Element-level Security Requirements Macro Requirements Procedure

Revision

Version 3
4/11/25 6:34 PM

SME

Charles Wilson

Abstract

This document describes the procedure used to create macro cybersecurity requirements supporting the 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 macro requirements 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 macro creation. 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 macro requirement creation.

Background Information

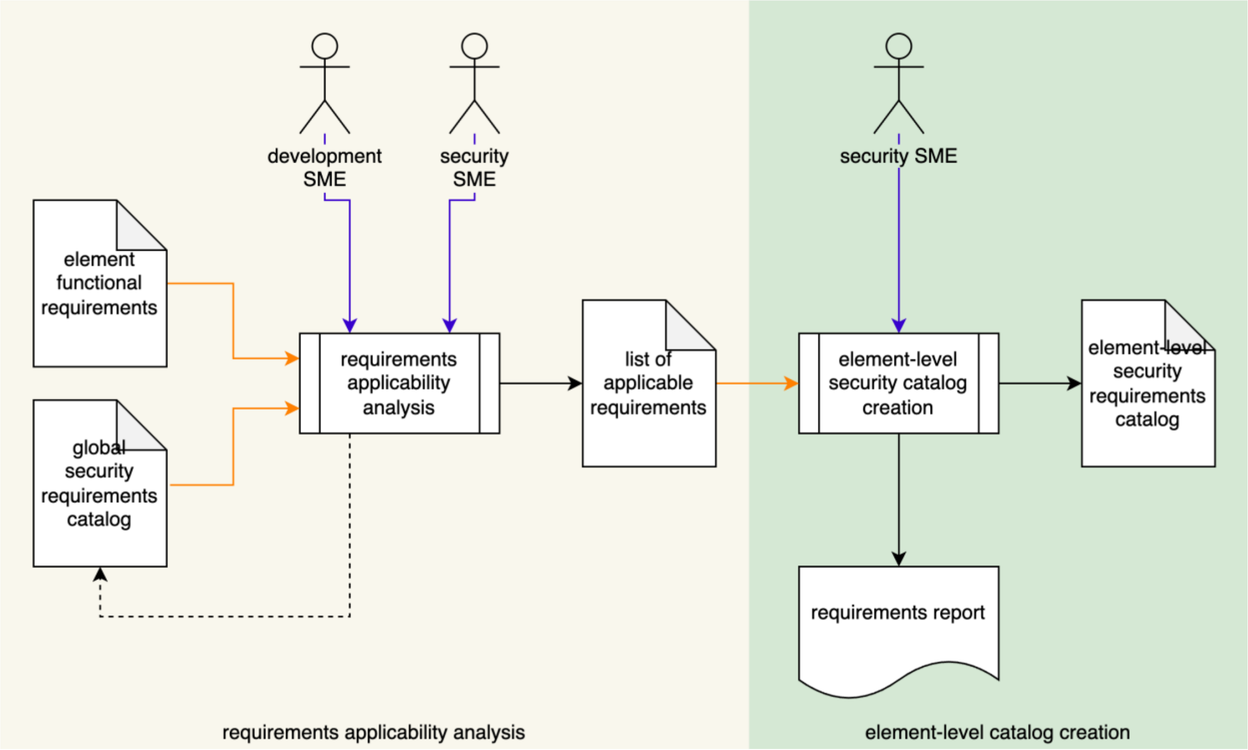
It is required that the cybersecurity SME has read and understands the AVCDL **Element-level Security Requirements** and **Security Requirements Taxonomy** [3] secondary documents. Additionally, that the cybersecurity SME has taken training relevant to this activity.

Prerequisites – Input Materials

It is required that the cybersecurity group provides a global security requirements catalog. It is also required that there is sufficient documentation available for the creation of the macro.

Security Requirements Process Review

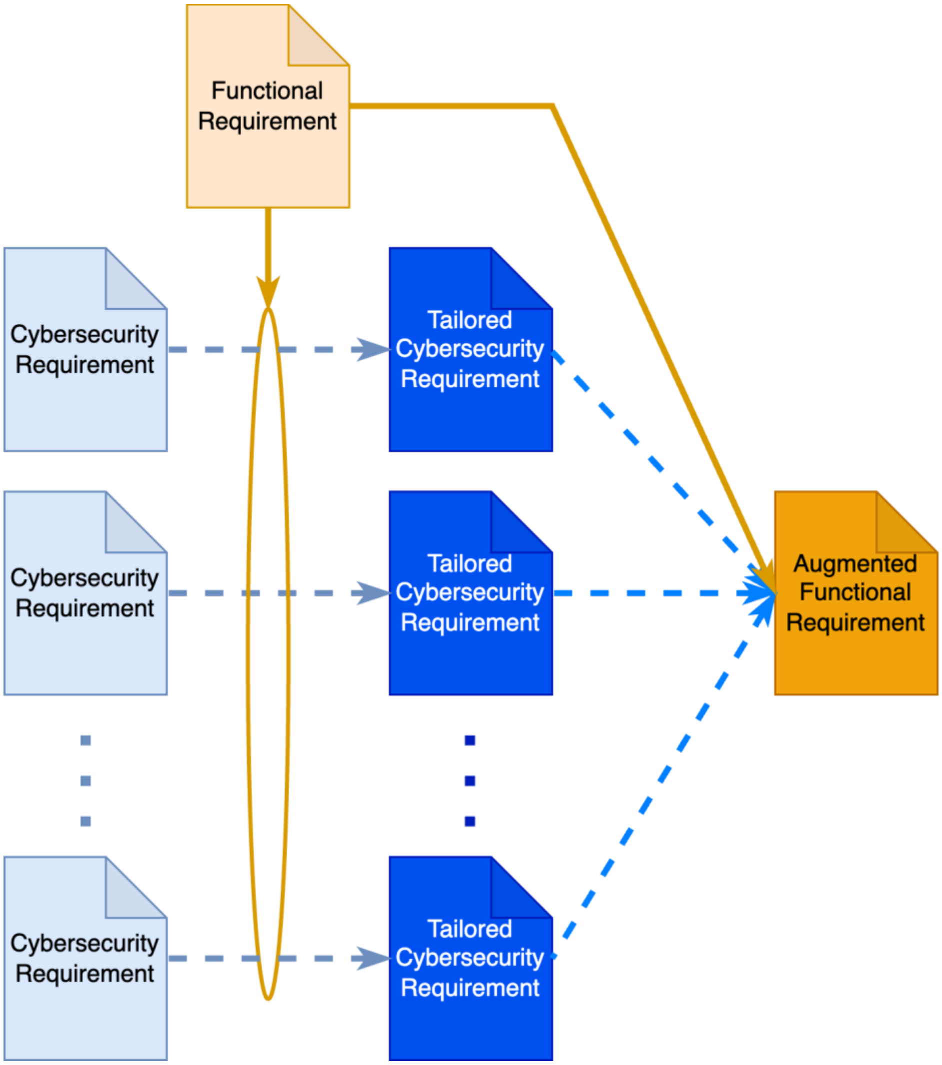
The workflow diagram of the **Element-level Security Requirements** is shown below.


development SME
security SME
security SME
element functional requirements
global security requirements catalog
requirements applicability analysis
list of applicable requirements
element-level security catalog creation
element-level security requirements catalog
requirements report
requirements applicability analysis
element-level catalog creation

The important things to focus on here are the **element functional requirements**, **global security requirements catalog**, **list of applicable requirements**, and **element-level security requirements catalog**.

Requirement Relationships

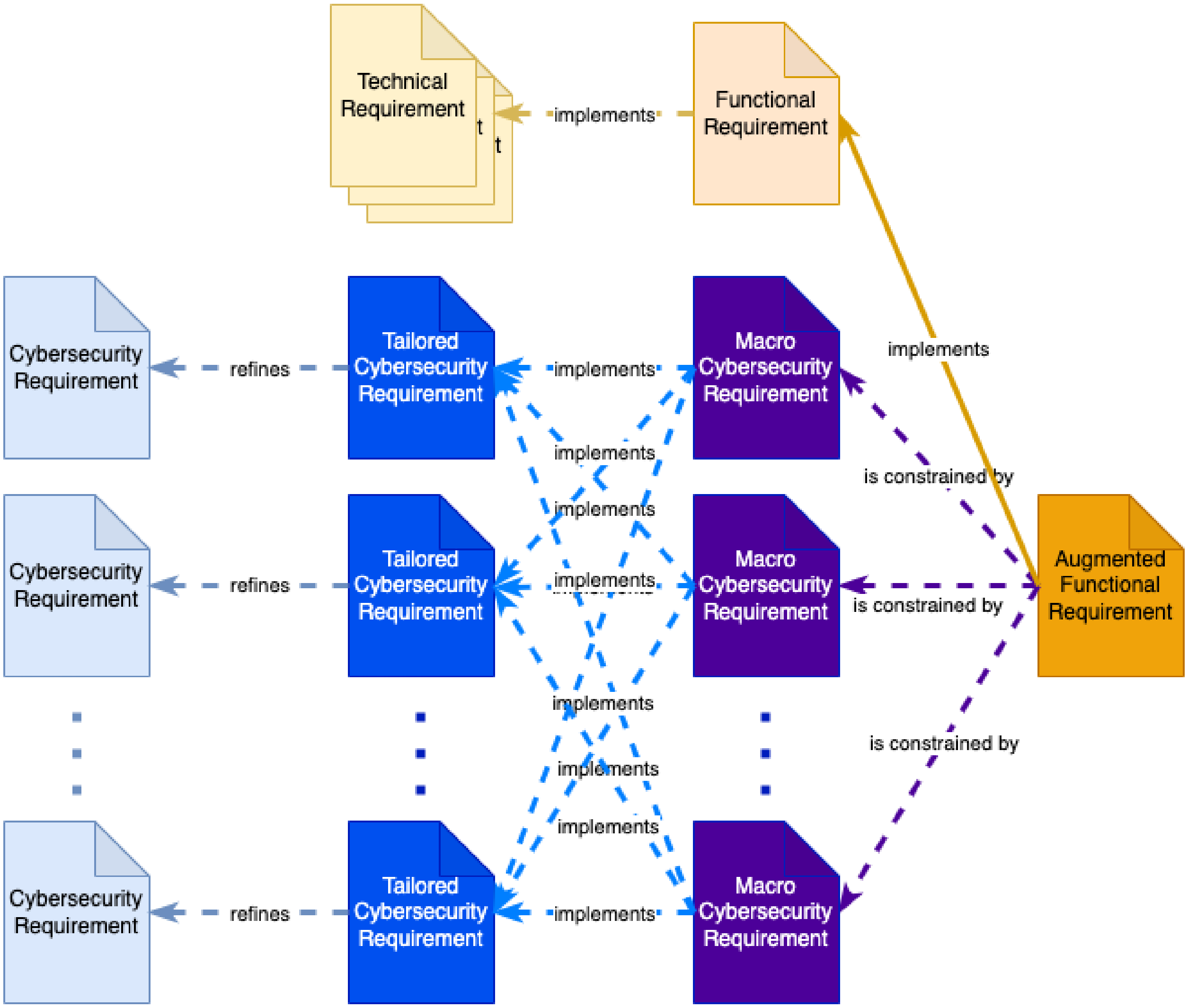
Consider the following diagram from the AVCDL training video **Cybersecurity Requirements** [4].


Functional Requirement
Cybersecurity Requirement
Cybersecurity Requirement
Cybersecurity Requirement
Tailored Cybersecurity Requirement
Tailored Cybersecurity Requirement
Tailored Cybersecurity Requirement
Augmented Functional Requirement

Here we have a set of **cybersecurity requirements** (in light blue) representing the **list of applicable requirements** taken from the **global security requirements catalog** based on their applicability to one of the **element functional requirements** (in tan), a corresponding set of **tailored cybersecurity requirements** (in dark blue) which when attached to the **functional requirement** comprise the **augmented functional requirement** (in burnt orange).

Because the typical interaction between two elements utilizes highly abstracted communication mechanisms capable of supporting multiple cybersecurity properties, and because these abstractions may be used across multiple elements within the system, we are motivated to collect sets of cybersecurity requirements into similarly abstracted macro cybersecurity requirements. This reduces the time and complexity of determining the cybersecurity requirements applicable to the functional requirements for the element under consideration.

Consider the following diagram also from the AVCDL **Cybersecurity Requirements** training video.

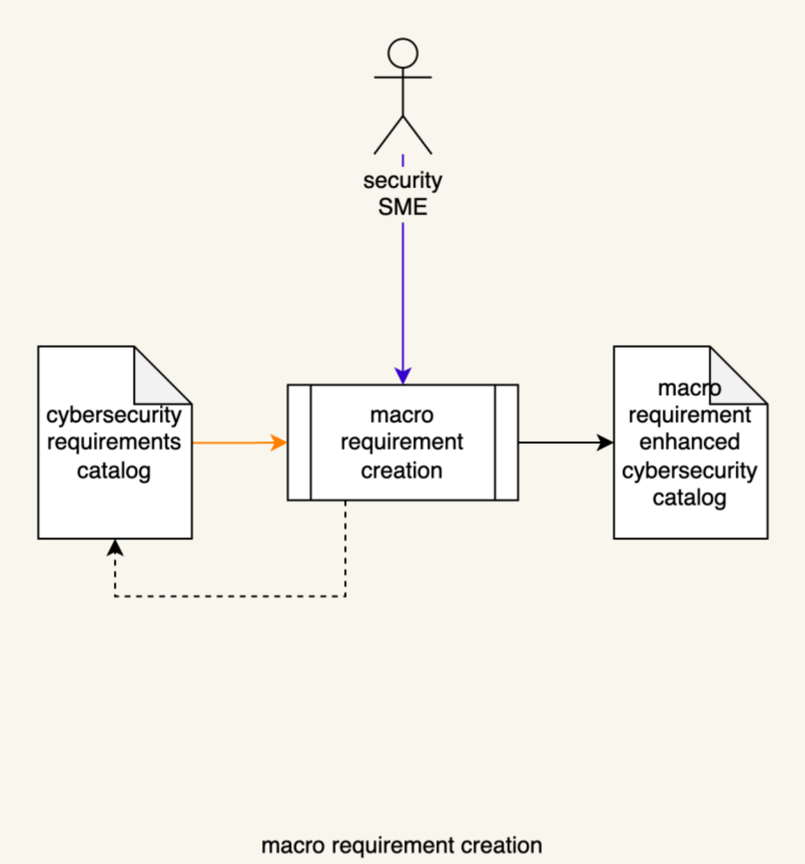


Here we have a set of **macro cybersecurity requirements** (in purple) which are comprised of sets of **tailored cybersecurity requirements** (in dark blue). This greatly reduces the number of cybersecurity requirements needed to be attached to the functional requirement. It also simplifies the various tests which need to be run.

Note: Untailored global cybersecurity requirements may be used to create macro requirements.

Macro Creation Activity

The workflow diagram for the macro creation activity is shown below.


security SME
cybersecurity requirements catalog
macro requirement creation
macro requirement enhanced cybersecurity catalog
macro requirement creation

The **Security SME** reviews the abstraction, for which a macro requirement is desired, against the **cybersecurity requirements catalog**. Requirements applicable to the cybersecurity abstraction are identified. A macro requirement with an "implements" relationship to the subset of requirements from the catalog supporting the abstraction is created and added to the **macro requirement enhanced cybersecurity catalog**.

Note: If gaps are identified in the **cybersecurity requirements catalog**, it will be updated.

Note: The **cybersecurity requirements catalog** called out here may be the **global security requirements catalog** or a derivative thereof. The choice of where within the requirements hierarchy to apply the abstraction necessary to implement a macro is left to the discretion of the cybersecurity group.

Methodology

The approach to take when determining a cybersecurity requirement's applicability for inclusion in a macro requirement is to consider the cybersecurity properties supported by the macro requirement's abstraction. Consider the following entries from the AVCDL **cybersecurity requirements per taxonomy** [6] Excel workbook.

CR050 Credentials shall be encrypted when transmitted across trust boundaries.
CR051 PII shall be encrypted when transmitted across trust boundaries.
CR052 Communication crossing trust boundaries that cannot be secured shall be isolated.
CR053 Communication crossing trust boundaries shall ensure data confidentiality.
CR054 Communication crossing trust boundaries shall ensure data integrity.
CR055 Communication crossing trust boundaries shall ensure data availability.
CR056 Communication crossing trust boundaries shall be authenticated.
CR057 Custom protocols that support a retry mechanism shall implement rate limiting.
CR058 Custom protocols shall use current best practices for authentication and key exchange.
CR059 Standard network protocols shall be secured using cybersecurity best practices.

For example, SecOC security profile 1 [7] supports requirements CR050, CR054, CR056, and CR058 (highlighted in yellow).

Note: It will probably be necessary to be very specific when identifying the macro requirement. As is the case of SecOC, not all profiles provide support for all the requirements that profile 1 does.

The above abstraction is for a communication protocol. These are layer-specific macros. A different abstraction might be for a specific asset type. Consider the following entries also from the AVCDL **cybersecurity requirements per taxonomy** [6] Excel workbook.

CR020 The system shall enter a safe state when a safety-critical data store is not available.
CR021 Configuration data confidentiality shall be protected using access controls.
CR022 Configuration data integrity shall be validated prior to use.
CR023 Configuration data shall only be accessed by authenticate entities.
CR024 Configuration data authenticity shall be assured.
CR025 Configuration data modification shall be recorded in the audit logs.
CR026 Configuration data modification shall only be made by authorized entities.

These requirements all address configuration data. It would be reasonable to create macro requirements for these specific asset types.

Macro Requirements Template

The element cybersecurity macro requirements may be documented using the **AVCDL cybersecurity macro requirements template** Microsoft Excel workbook [5].

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
- Macro Requirements
- Legend

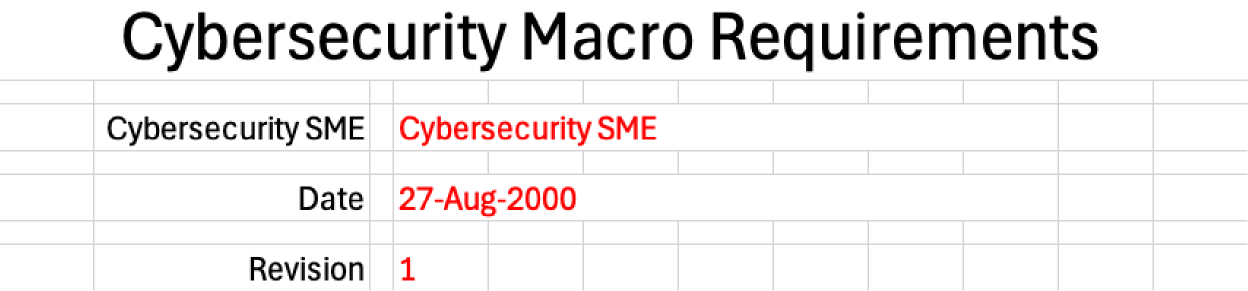
These sheets will be addressed in turn.

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 may be 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 Macro Requirements

Cybersecurity SME	Cybersecurity SME
Date	27-Aug-2000
Revision	1

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

Cybersecurity SME

This is the cybersecurity subject matter expert performing the analysis.

Date

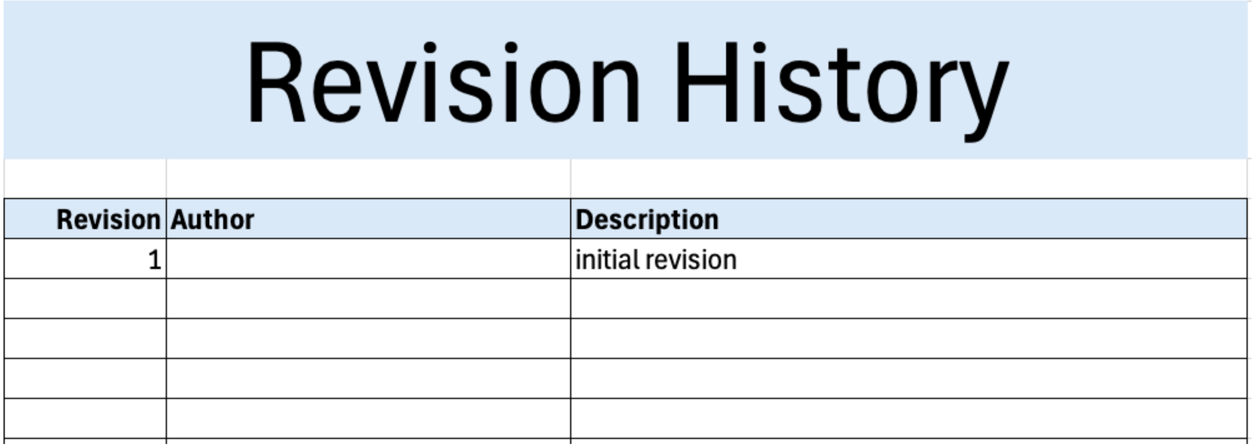
This is the date when the analysis of the element model was performed or updated. The date should be updated whenever the analysis is updated.

Revision

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

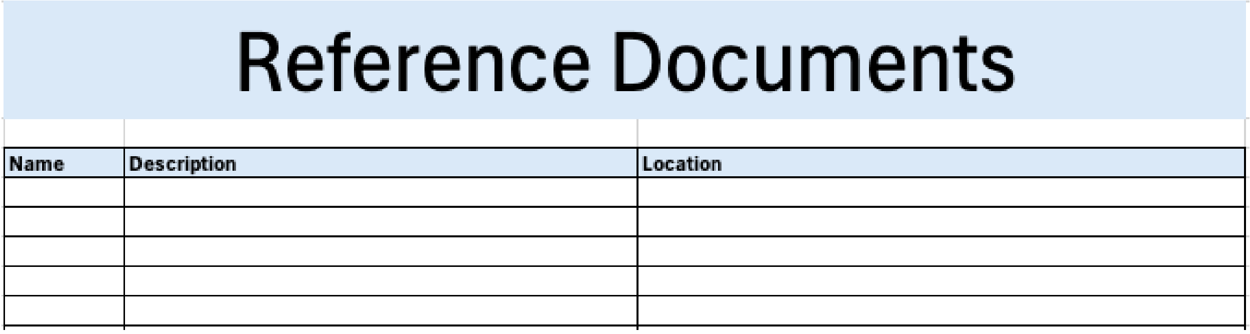
Description

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

Reference Documents

Note: These references are those necessary for the creation of macro requirements.

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



Reference Documents

Name	Description	Location

Name

This is the name of the document being referenced.

Description

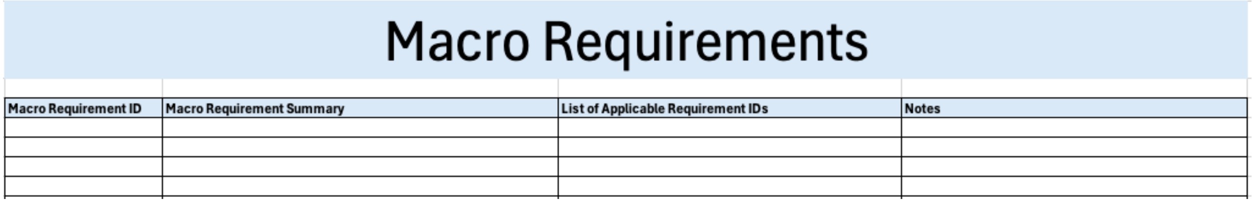
This is a brief description of the document being referenced.

Location

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

Macro Requirements

The **macro requirements** sheet of the workbook is shown below:



Macro Requirements

Macro Requirement ID	Macro Requirement Summary	List of Applicable Requirement IDs	Notes

Macro Requirement ID

This is the unique ID of the macro requirement.

Macro Requirement Summary

This is the description of the macro requirement.

List of Applicable Requirement IDs

This is the comma-separated list of cybersecurity requirement IDs applicable to the macro requirement.

Note: As mentioned earlier, these requirements may be chosen from any level within the cybersecurity requirements hierarchy (global, tailored, macro, …).

Notes

This is a general notes field.

Legend

Note: This template does not use the legend sheet. It should not be deleted however, as the templates version number is on this sheet.

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. **Cybersecurity Requirements** (AVCDL training video)
5. **AVCDL cybersecurity macro requirements template** (AVCDL template)
6. **cybersecurity requirements per taxonomy** (AVCDL reference document)
7. **Specification of Secure Onboard Communication Protocol** https://www.autosar.org/fileadmin/standards/R20-11/FO/AUTOSAR_PRS_SecOcProtocol.pdf