Automating fuzz test generation to improve the security of the Controller Area Network

Daniel S. Fowler*
fowlerd3@coventry.ac.uk
orcid.org/0000-0001-6730-2802
*primary contact

Jeremy Bryans
jeremy.bryans@coventry.ac.uk
orcid.org/0000-0001-9850-8467

Siraj Shaikh
siraj.shaikh@coventry.ac.uk
orcid.org/0000-0002-0726-3319

Keywords

#automotive #cyber-security #testing #fuzzing #ecu #car

A Different Automotive Crash Test

Engineers design functional behaviour, but testing for cyber-security is difficult because it requires examining the system beyond the functional design.

Fuzz testing (multiple calls to systems interfaces over a wide value space) has been successfully used to reveal vulnerabilities, yet it has seen little use in the automotive domain.

An automated analysis of the in-vehicle network specification, the database of communications (DBC) file, can be used to generate fuzz tests. These unexpected system inputs will reveal unconsidered operational cases to reveal security flaws prior to manufacture.

Are Hack Proof Cars Possible?

"determined intruders will always find a way to compromise their targets"
Security expert Richard Bejtlich[1]

"Hackers Remotely Kill a Jeep on the Highway - With me in it", Andy Greenberg[2]. After 3 years of research by Charlie Miller and Chris Valasek.

Testing the Unknowns

"Cybersecurity should be a top priority for manufacturers of self-driving vehicles and it must be an integral feature of self-driving vehicles from the very beginning of their development."
U.S. Senate Committee on Commerce, Science and Transportation[3]

The DBC File is a Text Format

The signal values can be fuzzed:

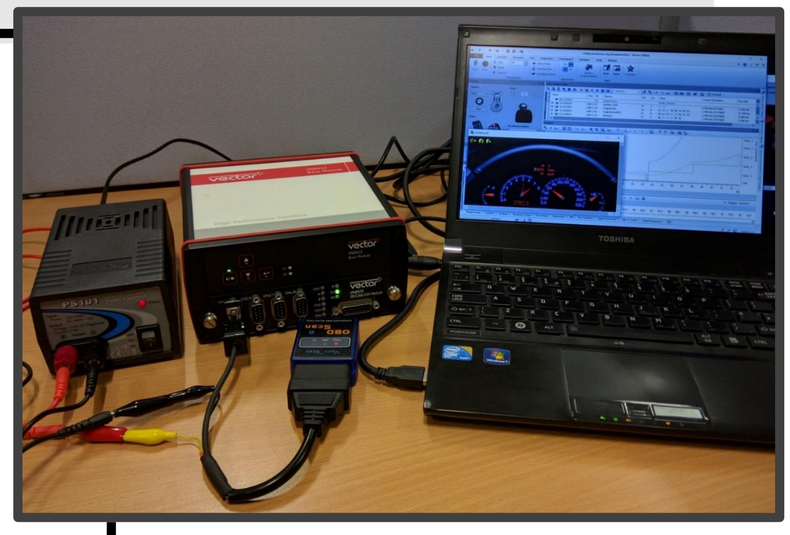
```
BO_ 0 EngineInfo: 8 Gateway
SG_ Comf_Gear : 40|8@1+ (1,0) [0|8] ""
SG_ Comf_EngSpeed : 24|16@1+ (1,0) [0|8000] "rpm"
SG_ Comf_EngTemp : 16|8@1- (1,32) [-50|150] "degC"
SG_ Comf_CarSpeed : 8|8@1+ (1,0) [0|255] "km/h"
SG_ Comf_GearLock : 0|8@1- (1,0) [1|2] ""
```

Fuzzing the Cyber-Physical

Fuzz testing has been successful in finding vulnerabilities in other software domains. With vehicles now being connected cyber-physical systems, automotive engineering needs to apply similar techniques to reduce vulnerabilities.

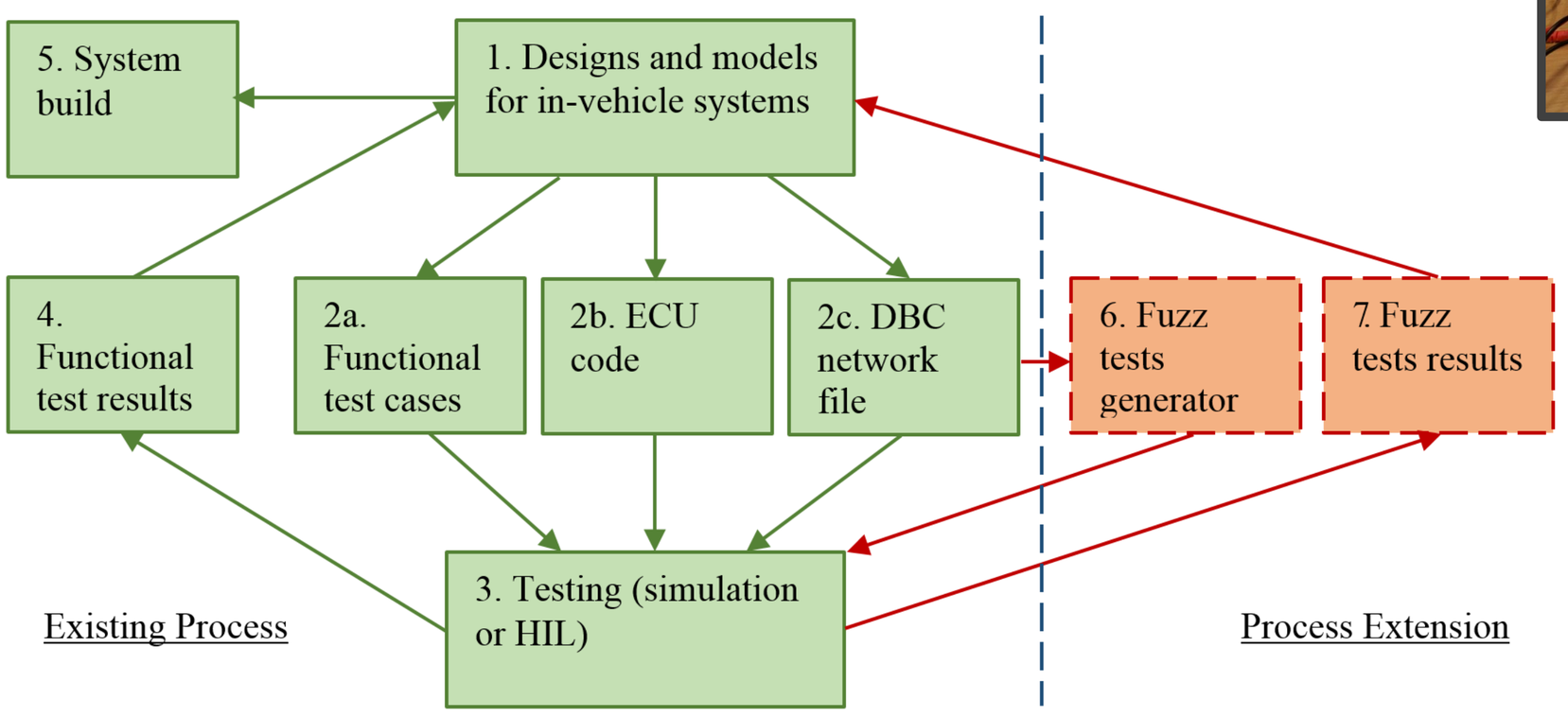
Whilst the fuzzer program can be engineered to monitor the software and network response, a challenge exists to monitor the physical world. Existing development processes use simulators and HIL testbeds, programmable to address the problem. However, can the real car be fuzzed?

Automate for Efficiency



An Automotive Tool

The research is a methodology for ECU, CAN bus and vehicle cyber-physical fuzzing. Validation of the methodology can provided a useful tool extendable to other sectors. CAN is used in industrial, medical and other transport domains.



Acknowledgements to Anthony Baxendale and Paul Wooderson for the support of HORIBA MIRA Ltd.

1. The Practice of Network Security Monitoring: Understanding Incident Detection and Response - No Starch Press 2013
2. Wired.com – July 2015
3. Principles for Bipartisan Legislation on Self-Driving Vehicles – June 2017