Design Showing Security Considerations

# Revision

Version 5

7/22/22 10:39 AM

# SME

Charles Wilson

# Abstract

This document details the process used to determine the applicability of cybersecurity requirements to product elements under consideration.

# Group / Owner

Development / Software Developer

# Motivation

**ISO/SAE 21434** mandates that cybersecurity requirements be established for all cybersecurity-relevant items of a product.

# License

This work was created by **Motional** and is licensed under the **Creative Commons Attribution-Share Alike (CC BY-SA-4.0)** License.

[**https://creativecommons.org/licenses/by/4.0/legalcode**](https://creativecommons.org/licenses/by/4.0/legalcode)

# Overview

The following diagram illustrates the process to be used for associating cybersecurity (non-functional) requirements with product element’s functional requirements:

Diagram

Description automatically generated

Since requirements are tracked in a requirement tracking system, traceability is established through its use.

This will support for the following:

* Verification of security consideration prior to development
* Information for V&V activities
* Refinement of the cybersecurity threat model
* Verification of implementation of security considerations

# Process

## Design Security Analysis

|  |  |
| --- | --- |
| Inputs | Element development design  Product-level security requirements catalog |
| Outputs | identified security requirements |
| Participants | Security SME  Development SME |

Diagram

Description automatically generated

A **Development SME**, working in conjunction with a **Security SME**, will review the product element’s design and identify applicable requirements from the product-level cybersecurity catalog **[1]**. The **Security SME** will generate a **Design Security Analysis Report**. Should deficiencies in either the **Element Development Design** or the **Product-level Security Requirements Catalog** be identified, updates will be made. The design security analysis should consider the best practices described in **Secure Design Principles [2]**.

## Applicability Analysis

|  |  |
| --- | --- |
| Inputs | Identified security requirements |
| Outputs | Updated development requirements |
| Participants | Development SME |

Diagram

Description automatically generated

The Development SME will attach the identified (non-functional) security requirements to the applicable product element functional requirements as a strict dependency. This results in an updated set of development requirements. A **Requirements Report** is produced.

**Note:** Additional artifacts may be generated from the requirement tracking system as needed for audit purposes.

# Notes

1. The global cybersecurity requirements catalog is a set of cybersecurity requirements based on a gap analysis of existing cybersecurity requirements viewed through the lens of the **Security Requirements Taxonomy**. This global catalog serves as the basis for the product-level catalog, which is tailored to the product during the requirements phase. It is this specialized catalog referenced here.

# References

1. **Security Requirements Taxonomy** (AVCDL secondary document)
2. **Secure Design Principles** (AVCDL secondary document)