A Risk Assessment Framework for Automotive Embedded Systems

by Mafijul Islam, *Aljoscha Lautenbach*, Christian Sandberg, Tomas Olovsson

Abstract – The automotive industry is experiencing a paradigm shift towards autonomous and connected vehicles. Coupled with the increasing usage and complexity of electrical and/or electronic systems, this introduces new safety and security risks. Encouragingly, the automotive industry has relatively well-known and standardised safety risk management practices, but security risk management is still in its infancy.

In order to facilitate the derivation of security requirements and security measures for automotive embedded systems, we propose a specifically tailored risk assessment framework, and we demonstrate its viability with an industry use-case. Some of the key features are alignment with existing processes for functional safety, and usability for non-security specialists.

The framework begins with a threat analysis to identify the assets, and threats to those assets. The following risk assessment process consists of an estimation of the threat level and of the impact level. This step utilises several existing standards and methodologies, with changes where necessary. Finally, a security level is estimated which is used to formulate high-level security requirements.

The strong alignment with existing standards and processes should make this framework well-suited for the needs in the automotive industry.