheitslücken mit Polyspace

Christian Guß



Cybersecurity – Emerging Topic in the Auto Industry

On-Board & V2X Communication

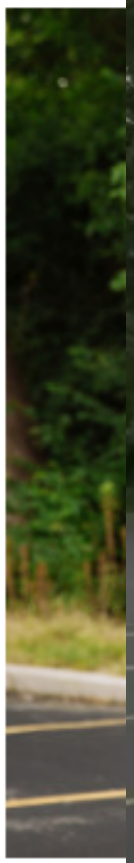


- Growing communication of on-board systems, sensors and external sites
- Car becomes another node of IoT
- Security of automotive embedded systems increasingly important (possible cyber attacks)

FCA recalls 1.4 Million cars after Jeep hack

http://www.blogcdn.com/www.autoblog.com/media/2013/02/2014-jeep-cherokee-1.jpg

Embedded Software Security New Challenge



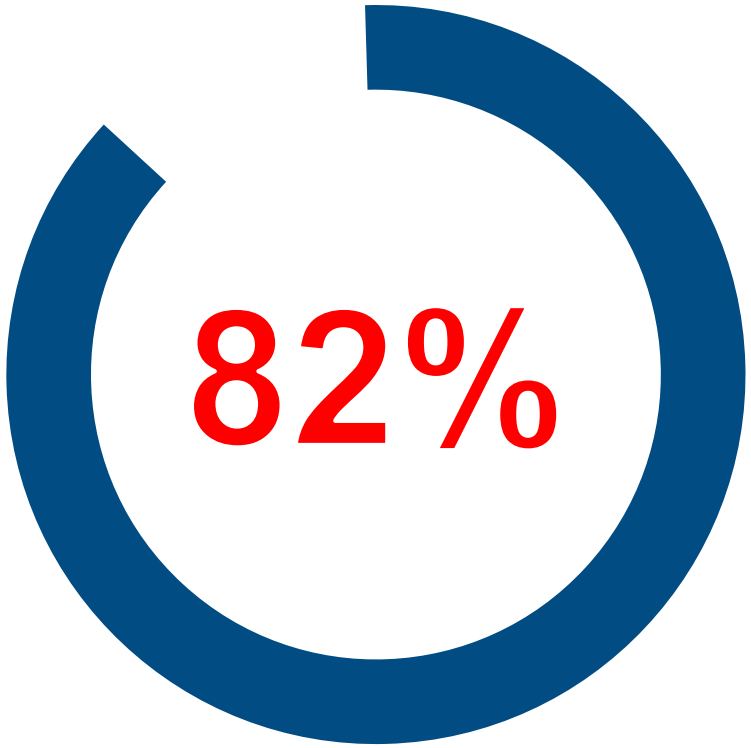
Miller (le
drove it

ON THE

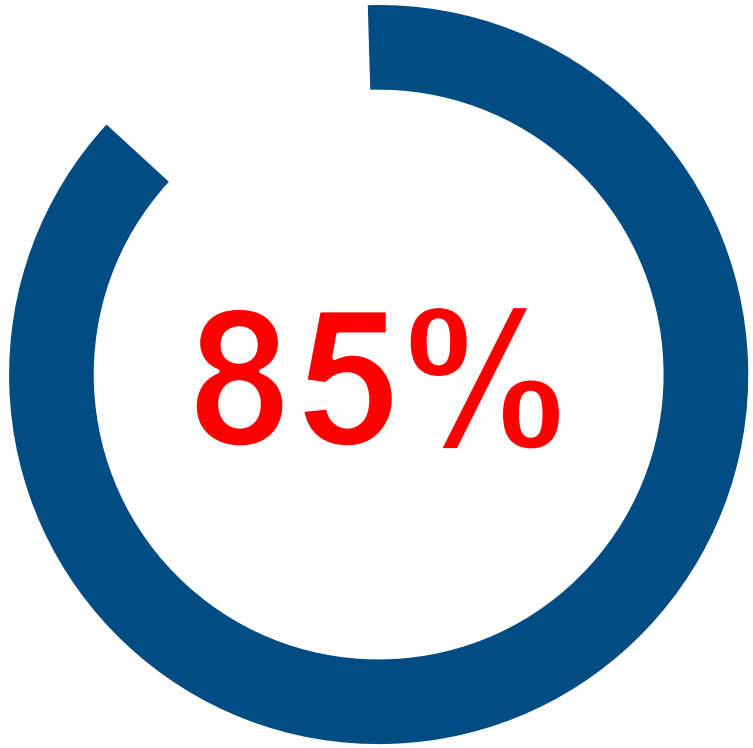
Source: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

2016 KPMG Consumer Loss Barometer Study Key Cyber Automotive Findings

Security is on consumers' mind



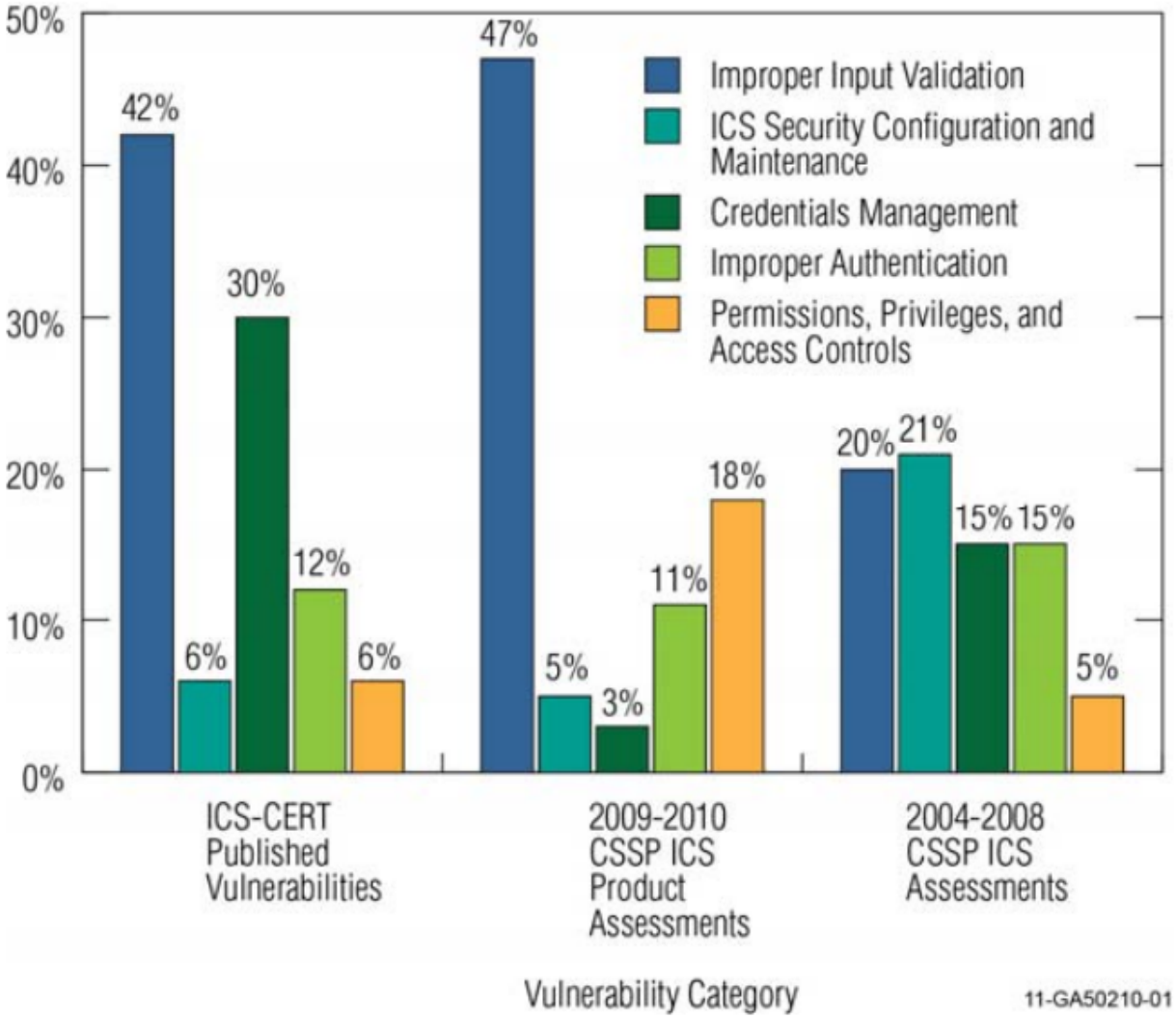
…of customers would never buy from automaker if they had been hacked



…of automakers admit their organization have been breached in the past 2 years

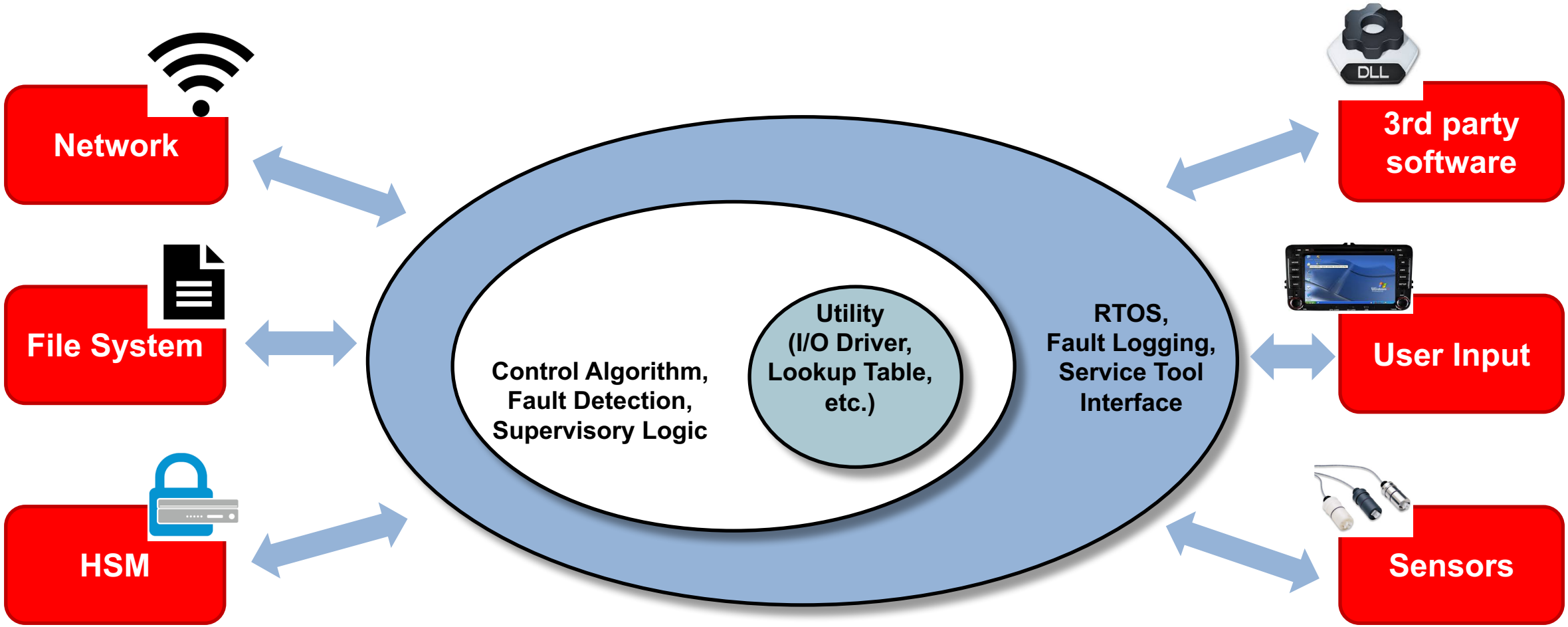
according to 2016 KPMG Consumer Loss Barometer study

Cybersecurity – Emerging Topic in the Internet of Things

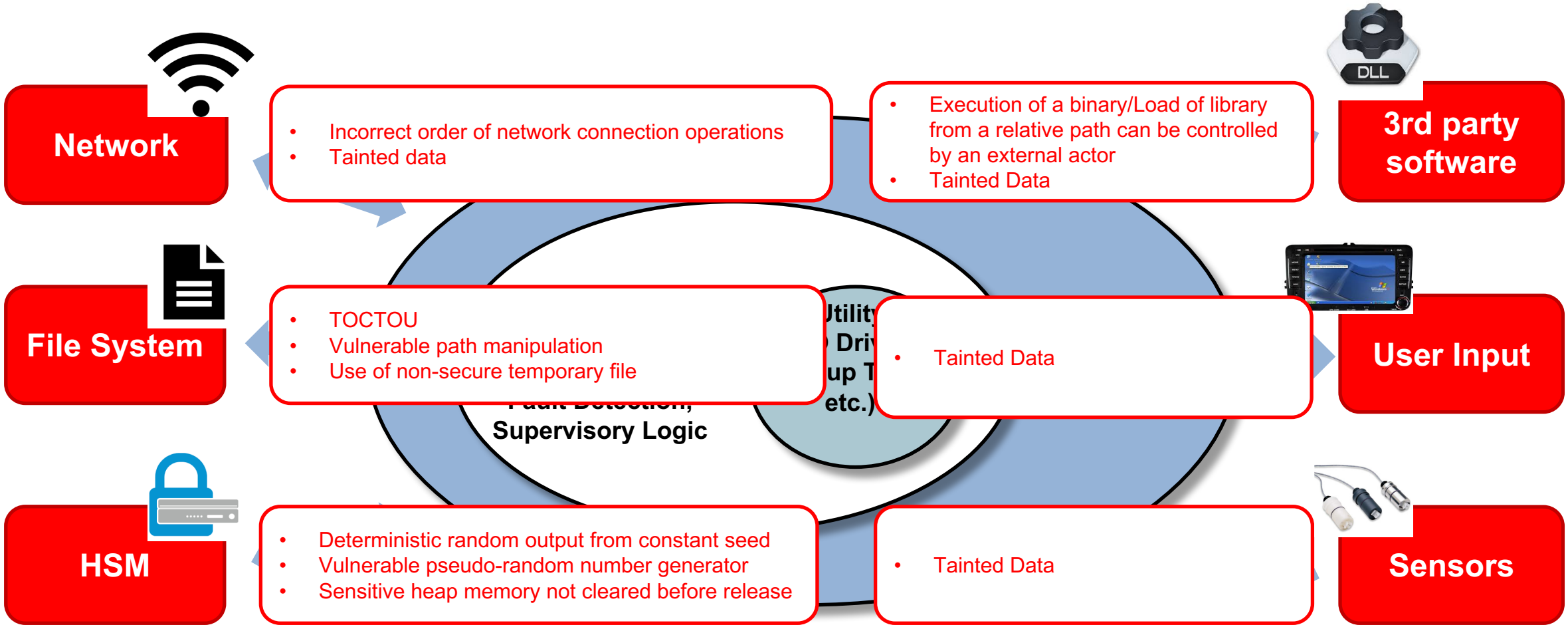


Source:
„Industrial Control Systems (ICS)
Cyber Emergency Response Team“ (ICS-CERT)

Embedded Software External Interactions

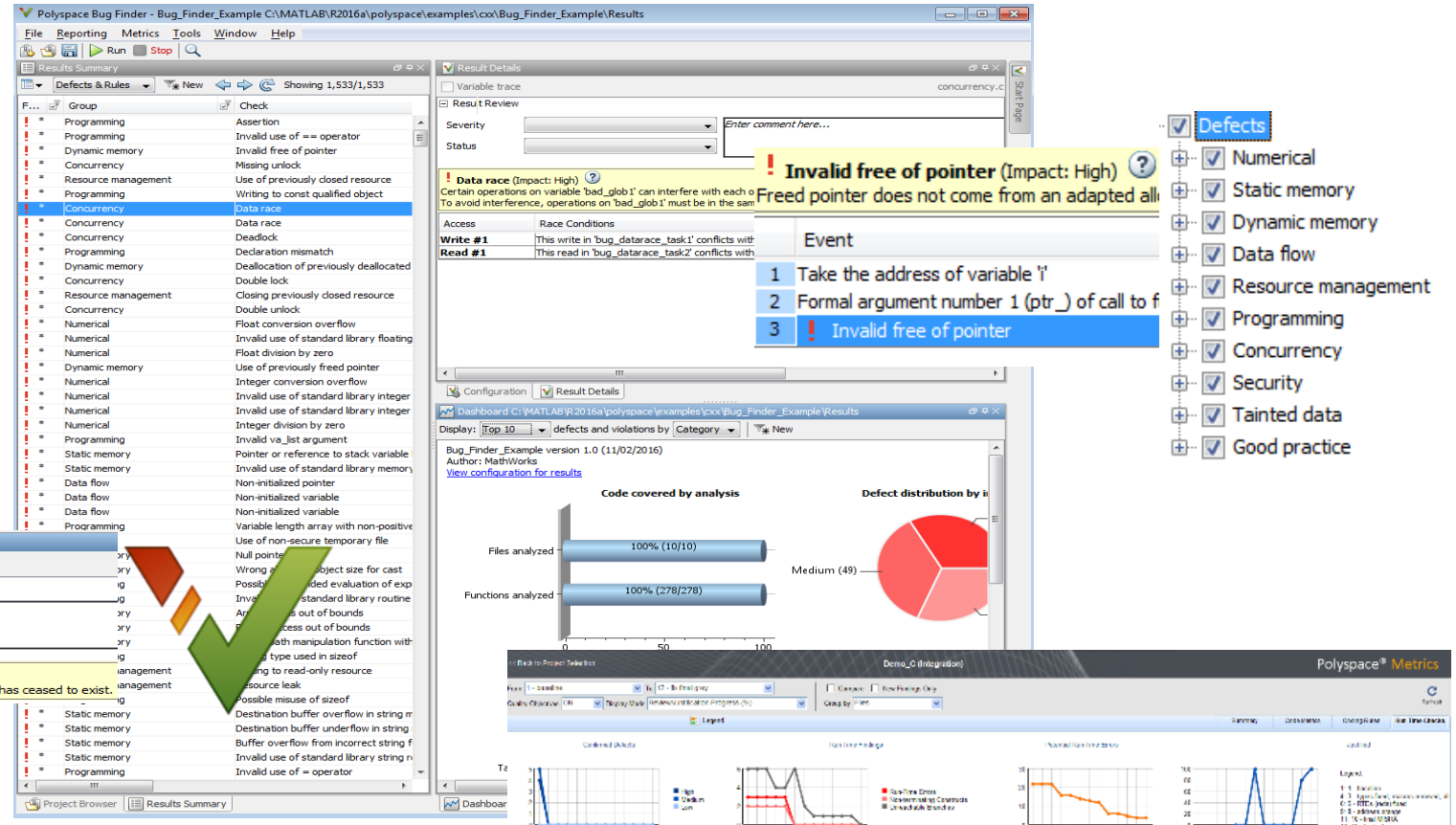


Embedded Software Security Concerns

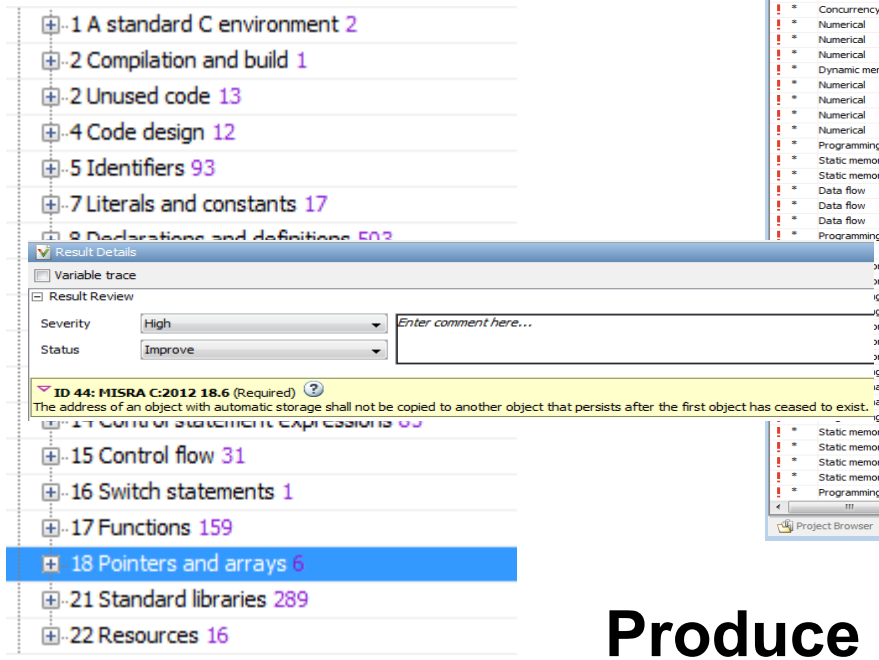


Polyspace helps you to....

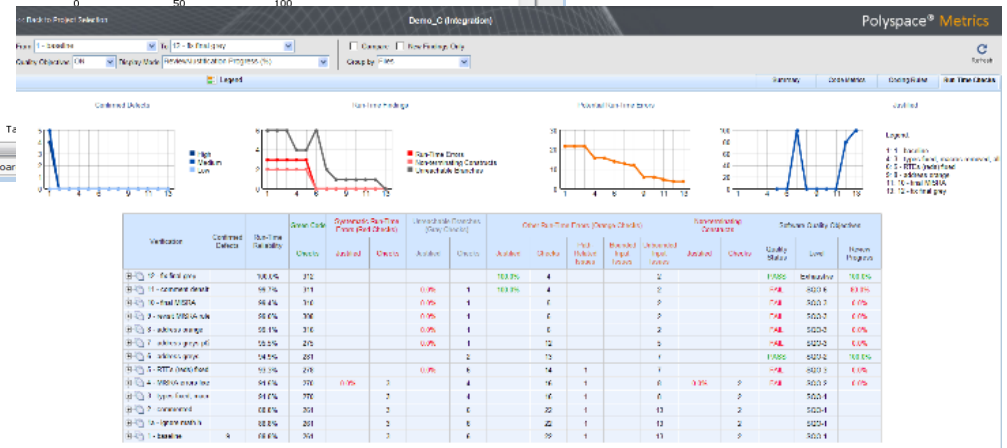
Identify and prove absence of critical defects



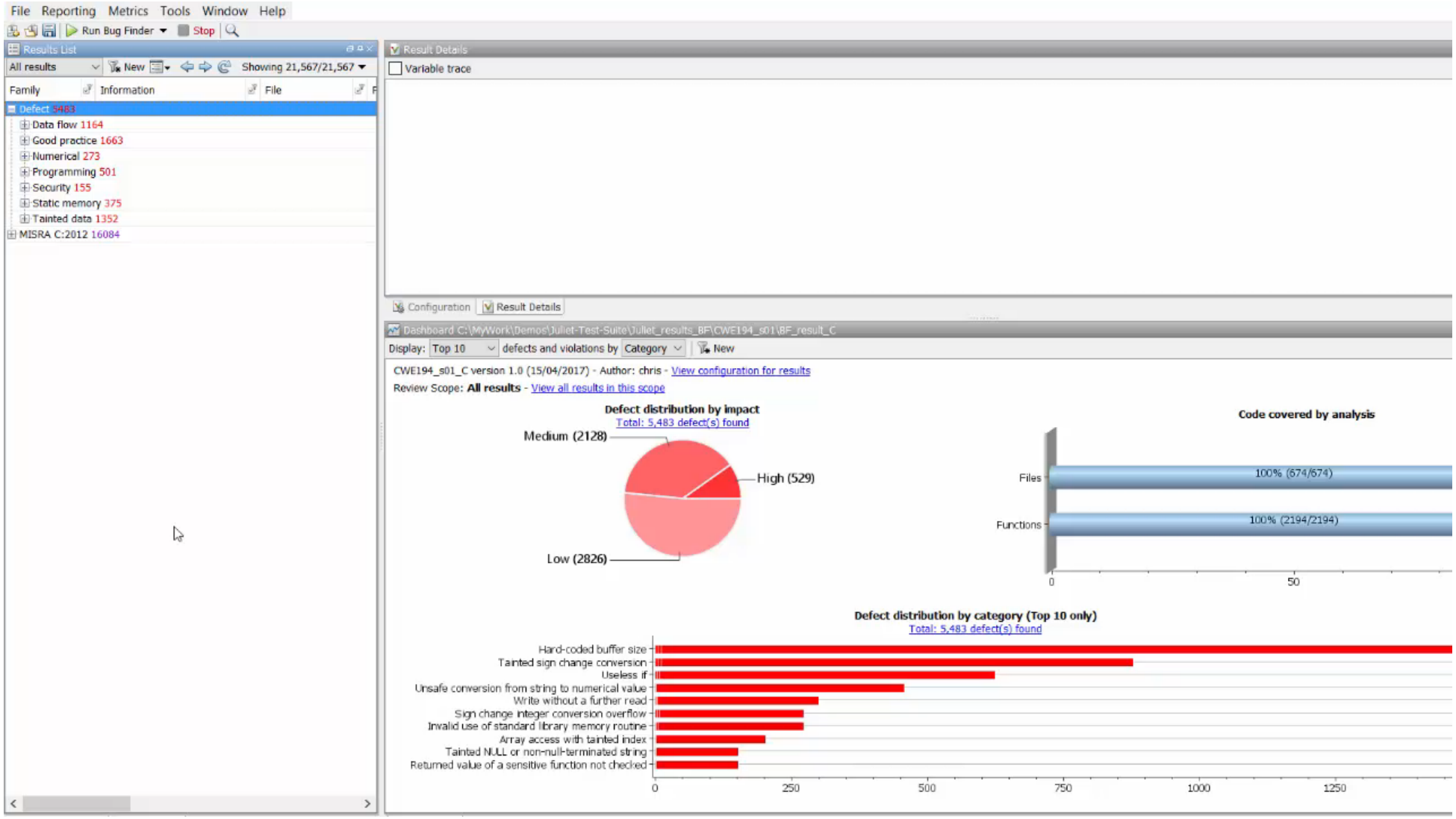
Enforce coding rules



Produce and monitor quality metrics



What is “Tainted Data”?



Cybersecurity – Industry Activities & Standards

SAE – Vehicle Cybersecurity Systems Engineering Committee

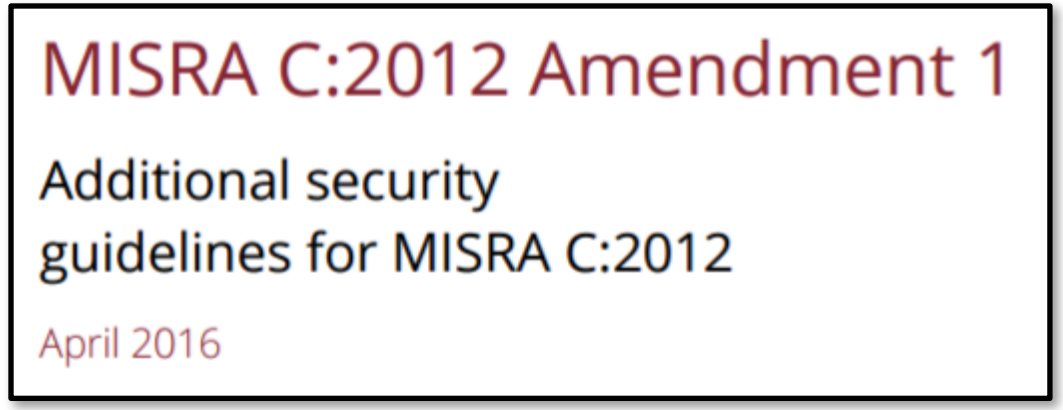
- SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
- SAE J3101 - Requirements for Hardware-Protected Security for Ground Vehicle Applications (WIP)
- SAE “Cybersecurity Assurance Testing Task Force” (TEVEES18A1)

Coding standards & practices that we observe at automotive customers

- CERT C
- ISO/IEC TS 17961 – C Secure Coding Rules
- CWE – Common Weakness Enumeration
- MISRA-C:2012 Amendment 1

Polyspace helps you to....

- ✓ Enforce **new coding rules**
  (all of them required or mandatory)



- ✓ **1 new directive** [4.14]
- ✓ **13 new rules** on
  - ✓ Expressions [12.5]
  - ✓ Standard libraries [21.13, 21.14, 21.15, 21.16, 21.17, 21.18, 21.19, 21.20]
  - ✓ Resources [22.7, 22.8, 22.9, 22.10]
- ✓ Changes to existing rules [21.8]

Example of new MISRA directive 4.14

MISRA C:2012 D4.14 (Required)
The validity of values received from external sources shall be checked.
Division (/) operation operands are from an unsecure source. Check for:
- Denominator of zero.
- Numerator of minimum value and denominator of -1.

	Event	File	Scope	Line
1	Formal parameter is a tainted value	tainteddata.c	bug_taintedintdivision()	108
2	MISRA C:2012 D4.14	tainteddata.c	bug_taintedintdivision()	109

Configuration | Result Details

Source

tainteddata.c

```
104
105 /*============================================================================
106  *  USING TAINTED DATA AS NUMERATOR IN DIVISION
107  *============================================================================*/
108 int bug_taintedintdivision(int usernum, int userden) {
109     int r =  usernum/userden;                  /* Defect: Parameter is not checked before being used as numerator */
110     print_int(r);
111     return r;
112 }
```

Summary

Cybersecurity …

- ✓ enable new future markets
- ✓ entire vehicle lifecycle process
- ✓ by design