SAE J3061

Introduction to Cyber Security (IT-30)

An *Attendance Certificate* shall be issued to each participant

Duration	1 day
Prerequisites	None
Language	Italian or English
Training material	English

Programme

Part 1 - Introduction and Purpose

Part 2 - General Approach
- 2.1 SAE J3061 Process Overview
  - 2.1.1 Functional Safety VS Cybersecurity
  - 2.1.2 Key principles
  - 2.1.3 Cybersecurity Management
  - 2.1.4 Process Implementation
- 2.2 Other standards

Part 3 - AUTOSAR Security Support
- 3.1 AUTOSAR overview
- 3.2 AUTOSAR security modules overview

Part 4 - Basic Security Requirements
- 4.1 Overview about the adopted approach
- 4.2 Basic Security Requirements
  - 4.2.1 Secure ECU Modes
    The secure ECU Modes represent stages in the ECU lifetime from production to field to disposal
  - 4.2.2 Secure Diagnostics
    They ensure the safe behavior in terms of liability and legal duties
  - 4.2.3 Privacy Protection
    The applicable protection to Identifiable Data, Personal Data and Secret Data
  - 4.2.4 ECU Unique Identifier (ECU-UID)
    Rules for ECU identification
  - 4.2.5 Handling and Management of Security Artifacts
    Cryptographic methods and base practices for data that requires special protection
  - 4.2.6 Software Robustness
    SW reuse concept and secure SW development: boot mechanism and data storage
  - 4.2.7 Hardware Robustness

Exida Development, via Ribes 5, 10015 Colleretto Giacosa (TO), Italy
info@exida-dev.com
+39 0125 1925 223

What it means to design and build a safe and protected HW

4.2.8 Secure Date and Time

Secure vehicle time used by the Secure Onboard Communication

4.2.9 Secure Onboard Communication

Diagnostics services for key management and secured messages transport

4.2.10 Manipulation Detection

Monitoring of basic and extended protection and of unprotected behaviors

4.2.11 Secure Feature Activation

Secure Tokens and activation / deactivation of the SW features

4.3 Project-Specific Security Measures

Functional/Technical Cybersecurity Concept

Part 5 - SAE J3061 Threat Analysis and Risk Assessment (TARA)

5.1 Threat Identification, Risk Assessment / Threat Classification, Risk Analysis

5.2 Methods and techniques (EVITA, ETSI TVRA, OCTAVE, HEAVENS ...)

5.3 Confidentiality, Integrity, and Availability (CIA) analysis

5.4 Examples