# Title

I'm Charles Wilson, senior principal engineer at motional responsible for cybersecurity development lifecycle practice.

This presentation will cover the supplier cybersecurity process mapping.

# Supply Chain Training Path

# This diagram shows the overall AVCDL supply chain training path.

# If you're taking this training, it's assumed that you've already completed the supply chain overview training.

# This training covers vendor cybersecurity process to AVCDL mapping.

# Additional trainings will cover:

# manufacturer disclosure statement (AVCMDS),

# supplier self-report cybersecurity maturity,

# cybersecurity requirements,

# tailoring the cybersecurity interface agreement,

# service level agreements (SLAs),

# software bill of materials (SBOM),

# attack surface analysis,

# and threat modeling.

# Introduction – Lithium Hydroxide Canister

The classic metaphor of the square peg and the round hole is about a mismatch between what we have and what we need.

What happens when this mismatch becomes not just inconvenient, but life threatening?

This is a lithium hydroxide canister.

It takes the shape of a literal square peg and the hose coming out of it goes into a literal round hole.

# Introduction – Finished Adapter

Here’s the lithium hydroxide canister in place.

That square peg has been attached to the round hole, after a fashion.

Let’s zoom out a bit and give this scene some context.

# Introduction – Context

Here we can see two of the Apollo 13 astronauts whose lives were directly impacted by this device.

The third astronaut is holding the camera.

That adapter, that lithium hydroxide container removes CO2 from the atmosphere, allowing the astronauts to breathe.

This square peg and this round hole show what the consequences can be when you have mismatches between what you have and what you need.

So how we can keep these types of problems from cropping up within the context of cybersecurity between the supplier and the customer.

We're going to do that by creating a mapping between the processes that the vendor uses and the ones that the customer uses.

# Supplier Processes

Here's a typical set of supplier processes.

You'll note that it's using the classic V-diagram that we see so often.

Although easy to understand, its processes are very general.

Also, they don’t directly map to the AVCDL or 21434 for that matter.

# AVCDL

And here's the AVCDL.

You'll note that there is a much higher resolution in terms of the activities that are undertaken.

Now, let's see how we bring these two together.

# Supplier Processes Overlay

If we overlay the supplier processes onto the AVCDL, the complexity that arises becomes very evident.

Many of the supplier processes cover multiple AVCDL processes.

In order for a supplier using their processes and a customer using the AVCDL (or vise versa) to communicate, there needs to be a clear and defined mapping between these two disparate approaches.

# Process Mapping Use in Supplier Selection

This diagram shows the major documents used in both the supplier selection **request for information** (RFI) and **request for quote** (RFQ) activities, as well as the development production and post-production activities.

Although the **supplier self-reported maturity** and the **supplier cybersecurity manufacturer's disclosure statement** are the two primary documents enabling the creation of the **tailored cybersecurity requirements**

and **cybersecurity interface agreement**,

it is the **vendor process – AVCDL product mapping** that allows us do this when there are established supplier processes.

It’s critical to both the requirement tailoring and CIA creation that the processes being addressed be clearly understood by both the supplier and customer.

Process mapping ensures that both parties are on the same page.

# Process Mapping Material

There are three documents within the AVCDL document set that support the creation of the supplier process to AVCDL requirement product mapping.

These are

* the **Understanding Supplier Cybersecurity Process Mapping** elaboration document
* the **434 req-AVCDL product** sheet of the **vendor process - AVCDL product mapping template** spreadsheet workbook
* And the **434 req-vendor process** sheet of the **vendor process - AVCDL product mapping template** spreadsheet workbook

# Understanding the AVCDL Phase Requirements - 1

In order to create the process mapping, it's necessary that the supplier review the AVCDL documentation.

The starting point for this is the AVCDL primary document itself.

This provides the overview of the cybersecurity development lifecycle and establishes the framework upon which both the phases and the phase requirements exist.

# Understanding the AVCDL Phase Requirements - 2

Within the AVCDL primary document each of the phase requirements is listed.

For each of the phase requirements, summary information and a list of secondary documents elaborating on that material is provided.

# Understanding the AVCDL Phase Requirements - 3

The secondary documents referred to in the phase requirements shown in the AVCDL primary document contain detailed information as to the processes that are expected to take place in order to satisfy the phase requirement.

# Process Mapping Documentation - 1

Here you can see the relationship between the various AVCDL documents covering supplier process to AVCDL phase requirement product mapping.

We can see that the **vendor process – AVCDL product mapping template** is used to create the **vendor process – AVCDL product mapping** document. A specific instance of the process mapping template.

The dotted lines surrounding those two documents is used to indicate that the **Understanding Supply Chain Process Mapping** elaboration document refers to both of those documents taken together.

# Process Mapping Documentation - 2

Within the larger supplier document landscape, the **vendor process – AVCDL product mapping** is used to inform the creation of the **tailored cybersecurity requirements** document when the supplier has an established set of cybersecurity processes.

This conditional nature is indicated by the dotted orange line as opposed to the solid ones used with the other documents feeding into the **tailored cybersecurity requirements** document.

Having this mapping ensures that the **tailored cybersecurity requirements** are conveyed is a manner that makes sense to both the supplier and customer.

This diagram is derived from the **Supplier Cybersecurity Guidance Documents** diagram in the **Understanding Supply Chain Interaction in an AVCDL Context** elaboration document.

Supplier Cybersecurity Process Mapping Workflow

Let’s consider the process for creating the mapping between the supplier’s processes and the AVCDL phase requirement processes.

Here's the workflow to be used.

This diagram is taken from the **Understanding Supplier Cybersecurity Process Mapping** elaboration document.

As you can see, there are three activities that take place, detailing of the supplier cybersecurity processes, creation of the supplier to AVCDL mapping, and verification of the mapping.

In the supplier cybersecurity process detailing activity, the supplier’s cybersecurity SME uses

the **vendor processes document set** in conjunction with the **AVCDL document set**

to complete the **vendor process to AVCDL product mapping template**.

This results in the creation of a **vendor to AVCDL map (with vendor process added)** document specific to the supplier.

The customer’s cybersecurity SME uses this document to create a **completed vendor to AVCDL map**.

This map is then reviewed by the customer SME. If process gaps are found, these are fed back to the supplier.

The supplier will either create an update including the omitted process or confirm that a process gap exists.

Once it's been determined that there are no unacknowledged process gaps, the document is considered to be verified.

Mapping Worksheet – 21434 to AVCDL Phase Requirements

The **434 req-AVCDL product** sheet of the **vendor processes - AVCDL product mapping template** workbook serves our a starting point for mapping.

It provides a mapping between the 21434 requirements, their associated work products, and the AVCDL.

This is important because it doesn't require the supplier to have an in-depth knowledge of 21434.

The materials provided in the AVCDL including the **AVCDL Phase Requirement Product ISO 21434 Work Product Fulfillment Summary** certification document

in conjunction with all of the other AVCDL documents provide extensive explanation as to how each of the 21434 requirements is satisfied.

This serves as a basis from which the supplier can then create their own mapping to the 21434 requirements.

Mapping Worksheet – 21434 to Supplier Processes

Next the supplier will take the **434 req-vendor process** sheet of the **vendor process - AVCDL product mapping template** workbook

and completes it, replacing the top rows listing the AVCDL materials divided into phases and phase requirements

with their corresponding phases and processes,

showing how those map onto the corresponding 21434 requirements.

Mapping Worksheet - AVCDL to Supplier Processes

Once the supplier has completed mapping their processes against 21434, they'll return the workbook to the customer.

The customer’s cybersecurity SME will then take both the ‘434 to AVCDL and ‘434 to supplier mappings and bring them together in the AVCDL to supplier process mapping.

This will take the AVCDL processes on the left and the supplier processes across the top, and show how those map to each other using 21434 as a basis for alignment.

It's this spreadsheet that will be used in order to determine supplier process gaps.

And it's this spreadsheet that will be used to allow the vendor and the customer to communicate various process distinctions.

Those gaps will need to be filled with additional processes, either supplied from the AVCDL, or created by the supplier.

It is recommended that when creating the mapping, that you first handle the simple case where a single AVCDL or supplier process maps to a single 21434 requirement.

Then move on to the cases of one to many or many to one mappings.

Always Verify

Because of the overall complexity of the cybersecurity processes throughout the development lifecycle,

it's important that the mapping between supplier and customer processes be clearly documented.

It's important to verify what those processes do.

Since the processes are documented, they should be able for review to determine that they in fact, do provide the coverage they proport.

AVCDL on GitHub

All AVCDL materials, both in source and distribution forms, are available on our GitHub site, as shown here.

Because of the size of the repository, it's recommended that you either clone the repository or download a ZIP archive of it, if you're not familiar with using git.

Instructions for downloading a ZIP archive are linked to on the repository’s front page.

Supply Chain Training Path – Next Steps

The next step in this training sequence is to complete the two other courses at this level, if you haven’t already.

The **AVCMDS** training covers the supplier’s cybersecurity manufacturer disclosure statement.

The **supplier self-report cybersecurity maturity** training covers how a supplier self-reports the maturity of their processes in the context of the AVCDL.

Once the three trainings at this level are complete, you should proceed to the **security requirements** training.

References

Here are references to the source material used in the creation of this presentation.

They'll also be included in the video description.

Additionally, this presentation’s source material will be provided on the AVCDL GitHub repository.