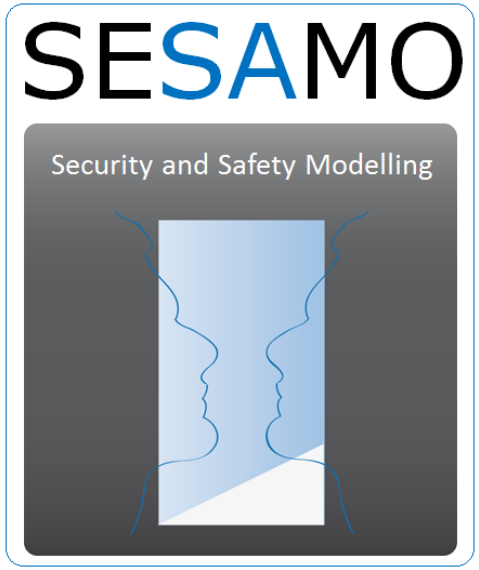


CASE STUDY ON COMBINED VALIDATION OF SAFETY & SECURITY REQUIREMENTS

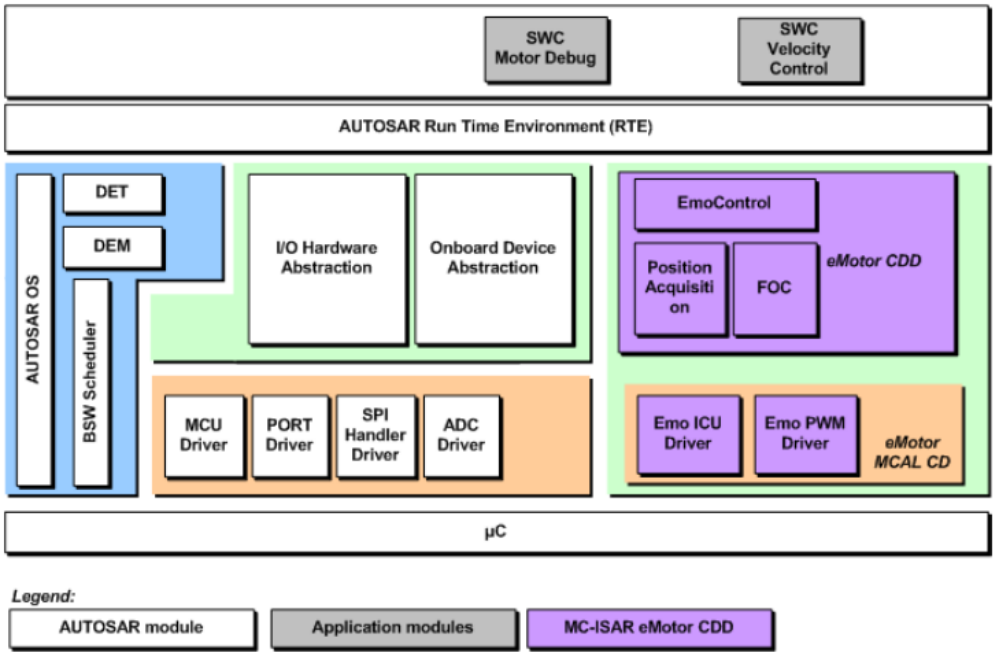
Michal Sojka, Michal Kreč, Zdeněk Hanzálek
Czech Technical University in Prague

Car hacking

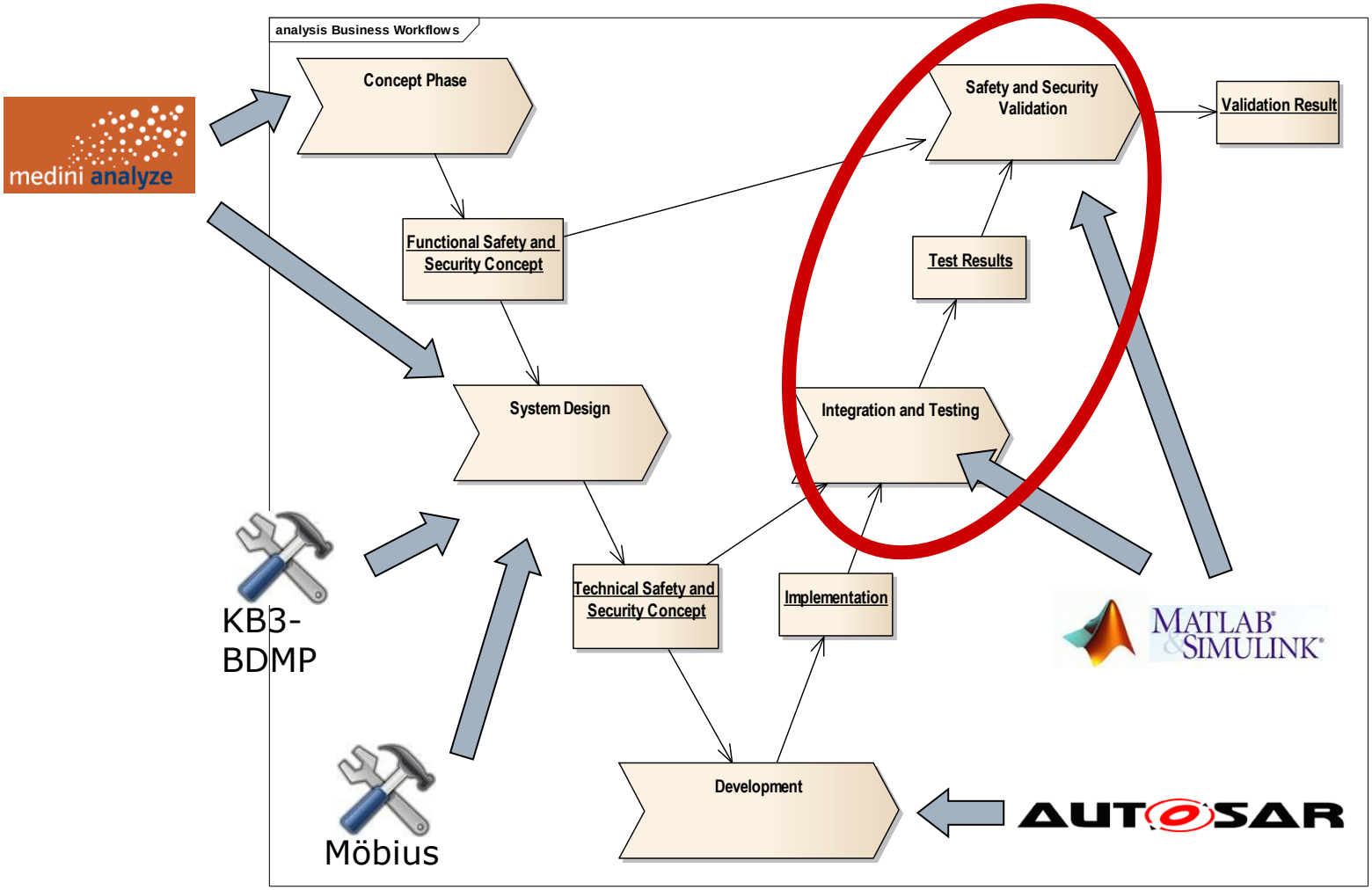
Charlie Miller and Chris Valasek “hacking” breaks in their Toyota.

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



Development process



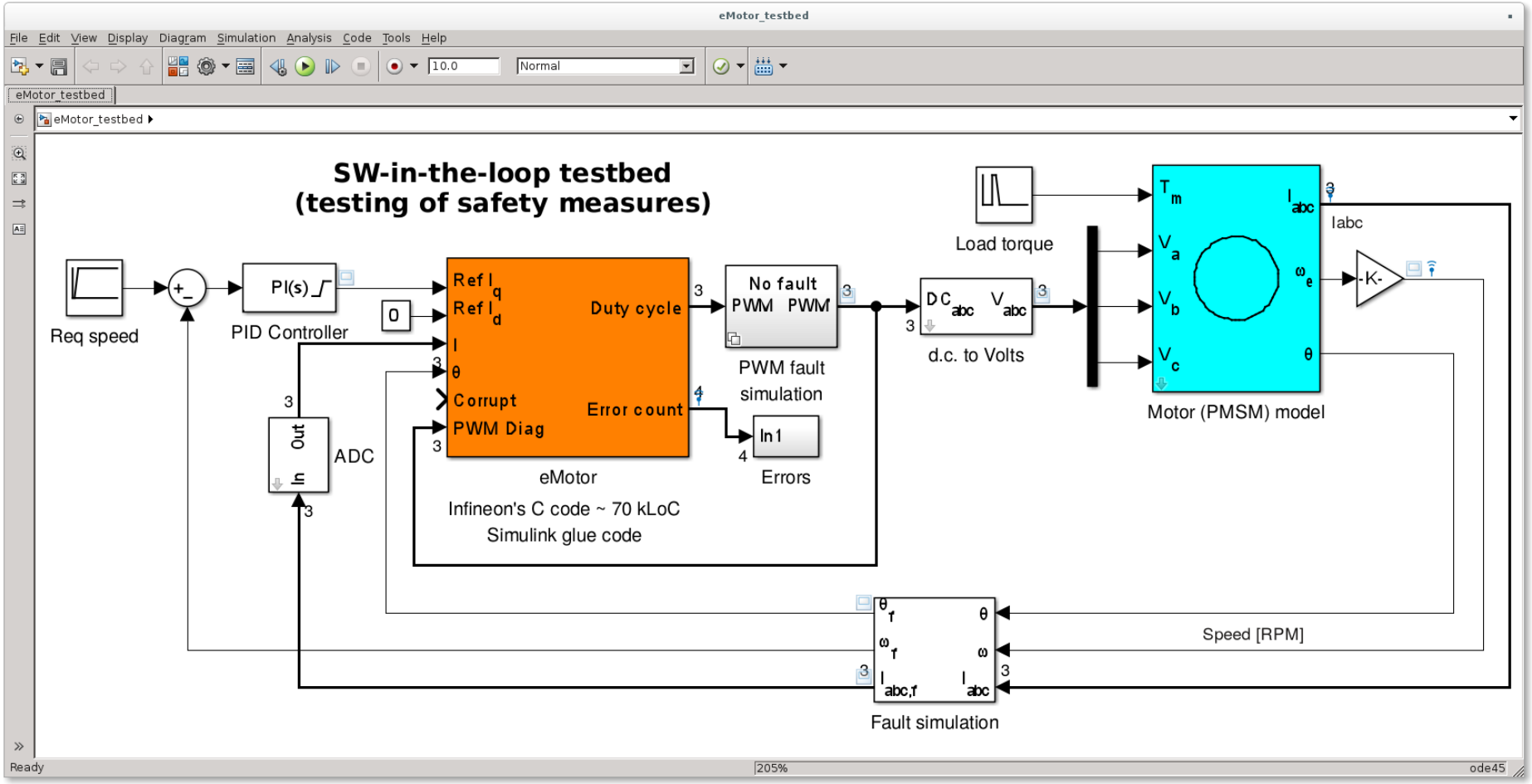
Overview

- Implemented security extension of CAN bus (message authentication protocol)
  - 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

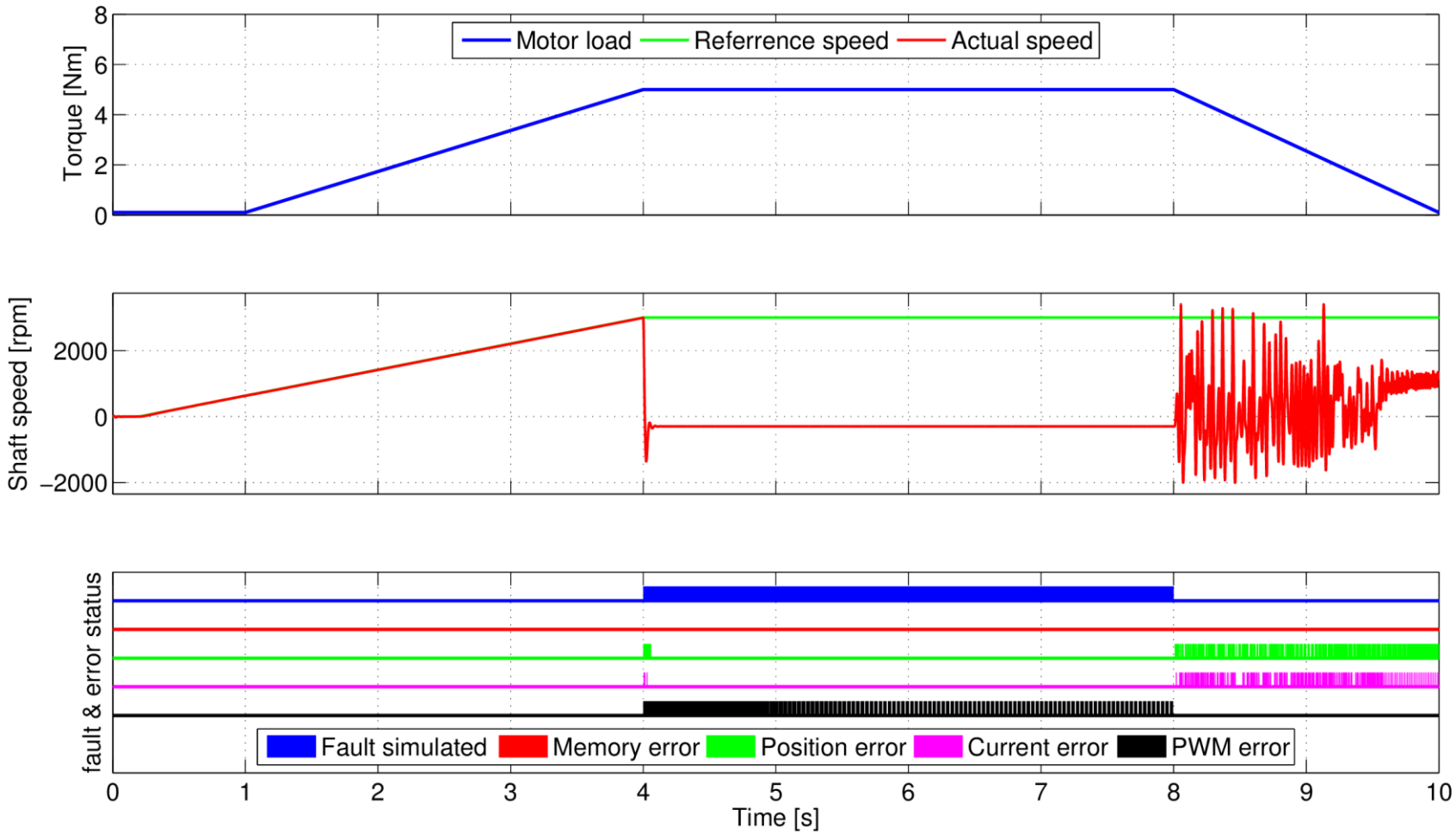
Tested properties

- 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

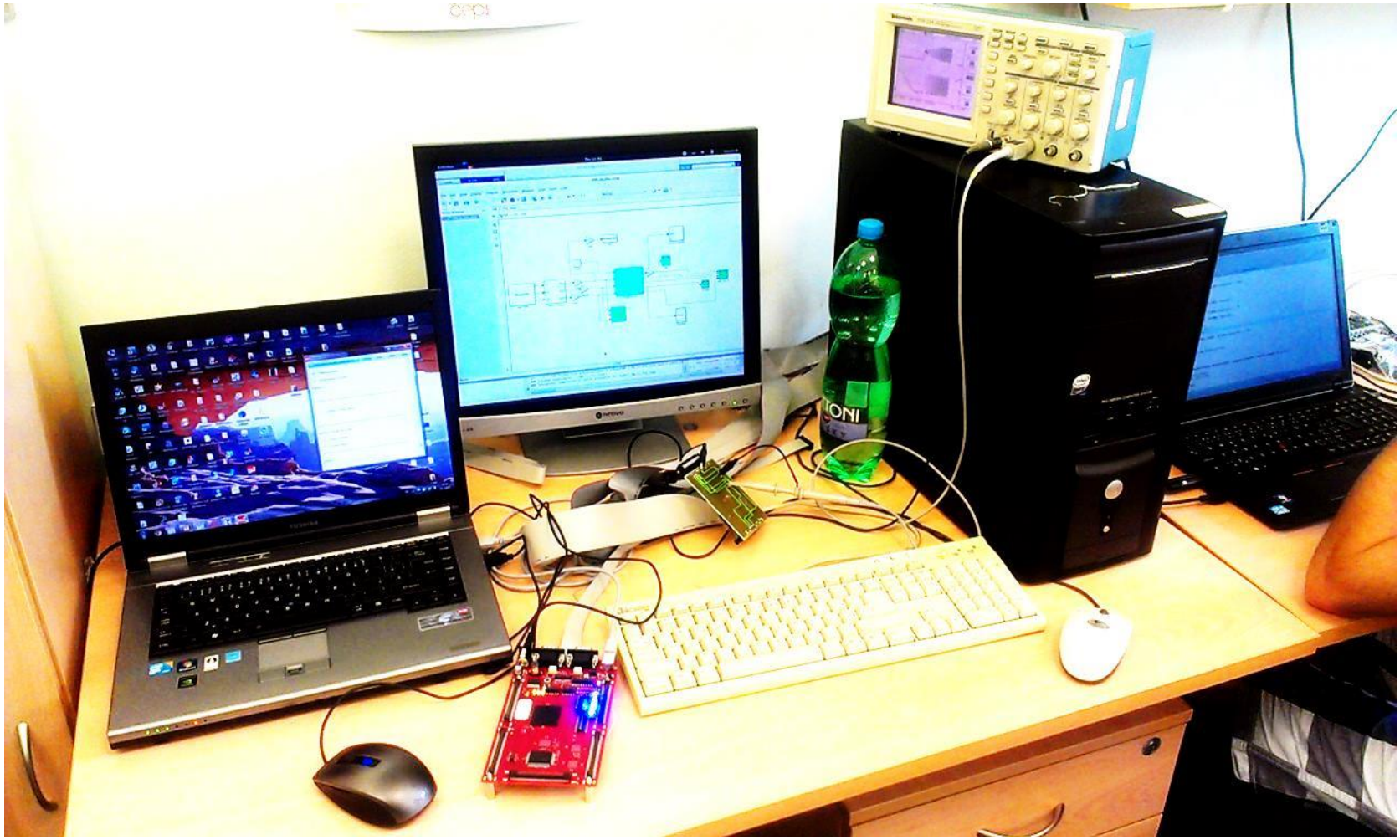
SW-in-the-loop



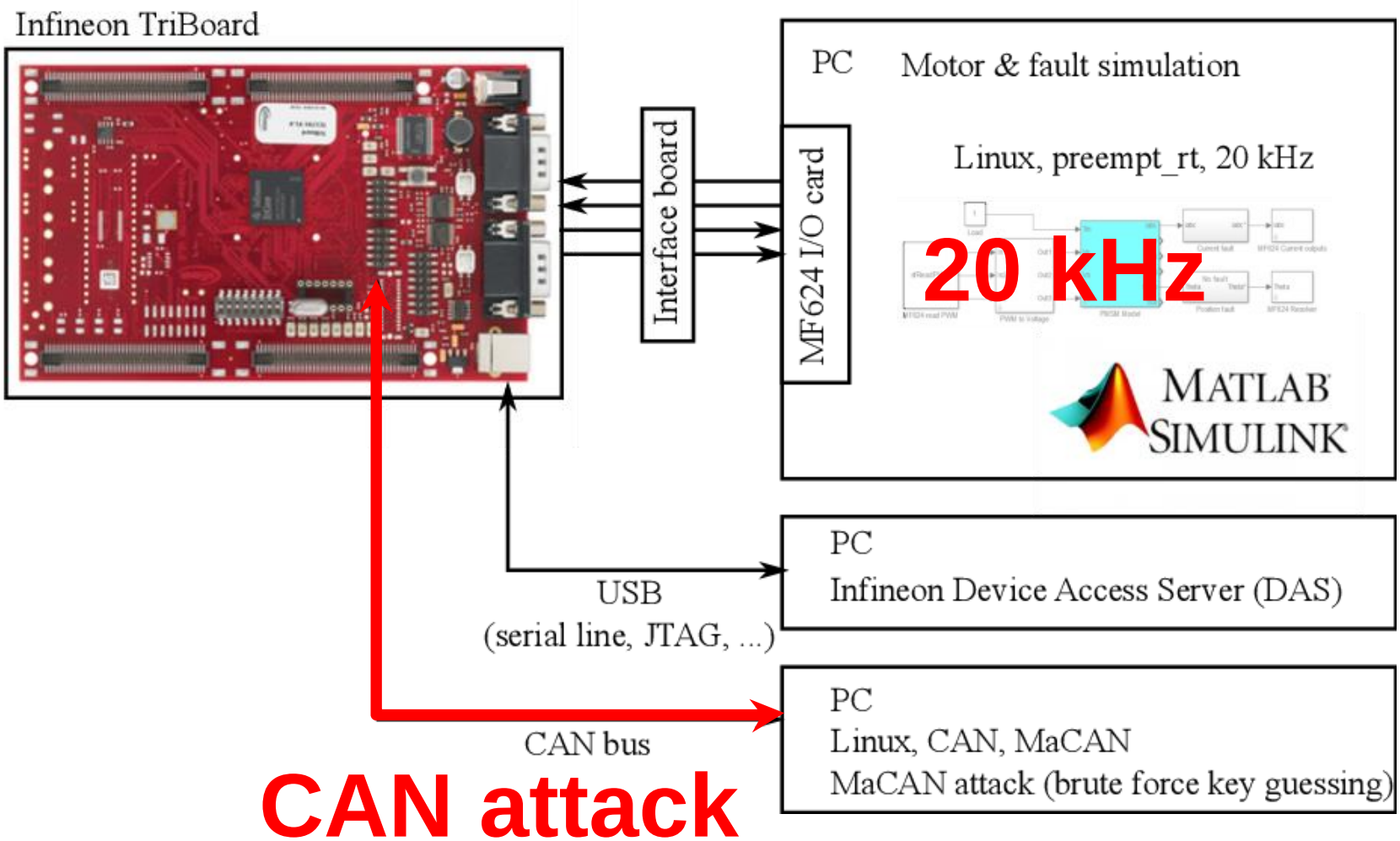
SW-in-the-loop results



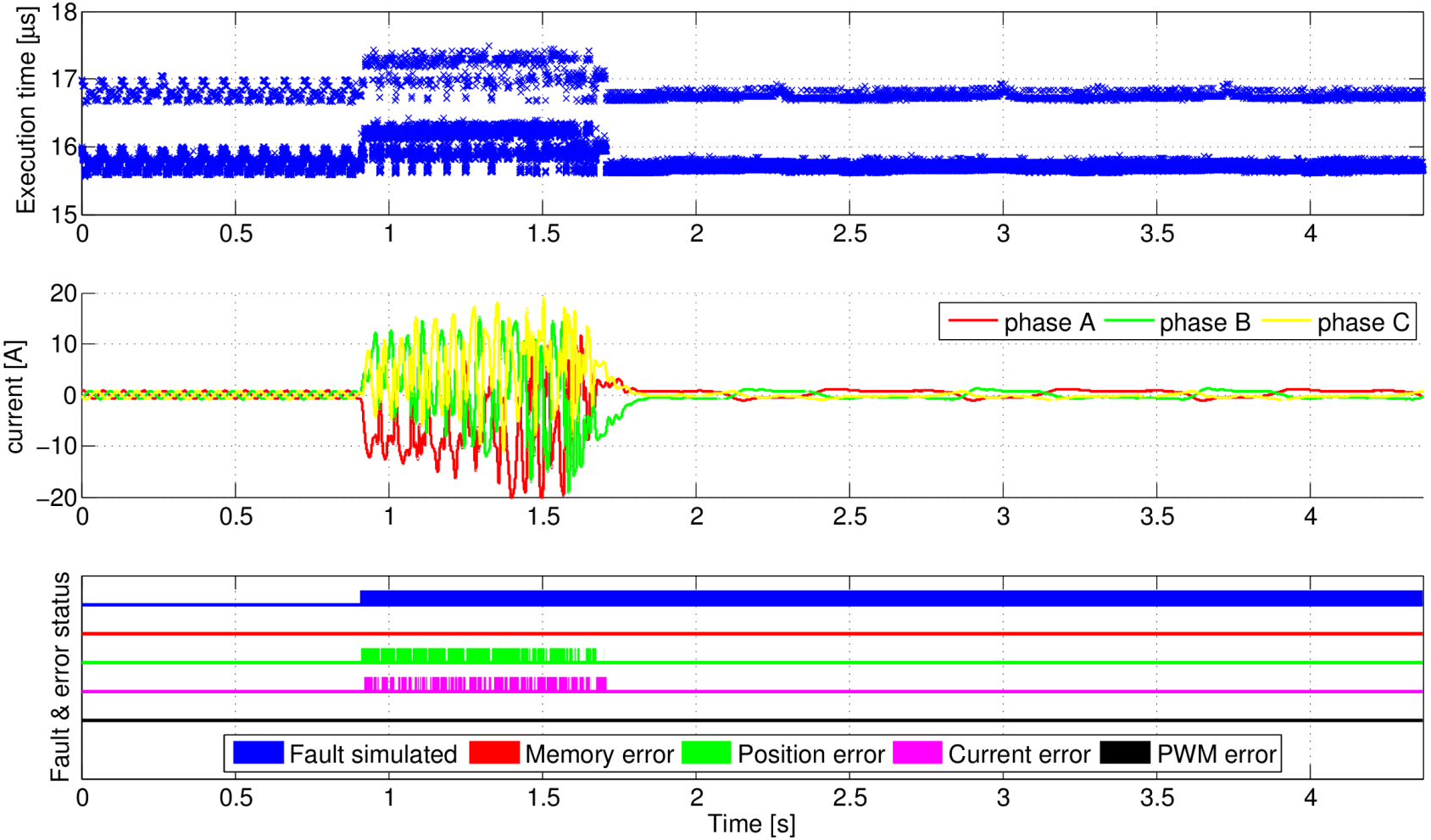
HW-in-the-loop testbed



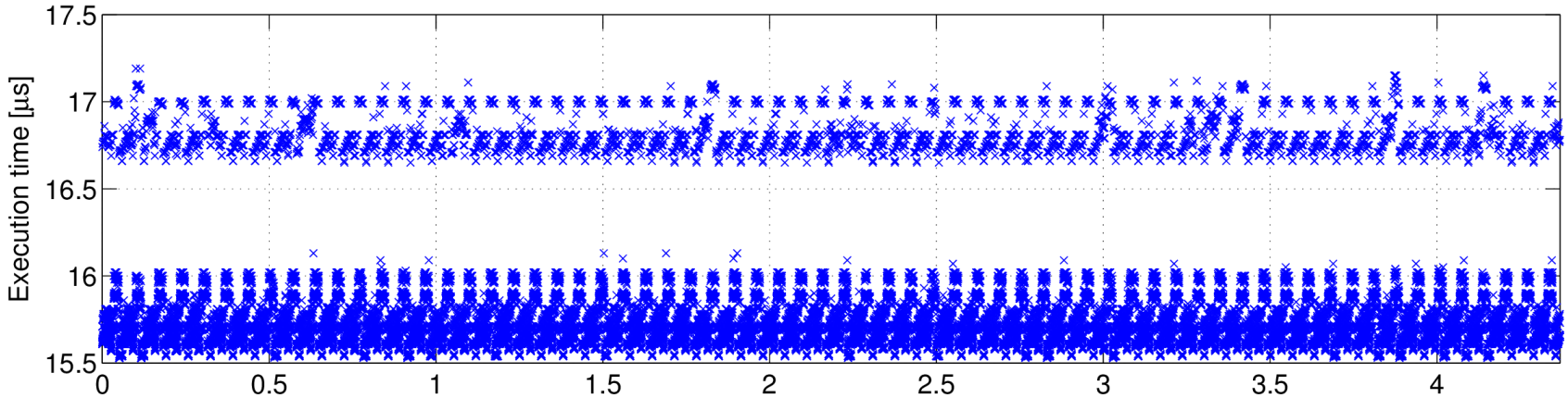
HW-in-the-loop testbed



HIL results – fault simulation



HIL under CAN bus attack



- 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