Understanding the AVPDL

Revision

Version 3
12/13/22 3:35 PM

Author

Charles Wilson

Abstract

This document describes a proposal for a framework with which to manage the complete autonomous vehicle product development lifecycle.

Motivation

This document is motivated by the need to ensure a proper understanding of the basis of the autonomous vehicle product development lifecycle.

Audience

The audience of this document are those tasked with creating a development lifecycle.

Note: This document is not subject to certification body review.

License

Overview

When the goal of a company is to produce safety-critical systems in the form of autonomous vehicles, it is critical to appreciate that this product will be subject to various regulatory and statutory bodies and standards. These include **ISO 9000** [5] (quality), **ISO 26262** [3] (safety) and **ISO/SAE 21434** [4] (cybersecurity). Implicit in compliance with these standards is the compliance with a host of others upon which these rest. These include **ISO/IEC 15288** [1] (systems lifecycle) and **ISO/IEC 12207** [2] (software lifecycle).

Each of these standards addresses distinct lifecycle phases. However, differences exist between the various standards as to the names and number of phases. Given that these could each individually form the basis of a framework for driving the product development lifecycle, it is important to establish a common framework within which all can be applied.

The adoption of a common framework is all the more important as formal development presupposes the existence of phase gates used to provide traceability milestones. It is equally important that the phases be chosen in such a way that there is minimal additional overhead to existing development processes.

Phase Alignment

Broadly speaking, the abovementioned standards group lifecycle management activities into three main areas:

- Governance (organizational processes)
- Product Development
- Supplier Relationship

By its very nature, governance is a highly centralized activity requiring process uniformity. This implies that quality, management, product development, safety, and cybersecurity processes all conform to the organizational standard in the area of governance. Supplier relationships need to be managed in a similar manner.

What remains are the development phases of the product lifecycle. Here there is much more variability as to the number and type of phases called out.

Even with all this apparent complexity, it is possible to harmonize these disparities in a way which allows for both expression of compliance with various standards and also the insertion of process gates by which process control is maintained.

The following table shows the AVPDL phases and how they relate to the various standards.

AVPDL	15288	12207	26262	21434
organization processes	technical processes	technical processes	management of functional safety	overall cybersecurity management
			supporting processes	project dependent cybersecurity management
foundation phase	N/A	N/A	concept phase	concept phase
requirements phase	requirements definition	requirements definition	safety requirements	cybersecurity requirements
	requirements analysis	system requirements analysis	hazard analysis / risk assessment	cybersecurity assessment
design phase	architectural design	system architectural design	architectural design	cybersecurity design
implementation phase	implementation	implementation	implementation	development
	integration	system integration	integration and verification	integration and verification
verification phase	verification	system qualification testing		
	transition	software installation		
		software acceptance support		
release phase	validation		production	production
operation phase	operation	software operation	operation, service and decommissioning	continuous cybersecurity activities
	maintenance	software maintenance		operation and maintenance
decommissioning phase	disposal	software disposal		decommissioning
supplier processes	agreement processes	agreement processes	supporting processes	distributed cybersecurity activities

Phase Gates

In order to ensure that no group's processes go unfulfilled, phase gates must be used. Phase gates would be located in any phase where a group identified their need. This arrangement allows for a single phase gate to exist satisfying all team requirements for that phase. The following table shows the gates (◇) required by the cybersecurity and project management teams:

		Security	Safety	PMO	Hardware	Software	Quality
organization processes		N/A					
phases	foundation		🟨	◇	🟨	🟨	🟨
	requirements	◇	🟨		🟨	🟨	🟨
	design	◇	🟨	◇	🟨	🟨	🟨
	implementation	◇	🟨	◇	🟨	🟨	🟨
	verification	◇	🟨	◇	🟨	🟨	🟨
	release	◇	🟨	◇	🟨	🟨	🟨
	operation	N/A					
	decommissioning						
supplier processes							

In this example, all phases from foundation through release are gated because between the two groups all those phases require at least one phase gate.

Supplementary Documents

As noted earlier, the AVPDL is a framework. Supplementary documentation is required to meet the requirements of the various regulatory bodies and to provide clear guidance as the asks by each team on those creating the product. The AVCDL and its secondary documents represent the expression of this type of material. It is recommended that each group create a similarly styled document set.

Note: This approach taken in the AVCDL was assessed by TÜV to be compliant **ISO/SAE 21434**.

References

1. **ISO/IEC 15288 Systems and software engineering - Systems life cycle processes** https://en.wikipedia.org/wiki/ISO/IEC_15288
2. **ISO/IEC 12207 Systems and software engineering - Software life cycle processes** https://en.wikipedia.org/wiki/ISO/IEC_12207
3. **ISO 26262 Road vehicles - Functional safety** https://en.wikipedia.org/wiki/ISO_26262
4. **ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering** https://www.sae.org/standards/content/iso/sae21434/
5. **ISO 9000 Quality management systems** https://en.wikipedia.org/wiki/ISO_9000
6. **Autonomous Vehicle Cybersecurity Development Lifecycle** (AVCDL primary document)