# Title

I’m Charles Wilson, Senior Principal Engineer at Motional responsible for the cybersecurity development lifecycle practice. This presentation will cover the incremental adoption of the AVCDL.

# AVCDL Core Document Set

The AVCDL is a comprehensive cybersecurity development lifecycle. Its very scope presents a challenge to wholesale adoption. Here we see an overview of the AVCDL core document set. There's the primary document, a set of secondary documents, and associated supporting material.

# AVCDL Materials

If we look a little deeper, that supporting material extends into blog posts, elaboration documents, supply chain materials, templates to go along with the supply chain materials, and tracking documents used in the creation of the AVCDL.

[pause]

Basically, it's everything that you need in order to do product cybersecurity. Now, this is a good thing if you have a relatively mature organization with respect to cybersecurity, because you'll use the AVCDL to determine what edge cases you're not covering. If on the other hand, your organization has had no cybersecurity group within it in the past, or has a severely limited number of activities which are done in cybersecurity, then the AVCDL presents an overwhelming challenge.

[pause]

Let's look at how the AVCDL is put together and how we can reduce the complexity of it by adopting it in an incremental fashion.

# AVCDL Framework (1)

Let’s start with the AVCDL framework itself. As you can see, the framework is divided into three major areas. The first area (the foundation phase) includes those activities necessary throughout the entire lifecycle. The second area (the developmental phases) includes those activities which need to be performed in the creation of the product. The third and final area (the post-developmental phases) include those activities performed once the product has been released.

Now let's look at each of these areas in turn.

# AVCDL Framework (2)

The foundation phase activities are broad in scope and highly impactful in that once these activities are in place, they're applied throughout the lifetime of every project. Because of this, these activities need to be given special attention. They will have ripple effects both within a particular product’s development and also across the entire families of products to which they're applied.

# AVCDL Framework (3)

Arguably the developmental phase activities are the most flexible in terms of how and when they're implemented. This is because these activities are the most tactical. Many of them can be implemented in isolation. The exception are the gates, as they're used to synchronize various activities and groups within the organization. That being said, the gates are intended to be very light touch activities, and in general, gate management is the responsibility of project management, not cybersecurity.

AVCDL Framework (4)

Post-developmental (also known as operational) activities, split the difference between the foundational and the developmental behaviors, in that they have long term impact because the product is out in the field and is being managed, but they also have a lot of interaction with operational technology activities. At the same time, they're highly focused in terms of the way that decommissioning is handled for cybersecurity, which has a much more active involvement when compared with the rest of the organization.

Incremental Adoption Spectrum (1)

Now, let's consider the approach that we'll take in grouping the AVCDL activities for incremental adoption.

[pause]

If we consider a spectrum of adoption where we have tactical activities on one end and strategic ones on the other, we can think about five stages for grouping. We’ll then put the various AVCDL activities into these stages based on their complexity and organizational impact.

Incremental Adoption Spectrum (2)

The stages are barebones,

Incremental Adoption Spectrum (3)

tactical,

Incremental Adoption Spectrum (4)

tracked,

Incremental Adoption Spectrum (5)

managed,

Incremental Adoption Spectrum (6)

and mature.

[pause]

The further you progress from tactical to strategic, the greater the interplay and interdependence there'll be between various activities and with other groups within the organization. It's far easier to implement the earlier stage activities and make adjustments to your organization's tooling as you progress. Implementing the later stage activities and attempting to backfill the earlier stage ones will lead to a lot of churn should changes be required.

Prioritized Phase Requirements

Here's an overview of the AVCDL phase requirements assigned to these five stages. As you can see, the barebones stage has very few activities. As we progress to the tactical stage, we get a much larger chunk, with slightly fewer in tracked stage. By the managed stage nearly all activities have been included, with the mature stage having almost nothing.

Let's look at some interesting characteristics of this decomposition.

Preliminary vs Full Implementation (1)

Four of the phase requirements

* tool chain support,
* threat prioritization plan,
* security design review, and
* source code review

are implemented in two separate stages (an initial implementation and a final one). This is because of their interplay with other activities within the AVCDL, as well as with the greater organizational interaction required by their implementation.

Preliminary vs Full Implementation (2)

In the case of the security design review and the source code review, they'll be fully implemented in the tracked stage.

Preliminary vs Full Implementation (3)

Whereas the tool chain support and threat prioritization plan won't be fully implemented until the managed stage.

Safety-related Phase Requirements

Additionally, the safety related phase requirements have been grouped together because of their tight coupling.

Incremental Implementation Stages

Now, let's look at each of the implementation stages and what they entail.

Barebones

The barebones stage activities require the least from the development teams. These are activities that can be undertaken by cybersecurity SMEs in conjunction with devops. They represent the lowest hanging fruit. All of them are developmental in nature. Configuring the secure build, secure settings, deprecation of unsafe functions, and static analysis are all things which are typically already in place in the build process. What we're trying to achieve is the application of cybersecurity relevant settings in these areas in order to enhance what would otherwise be no security whatsoever.

Tactical

The tactical stage is focused on the secure and correct implementation of the system. All three areas of the AVCDL are addressed. There’s now interaction with the development and operations teams, with more interaction with the devops team. As noted earlier, there are several activities in the stage which are preliminary. These activities don't need to be implemented as formally at this point as the others. They're included because they're needed to support other activities in this stage.

[pause]

Additionally, we also have activities which are included because they are relevant to the interaction between cybersecurity and safety.

[pause]

The tactical stage is concentrated in the implementation phase with some activities from the foundation and operation phases being included.

Tracked

The track stage is focused on the secure design of the system. In this stage, the activities of the requirements and design phases of the AVCDL are addressed. This requires far more coordination with the systems engineering and development teams early on in the creation of the system. Additionally, we're picking up more elements from the foundation phase, specifically in the areas of requirements and deployment.

Managed

The managed stage is focused on the management of the end-to-end life of the system. In this stage, the interaction between cybersecurity and project management is emphasized as seen here by the inclusion of the five gates within the developmental phases. We also pick up the threat model review, the attack surface analysis review, and final review. Additionally, we look at the decommissioning processes and we finish out the toolchain support, and the threat prioritization plan.

 Mature

In our last stage, the mature stage, we're focusing on the long-term support of the system. Specifically, attention is given to training and ownership activities. One could argue that the roles and responsibilities need to be established ahead of time before anything else happens.

However, in reality, the roles and responsibilities and training material tend to be the last things formally added to the system.

Supply Chain Activities

One thing not addressed up to this point is the supply chain.

As with any complex system, you have to consider the supply chain and its relationship with respect to cybersecurity. Within the AVCDL, there are three activities called out. These are

* the autonomous vehicle cybersecurity manufacturer's disclosure statement or AVCMDS,
* the supplier self-reported cybersecurity maturity assessment or CMM and
* the cybersecurity interface agreement or CIA.

it's really unlikely that any two organizations will have the same level of maturity with respect to their processes and so doing these three activities is critical to the success of a project regardless of the relative maturity of the two organizations.

This is because by undertaking these activities, you're able to align the cybersecurity activities of both the supplier and the customer and identify the gaps that exist in the two organizations. If you have suppliers or you are a supplier, you should undertake to complete this information.

Evaluating Your Status

Regardless of where you're starting from, it's important to evaluate what your own organization's maturity is and to keep track of it as you progress through the evolution of your organization’s maturity. For that, we can use the supplier cybersecurity maturity assessment. Simply perform the assessment on your own organization.

Mapping Your Status

To track progress over time the AVCDL provides an Excel spreadsheet with a spider plot of all AVCDL phase requirements. This can be used to generate a time series chart, like the one seen here.

Summary

In summary, remember that although the cybersecurity lifecycle is really large and fairly complex, the problem is still tractable.

You should start by doing a cybersecurity maturity self-assessment to find out where you’re starting from.

Remember to consider the supply chain.

And finally, track the progress that you're making as you go.

This last point is helpful both from an internal standpoint and also because one of the aspects of cybersecurity for things like ISO/SAE 21434 or UN R155 is that you should be making ongoing progress in your product cybersecurity posture.

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.

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.