Attack Surface Analysis
Analysis Procedure

Revision

Version 5
11/21/24 2:29 PM

SME

Charles Wilson

Abstract

This document describes the procedure used to perform the analysis activity of attack surface analysis as described in the AVCDL secondary document **Attack Surface Analysis Report** [2].

Group / Owner

Security / Security Architect

Motivation

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

Audience

The audience of this document is the cybersecurity practitioner who will be conducting the attack surface analysis.

Completeness of Output

Since the attack surface 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.

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 entered into the organization's document management system as a document of record.

Creation of Model

Model creation is documented in the AVCDL **Attack Surface Analysis – Model Creation Procedure** tertiary document [3].

Entry Criteria

This document assumes that the reader understands the purpose of the attack surface analysis. Further, that the reader has read and understood the AVCDL **Attack Surface Analysis Report** secondary and **Attack Surface Analysis – Model Creation Procedure** documents [2, 3].

Prerequisites – Cybersecurity ASA SME

Qualifications

It is required that the ASA 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 ASA SME understands the purpose of an attack surface analysis.

Background Information

It is required that the ASA SME has read and understood the AVCDL **Attack Surface Analysis Report** secondary and **Attack Surface Analysis – Model Creation Procedure** tertiary documents. Additionally, that the ASA SME has taken training relevant to this activity.

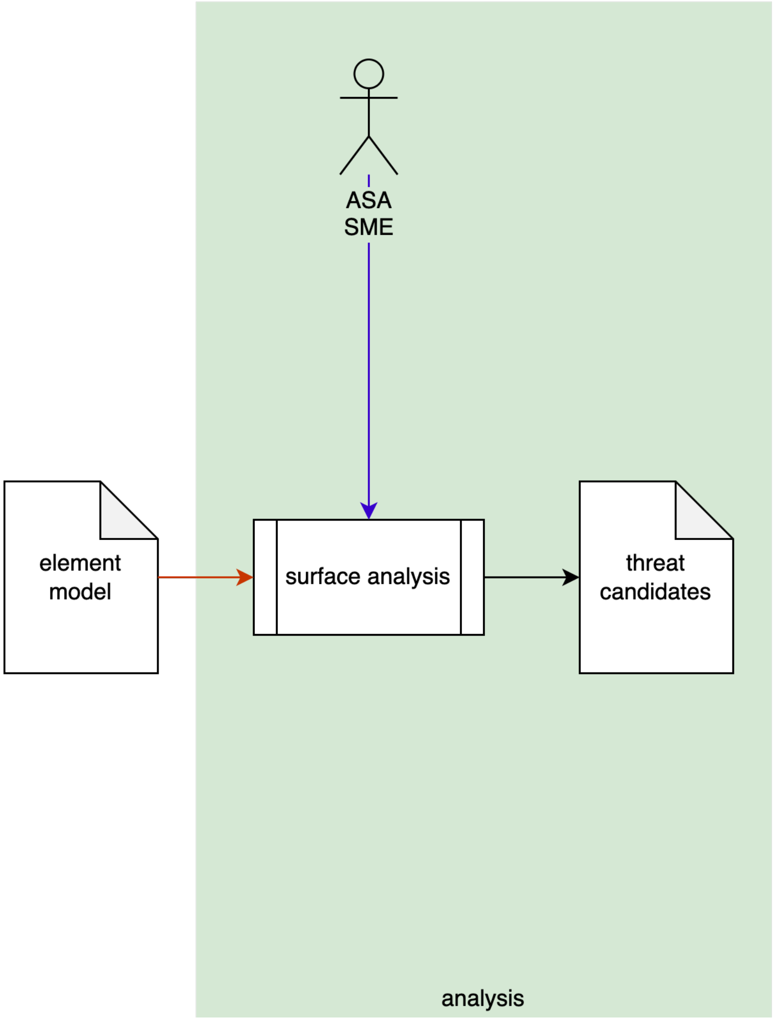
Prerequisites – Input Materials

It is required that the cybersecurity group provide an element model for analysis. It is also required that the development group provide all relevant documentation related to the element under consideration necessary to complete the procedure.

Note: Because the depth of analysis is variable, the specific documentation required will be determined and provided to the development group by the ASA SME prior to the start of the element model's analysis.

Analysis Activity

The workflow diagram for the analysis activity of the Attack Surface Analysis (**ASA**) is shown below.



The ASA SME processes the element model to evoke a set of threat candidates. Candidates are those features of the element's presented surface which are not required for the production system. These features may include services, ports, APIs, protocols, etc.

NOTE: It is important to appreciate that this procedure covers the analysis activity only. The output is a set of threat candidates (potential issues). These will be addressed in the final attack surface analysis activity which is documented in the AVCDL **Threat Prioritization Plan** secondary document [7].

Analysis Methodology

The basic approach to take when analyzing the element model's attack surface is to consider the necessity of each of its features. For each feature in turn, assess whether that feature presents excessive exposure to the element beyond what is minimally 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.

Input to the analysis may be an attack surface analysis element model documented in an **AVCDL attack surface analysis model** Microsoft Excel workbook [4].

Physical Port Considerations

Source

The **physical ports** sheet of the workbook is the source for this analysis.

Questions

Is the port used?

Is the port required for the core functionality of the element?

Is the port only required during development?

Is the port only required for diagnostics?

Is the port only required for provisioning (includes software and configuration data)?

Is the port removable?

Note: Issues relating to physical security (such as covers, locks, tamper-evident seals, …) are outside the scope of a cybersecurity attack surface analysis and not subject to consideration here. These issues should be recorded in the appropriate concerns register and communicated to the group(s) responsible for such issues.

Logical Port Considerations

Source

The **logical ports** sheet of the workbook is the source for this analysis.

Questions

Is the port used?

Is the port number appropriate?

Note: Use and assignment of logical port numbers is governed by the **IANA** [8] with specifics regarding the management of the port registry documented in **RFC 6335** [9].

Is the port required for the core functionality of the element?

Is the port only required during development?

Is the port only required for diagnostics?

Is the port only required for provisioning (includes software and configuration data)?

Is the port owned by a single process?

Is the port only open for the duration required by the operation?

Does the protocol running on the port require non-trivial authentication?

Note: The subject of authentication is covered in the **NIST SP 800-63 Digital Identify Guidelines** [10] document collection.

Process Considerations

Source

The **processes** sheet of the workbook is the basis for this analysis.

Questions

Is the process used?

Is the process required for the core operation of the element?

Is the process only required during development?

Is the process only required for diagnostics?

Does the process have a unique owner?

Is the process required to be privileged?

Is the process used only for provisioning / update?

Is the process the manager of a system-critical resource?

Element Analysis Template

The attack surface analysis issues may be documented using the **AVCDL attack surface analysis issues 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 issues workbook. They are:

- Cover sheet
- Revision history
- Reference documents
- Identified Issues
- Legend

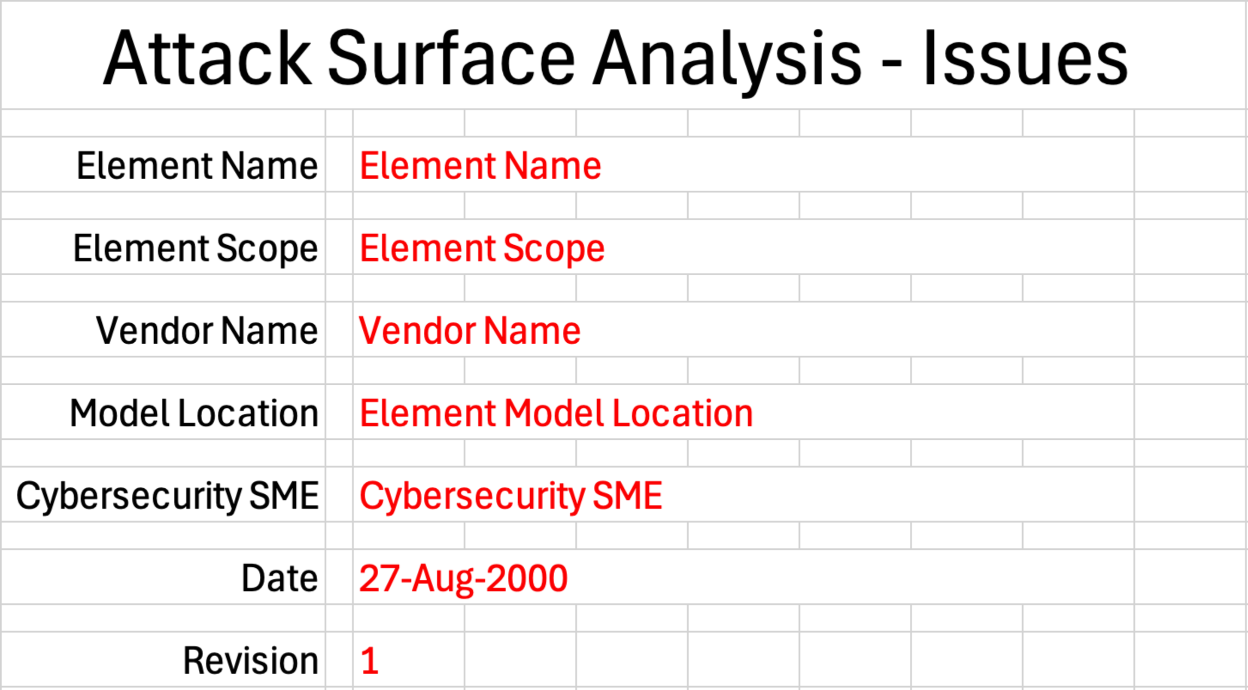
These sheets will be addressed in turn.

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:



Attack Surface Analysis - Issues

Element Name	Element Name
Element Scope	Element Scope
Vendor Name	Vendor Name
Model Location	Element Model Location
Cybersecurity SME	Cybersecurity 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.

Note: This should be the same as in the element model document.

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.

Note: This should be the same as in the element model document.

Vendor Name

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

Note: This should be the same as in the element model document.

Model Location

This is the location of the element model being analyzed. It may be a physical location or a URL.

Cybersecurity SME

This is the cybersecurity subject matter expert performing the attack surface analysis.

Date

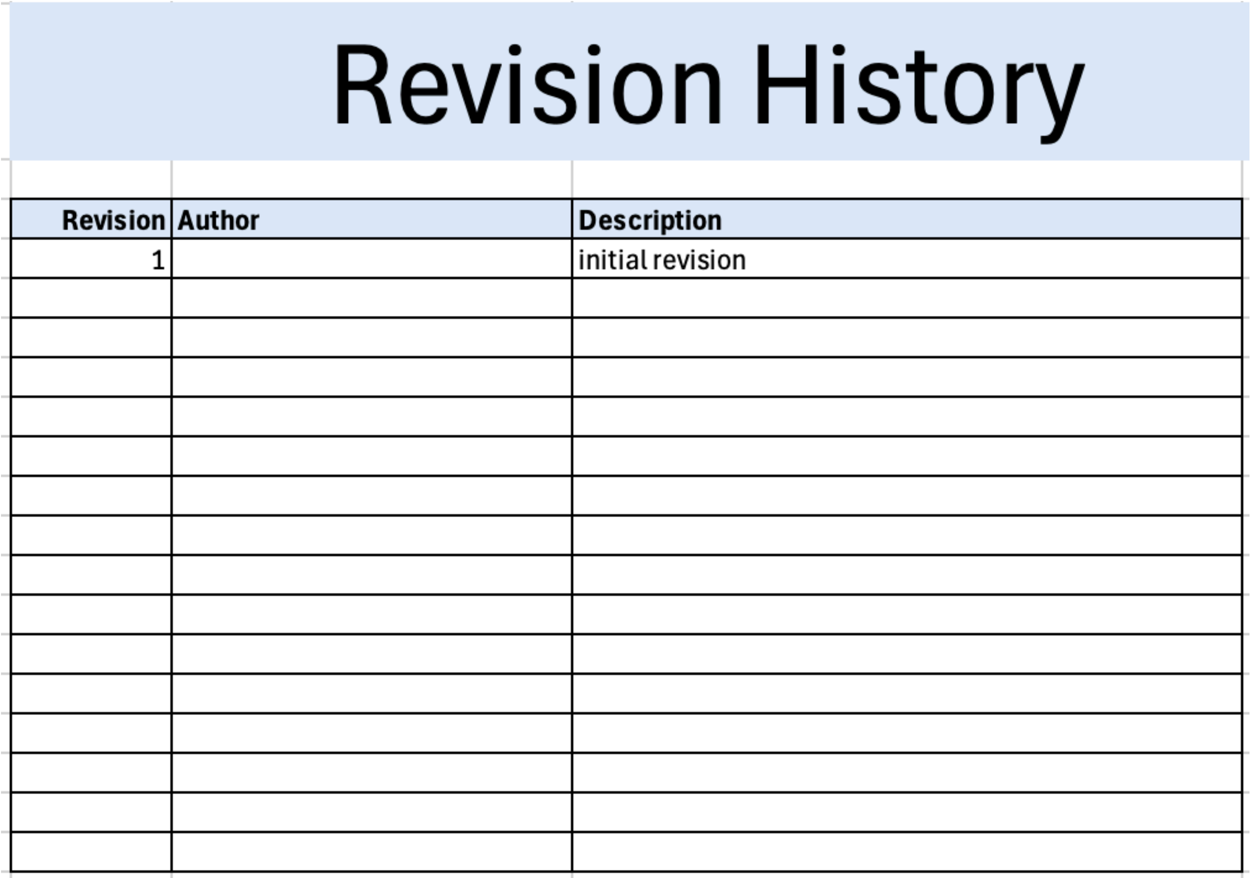
This is the date when the analysis of the element model was performed or updated. The date should be updated whenever the analysis is updated.

Revision

This is the revision number of the attack surface analysis issues 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 that listed on the cover sheet.

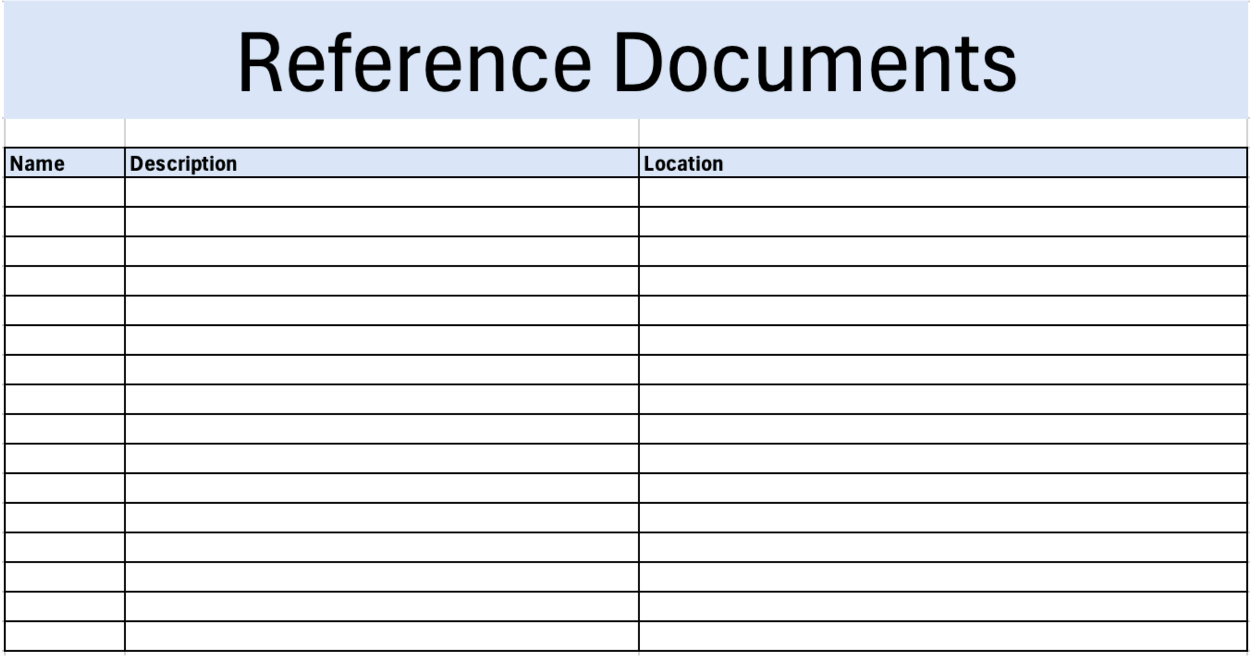
Description

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

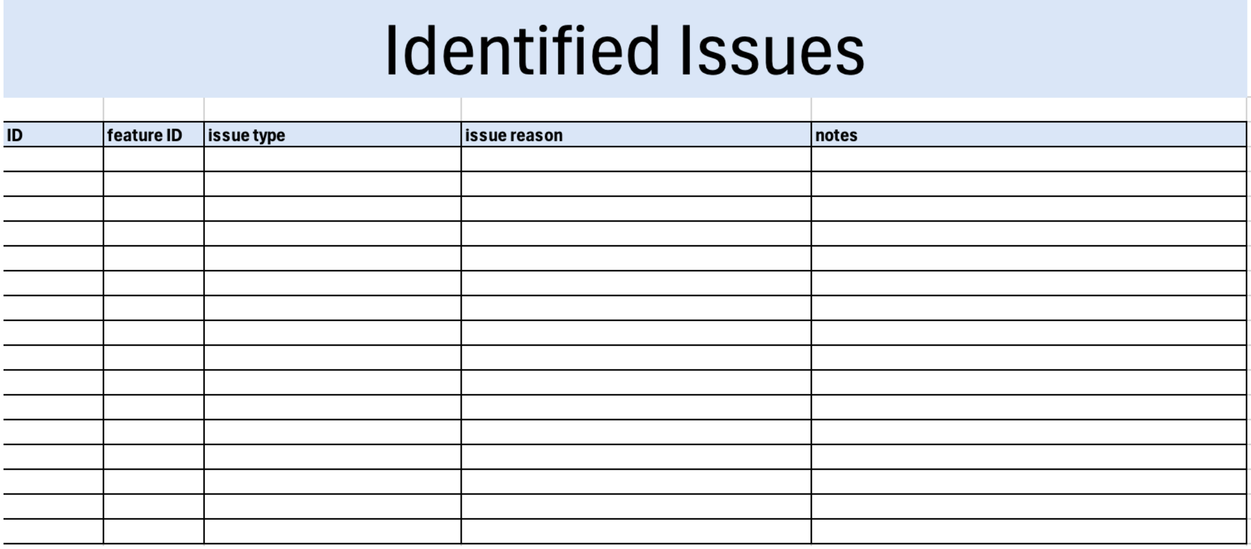
This is a brief description of the document being referenced.

Location

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

Identified Issues

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



Identified Issues

ID	feature ID	issue type	issue reason	notes

ID

This is the unique ID of the issue.

feature ID

This is the unique ID corresponding to the feature where the issue presents itself.

Issue Type

This is the type of the issue. Issue types include:

- Data connection lifetime
- Data structures
- Diagnostics
- Features
- Memory pressure susceptibility
- Ports
- Protocols
- Remote execution
- System services
- User accounts

Issue Reason

This is the reason for raising this issue. Issue reasons include:

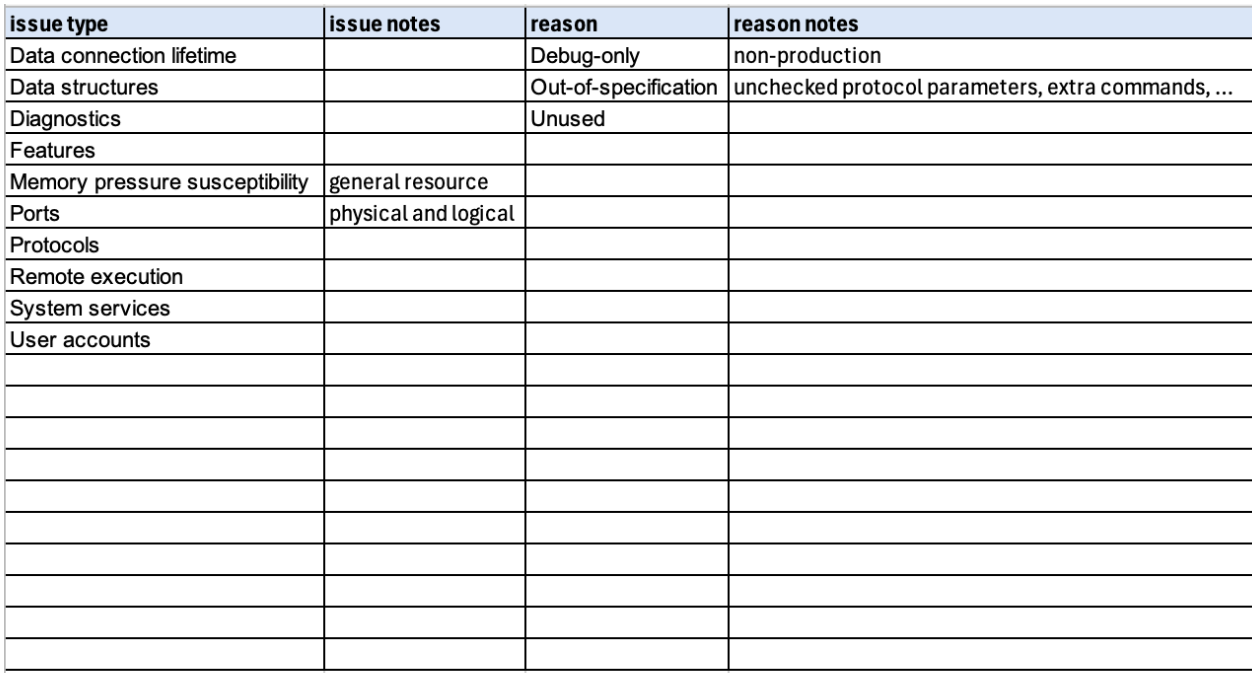
- Debug-only
- Out-of-specification
- Unused

Notes

This is a general notes field.

Legend

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



issue type	issue notes	reason	reason notes
Data connection lifetime		Debug-only	non-production
Data structures		Out-of-specification	unchecked protocol parameters, extra commands, ...
Diagnostics		Unused	
Features			
Memory pressure susceptibility	general resource		
Ports	physical and logical		
Protocols			
Remote execution			
System services			
User accounts			

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 document management system as a document of record.

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

References

1. **AVCDL** (AVCDL primary document)
2. **Attack Surface Analysis Report** (AVCDL secondary document)
3. **Attack Surface Analysis – Model Creation Procedure** (AVCDL tertiary document)
4. **Attack surface analysis model template** (AVCDL template)
5. **Attack surface analysis issues template** (AVCDL template)
6. **Threat Modeling Report** (AVCDL secondary document)
7. **Threat Prioritization Plan** (AVCDL secondary document)
8. **Service Name and Transport Protocol Port Number Registry**
   `https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml`
9. **Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry**
   `https://www.rfc-editor.org/rfc/pdfrfc/rfc6335.txt.pdf`
10. **NIST SP 800-63 Digital Identify Guidelines**
    `https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines`