

PhD position : Security and Safety of Complex Systems with AltaRica (SSA)

20 03 2020 12:00

Failures of safety-critical embedded systems used in industries such as aeronautics, automotive, railway or nuclear can lead to catastrophic consequences. These more and more connected complex systems, also known as Cyber-Physical Systems (CPS), also have to face cyber-attacks, which most of time cause serious dysfunctions and undermine the security of such systems. For instance, in 2015, an attack via the SPRINT cellular network targeted a Jeep Cherokee. The vehicle happens to be fitted with a multimedia device named Uconnect, connected to a CAN bus using a Renesas V850 processor; at the software level, it also manages the cellular open TCP port 6667 to support a Dbus service for interprocess communication (IPC) and remote procedure call (RPC). The security breach consisted in injecting a modified firmware into the V850 co-processor, exploiting a “buffer overflow” error. It became then possible, and actually tested in the field, to remotely, over-the-air, inject CAN packets into the TCP port, and thus taking the hand over the car's various controls, from the radio volume to the brakes: clearly a serious design flaw...

The relationships between security and safety are thus at the heart of the current concerns of specialists in the field of complex embedded systems. In fact, one can no longer consider designing safe systems without ensuring them to be also secured. For instance, a vulnerability may compromise the functional safety of an autonomous car, while, on the other hand, a safety constraint such as the introduction of redundant components or diagnostic ports can increase the attack surface of the system. The increasing complexity of software and hardware components used in complex embedded systems has thus motivated the adoption of new approaches to anticipate security and safety problems. In particular, system designers have been advised to adopt an early modeling and validation approach against potential threats during the design phase to reduce the costs of lately detected errors and correction time.

Mots-clés : sécurité, sûreté de fonctionnement, langage formel, système embarqué, système complexe, Cyber-Physical System.

Keywords: security, safety, formal language, embedded system, complex system, Cyber Physical System.

Contact

Nga Nguyen: nn@eisti.eu, nga.nguyen@cyu.fr, 01 34 25 10 21