Element-level Security Requirements Analysis Procedure

Revision

Version 4
4/14/25 2:34 PM

SME

Charles Wilson

Abstract

This document describes the procedure used to perform the cybersecurity requirements applicability analysis 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**.

License

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 applicability analysis.

Necessity of Development Input

Since the requirements analysis is an as-is analysis, it is critical to ensure that the information gathered is as accurate and complete as possible. As with any cybersecurity assessment, it is not the place of the cybersecurity SME to make assumptions on the part of engineering. All information should be sourced from and confirmed by the owner of the element under consideration.

Completeness of Output

The completeness of the output of this activity is highly dependent upon the input provided. As stated in the preceding section, the cybersecurity SME should not be filling in the blanks in order to perform their tasks.

When information is not available for either a given section of the template or parts thereof, this should be noted. Major omissions should be recorded in the cybersecurity risk register.

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 analysis. 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 analysis.

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.

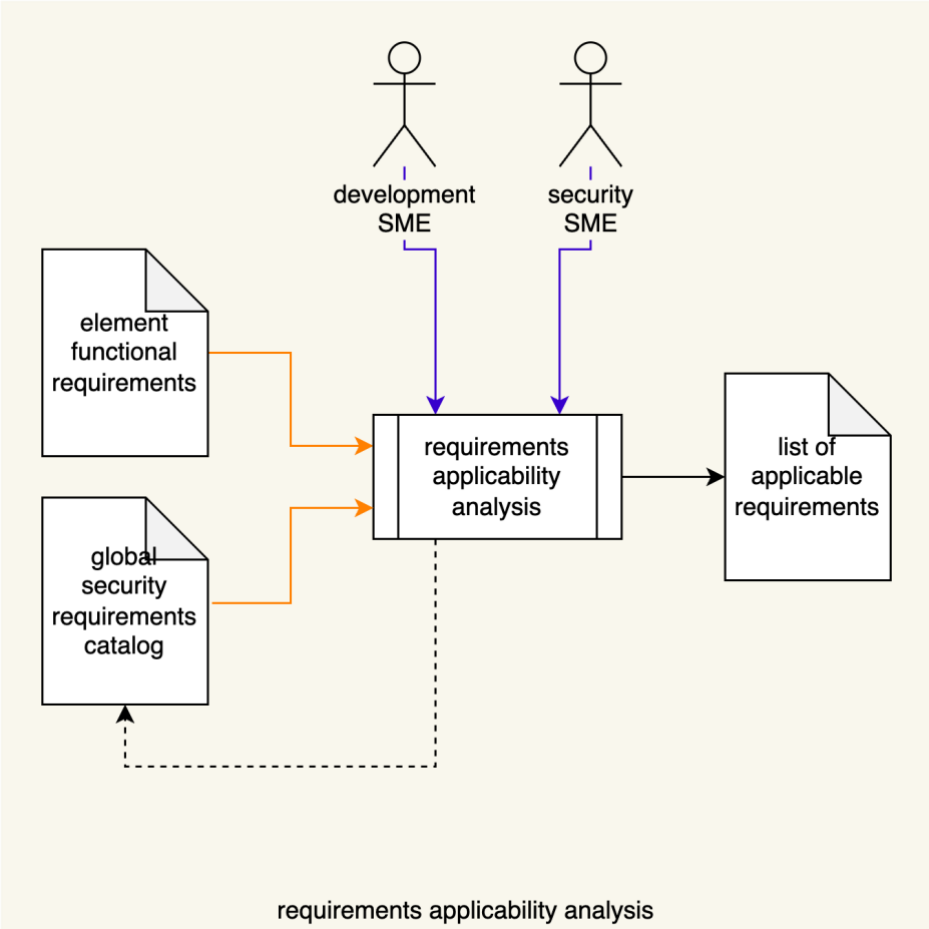
Prerequisites – Input Materials

It is required that the cybersecurity group provides a global security requirements catalog. It is also required that the development group provide all relevant documentation related to the element under consideration necessary to complete the procedure. Specifically, the development group is required to provide the set of functional requirements for the element under consideration.

Note: The necessity of having the functional requirements for the element under consideration cannot be overstated. It is not possible to accurately determine what cybersecurity requirements are applicable without this information.

Analysis Activity

The workflow diagram for the analysis activity of the Element-level Security Requirements is shown below.



requirements applicability analysis

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.

Note: This activity need only be undertaken for cybersecurity-relevant elements. Refer to the AVCDL secondary document **Element Cybersecurity Relevancy** [7] for details as to how to establish cybersecurity relevancy.

Analysis Methodology

The basic approach to take when analyzing the element for cybersecurity requirements applicability is to consider the cybersecurity controls necessary for each of its features. For each feature in turn, assess whether that feature presents the possibility of compromise to the cybersecurity properties required for proper operation of the element.

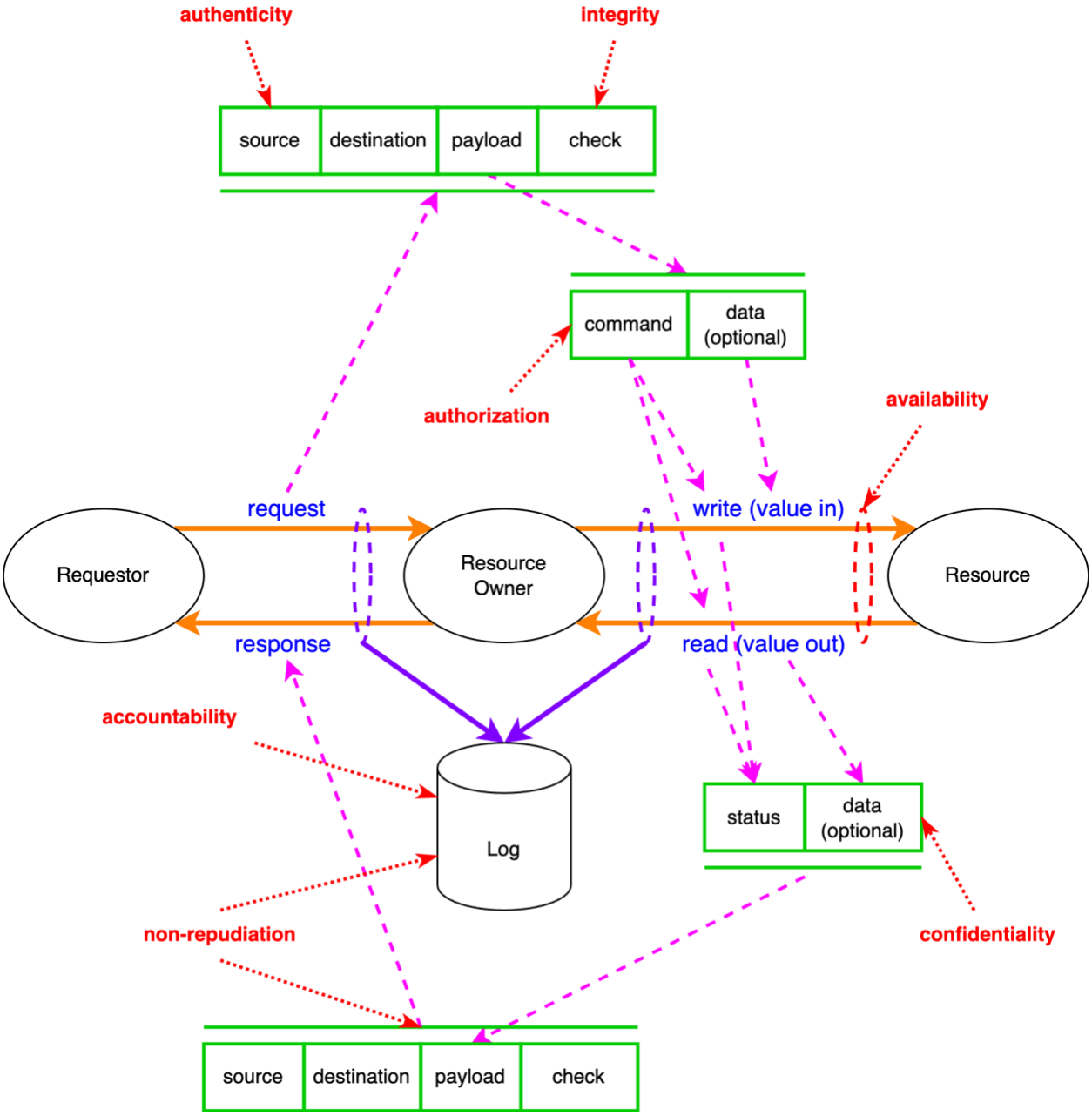
Note: These considerations are made for those features that will be present in the released product. Features only present during development should be noted but should not be considered as a potential source of threats.

Keep in mind that cybersecurity requirements are non-functional constraints on the element's functional requirements. If a desired cybersecurity-related requirement adds to or alters the functional requirement's fundamental behavior, then it is actually a functional requirement with cybersecurity properties. An example of this might be the desire to have cybersecurity-relevant events logged in the absence of a feature within the element that performs logging. This is an instance where analysis of the element exposes a feature deficiency.

Note: Any feature deficiencies should be reported to the development SME for development to address. It is not within the scope of cybersecurity to create functional requirements for other groups.

Application of Cybersecurity Controls

Consider the following diagram from the AVCDL elaboration document **Understanding the Extended CIA Working Model** [4].



Control points correspond to the places where cybersecurity properties (in red) apply with respect to the **resource owner**. In the case of element analysis, the element is considered to be the **resource owner**.

Layer ➔ Asset ➔ Property

The **layer-asset-property** sort sheet of the AVCDL working material document **cybersecurity requirements per taxonomy** [6] sorts the global cybersecurity requirements by layer, asset, and property as the name indicates. This view of the data is useful in that it quickly separates the requirements into three primary buckets:

- Hardware-specific (physical things)
- Communication-specific (message transport)
- Application-specific (processes)

Generally speaking, assets are fairly well grouped within their respective layers.

Finally, the specific cybersecurity properties are grouped.

This leads to a fairly easy to work with requirements arrangement.

Hardware-specific Requirements

There are only four (4) hardware-specific requirements. These are:

CR060 Cryptographic operations shall use a mechanism that is backed by a hardware root of trust.
CR061 Hardware components shall enable only the utilized connective features.
CR062 Non-essential physical communication ports shall be disabled.
CR063 Hardware shall have a unique, immutable identifier.

It is unlikely that these requirements will be applicable at levels of decomposition below the system level.

Communication-specific Requirements

There are ten (10) communication-specific requirements. These are:

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.

Properly constructed functional requirements will lend themselves to the creation of a DFD for the element. Although not strictly required, a DFD is useful when dealing with communication related requirements.

Application-specific Requirements

The bulk of the global cybersecurity requirements are application specific. These will not be enumerated here.

In order to properly address application-specific functional requirements and attach their cybersecurity counterparts, it may be helpful to have an element software diagram. This may take the form of a UML or DFD decomposition.

Note: Where possible, individual executables (applications, services, drivers) should be considered separately.

Within the application-specific requirement set, it is useful to handle each asset type in turn.

Element Analysis Template

The element cybersecurity requirements analysis issues may be documented using the **AVCDL element cybersecurity requirements analysis 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**
- **Analysis**
- **Legend**

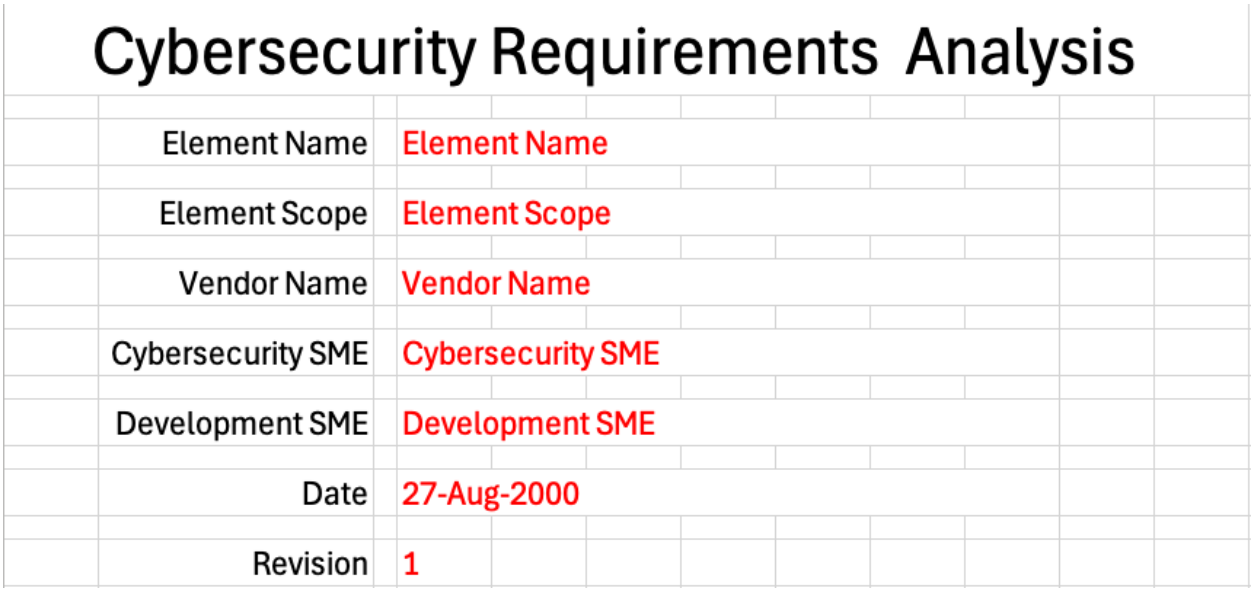
These sheets will be addressed in turn.

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 Analysis	
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

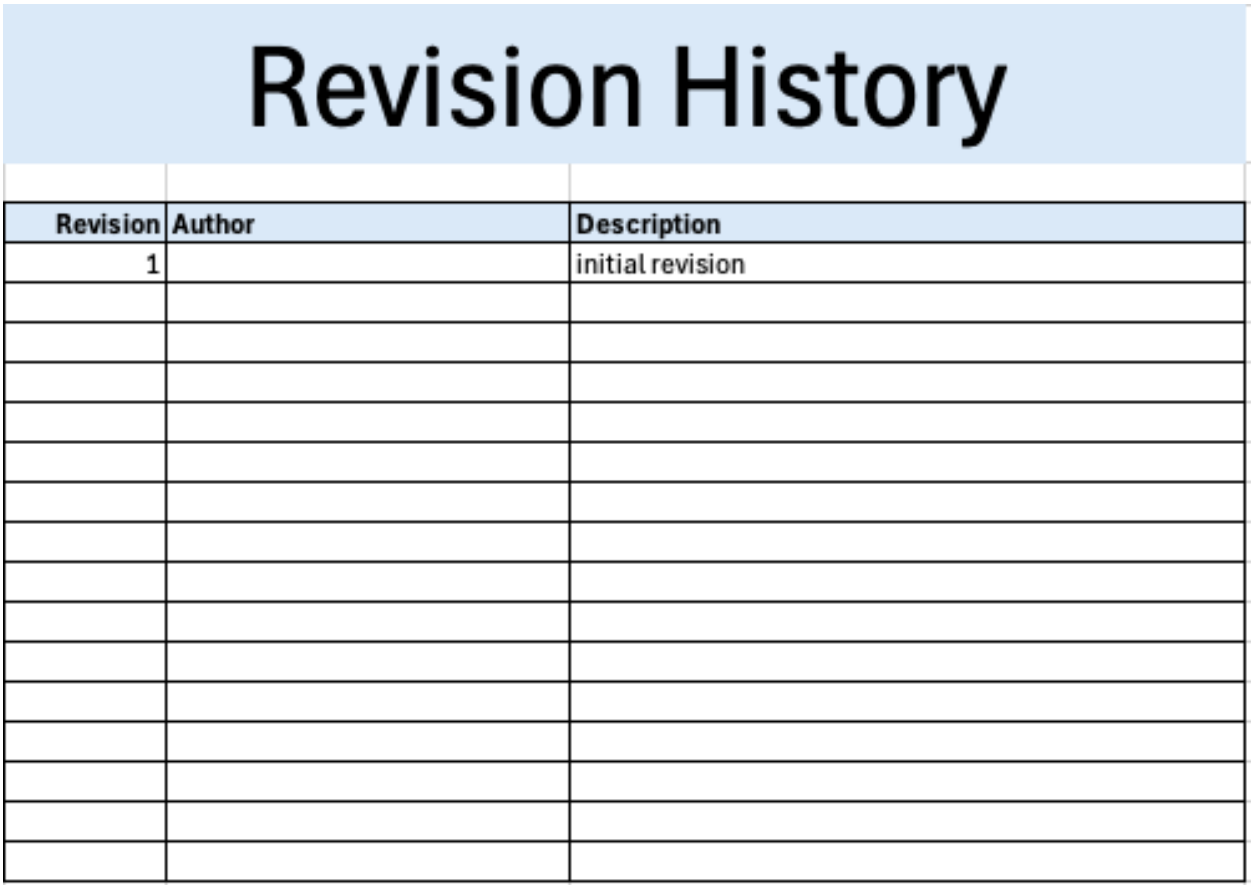
This is the date when the analysis of the element model was performed or updated. The date should be updated whenever the analysis is updated.

Revision

This is the revision number of 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.

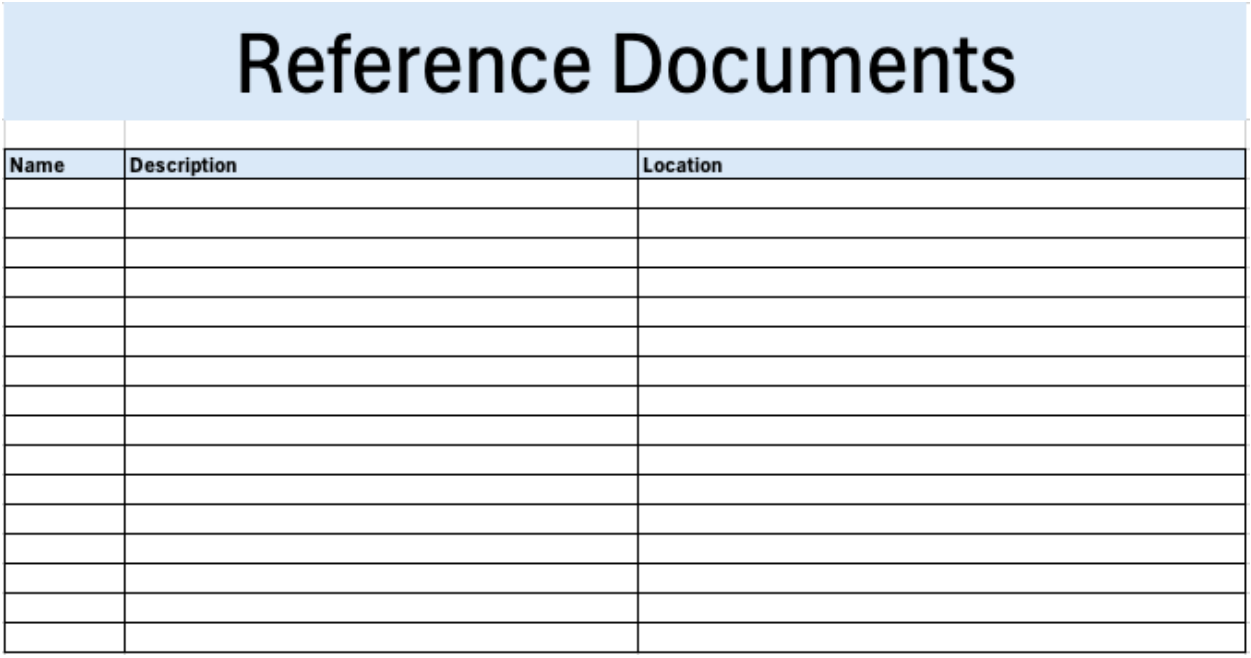
Description

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 analysis of the element model.

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



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

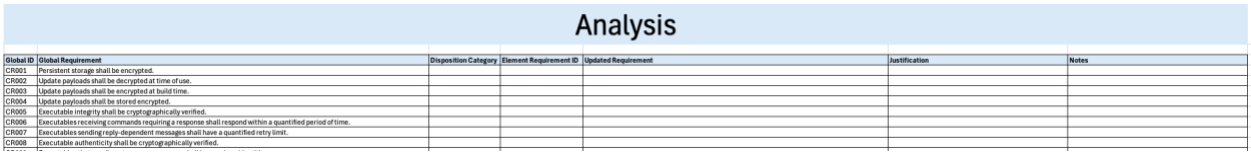
This is a brief description of the document being referenced.

Location

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

Analysis

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



Analysis

Global ID	Global Requirement	Disposition Category	Element Requirement ID	Updated Requirement	Justification	Notes
CR001	Persistent storage shall be encrypted.					
CR002	Update payloads shall be decrypted at time of use.					
CR003	Update payloads shall be encrypted at build time.					
CR004	Update payloads shall be stored encrypted.					
CR005	Executable integrity shall be cryptographically verified.					
CR006	Executables receiving commands requiring a response shall respond within a quantified period of time.					
CR007	Executables sending reply-dependent messages shall have a quantified retry limit.					
CR008	Executable authenticity shall be cryptographically verified.					

Global ID

This is the unique ID of the global catalog requirement.

Global Requirement

This is the description of the global requirement.

Disposition Category

This is the disposition of the requirement with respect to the element. Categories include:

- Not Applicable
- As Is
- Derived
- New

Note: An explanation of each category is found in the **Element-level Security Requirements** AVCDL secondary document.

Element Requirement ID

This is the unique ID of the element-specific requirement.

Updated Requirement

This is the description of the element-specific requirement.

Justification

This is the rationale for changes made for requirement tailoring.

Notes

This is a general notes field.

Legend

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

Category
not applicable
as is
derived
new

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. **Understanding the Extended CIA Working Model** (AVCDL elaboration document)
5. **AVCDL element cybersecurity requirements analysis template** (AVCDL template)
6. **cybersecurity requirements per taxonomy** (AVCDL reference document)
7. **Element Cybersecurity Relevancy** (AVCDL secondary document)