CASE STUDY ON COMBINED VALIDATION OF SAFETY & SECURITY REQUIREMENTS

Michal Sojka, Michal Kreč, Zdeněk Hanzálek
Czech Technical University in Prague
Charlie Miller and Chris Valasek “hacking” breaks in their Toyota.
Infineon’s e-Motor Use Case

- HW and SW for control of electric (PMSM) motors in cars
- AUTOSAR Complex Device Driver
- “Safety element out of context”, ASIL D
Overview

- Implemented security extension of CAN bus (message authentication protocol)
  - [https://github.com/CTU-IIG/macan](https://github.com/CTU-IIG/macan) (GPLv2)
- Integrated with e-Motor prototype
- Developed SW/HW-in-the-loop (SIL/HIL) testbeds with Matlab/Simulink
- Performed combined testing of safety and security properties
Tested properties

- Safety (SIL/HIL testbeds)
  - Functionality of implemented safety measures
  - Simulation of faults (demo)
  - e-Motor algorithm execution time

- Security (HIL testbed)
  - Attack the e-Motor over CAN bus
  - Flood the bus with speed requests with faked signature
  - Validate safety properties under the presence of the attack
SW-in-the-loop testbed (testing of safety measures)

PID Controller
Req speed

Ref I_q
Ref I_d

1

Corrupt
PWM Diag

Duty cycle

No fault
PWM

PWM fault simulation

ADC

Out

In

ADC

In

Fault simulation

Speed [RPM]

Motor (PMSM) model

Load torque

T_m

V_a

V_b

V_c

DC

abc

V_{abc}
d.c. to Volts

In1

Errors

In1

Errors

In1

Errors

SW-in-the-loop

Infineon's C code ~ 70 kLoC
Simulink glue code

SIES 2014, Pisa, Italy
SW-in-the-loop results

Torque [Nm]

Motor load  Reference speed  Actual speed

Shaft speed [rpm]

Time [s]

Fault & error status

Fault simulated  Memory error  Position error  Current error  PWM error
HW-in-the-loop testbed
HW-in-the-loop testbed

Infineon TriBoard

PC
Motor & fault simulation

Linux, preempt_rt, 20 kHz

MF624 I/O card

20 kHz

USB
(serial line, JTAG, ...)

CAN bus

CAN attack

PC
Infineon Device Access Server (DAS)

PC
Linux, CAN, MaCAN
MaCAN attack (brute force key guessing)
HIL results – fault simulation

Execution time [μs]

Current [A]

Fault & error status

Phase A
Phase B
Phase C
Fault simulated
Memory error
Position error
Current error
PWM error

Time [s]
No significant difference from normal operation was found.

E-Motor safety is not undermined by executing brute force attack on CAN.
Conclusion

- Developing SIL/HIL testbeds consumes a lot of resources
- It is economic to combine safety & security testing activities