According to a market report from McKinsey¹ “global connected car market revenues are likely to increase six-fold by 2020”. However, additional connectivity brings increased cyber security risk.

NCC Group provides cyber security training and assurance services to OEMs, tier-1 and tier-2 suppliers and connected vehicle infrastructure providers.

The profile of connected car cyber security has risen dramatically in recent years. As the complexity of vehicle systems increases, so does the attack surface and the number of potential entry points that cyber criminals can attack.

J3061 is the “Cyber Security Guidebook for Cyber-Physical Vehicle Systems”. It has been produced by the VESSC (Vehicle Electrical System Security Committee) at the SAE (Society of Automotive Engineers) and has been widely reported as “the world’s first standard on automotive cybersecurity”. However, strictly speaking it’s not a standard, rather a guidebook containing a set of high-level guiding principles for cyber security as it relates to automotive cyber-physical systems.

The document recommends that a cyber security process be applied for all automotive systems that are responsible for functions that are ASIL (Automotive Safety Integrity Level) rated per ISO 26262, or that are responsible for functions associated with propulsion, braking, steering, security or safety.

It also recommends that a cybersecurity process be applied for automotive systems that handle PII (Personally Identifiable Information). This point is particularly relevant within the European Union, as the GDPR (General Data Protection Regulation) can enforce tough penalties²: “organisations can expect fines of up to 4% of annual global revenue or €20 million, whichever is greater” as a result of a breach of the regulations.

However, privacy legislation in other jurisdictions around the world, for example North America, can also result in severe sanctions for non-compliance.
Training Objectives

The objective of the J3061 course is to provide an overview of Automotive Cyber Security in order for the attendees to gain an understanding of each of the guiding principles with a deep dive into initial and critical elements within.

NCC Group has been advocating the use of a Secure Development Lifecycle within the Automotive sector for several years now – one of the key recommendations within J3061.

This training course clearly explains how J3061 can be integrated into your current development practices and how it aligns to the ASDL (Automotive Secure Development Lifecycle).

Implementation of such a framework should be considered by those wanting to increase their capability maturity, however it is not a requirement to accept or implement it in its entirety.

Duration

This is a 1-day course and can either be delivered at your premises or at one of our NCC Group offices.

Sources