Element-level Security Requirements Catalog Creation Procedure

Revision

Version 3
4/11/25 6:39 PM

SME

Charles Wilson

Abstract

This document describes the procedure used to perform the cybersecurity requirements tailored catalog creation activity described in the AVCDL secondary document **Element-level Security Requirements** [2].

Group / Owner

Security / Security Architect

Motivation

This document is motivated by the need to have element-appropriate cybersecurity requirements. This is necessary given the nature of safety-critical, cyber-physical systems, subject to certifications such as **ISO/SAE 21434** and **ISO 26262**.

Note: Within the context of this document, the terms ***security*** and ***cybersecurity*** are used interchangeably. It is presumed that the term ***security*** is being used in reference to ***cybersecurity*** and not ***physical security***.

Audience

The audience of this document is the cybersecurity practitioner who will be conducting the cybersecurity requirements catalog creation.

Disposition of Output

Once completed, the generated output should be managed in the organization's requirements management system (RMS) as a document of record.

Entry Criteria

This document assumes that the reader understands the purpose of the cybersecurity requirements management. Further, that the reader has read and understood the AVCDL **Element-level Security Requirements** secondary document.

Prerequisites – Cybersecurity SME

Qualifications

It is required that the cybersecurity SME is both a qualified and trained security architect (shown above on title page as **Owner**) as defined by the **NIST NCWF** role SP-ARC-002 and detailed in section **12.7 Security Architect** of the AVCDL primary document [1].

Knowledge

It is required that the cybersecurity SME understands the purpose of a cybersecurity requirements tailoring and requirements management.

Background Information

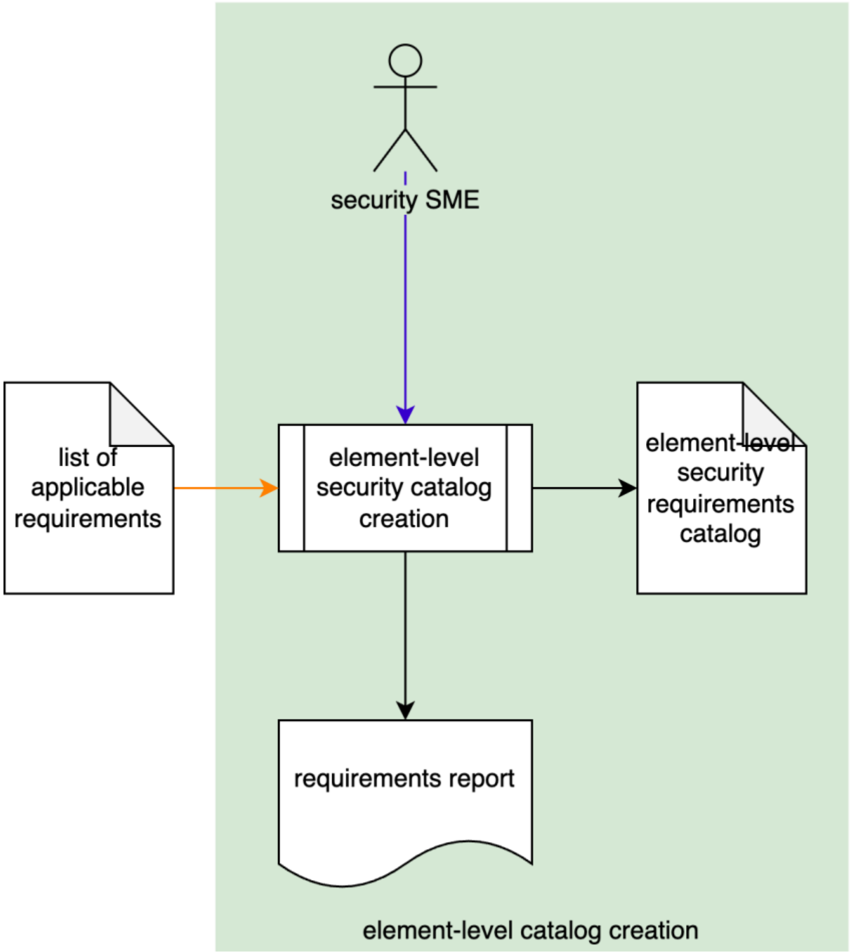
It is required that the cybersecurity SME has read and understands the AVCDL **Element-level Security Requirements** and **Security Requirements Taxonomy** [3] secondary documents. Additionally, that the cybersecurity SME has taken training relevant to this activity.

Prerequisites – Input Materials

It is required that the cybersecurity group provides a list of cybersecurity requirements applicable to the element under consideration.

Catalog Creation Activity

The workflow diagram for the tailored catalog creation activity of the **Element-level Security Requirements** is shown below.


security SME
list of applicable requirements
element-level security catalog creation
element-level security requirements catalog
requirements report
element-level catalog creation

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

Methodology

The approach to take when performing the catalog creation activity is to deduplicate and/or tailor the **list of applicable requirements** and then assign the resultant **element-level security requirements catalog** entries to their corresponding element functional requirements.

Note: Deduplication and tailoring may be done in any order. It may make sense to do one first depending upon the particulars of the requirement under consideration.

Note: It is possible that neither tailoring nor deduplication are required.

Deduplication

The process of deduplication is straightforward. Duplicate requirements within the **list of applicable requirements** are removed.

Note: Only those requirements which are identical are applicable to this step.

Tailoring

When a requirement lacks sufficient specificity to enable its application, it is necessary to tailor the requirement. Such tailoring yields a derivative requirement with additional constraints.

Note: Any additional constraints applied to the derivative requirement should be both minimal and not break its INCOSE compliance.

Assignment

Once any necessary deduplication and tailoring has been performed on the **list of applicable requirements**, what remains is the **element-level security requirements catalog**. This set of cybersecurity requirements is then attached to the element’s functional requirements with an “**is constrained by**” relationship.

Note: Because of deduplication, there may be a **many-to-many** relationship between the cybersecurity requirements and the element’s functional requirements.

Requirements Catalog Template

The element cybersecurity requirements catalog may be documented using the **AVCDL element cybersecurity requirements catalog template** Microsoft Excel workbook [4].

Note: Other forms of documentation are permissible so long as they provide the information laid out in this document.

There are five sections in the workbook. They are:

- Cover sheet
- Revision history
- Reference documents
- Catalog
- Legend

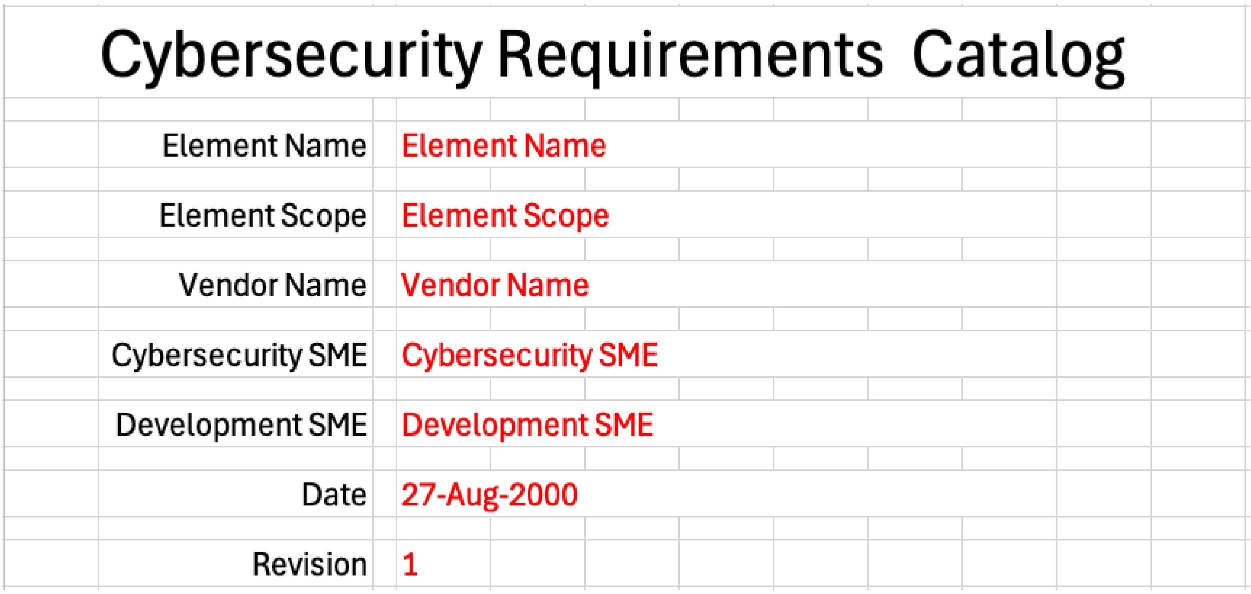
These sheets will be addressed in turn.

Duplication of Rows in the Various Sheets

When there is the need to add rows to the various sheets of the workbook, be sure to duplicate an existing row. This is because validation checks are attached to some of the cells which also enables the use of dropdown lists.

Cover Sheet

The **cover sheet** of the workbook is shown below:



Cybersecurity Requirements Catalog

Element Name	Element Name
Element Scope	Element Scope
Vendor Name	Vendor Name
Cybersecurity SME	Cybersecurity SME
Development SME	Development SME
Date	27-Aug-2000
Revision	1

Fields to be completed are shown in **red**.

Element Name

The **element name** is the element under analysis.

Element Scope

The scope of the element is left to the discretion of the customer. Examples of element scopes include system, sub-system, component, component software (non-OS), and component OS.

Note: In this context, **the customer** refers to the entity requiring the analysis activity.

Vendor Name

This is the name of the vendor responsible for the element under analysis.

Cybersecurity SME

This is the cybersecurity subject matter expert performing the analysis.

Development SME

This is the development subject matter expert providing element information for the analysis.

Date

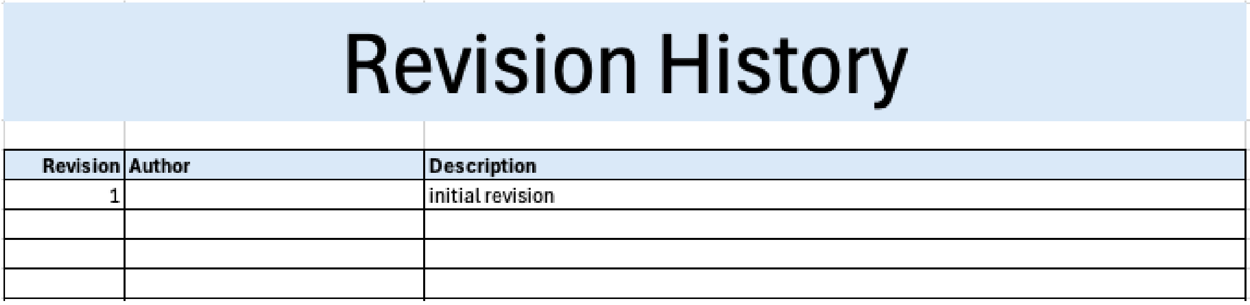
This is the date when the analysis of the element model was performed or updated. The date should be updated whenever the analysis is updated.

Revision

This is the revision number of the document. The revision number is a monotonic and increasing integer, starting at 1. It should be incremented every time the document is updated.

Revision History

The **revision history** sheet of the workbook is shown below:



Revision History

Revision	Author	Description
1		initial revision

Revision

The **revision** corresponds to that listed on the cover sheet.

Author

The **author** corresponds to the cybersecurity SME listed on the cover sheet.

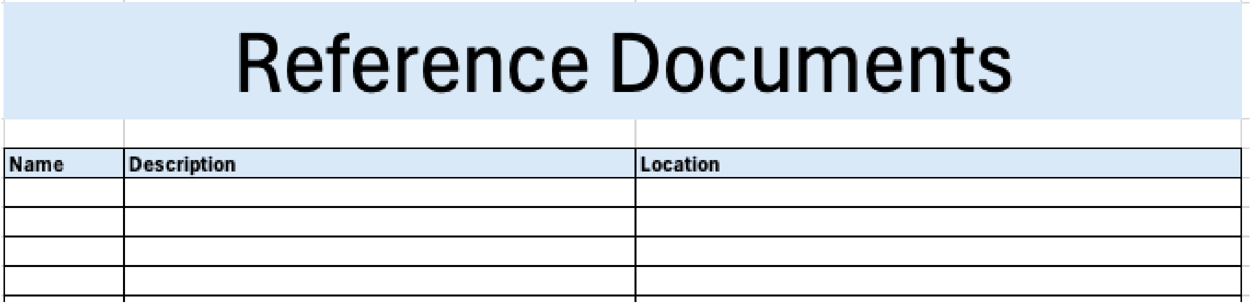
Description

This is a brief description of changes made to the analysis since it was last updated.

Reference Documents

Note: These references are those necessary for the analysis of the element model.

The **references** sheet of the workbook is shown below:



Reference Documents

Name	Description	Location

Note: The element model need not be included as its location is shown on the cover sheet.

Name

This is the name of the document being referenced.

Description

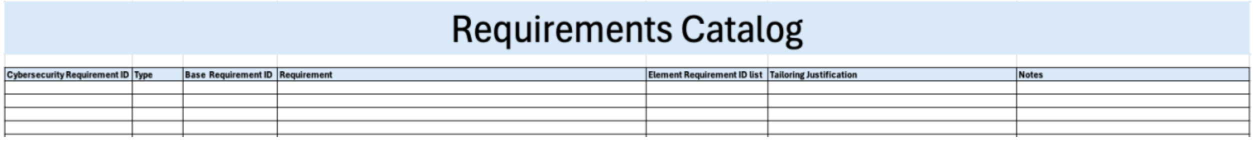
This is a brief description of the document being referenced.

Location

This is the location of the document being referenced. It may be a physical location or a URL.

Catalog

The **catalog** sheet of the workbook is shown below:



Requirements Catalog

Cybersecurity Requirement ID	Type	Base Requirement ID	Requirement	Element Requirement ID list	Tailoring Justification	Notes

Cybersecurity Requirement ID

This is the unique ID of the cybersecurity requirement.

Type

This is the type of the requirement with respect to the element. The type may be one of the following:

- As Is
- Derived

Note: Unless the requirement has been tailored, **as is** should be selected.

Base Cybersecurity Requirement ID

This is the unique ID of the base cybersecurity requirement tailored for the element.

Requirement

This is the description of the requirement.

Element Requirement ID list

This is the list of unique IDs of the element-specific functional requirements to which the cybersecurity requirement applies.

Tailoring Justification

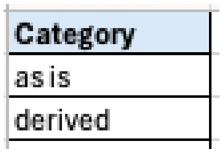
This is a justification for having tailored the base cybersecurity requirement for the element.

Notes

This is a general notes field.

Legend

The **legend** sheet of the workbook is shown below:



Category
as is
derived

The **legend** sheet information is used to make the completion of the document easier by providing dropdown lists for common values. It also ensures that spelling errors do not creep into the generated material.

Note: The legend sheet should not be edited. If an unlisted value is required, the template should be separately revised.

Exit Criteria

This procedure is considered complete once the generated output has been entered into the organization’s RMS as a document of record.

Note: The processes and procedures for entering documents into the RMS, or the updating thereof, are outside the scope of this document.

References

1. **AVCDL** (AVCDL primary document)
2. **Element-level Security Requirements** (AVCDL secondary document)
3. **Security Requirements Taxonomy** (AVCDL secondary document)
4. **AVCDL element cybersecurity requirements catalog template** (AVCDL template)