Element Cybersecurity Relevancy

Revision

Version 6
1/2/24 7:28 PM

SME

Michael Maass
Charles Wilson

Abstract

This document describes a process by which the cybersecurity relevance of an element may be determined.

License

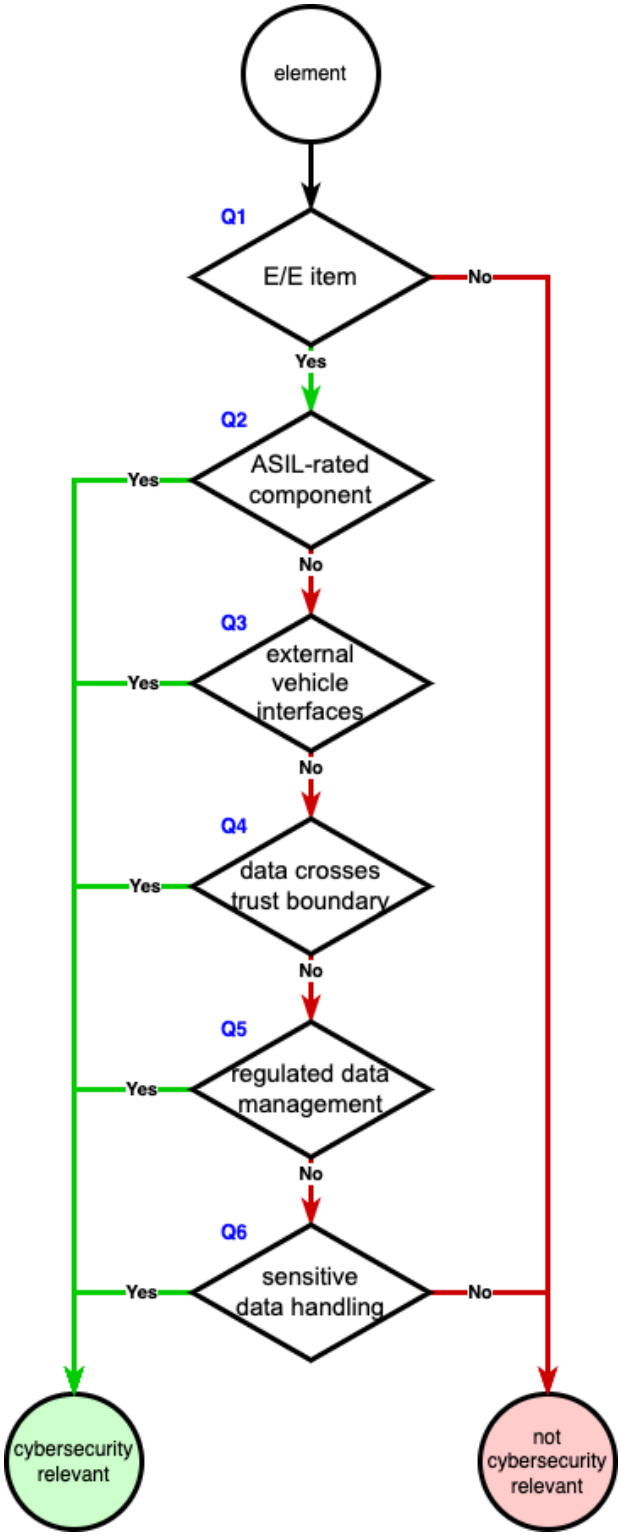
Overview

Given the complexity of the system of systems which comprise a vehicle, it is useful to have a way to reduce the scope of cybersecurity activities to those elements which are cybersecurity relevant. This document presents a process allowing for efficient identification of those elements which should have more rigorous cybersecurity treatment.

Note: The questions in this document were adapted from **ISO/SAE 21434** Annex D. They have been refined to be more actionable.

Flowchart

The following flowchart shows the manner in which the cybersecurity relevancy of a component is determined.



Questions

1. Is the element an E/E item, component, or system?

Note: The element may be hardware, software, or a combination of the two.

If the element is not an E/E item, component, or system; it is **not** cybersecurity relevant. Otherwise, the element should be considered using the following questions.

If the element fulfills **any** of the following conditions, it is considered cybersecurity relevant. If **none** the following conditions are fulfilled, it is **not** cybersecurity relevant.

2. Is the element ASIL-rated?

Note: Any non-QM **ISO 26262** ASIL rating [1] satisfies this condition.

3. Does the element have interfaces external to the vehicle?

Note: This applies to both active and inactive (disabled) interfaces.

Note: User accessible interfaces within the vehicle should also be considered.

4. Does the element handle data that crosses a trust boundary?

Note: Trust boundaries include, but are not limited to; physical, privilege, and network.

5. Does the element collect or process personally identifiable information (**PII**) or any other regulated user data?

Note: This covers data regulated by the EU (under GDPR) and other jurisdictions.

6. Does the element directly handle sensitive data?

Note: Sensitive data includes executables, configuration data, databases, unstructured data, credentials, and logs. These are detailed in the **Security Requirements Taxonomy** [4] **AVCDL** secondary document.

Disposition

Elements determined to be cybersecurity relevant are subject to treatment for association of cybersecurity requirement as detailed in **Product-level Security Requirements** [2] and reviewed **Design Showing Security Considerations** [3].

References

1. **ISO 26262-3:2018 Road vehicles – Functional safety – Part 3: Concept phase** https://www.iso.org/standard/68385.html
2. **Product-level Security Requirements** (AVCDL secondary document)
3. **Design Showing Security Considerations** (AVCDL secondary document)
4. **Security Requirements Taxonomy** (AVCDL secondary document)