Attack Surface Analysis
Model Creation Procedure

Revision

Version 5
1/3/25 10:16 AM

SME

Charles Wilson

Abstract

This document describes the procedure used to perform the model creation 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.

Analysis of Model

Model analysis is documented in the AVCDL **Attack Surface Analysis – Analysis Procedure** tertiary document [4].

Entry Criteria

Prerequisites – Development SME

Qualifications

It is required that the development SME is both a qualified and trained development SME with expertise in the element under consideration.

Note: The specific qualifications and training of development SMEs necessary to assert expertise in providing accurate information regarding the element under consideration is outside the scope of this document.

Note: The development group is responsible for determining and making available the appropriate SME for the analysis of the element under consideration.

Knowledge

It is required that the development SME have expertise in the element under consideration.

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 document. Additionally, that the ASA SME has taken training relevant to this activity.

Prerequisites – Input Materials

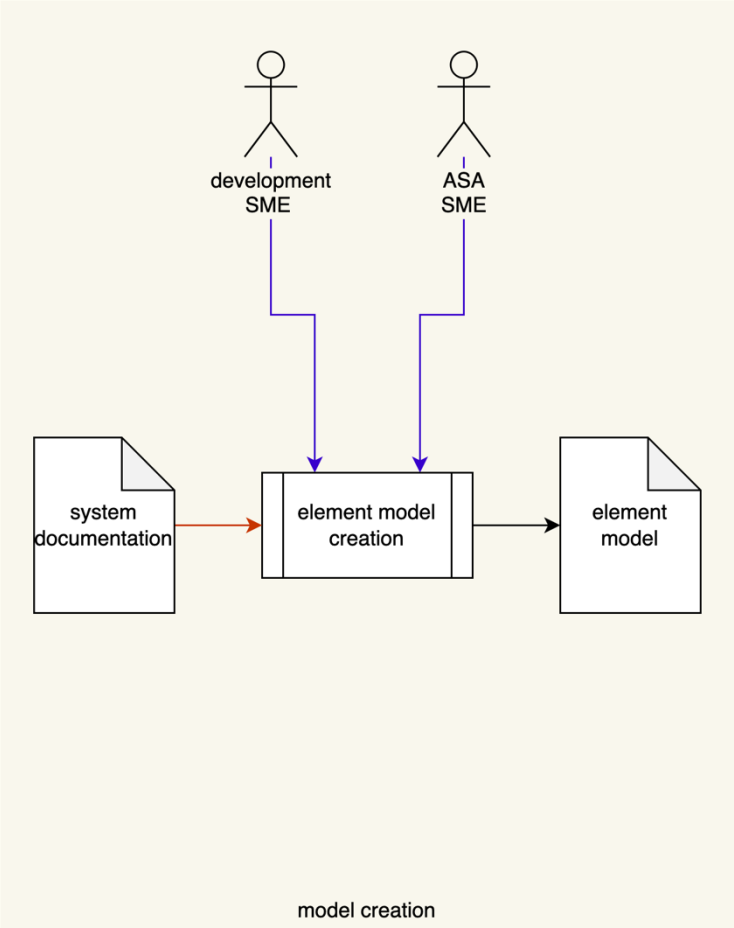
It is required that the development group provide all relevant documentation related to the element under consideration necessary to complete the procedure.

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's model creation.

Model Creation Activity

The Attack Surface Analysis (**ASA**) model creation activity workflow diagram is shown below.

Note: For context, see the AVCDL **Attack Surface Analysis Report** secondary document.



The ASA SME works with the development SME(s) to create a model (**output**) of the system suitable for analysis. Any existing documentation regarding the element is used as **input** to this process. For this activity, models should be created using a formal modeling tool when possible. This may be a set of models depending on the complexity of the system.

Note: System documentation may include existing models of the element should they exist.

Methodology

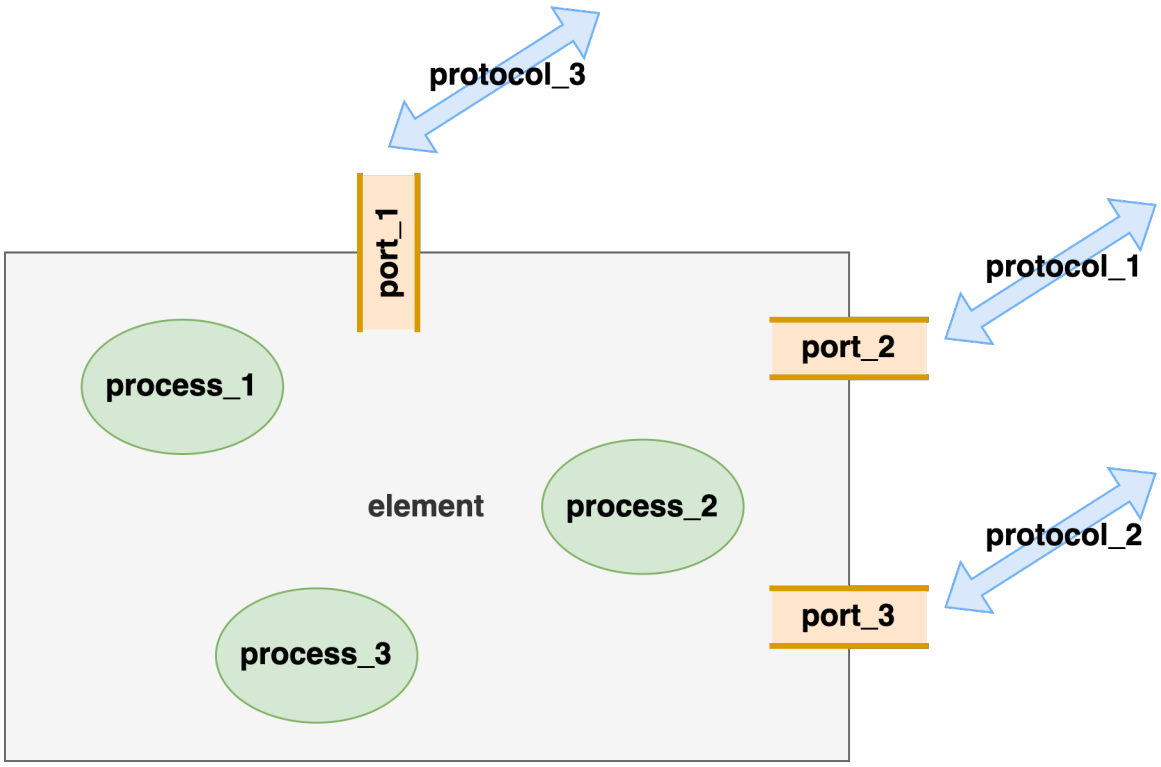
Abstraction Levels

Unlike most other cybersecurity activities, attack surface analysis can be applied to multiple types of abstractions. Because of this, the information necessary to perform the analysis varies accordingly. The specific information will be covered in the Element Model Creation Template section of this document.

The abstraction levels are:

- Physical
- Logical
- Process

The following is a block diagram showing various features of interest when performing an attack surface analysis.



The **physical** abstraction level is concerned with the element's ports (**tan**). The **logical** abstraction level focuses on the communication protocols (**blue**) being used by the element. Finally, the **process** abstraction level considers the processes (**green**) in use within the element.

Note: A given attack surface analysis is performed at a single abstraction level.

Ideally, the analysis should be conducted on each level in turn (physical ➔ logical ➔ process). This corresponds to an attack surface analysis with two distinct types of refinement, one at the abstraction level (one level informs another) and the other within each level (the level gets better).

Note: The lower the abstraction level, the more detail required to perform the analysis.

Note: An attack surface should always have a hierarchical decomposition. The analysis should mirror this. It isn't unreasonable to address the logical ports for each physical port as a separate analysis document. In this case the physical diagram is still referenced but the scope is elaborated as being restricted to a specified subset. This naturally increases the number of analysis documents that need to be tracked together.

Development – Cybersecurity SME Interaction

As with most cybersecurity activities, the primary driver of this activity is the cybersecurity ASA SME. The development SME is responsible for providing information regarding the element, but the ASA SME should not presume that the development SME is familiar with cybersecurity practices in general or attack surface analysis in particular.

Element Model Creation Template

The attack surface analysis model may be documented using the **AVCDL attack surface analysis model template** Microsoft Excel workbook [3].

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

There are eight sections in the workbook. They are:

- Cover sheet
- Revision history
- Reference documents
- Section 1 element diagrams
- Section 2 physical ports
- Section 3 logical ports
- Section 4 processes
- Legend

These sheets will be addressed in turn.

Note: Only one of the sections (2, 3, 4) will be used for any given model creation. This was discussed in greater depth in the **Analysis Methodology** section of this document.

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

Fields to be replaced 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 of the customer. Examples of element scopes include system, sub-system, component, component software (non-OS), and component OS.

Model Type

The **model type** indicates which type of model is being created. The options are:

- Physical
- Logical
- Process

Note: Once the model type has been determined, only the corresponding section (2, 3, or 4) should be filled out.

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 attack surface analysis.

Development SME

This is the development subject matter expert providing the information regarding the element.

Date

This is the date when the element under analysis 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. 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

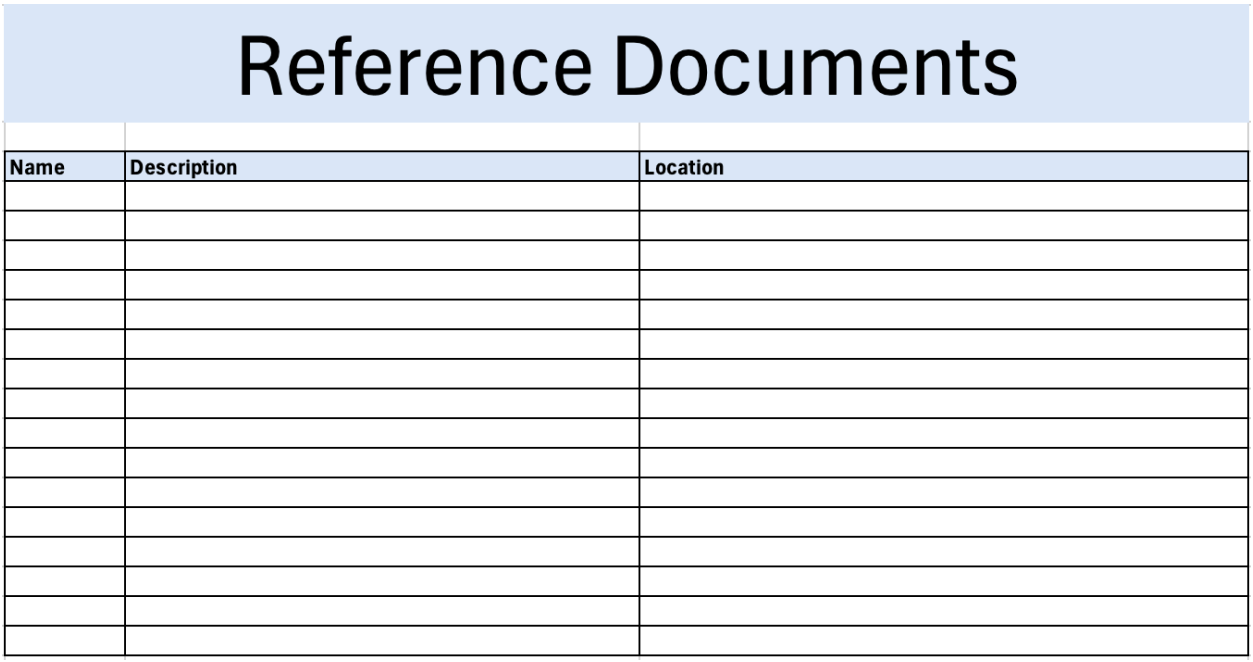
The **author** corresponds to that listed on the cover sheet.

Description

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

Reference Documents

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



Name

This is the name of the document being referenced.

Description

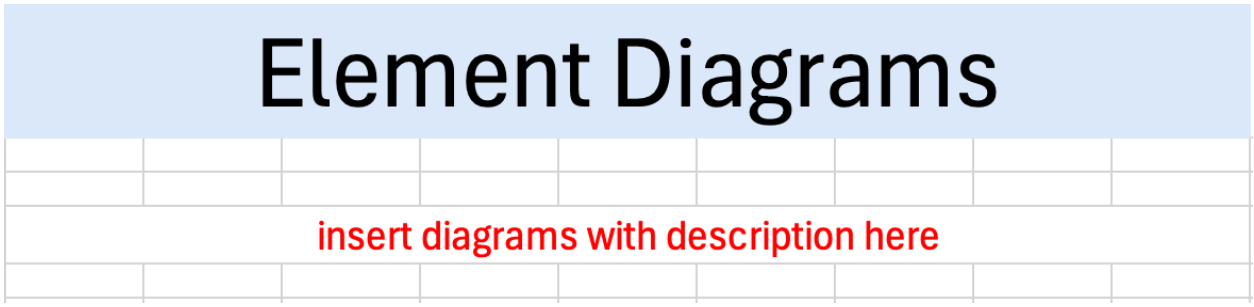
This is a brief description of the document being referenced.

Location

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

Section 1 – Element Diagrams

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



Element diagrams are inserted images with attendant explanations. The intent of these diagrams is to provide a mechanism for discussing the various attack surfaces. The diagram gives the various features (ports, protocols, and processes) a context which lists alone cannot.

The utility of the element model diagram is that it aides in the collection of the analysis inputs. In practice, each of these features should be uniquely enumerated to clearly document issues identified in the analysis.

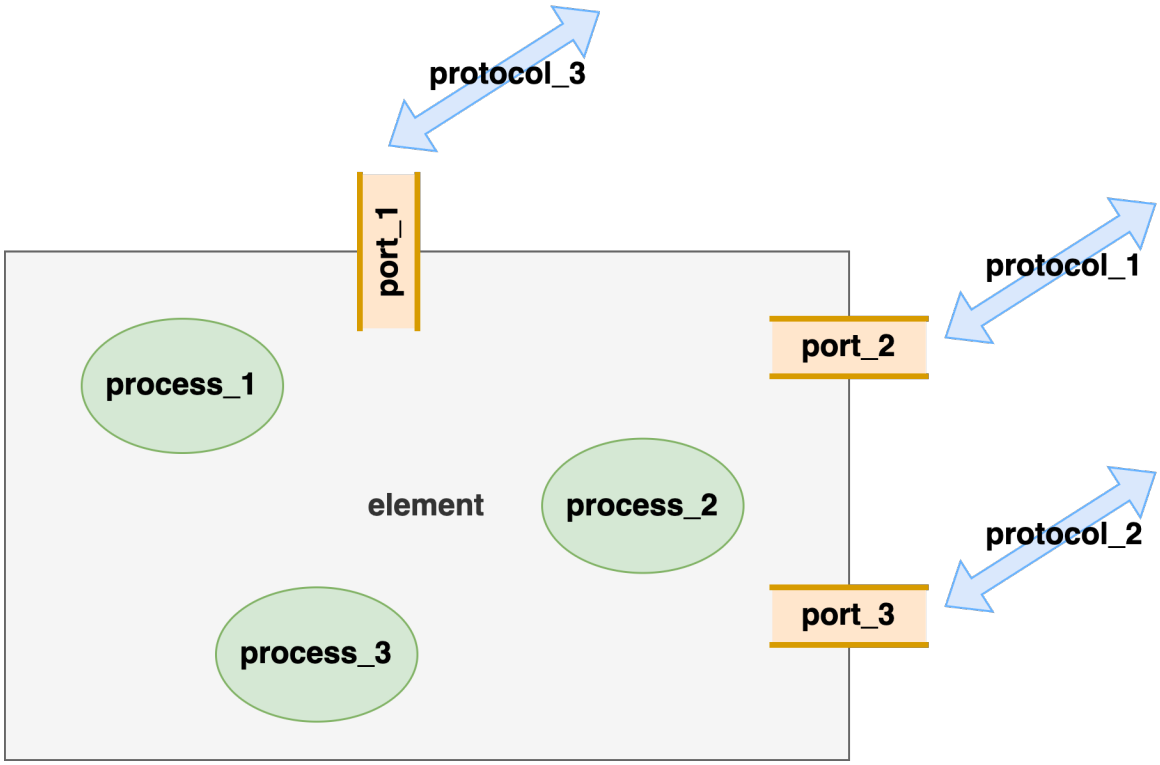
The unique identifiers (names) of the various parts of the diagram should correspond to those used in the other sections of the analysis workbook.

There are many possibilities for the diagrams included. These range from annotated photographs or CAD drawings in the case of physical elements, block diagrams which are useful at the system level, and DFDs for purely software scope elements.

The requirement for this section is that at least one visualization that appropriately conveys the structure of the element be included.

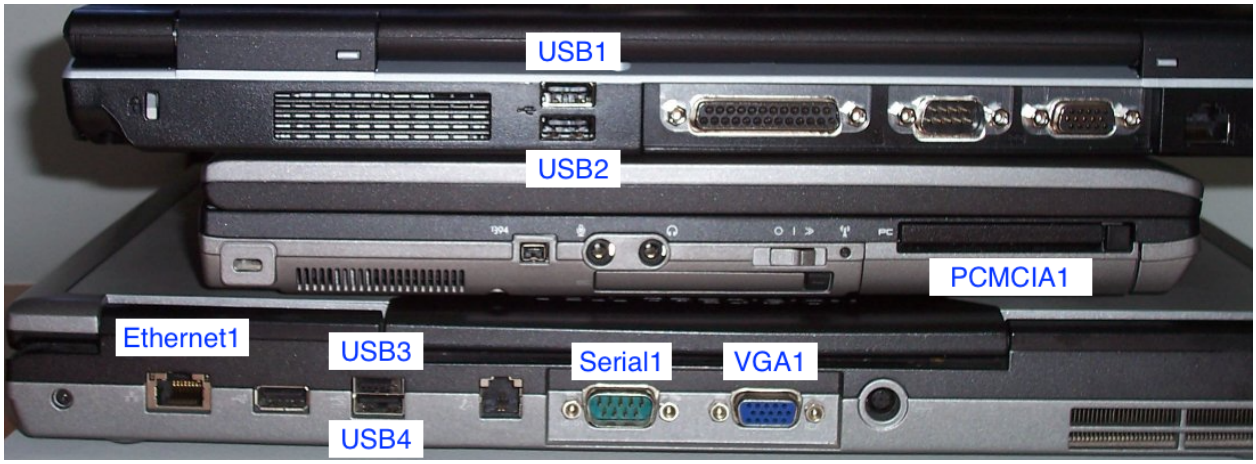
Element Diagram Examples

The following is an element model block diagram.



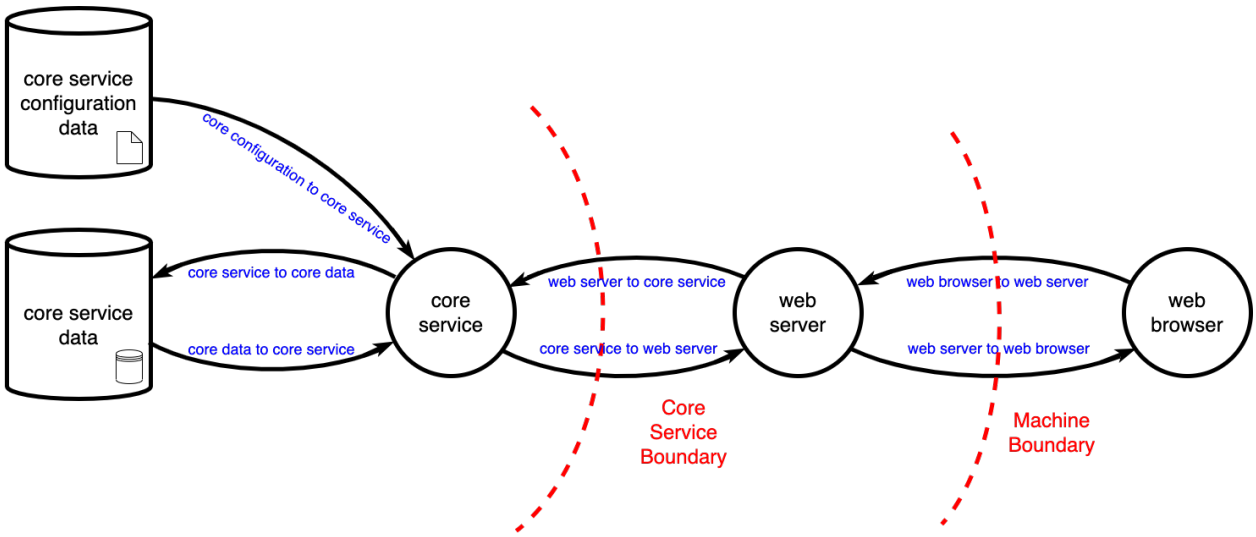
The element under consideration is shown as a grey box. Ports (physical or logical) are shown in **tan**. These are placed on the perimeter of the element. Communication protocols are shown as **blue** arrows and may be single- or double-headed depending on the use case. Finally, processes are shown in **green** ovals.

The following is an annotated photo identifying the physical ports.



Here the various ports are annotated with unique identifiers for use in later sections. This type of diagram should be used as the basis for the creation of the block diagram style shown in the earlier example.

The following is a DFD (data flow diagram) showing various processes, resources and data flows.



As with the previous two examples, all pertinent features are shown with unique identifiers. This style of diagram is typically used when the element is software-only.

Section 2 – Physical Ports

The **physical ports** sheet of the workbook is shown below:

Physical Ports

ID	name	interface	description	purpose	requirement ID	notes

ID

This is the unique ID of the physical port corresponding to the one indicated in the element diagram sheet.

Name

This is the common name of the physical port.

Interface

This is the type of interface presented by the port. Interfaces include:

- Analog
- CAN
- Ethernet
- JTAG
- RS232
- RS422
- USB

Note: For the purposes of an attack surface analysis, it is unnecessary to elaborate on the physical interface's connector.

Description

This is a brief description of the port.

Purpose

This is the reason for the port being present.

Requirement ID

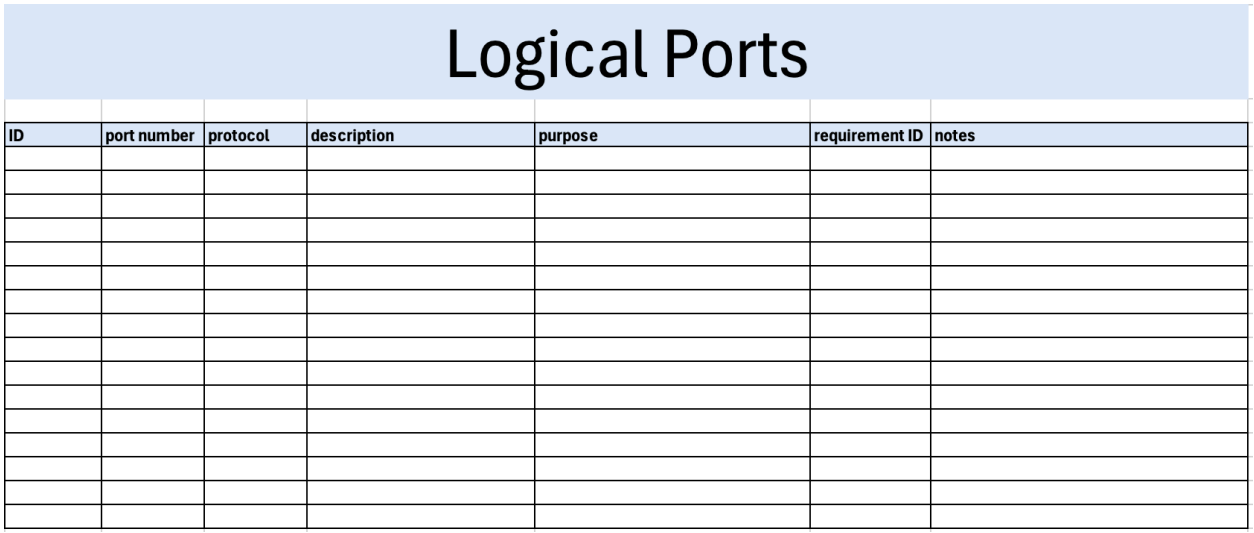
This is the ID of the requirement justifying the presence of the port.

Notes

This is a general notes field.

Section 3 – Logical Ports

The **logical ports** sheet of the workbook is shown below:



Logical Ports

ID	port number	protocol	description	purpose	requirement ID	notes

ID

This is the unique ID of the logical port corresponding to the one indicated in the element diagram sheet.

Note: An ID refers to a port number-protocol pair.

Port Number

This is logical port's IANA port number.

Protocol

This is the protocol being used on port. Protocols include:

- DHCP
- DNS
- DoIP
- FTP
- gPTP
- HTTP
- HTTPS
- ICMP
- MQTT
- NTP
- SMTP
- SNMP

- SOME/IP
- SOVD
- SSH
- TCP
- TFTP
- TLS
- UDP
- custom

Description

This is a brief description of the port.

Purpose

This is the reason for the port being used.

Requirement ID

This is the ID of the requirement justifying the presence of the port.

Notes

This is a general notes field.

Section 4 – Processes

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

Processes							
ID	name	process type	process owner	description	purpose	requirement ID	notes

ID

This is the unique ID of the process corresponding to the one indicated in the element diagram sheet.

Name

This is the common name of the process.

Process Type

This is the type of process. Process types include:

- kernel
- service / daemon
- system
- user

Process Owner

This is the ACL owner of the process.

Description

This is a brief description of the process.

Purpose

This is the reason for the process being present.

Requirement ID

This is the ID of the requirement justifying the presence of the process.

Notes

This is a general notes field.

Legend

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

interface	protocol	protocol (expanded)	process type	model type
Analog	custom	custom protocol	kernel	physical
CAN	DHCP	Dynamic Host Configuration Protocol	service/daemon	logical
Ethernet	DNS	Domain Name System	system	process
JTAG	DoIP	Diagnostic communication over IP	user	
RS232	FTP	File Transfer Protocol		
RS422	gPTP	Generalized Precision Time Protocol		
USB	HTTP	Hypertext Transfer Protocol		
	HTTPS	Hypertext Transfer Protocol Secure		
	ICMP	Internet Control Message Protocol		
	MQTT	Message Queue Telemetry Transport		
	NTP	Network Time Protocol		
	SMTP	Simple Mail Transfer Protocol		
	SNMP	Simple Network Management Protocol		
	SOME/IP	Scalable service-Oriented MiddlewarE over IP		
	SOVD	Service-Oriented Vehicle Diagnostics		
	SSH	Secure Shell Protocol		
	TCP	Transmission Control Protocol		
	TFTP	Trivial File Transfer Protocol		
	TLS	Transport Layer Security		
	UDP	User Datagram Protocol		

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 template** (AVCDL template)
4. **Attack Surface Analysis – Analysis Procedure** (AVCDL tertiary document)