Short Paper: EMFI for Safety-Critical Testing of Automotive Systems

Colin O’Flynn

Purpose of this short paper

- Bridge between Safety & Security worlds, based on <u>*security perspective*</u>
- Encouragement of experienced embedded engineers with safety focus to use our tooling & technique.
- Demonstration of “real-world” example.

ISO 26262 Standards Fault Models?

- Several parts (each part is $/page)
- 26262-11 Section 5.1.2: Fault Modes

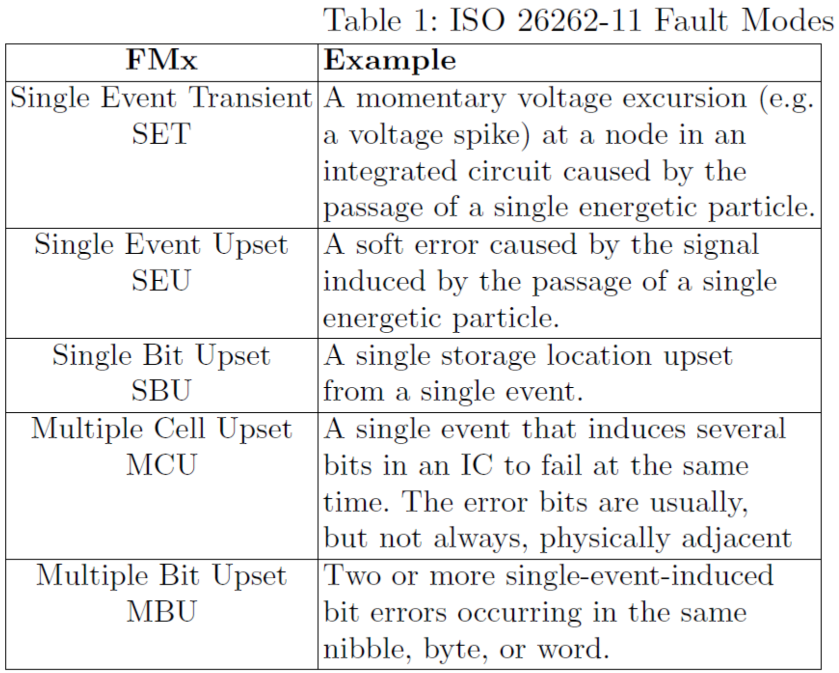


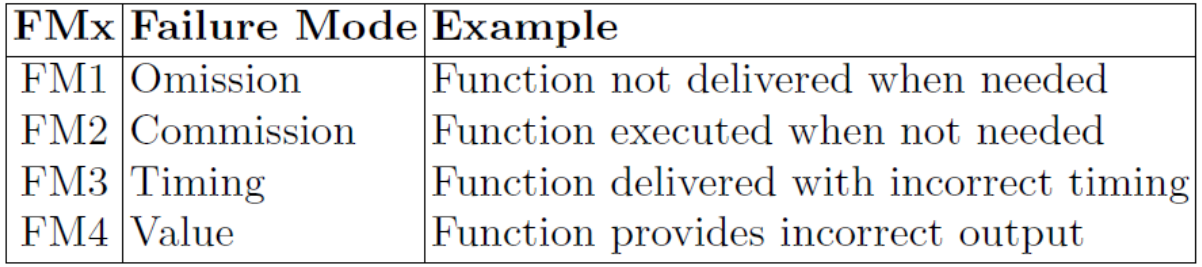
Table 1: ISO 26262-11 Fault Modes

FMx	Example
Single Event Transient SET	A momentary voltage excursion (e.g. a voltage spike) at a node in an integrated circuit caused by the passage of a single energetic particle.
Single Event Upset SEU	A soft error caused by the signal induced by the passage of a single energetic particle.
Single Bit Upset SBU	A single storage location upset from a single event.
Multiple Cell Upset MCU	A single event that induces several bits in an IC to fail at the same time. The error bits are usually, but not always, physically adjacent
Multiple Bit Upset MBU	Two or more single-event-induced bit errors occurring in the same nibble, byte, or word.

ISO 26262 Standards Fault Models?

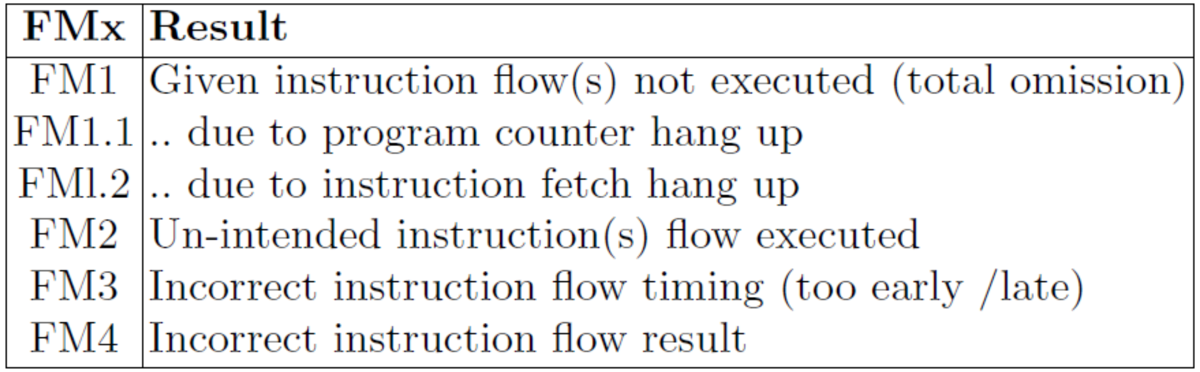
- 26262-11 Section 5.1.2”Failure Modes” & Application

Table 2: ISO 26262-11 Failure Modes

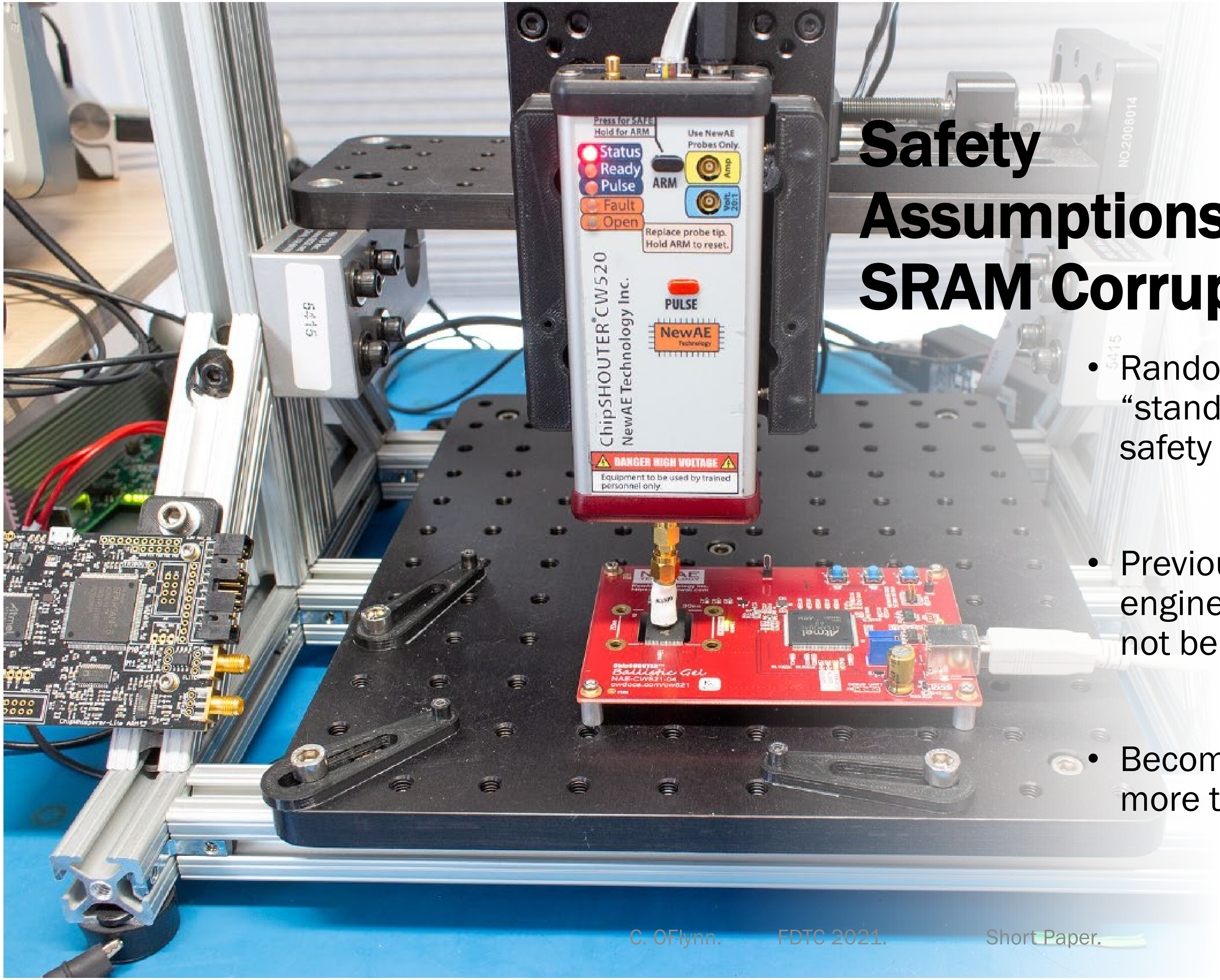


FMx	Failure Mode	Example
FM1	Omission	Function not delivered when needed
FM2	Commission	Function executed when not needed
FM3	Timing	Function delivered with incorrect timing
FM4	Value	Function provides incorrect output

Table 3: Failure Modes applied to CPU Instruction Flow



FMx	Result
FM1	Given instruction flow(s) not executed (total omission)
FM1.1	.. due to program counter hang up
FMl.2	.. due to instruction fetch hang up
FM2	Un-intended instruction(s) flow executed
FM3	Incorrect instruction flow timing (too early /late)
FM4	Incorrect instruction flow result



Safety Assumptions – SRAM Corruption

- Random bit flips of SRAM very “standard” assumption for safety engineering.
- Previous work in security engineering showed this might not be the same.
- Becomes question of setup more than fundamental fact…

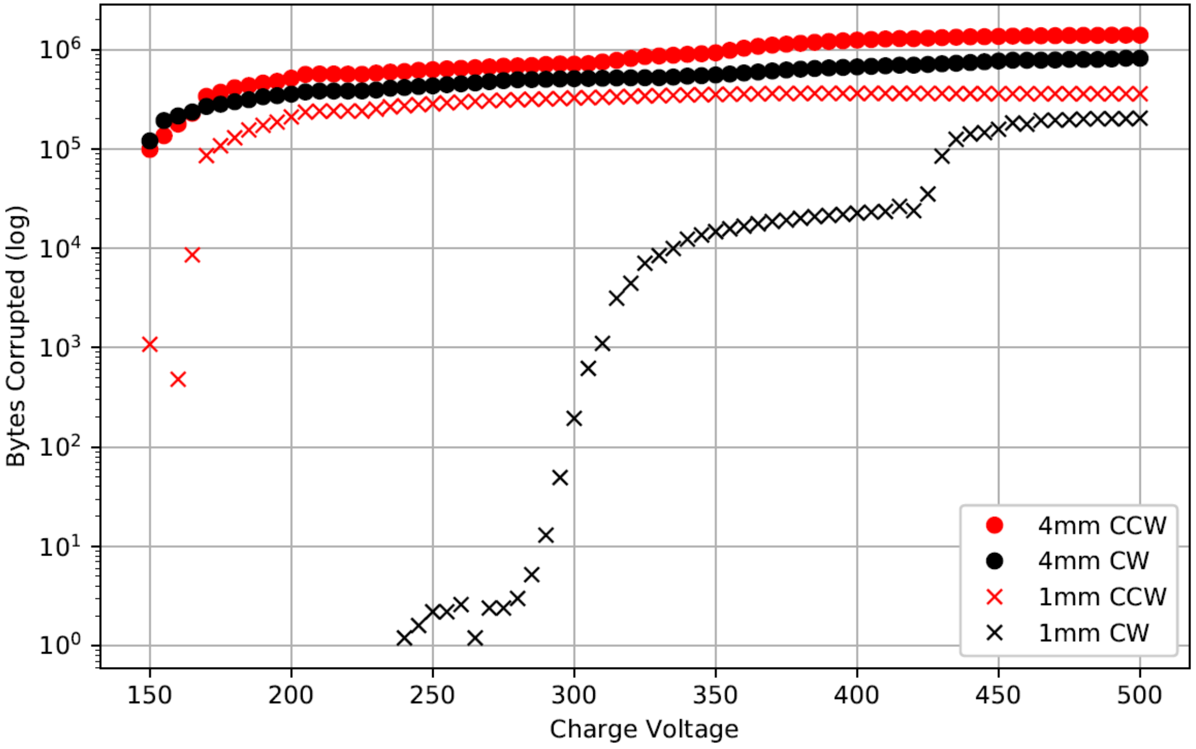
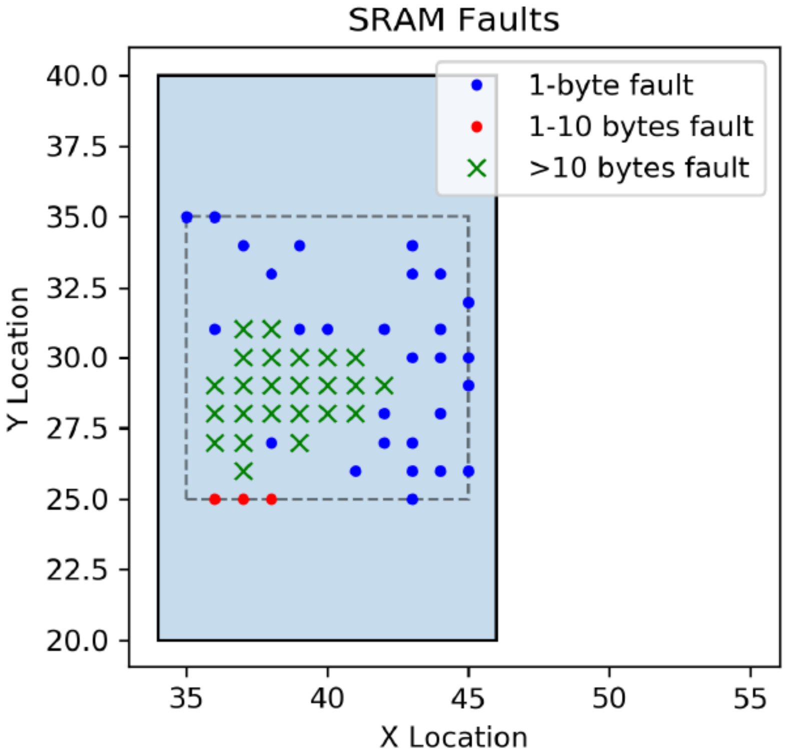


Fig. 3: Comparison of charge voltage and coils



Case Study: ECU in Toyota Corolla

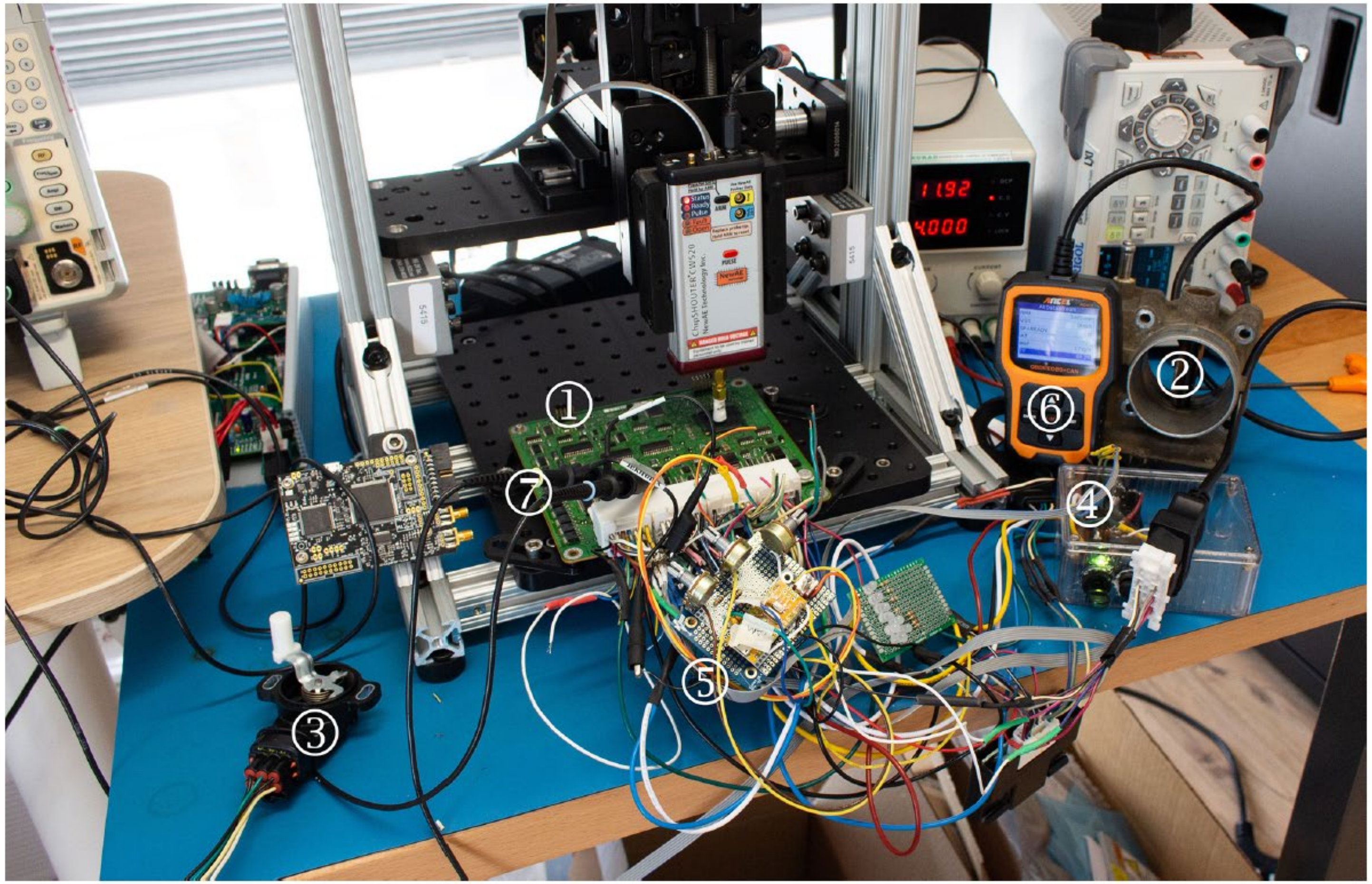
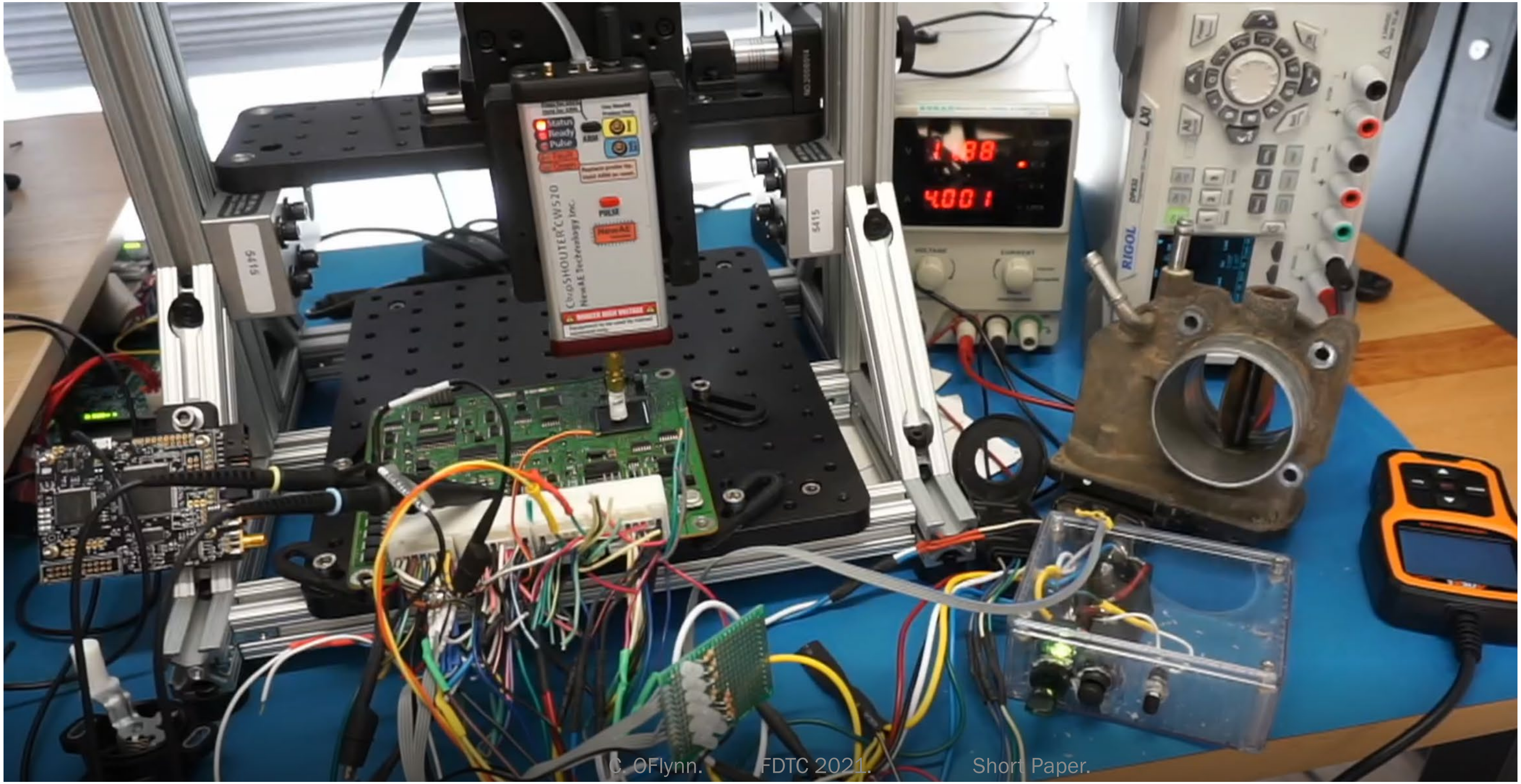
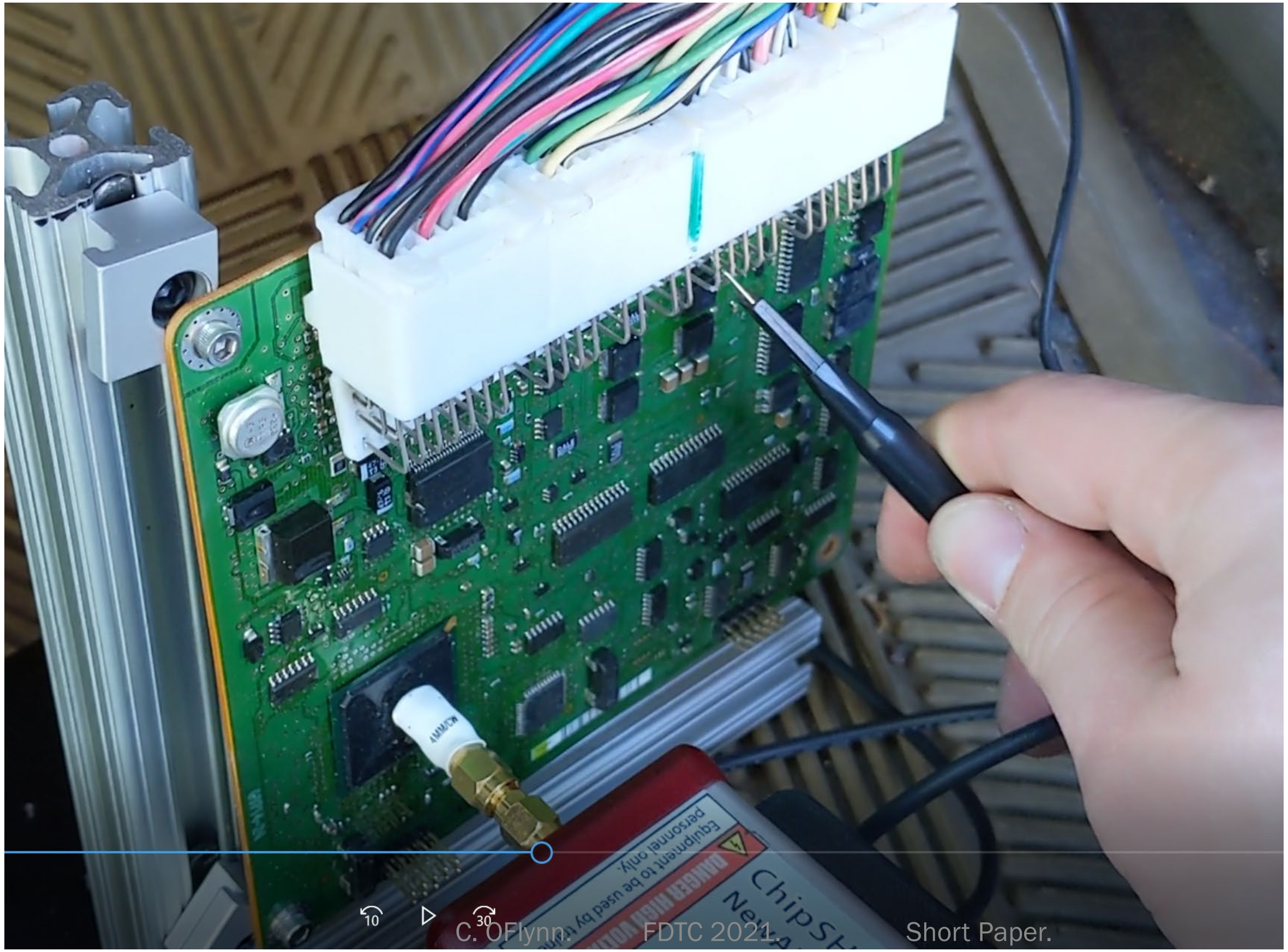


Fig. 6: The test bench showing: ① the ECU under test, ② the throttle body, ③ the position sensor, ④ the ignition switch, ⑤ sensor simulator, ⑥ OBD-II reader, and ⑦ scope probes on PWM signal.

Video Example – ECU on Bench



Video Example – ECU in Car



Conclusions

- Fault models from safety can be recreated with “security focused” equipment.

- Using black box fault attacks is possible for safety engineering.

- Considerable overlap where both safety & security can learn from relevant fields.