MICROSAR Cybersecurity

Agenda VectorAcademy

Delivery Format:	This Course is offered in Classroom **or** in Remote Format
Duration:	Classroom: 2 days Remote: 14 hours
Target Group:	ECU Developers
Prerequisites:	Participation in the "AUTOSAR Classic Platform Course" or good knowledge about AUTOSAR Classic Platform
Goal:	Obtain an overview on the usage of Cybersecurity in an AUTOSAR based ECU and acquire practical skills to configure a MICROSAR Cybersecurity Basic Software

1. **Introduction to Basics in Automotive Cybersecurity**
   - Motivation for Cybersecurity in vehicles
   - Goals of Cybersecurity
   - Security principles and General approaches
   - Basics of crypto primitives
   - Solutions for implementing security primitives
   - Use cases

2. **Basic Concepts**
   - Basic concepts primitives
   - Basic concepts keys
   - Basic concepts jobs
   - Basics AUTOSAR crypto stack

3. **Walk-through Example: Cipher-based Message Authentication Code (CMAC)**
   - Show detailed configuration of crypto jobs for CMAC generation and verification
   - Show configuration of the crypto stack (Csm, CryIf and Crypto driver)

4. **Use Cases**
   - Secure Onboard Communication (SecOC) in detail, including freshness value management
   - Configuration of Security Manager in CANoe
   - MICROSAR KeyM component, including certificate handling
   - Overview in Secure Diagnostics
   - Overview in Transport Layer Security (TLS)

5. **Exercise (DaVinci Configurator)**
   - Configuration of the Crypto Stack (with SW Crypto Driver)
   - Configuration of cryptographic keys
   - Configuration of cryptographic jobs (encrypt and decrypt, MAC generation and verification)