ISO 21434 From a Software Supplier Point of View
Software implementation of vehicle function usually contains:
- ... use-case specific application components
- ... basic software components (BSW)

- BSW components provide functionality needed for many different ECUs
  - Functionality provided by BSW includes, e.g.,
    - communication middleware
    - diagnostics protocol handling
    - non-volatile storage access
  - Standardized BSW (e.g., AUTOSAR Classic, AUTOSAR Adaptive) enables reuse of BSW and application software
Example use case:
- An ADAS application persistently stores some data
- The confidentiality of this data has been identified as a cybersecurity property
- The storage device does protect the confidentiality of the data
- AUTOSAR BSW provides transparent encryption of non-volatile data as a feature to applications

How can context-specific elements and components out-of-context be integrated into a secure system?
V-Model: Adding Components Out-of-Context

Item Definition

TARA

Derivation of Cybersecurity Goals

Cybersecurity Concept

Assumptions on Context

Assumed Technical Cybersecurity Requirements ("Assumptions on Intended Use")

Component out-of-context (provided off-the-shelf)

Basic SW Development

Vehicle project with context

Cybersecurity Validation

Item Integration and Testing

Appl. SW Development

fulfills

requires

allocates

validates

Basic SW Development

Vehicle project with context

Cybersecurity Validation

Item Integration and Testing

Appl. SW Development

4
Assumptions on Context: System Model

- There is a lot of diversity in the potential systems that the component out-of-context is being integrated into
- Challenge: Ensure that *assumed technical cybersecurity requirements* are fulfilled in specific system

- Approach: Specify a **System Model** that describes...
  - What are the elements of the system?
  - What are the trust boundaries?
  - What are the interfaces?

- **Validation** of the system model has to be performed *within the project context*:
  - Is the system model a valid model for the actual system?
  - If the model is not valid, the *assumed technical cybersecurity requirements* are not necessarily fulfilled by the component out-of-context
Assumptions on Context: HW, SW & Integration Requirements

- Assumptions fall into different categories
  - (1) Assumptions on application software
  - (2) Assumptions on integration and configuration
  - (3) Assumptions on hardware

- Examples:
  - (1) Application software calls a certain initialization function
  - (2) Integrity of executed software is ensured (e.g., via secure boot)
  - (3) Confidentiality of hardware-internal data is ensured

- **Validation** of the assumptions has to be performed **within the project context**:
  - If assumptions are not fulfilled in the project context, the assumed technical cybersecurity requirements are not necessarily fulfilled by the component out-of-context
  - Detailed information on secure integration and configuration provided in *Security Manual*
Assumed Technical Cybersecurity Requirements

The *Assumed Technical Cybersecurity Requirements* represent what the component out-of-context provides security-wise.

The project’s security concept may allocate higher-level requirements to these requirements.

**Functional requirements:**

- Usually provision of security controls
- Examples:
  - **Secure NvM:** Provide mechanisms to protect and verify the confidentiality of non-volatile data
  - **Secure Communication:** Provide mechanisms to protect and verify the confidentiality, integrity, authenticity, and freshness of network messages

**Non-functional requirements:**

- Minimization of security weaknesses through security principles and process measures
- Examples:
  - **No Denial-of-Service:** Ensure the availability of provided functionality
  - **No Information Disclosure:** Use only specified interfaces to pass information between trust domains
Vulnerability Management for Components Out-of-Context

How to decide whether an issue is a security issue?

- **Problem:**
  - There are obvious security issues (e.g., cryptography broken), but...
  - Virtually all functionality provided by the BSW could be used in the project for security reasons
  - Then: An issue in this functionality could lead to a vulnerability in the specific context

- **Approach:**
  - An issue is security relevant if it leads to a violation of an assumed technical cybersecurity requirement
  - The issue report includes the violated assumed technical cybersecurity requirement

How to assess the risk of a security issue?

- **Problem:** The risk cannot be assessed without context
  - Attack feasibility depends on the context
  - Impact depends on the context

- **Approach:**
  - Enable and support risk assessment by Tier1/OEM by including all relevant information in issue report
Collaboration model for components out-of-context has unique characteristics.

It is important to establish a common understanding of these characteristics and their implications within the complete supply chain.
For more information about Vector and our products please visit

www.vector.com

Author:
Neudecker, Till
Vector Germany