J3061 Cybersecurity for Cyber-Physical Vehicle Systems

The problem

With the current technological advancements in ADAS and Autonomous vehicles, an automobile can interact with countless different systems and networks. These interactions through different communication protocols (Bluetooth, CAN, OBD-II, ethernet and others) can lead to serious cybersecurity threats.

Security flaws are already readily demonstrated with the CAN protocol which contains no encryption or authentication, by default. At the source code level, an automobile today can contain up to 200M lines of code (+500M by 2025). This code can contain security flaws that can be directly exploited. There are many other attack vectors such as wireless communication and malicious executables. In the news, attacks have been demonstrated on the Jeep Cherokee brakes and engine (2015), the Nissan Leaf remote app (2015), remote unlocking vulnerability affecting many OEM (2015) and the Tesla Model S brakes disabled remotely (2016).

With all these potential venues of attack and vulnerabilities, cybersecurity is a discipline that cannot be ignored and needs to be incorporated in your system development process from the very beginning.

Our offering

The CS group possesses the know how to perform complete security assessment and security process implementation of safety critical systems through the application of J3061. The CS group can:

- Ensure the principles of Secure Design have been applied
    - Judicious application of security measures to the system architecture
    - Recommendations of best appropriate practices for security measures dealing with authentication and encryption
    - Identification of gaps in Security Architecture
- Develop the Cyber Security Case
    - Analysis of how well security requirements have been met
    - A review of any outstanding security issues
    - Evidence and argumentation that the system is “secure” to the level identified during the initial system design
    - A plan of action to address outstanding security issues

- Identification of the security goals and performing the Threat Analysis and Risk Assessment (TARA)
- Develop an understanding of how to produce documentation that will meet the certification expectations
- Perform code reviews against the CERT C secure coding standard using coding analysis tools such as LDRA
- Provide the required expertise to help automotive clients develop tailored approaches to ISO 26262 and SAE J3061 combined with insights and specialized additional knowledge gained from experience in aerospace and other technical domains

Benefits

Our customers within the automotive industry can implement J3061 rapidly and efficiently, thanks to our support, and therefore ensure that their systems will be safe, and that people's life within and around vehicles will be safeguarded.

Why CS?

In order to meet these cybersecurity challenges, the CS group has assembled a highly skilled team with substantial experience in critical real-time software development and V&V.