Training Catalog

# Revision

Version 5

4/22/24 11:51 AM

# SME

Charles Wilson

# Abstract

This document describes the methodology to develop a training catalog needed in the creation of safety-critical, cyber-physical systems.

# Group / Owner

Security / Cybersecurity Instructor

# Motivation

This document is motivated by the need to have formal processes in place for the training of individuals involved in creation of safety-critical, cyber-physical systems for certification of compliance to standards such as **ISO/SAE 21434 (‘434)** and **ISO 26262 (‘262)**.

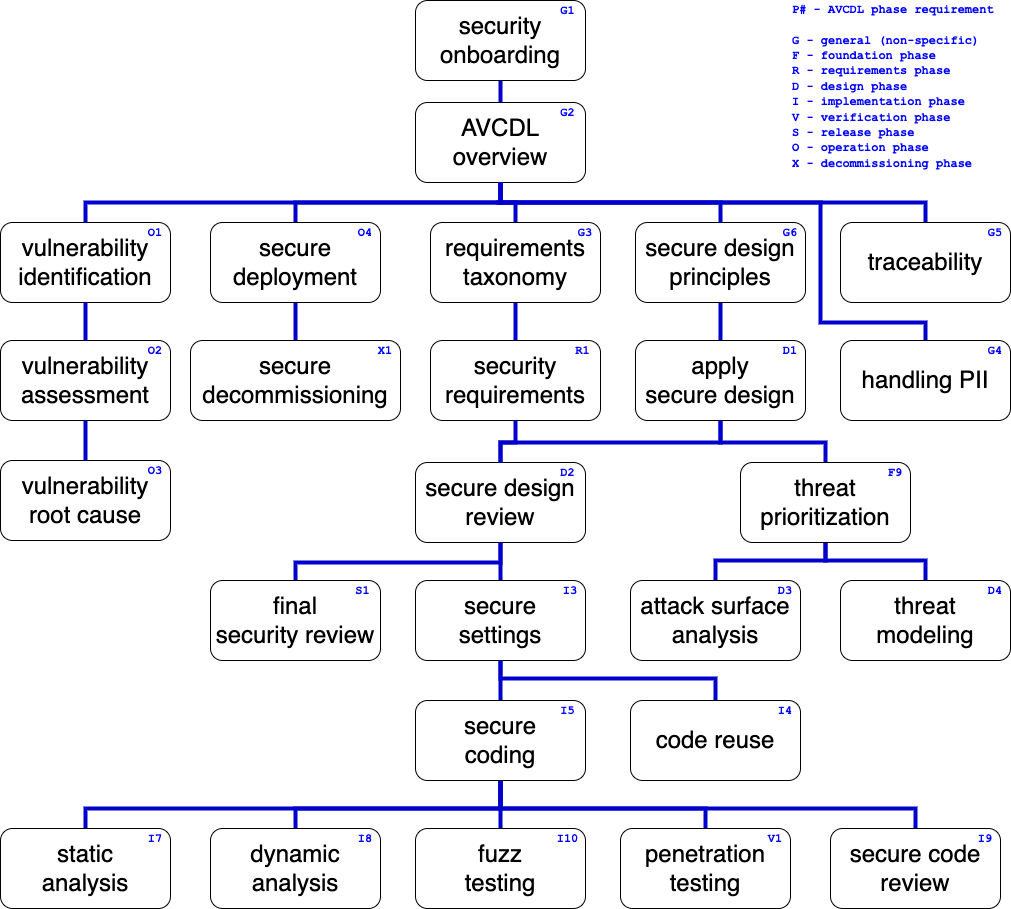
# License

This work was created by **Motional** and is licensed under the **Creative Commons Attribution-Share Alike (CC BY-SA-4.0)** License.

[**https://creativecommons.org/licenses/by/4.0/legalcode**](https://creativecommons.org/licenses/by/4.0/legalcode)

# Overview

The following diagram shows the cybersecurity development training path.



# Target Audience

Each training targets one or more of the following audiences:

* Organization
* Management
* Compliance
* Security
* Development

# Areas of Focus

There should be a general security awareness training covering the motivation for cybersecurity and its relationship to safety.

There are five distinct areas of training specified in **MSSDL** P1 **[1]**:

* Secure design
* Threat modeling
* Secure coding
* Security testing
* Privacy

Two additional areas are considered:

* Compliance
* Other

# Delivery Format

The delivery format for each training is determined by the audience, material and need for interaction. Three formats are currently considered:

* Recorded Video
* Live (in-person / teleconference)
* On-line

# Timeliness

Trainings should be taken in the sequence called out in the training path diagram. Ideally, they should be presented prior to the **AVCDL** phase to which they apply.

# Refresh Frequency

There should be an annual limited-scope refresher for each training based on area of focus.

# Management

Management of the training catalog is done in coordination between cybersecurity and corporate training.

# Tracking

Tracking of courses taken by employees is managed via the corporate training tracking system.

# Content Creation

The individual training course content is created and periodically updated by cybersecurity SMEs.

# References

1. **Essential Software Security Training for the Microsoft SDL**