Security Design Review Report

# Revision

Version 3

9/8/23 11:32 AM

# SME

Charles Wilson

# Abstract

This document describes the process to create a security design review report and information contained within it.

# Group / Owner

Security / Systems Requirements Planner

# Motivation

This document is motivated by the need to have traceability of the certification work products required for the certification of safety-critical, cyber-physical systems, such as **ISO/SAE 21434** and **ISO 26262**. Specifically, we need to document the outcomes of the review of the design process to determine the security deficiencies of the element being reviewed.

# License

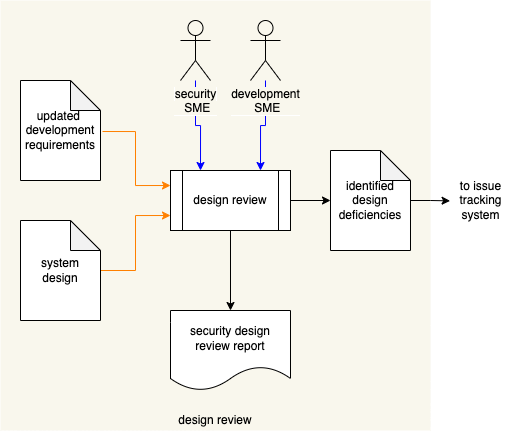
This work was created by **Motional** and is licensed under the **Creative Commons Attribution-Share Alike (CC BY-SA-4.0)** License.

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

# Overview

The **Security Design Review Report** captures the security deficiencies discovered during the security design analysis **[1]** process. This report is used to ensure that those discoveries are properly disposed.

The following diagram illustrates the process to be used:



# Process

## Design Review

|  |  |
| --- | --- |
| Inputs | system design  updated development requirements |
| Outputs | identified design deficiencies |
| Participants | Security SME  Development SME |

Diagram

Description automatically generated

A **Development SME**, working in conjunction with a **Security SME**, will review the system’s design based on the **updated development requirements** established in the activities described in **Design Showing Security Considerations** **[1]**. The **Security SME** will generate a **Security Design Report**. If deficiencies are identified, these will be enumerated and entered into the issue tracking system for remediation.

### Design Review Report

The design review report should detail the security deficiencies exposed during the design review. The report should be organized into summary and details sections. The summary includes:

* Description of the system
* Image of the system (typically a DFD)

The details section contains one or more diagrams. Each of these is organized into summary and data flow sections. The summary includes:

* Diagram title (unique)
* Description of the diagram’s scope
* Image of the diagram

Individual data flows are used to organize the individual deficiencies. Each of these is organized into a summary and deficiency list. The summary includes:

* Data flow ID (unique)
* Source of the data flow (originator)
* Destination of the data flow (recipient)
* Description of the data flow (payload)
* Image of the data flow in isolation

Individual deficiencies include:

* ID (unique)
* Category (**property** from the **Security Requirements Taxonomy [2]**)
* Security requirement not being satisfied (from the **updated development requirements**)
* Summary of the deficiency
* Detailed description of the deficiency
* Recommendation for remediation

It is recommended that the report be generated from a portable data representation so that it can be programmatically manipulated.

# References

1. **Design Showing Security Considerations** (AVCDL secondary document)
2. **Security Requirements Taxonomy** (AVCDL secondary document)