# Product-level Security Requirements

## Revision

Version 4
11/15/21 9:33 AM

## Content

Marwan Abi-Antoun

## Abstract

This document describes the process for creation of a set of security requirements to be used within a specific product.

## Group / Owner

Security / Security Architect

## Motivation

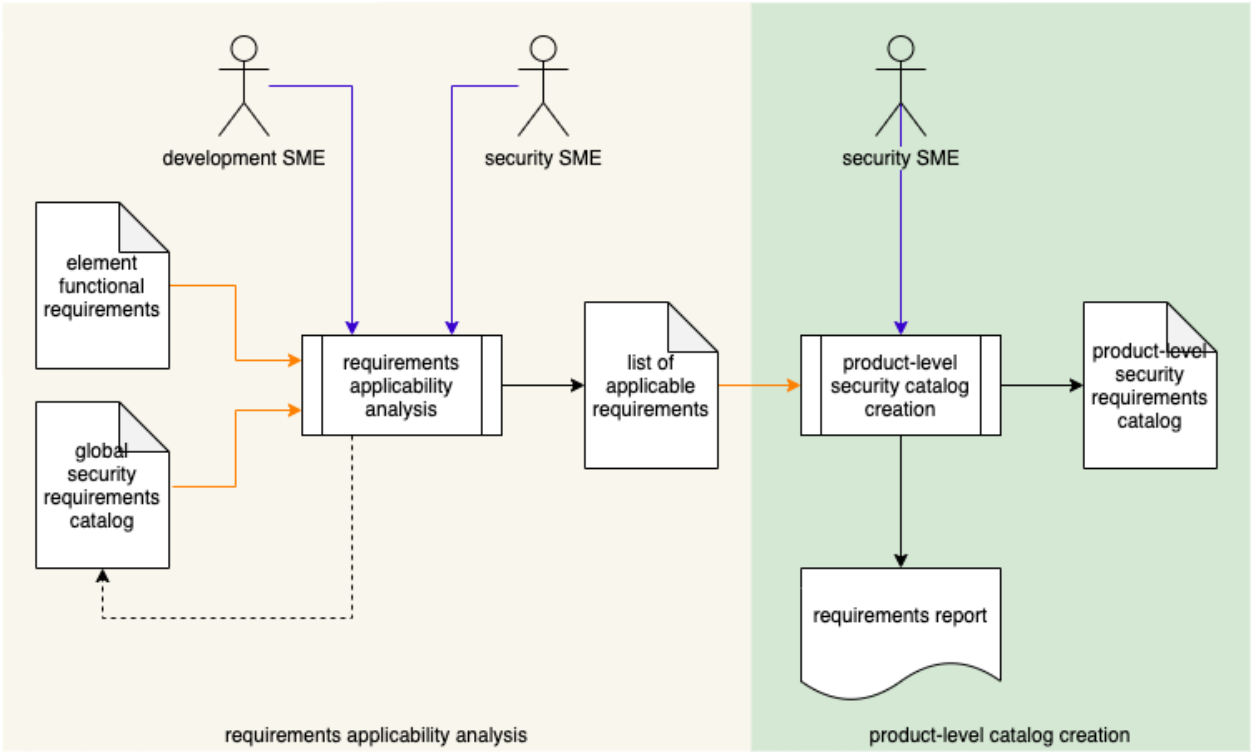
This document is motivated by the need to have formal processes in place for the creation of security requirements for the development of safety-critical, cyber-physical systems for certification of compliance to standards such as **ISO 21434** and **ISO 26262**.

## License

# Overview

Using the set of global security requirements as a base, the product under consideration is reviewed to determine what requirement tailoring is necessary.

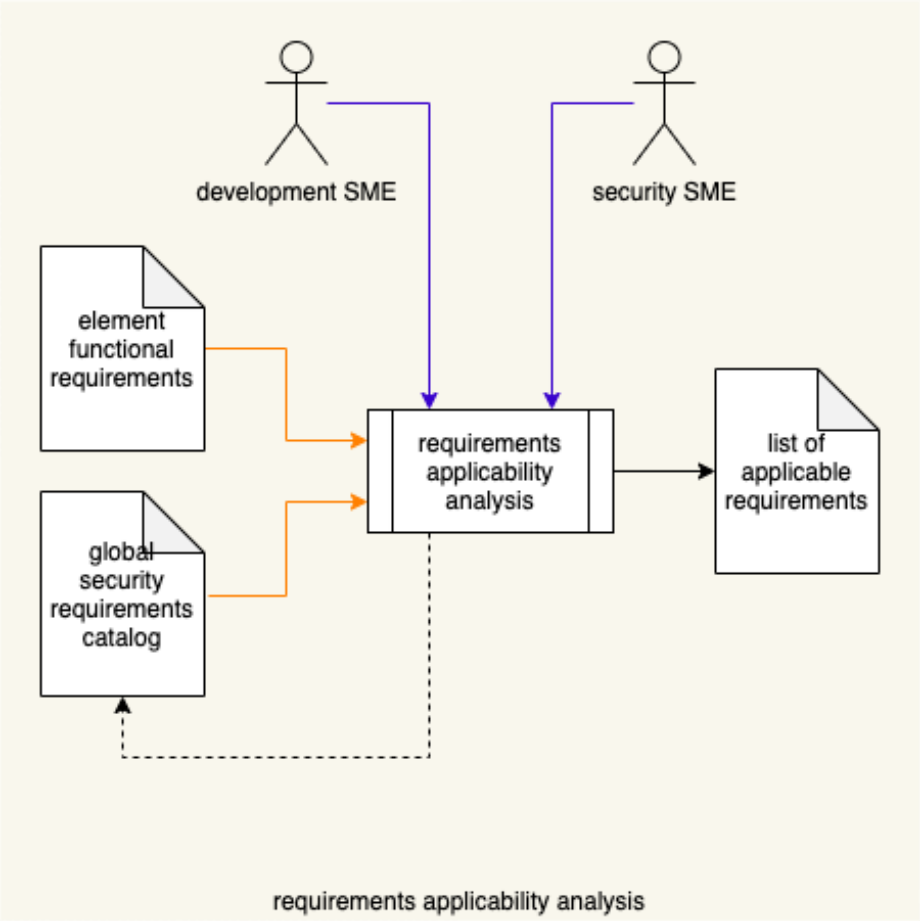
The following diagram illustrates the process used for creation of the product-specific security requirements catalog:



# Process

## Requirements Applicability Analysis

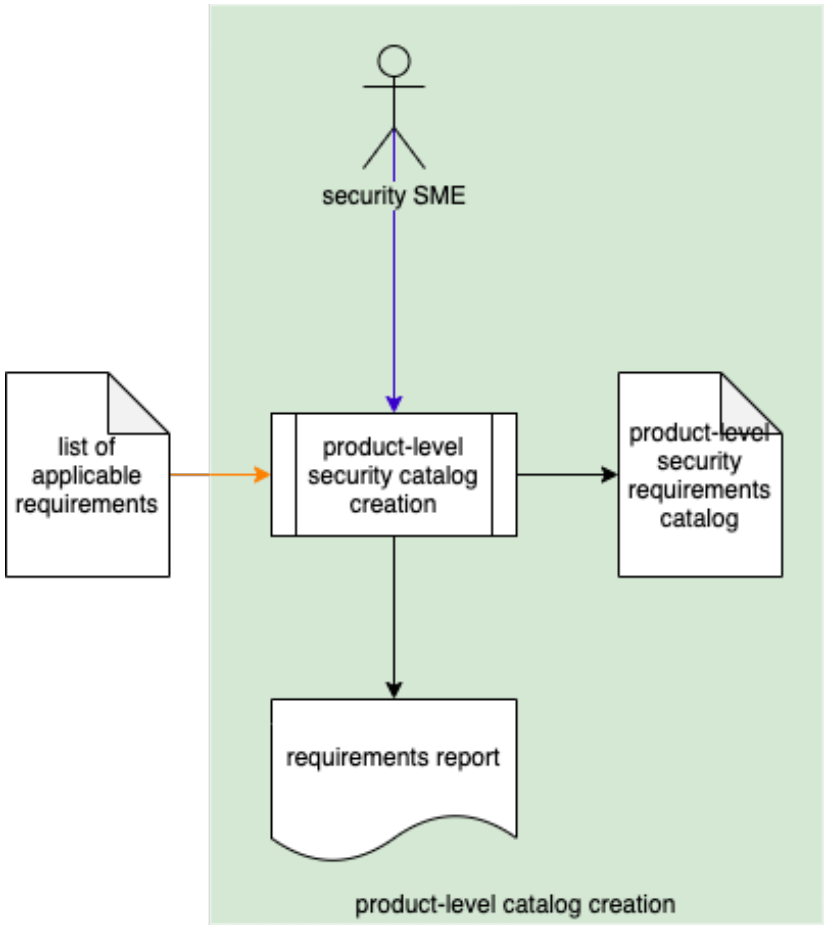
| | |
|---|---|
| Inputs | Element functional requirements<br>global security requirements catalog |
| Outputs | List of applicable security requirements |
| Participants | Security SME<br>Development SME |




The Security SME, together with Development SME(s), review the element's functional requirements against the global security requirements catalog. Requirements applicable to the element are identified. If gaps are identified in the global security requirements catalog, it will be updated. Additional detail is provided below.

# Product-level Catalog Creation

| | |
|---|---|
| Inputs | List of applicable security requirements |
| Outputs | Product-level security requirements catalog |
| Participants | Security SME |




The Security SME creates an element-specific product-level security requirements catalog from the list of applicable requirements generated during applicability analysis. These requirements are tailored to the element. A human-readable version of the catalog is generated for audit purposes.

# Applicability Analysis Detail

## Requirement Categorization

During applicability analysis the product requirements will be used to categorize requirements from the global security requirements catalog.

The requirements fall into the following categories:

| Category | Description |
|---|---|
| Not Applicable | These are global security requirements not applicable to the product based on its functionality. They are added to the product-level catalog but include a justification as to why they do not apply. |
| As Is | These global security requirements are applicable without modification to the product based on its functionality. They are added as is to the product-level catalog but may include additional comments. |
| Derived | These global security requirements are applicable but need to be specialized for the product. They are added to the product-level catalog and become derived. As part of the specialization, additional details are included in the derived copy. |
| New | These are additional, product-specific security requirements dictated by the product's unique functional requirements and do not have counterparts in the global security requirements catalog. |

**Note:** Global security requirements determined to be **not applicable** are retained (along with their justification) for auditing purposes.

**Note:** If functional requirements are available, they may be used in conjunction with the design.

**Note:** All product-level requirements stemming from the global requirements maintain links to their corresponding global security requirements.

**Note:** Changes to the functional requirements will necessitate a review of the product-level security requirements and their categorization.

# Requirement Analysis

The requirement categorization might be performed using a mix of top-down and bottom-up methodologies.

One such top-down analysis would be to use the notion of security topics. For instance, if a product deals with secure communication, the global security requirements tagged with that topic would be identified as relevant and included as product security requirements.

A bottom-up analysis might take the form of definition and use of concrete assets for the product. This might be done as follows:

1. Enumerate the concrete assets in the product based on a conceptual definition of the product, as well as the product's functional requirements.
2. Establish sub-typing relations between the product's concrete assets and the abstract assets from the security requirements taxonomy (each concrete asset is derived from an abstract one).
3. Review the global security requirements linked to the relevant abstract assets and include them as derived product security requirements.

# Implementation

The procedure for tailoring project security requirements is documented separately [2]. The procedure clarifies the notion of links, and how product security requirements are kept in their own workspace or project in the requirement management tool, one that is separate from the workspace for the global security requirements catalog.

# References


1. **Security Requirements Taxonomy** (AVCDL secondary document)
2. **Product-level Security Requirements Catalog Creation** (AVCDL tertiary document)