# Title

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

# Supply Chain Training Path

Here we see the AVCDL supply chain training path. At the top is the supply chain overview which is this presentation. Additional trainings will cover manufacture disclosure statements (the AVCMDS), supplier cybersecurity maturity, vendor cybersecurity process to AVCDL mapping, cybersecurity requirements, tailoring the cybersecurity interface agreement, service level agreements (SLAs), software bill of materials (SBOM), attack surface analysis, and threat modeling.

# Cybersecurity Standards and Regulations Ecosystem

Cybersecurity doesn’t exist in a vacuum. Here we can see how the international standards and regulations can be combined to form an ecosystem. The foundation of this ecosystem is the quality management system (how documents are recorded and tracked). Continuing upward, we have the systems development lifecycle followed by the software development lifecycle. Above that we have ISO 21434 for road vehicle cybersecurity engineering and ISO 24089 covering road vehicle software update engineering. These two form the basis for the UNECE regulations 155 and 156 covering the cybersecurity management systems (CSMS) and software update management systems (SUMS) respectively. Finally, the latest from the UNECE is the Ares proposal which will address automated driving systems (ADS). It’s a superset of R155 and 156.

# R155 At a Glance

Let’s consider the general categories covered by UNECE R155. The first is general boilerplate material applied to all UNECE regulations. The second is the cybersecurity management system or CSMS which deals with the product creation processes. The third, vehicle type covers product operation processes. Fourth is reporting which deals with product issue processes.

It’s important to note that R155 doesn’t just focus on the OEM, although the OEM is primarily responsible for ensuring compliance. There is an expectation within R155 that the entire supply chain conforms to the regulation, regardless of the supplier tier.

# R155 Supply Chain Scope

Here we see an illustration of a portion of the R155 supply chain showing various information flows. The OEM generates requirements for its tier 1 suppliers. The tier 1 suppliers in turn generate requirements for all of their lower tier suppliers. All suppliers are expected to provide evidence supporting their fulfillment of the requirements and their compliance with R155. This evidence accumulates as it feeds up the supply chain. Eventually, when the product is ready for certification, the OEM organizes the accumulated evidence and provides it to the approval authority.

If the evidence is compelling, the approval authority provides an approval of the type to the OEM. Measurement and control of requirements and evidence is established in the agreements between each customer and their supplier regardless of their position in the supply chain. The controlling agreement within the context of ISO 21434 is called the cybersecurity interface agreement or CIA.

# R155 Requirements

Implementation of R155 can be divided into four areas.

The first is fundamentals. This area is concerned with management systems. These systems track and document the evidence we have for the various activities we do. Management systems are expected to exist for development, production, and postproduction activities.

The second area is product development. In this area deals with risk identification, assessment, and treatment; the verification of the management of risk; cybersecurity testing; and most importantly, the freshness of the risk assessment. It’s critical that this information is kept up-to-date.

The third area is that of operations, it’s important that to have adaptable monitoring and response. It’s not sufficient just to have a set of rules in place for when the product is in operation. You have to be able to adapt to changing situations that occur over the lifetime of the vehicle. To that end, the focus is on tracking the cybersecurity controls used.

Also, it’s necessary to ensure that the risk mitigations in place are implemented in a timely fashion.

It’s important to be able to do threat extraction from the vehicle logs. Are the right pieces of information being recorded that will identify when a cybersecurity related activity or incident happens, such that you can use the information for both diagnostic and mitigation purposes?

Are supplier deficiencies being managed? This must be done regardless of what tier you’re in. Are you tracking to ensure that your suppliers are responding appropriately when cybersecurity issues arise?

The fourth area addresses the support suppliers provide to the OEM. The entire supply chain needs to be supporting the OEM since they are the party being held responsible under R155. Shared activities include critical element risk assessment, type risk protection, risk countermeasures, and sufficiency testing. All suppliers need to ensure that they are doing everything reasonable to detect and prevent cyberattacks. After releasing to their customer, suppliers need to monitor for cybersecurity events that occur and need to provide the ability to extract forensic information from their logs.

ISO 21434 Work Products and Requirements

As mentioned earlier in this presentation, ISO 21434 serves as the technical underpinning for R155. Here we see a portion of the 21434 work products showing their dependent requirements.

These work products and their dependent requirements have a much higher granularity when we compare them with those of R155 itself. This is to be expected from a technical specification.

AVCDL to ISO 21434 mapping

The AVCDL provides us a way to satisfy both R155 and ISO 21434. Here’s a portion of the mapping between the AVCDL phase requirements and the ISO 21434 work products.

As a lifecycle, the AVCDL more readily integrates with an established development process. Additionally, it's written in a manner which is far more accessible to those who don’t spend their time reading ISO and UNECE documents.

AVCDL document set

The AVCDL itself is comprised of four major document types.

The first is the overview, also known as the primary document. This document is entitled the Autonomous Vehicle Cybersecurity Development lifecycle, or AVCDL.

The second type are the process detail documents, also called the secondary documents. These seventy documents individually detail all the processes within the AVCDL.

Together, the primary and the secondary documents give us the what, the who and the when of the lifecycle. This material is completely company agnostic.

The third set of documents, the procedures or tertiary documents are the how of the lifecycle.

These documents are company specific as they tell us exactly what tools are used and what procedures are followed in order to implement the processes specified in the primary and secondary.

It is expected that every company adopting the AVCDL provide their own procedure documents.

The last type are the supporting materials documents.

These materials include spreadsheets, templates, and blog posts. The spreadsheets contain reference materials used to construct the AVCDL itself. The templates give AVCDL adopters a starting point for providing information to outside entities. And the blog posts describe and explain various aspects of the AVCDL.

AVCDL materials

Within the supply chain context, materials of interest include the primary and secondary documents, blog posts covering the supply chain, and elaboration documents describing how to use and interpret the various supplier materials.

Also of interest are the reference material for the cybersecurity interface agreement, AVCMDS, and the mapping between vendor processes and the AVCDL itself.

Finally, are the general information on how lifecycles are created for those organizations which don't have established development lifecycles.

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 take one of the three following courses.

The AVCMDS, which covers the manufacturers disclosure statement in the area of cybersecurity.

The supplier maturity training, which covers how a supplier self-reports the maturity of their processes in the context of the AVCDL.

Or the vendor process mapping training which covers how to take established vendor processes and map them to the corresponding AVCDL processes. This helps to ensure that no gaps will exist between the vendor and the customer in the area of cybersecurity.

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.