Yours, Mine, and Ours: The AVCDL and Cybersecurity Interface Agreements

Charles Wilson
Principal Engineer, Cybersecurity Development Lifecycle Practice

2021-07-23

Category: security-supply-chain

Tags: security, cybersecurity, autonomous vehicles, supply chain, AVCDL, CIA, cybersecurity interface agreement

My previous post, **AVCMDS: Cybersecurity Manufacturer Disclosure Statement**, introduced how the **AVCMDS** can be used to get a snapshot of a supplier's current capabilities. Its follow-up, **Where are You at? Level Setting Supplier Cybersecurity Maturity** provided insight into the maturity of a supplier's cybersecurity processes. In this post we'll bring the understanding gained from both instruments to guide the execution of a cybersecurity interface agreement (**CIA**) with the supplier.

What is a CIA?

ISO/SAE 21434 (**Road Vehicles – Cybersecurity Engineering**) [1] requires that CIAs be in place between suppliers and their customers along the supply chain. But what is a CIA?

The standard defines a cybersecurity interface agreement as an "agreement between *customer* and *supplier* concerning distributed cybersecurity activities." Although accurate, this definition is unsatisifying.

The UNECE WP.29 GRVA "*Proposal for amendments to the draft Regulations on Cyber Security and Software Updates*" [2] provides greater insight:

> *The current draft ISO/SAE 21434 standard defines Cybersecurity Interface Agreements (CIAs) for Development which are used for communicating the required cybersecurity activities across the supply chain including internal and external suppliers. Information shared through such interface agreement ensures that the required relevant cybersecurity information is exchanged across the supply chain without any intellectual property rights being violated. The respective replacement part manufacturers would need to obtain this information to ensure that the parts and components developed by them have*

> *the possibility to have the same level of security as that of the contracted suppliers.*

and

> *The current draft ISO/SAE 21434 standard defines Cybersecurity Interface Agreements (CIAs) for Production which are used for communicating the required cybersecurity activities across the supply chain including internal and external suppliers. Information shared through such interface agreement includes methods to confirm that the cybersecurity requirements for post-development like verification, validation, inspection, coding or configuration and calibration checks and related compatibility checks while performing system integration / installation / activation. This ensures that the required relevant cybersecurity information is exchanged across the supply chain without any intellectual property rights being violated.*

From these we see three distinct goals:

- Information sharing across the supply chain
- Preservation of individual organizational IP
- Establishment and confirmation of cybersecurity-related activities

What's Inside?

ISO/SAE 21434 specifies that a CIA include the following elements:

- Organizational contact information
- Identification of cybersecurity activities and responsibility
- Tailoring activities
- Identification of work products
- Information sharing
- Milestones
- Time frame of applicability of CIA

Having these elements in a formal document provides a basis for discussion between supplier and customer. This is especially true when there is a large disparity between the cybersecurity maturity of the parties. Additionally, it provides a place to capture details that would otherwise be held as informal knowledge. This information can be lost over the lifetime of the relationship.

All Roads Lead to Rome

As with the **AVCDL CMM** and **AVCMDS**, the **AVCDL** [3] serves as the basis for the CIA. The AVCDL was chosen because it is built around the development lifecycle rather than any specific certification standard. This means that as long as the AVCDL can be shown to satisfy any arbitrary certification standard, the maturity information will be transferable. The AVCDL identifies milestones in the form of phase gates, and work products. The AVCDL is a certification body-reviewed set of processes for attaining compliance with **ISO/SAE 21434**, **ISO 26262**, and **UNECE WP.29 R155**. By adopting the AVCDL as the basis, much of the structure and scope of the CIA naturally emerge.

Assigning Responsibility

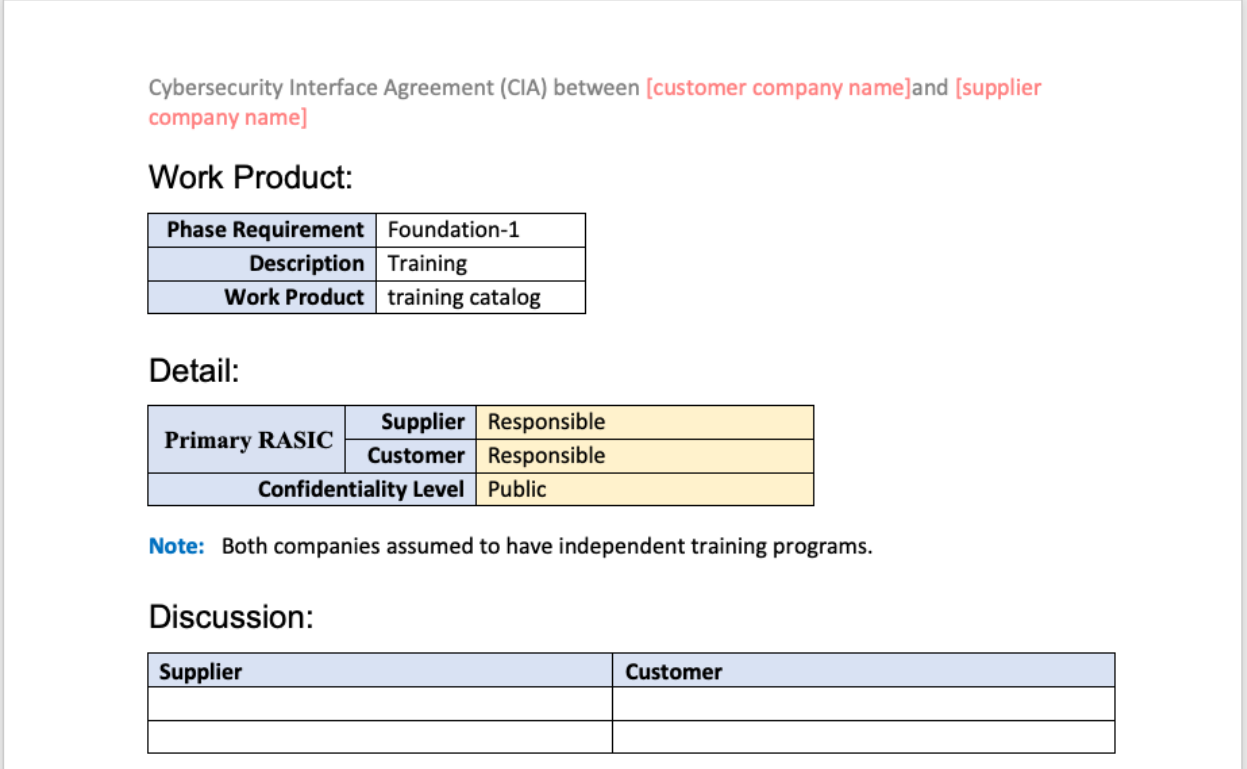
For each of the cybersecurity activities identified in the CIA, we are required to identify and assign responsibility levels to both the supplier and customer. We do this using a standard responsibility assignment matrix [4]. As specified in ISO/SAE 21434, the **RASIC** responsibility assignment matrix model is used. To simplify things, the highest level of responsibility is used rather attempting to identify all possibilities (for example: supporting vs. supporting and informed). A value is assigned to both the supplier and consumer.

Usually, there will be only one entity responsible for an activity. Static analysis is an example of this. The supplier is solely responsible for performing static analysis on any software they produce.

There may be cases when both the supplier and consumer bear responsibility for an activity. Training is one such case. It is expected that the supplier be responsible for training activities within their organization regarding the component they supply. The consumer is expected to be responsible for training within their organization regarding the proper use of that component within the larger system.

Picture This

The following image shows an example of one of the many AVCDL phase requirements and their associated work products included in the CIA.



Cybersecurity Interface Agreement (CIA) between [customer company name]and [supplier company name]

Work Product:

Phase Requirement	Foundation-1
Description	Training
Work Product	training catalog

Detail:

Primary RASIC	**Supplier**	Responsible
	Customer	Responsible
Confidentiality Level		Public

Note: Both companies assumed to have independent training programs.

Discussion:

Supplier	**Customer**

As can be seen, we identify the work product, it's associated AVCDL phase requirement, and work product. Next the RASIC information is shown along with the level of confidentiality to be applied to the information shared between the supplier and customer. This is followed by a free-form section allowing for the capture of discussion between the supplier and customer. This discussion goes far beyond what could be effectively captured in a simple spreadsheet.

Choose Wisely

It is at this point that I'll return to the **AVCMDS** and **AVCDL CMM** documents. We use both to evaluate whether the supplier has both the technical capability and process maturity to execute the various cybersecurity activities at the required level of responsibility.

Since the primary driver of using a particular supplier is the functionality of the element they bring to the table, a decision may be made to choose a supplier that does not have the expertise to perform the necessary cybersecurity-related activities. It is at this point where having the information provided by the **AVCMDS** and **AVCDL CMM** allows for a

timely discussion of options. These may range from providing process and practice guidance, to recommending third parties to work with the supplier, to allocating additional funds to cover activities within the capabilities of the supplier not currently being performed.

Information Sharing

Whenever entering into a supplier-consumer agreement, it is important to assign the level of confidentiality to be applied to the products of the various cybersecurity activities undertaken. This gives both parties the ability to share critical information without needing to be concerned that the information will be shared inappropriately.

Points of Discussion

Since the CIA covers the lifetime of the component as embodied in the consumer's system, there are many opportunities for discussion which need to be captured. The CIA we created incorporates the ability to capture these discussions for future reference.

The Devil's in the Details

At the end of the day, the CIA is a legally binding document between the supplier and consumer. The information it captures makes for a much simpler task for both the supplier and consumer's management and legal departments, who will need to approve it. Time should be allocated for the inevitable back-and-forth between the companies' various approval groups.

Getting the Goods

We provided the **AVCDL Cybersecurity Interface Agreement template** (MS Word) [5] and an explanatory document, **Understanding Cybersecurity Interface Agreements** [6], which goes into far greater detail. Follow the links in the references section below. The AVCDL secondary document **Cybersecurity Interface Agreement** [7] details the process undertaken to create a CIA.

References

1. **ISO/SAE DIS 21434 Road Vehicles – Cybersecurity Engineering**
   https://www.iso.org/standard/70918.html
2. **Proposal for amendments to the draft Regulations on Cyber Security and Software Updates**
   https://unece.org/DAM/trans/doc/2020/wp29grva/GRVA-05-17e.pdf
3. **Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL)**
   https://github.com/nutonomy/AVCDL
4. **Responsibility assignment matrix**
   https://en.wikipedia.org/wiki/Responsibility_assignment_matrix
5. **AVCDL Cybersecurity Interface Agreement template**
   https://github.com/nutonomy/AVCDL/raw/main/distribution/reference_documents/templates/AVCDL%20Cybersecurity%20Interface%20Agreement%20template.docx
6. **Understanding Cybersecurity Interface Agreements**
   https://github.com/nutonomy/AVCDL/raw/main/distribution/reference_documents/secondary_documents/Understanding%20Cybersecurity%20Interface%20Agreements.pdf
7. **Cybersecurity Interface Agreement**
   https://github.com/nutonomy/AVCDL/raw/main/distribution/reference_documents/secondary_documents/Cybersecurity%20Interface%20Agreement.pdf