

There and Back Again

Building a Cybersecurity Development Lifecycle from Scratch to Comply with ISO/SAE 21434 and UN R155

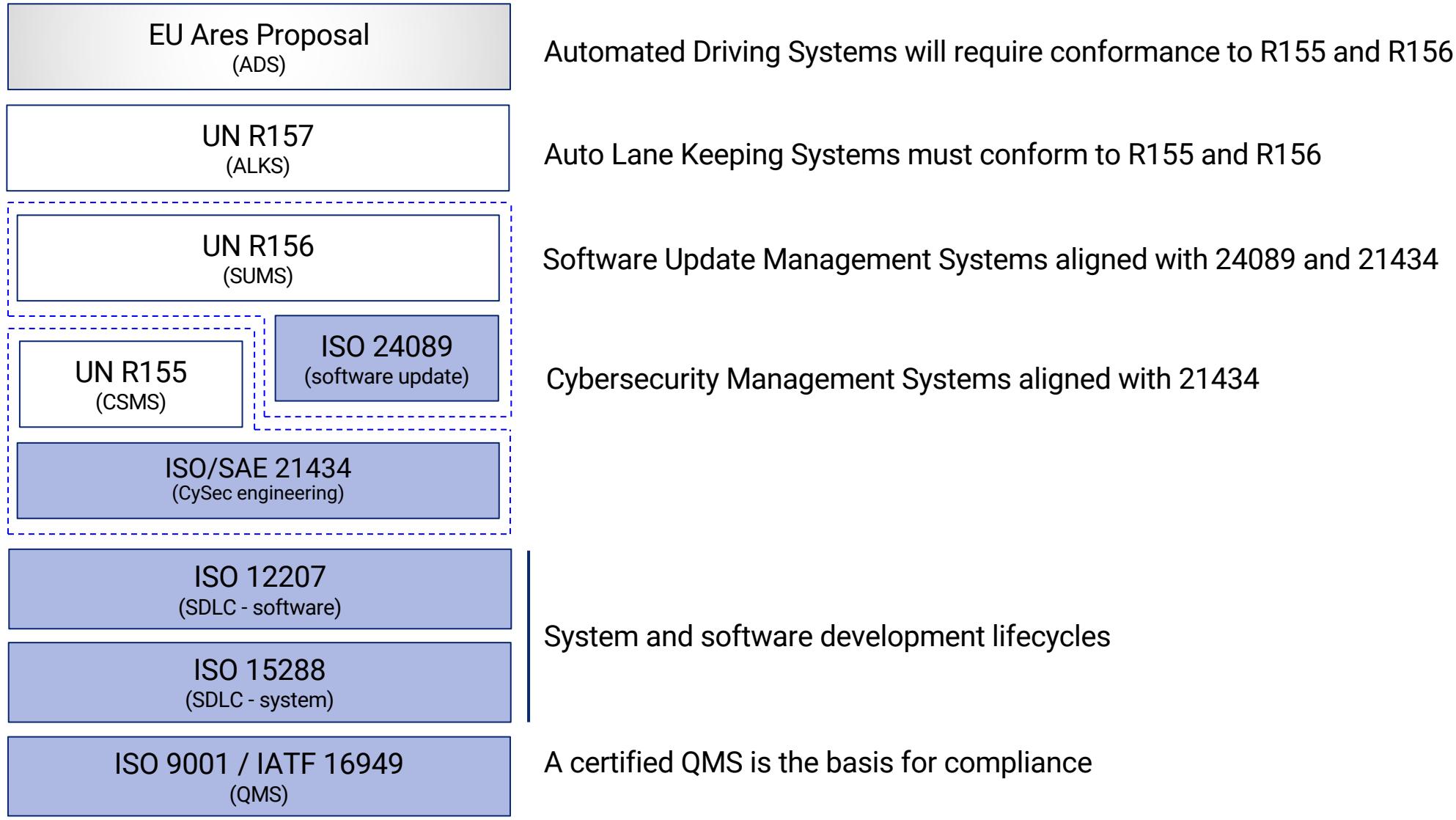
Charles Wilson
Technical Fellow, Cybersecurity Engineering
Motional

version 5
2024-04-01

Introduction

Standards and Regulations

Standards and Regulations Ecosystem

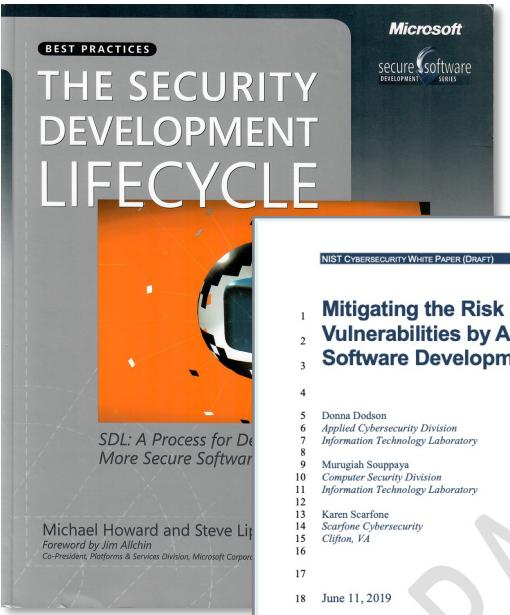


Standard

Regulation

Future

Reference Sources



NIST CYBERSECURITY WHITE PAPER (DRAFT) CSRC.NIST.GOV

Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22

Donna Dodson
Applied Cybersecurity Division
Information Technology Laboratory

Marugiah Souppaya
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

June 11, 2019

NIST Special Publication 800-181

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

William Newhouse
Stephanie Keith
Benjamin Scribner
Greg Witte

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-181>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

ECE/TRANS/505/Rev.3/Add.154

4 March 2021

Agreement

Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations*

(Revision 3, including the amendments which entered into force on 14 September 2017)

Addendum 154 – UN Regulation No. 155

Date of entry into force as an annex to the 1958 Agreement: 22 January 2021

Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/79 (as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97).

UNITED NATIONS

* Former titles of the Agreement:
Agreement concerning the Adoption of Uniform Conditions of Approval and Reciprocal Recognition of Approvals for Motor Vehicles, Equipment and Parts, done at Geneva on 20 March 1953 (original version);
Agreement concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these Prescriptions, done at Geneva on 5 October 1993 (Revision 2).

Downloaded from SAE International by Charles Wilson, Friday, September 17, 2021

SAE INTERNATIONAL

SURFACE VEHICLE STANDARD ISO/SAE 21434

Issued 2021-09

Road Vehicles - Cybersecurity Engineering

Foreword

INTERNATIONAL STANDARD ISO 26262-1

Second edition 2018-12

SAE International is a worldwide federation of national standards organizations of more than 128,000 engineers and related technical experts in the field of preparing International Standards is normally carried out by each member body interested in a subject for which a technical committee is the right to be represented on that committee. International n-governmental, in liaison with ISO, also take part in the work of the International Electrotechnical Commission (IEC) on all matters of standardization.

A document prepared under the direction of ISO/IEC Directives, Part 2 (see www.iso.org/directives) is a document prepared for its further amendment by ISO/IEC Directives, Part 1 and the SAE Technical Standard Board Policy. In particular, the different types of ISO documents should be noted. This is with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

that some of the elements of this document may be the subject of patent rights. The SAE International reserves the right to hold these rights identified during the development of the document will be informed of patent declarations received (see www.iso.org/patents).

printed in the context of its implementation, no part of this publication may be reproduced or utilized mechanically, including photocopying, or posted on the internet or an intranet, without prior written permission from SAE International or the respective address below or ISO's member body in the country of the publication.

Road vehicles — Functional safety —

Part 1: Vocabulary

Véhicules routiers — Sécurité fonctionnelle —

Partie 1: Vocabulaire

SAE International
Tel: +1 724-776-4970 (outside USA)
Fax: +1 724-776-0704
Email: CustomerService@sae.org
SAE WEB ADDRESS: <http://www.sae.org>

Reference number
ISO 26262-1:2018(E)

© ISO 2018

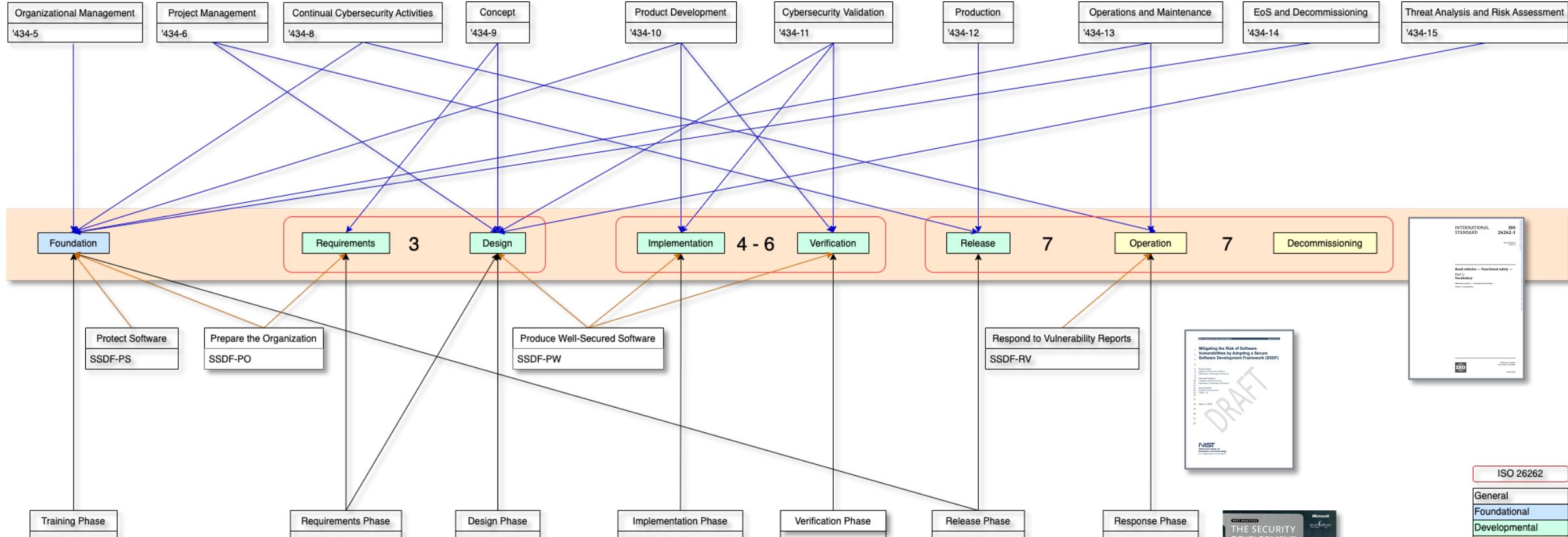
How the Standards Line Up

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

Lifecycle Phase Harmonization

AVPDL	15288 (SDLC system)	12207 (SDLC software)	26262 (safety)	21434 (cybersecurity)
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
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		
verification phase	verification	system qualification testing	integration and verification	integration and verification
	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

How Sources Inform the AVCDL

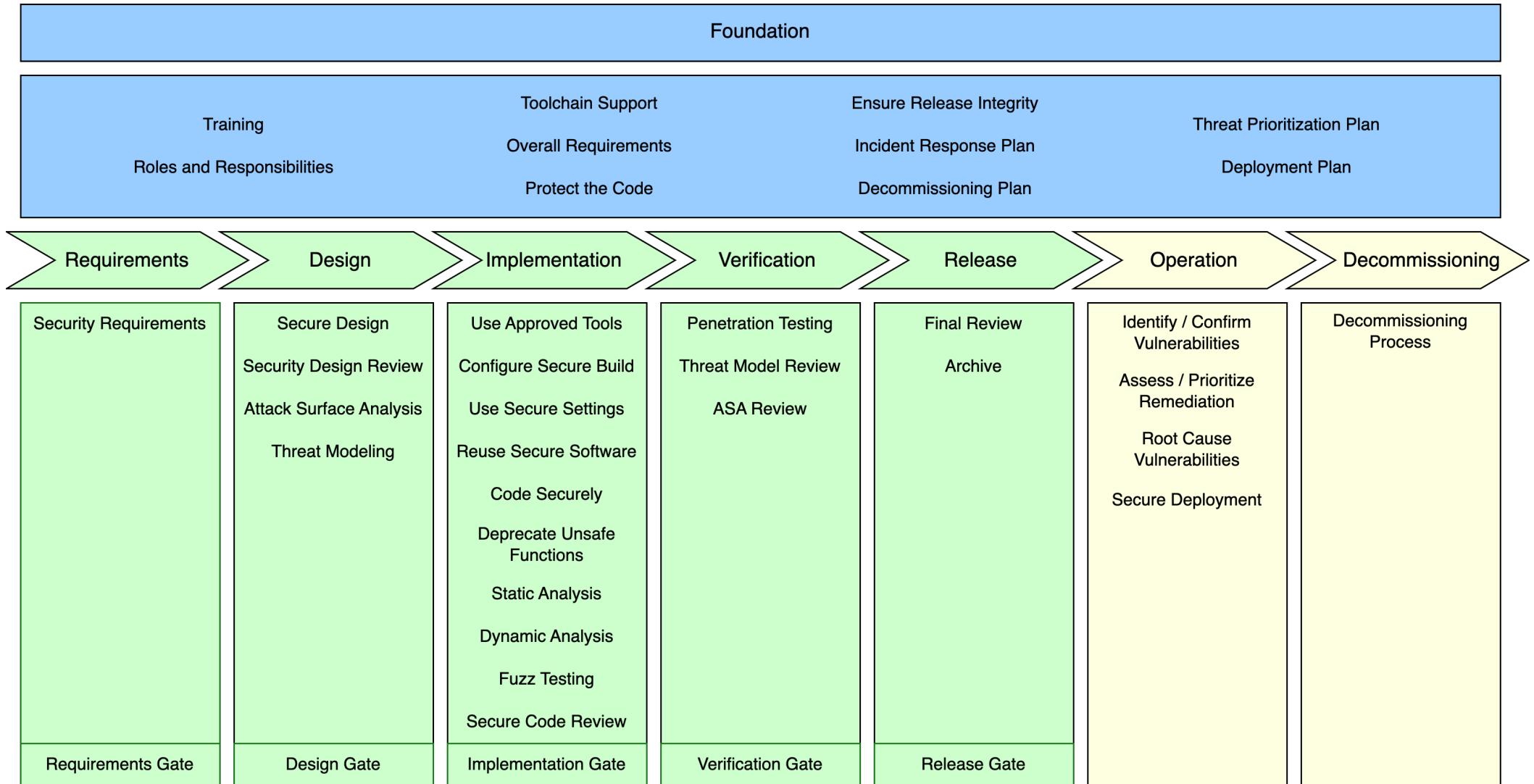


ISO/SAE 21434 – AVCDL Mapping

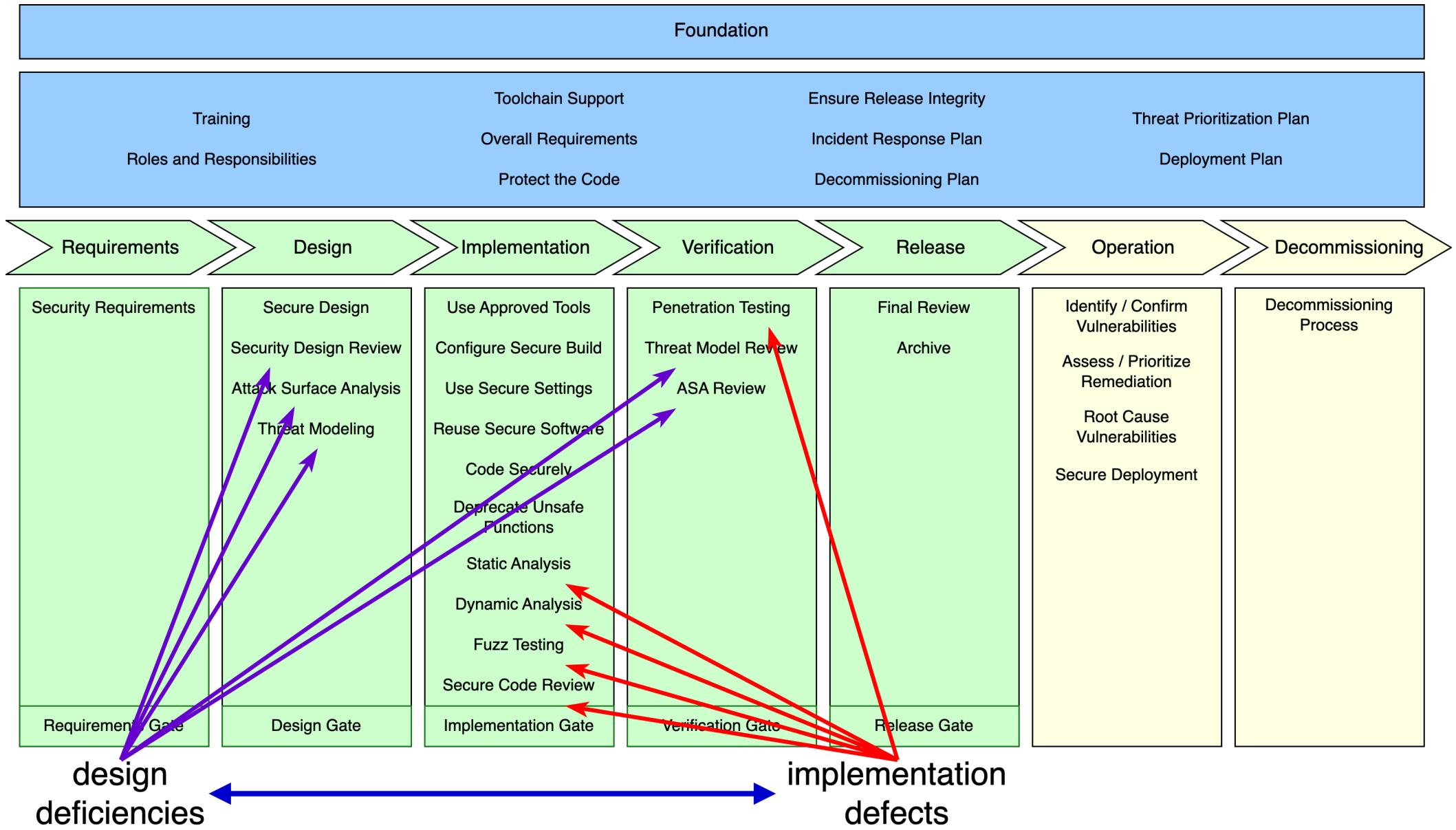
		Foundation																Requirement			Design			Implementation							Verification		Release		Operation			Dec.	Supplier
		1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	1	2	3	4				
Distributed Cybersecurity Activities	WP-07-X1	RQ-07-01	evaluate supplier cybersecurity capability																																				
	WP-07-X2	RQ-07-03	supplier cybersecurity quote																																				
		RQ-07-04	supplier cybersecurity interface agreement																																				
	WP-07-01	RQ-07-06	supplier vulnerability activities																																				
		RQ-07-07	extra-security CIA conflict																																				
Continual Cybersecurity Activities	WP-08-01	RQ-08-01	cybersecurity monitoring sources									X																											
	WP-08-02	RQ-08-02	cybersecurity triage triggers					X																															
	WP-08-03	RQ-08-03	cybersecurity event triage						X																														
	WP-08-04	RQ-08-04	cybersecurity event assessment						X																														
	WP-08-05	RQ-08-05	identified weakness analysis						X																														
		RQ-08-06	weakness rejection rationale						X																														
	WP-08-06	RQ-08-07	vulnerability management						X	X									X																				
	WP-08-X1	RQ-08-08	apply incident response protocols						X																														
Concept	WP-09-01	RQ-09-01	item definition										X	X																									
		RQ-09-02	item operational information										X	X																									
	WP-09-02	RQ-09-03	item analysis												X																								
		RQ-09-04	risk treatment													X	X																						
	WP-09-03	RQ-09-05	risk treatment to cybersecurity goal mapping														X																						
	WP-09-04	RQ-09-06	cybersecurity claims															X																					
	WP-09-05	RQ-09-07	goals / claims verification report															X																					

AV/CMDs X Supplier Self-reported Maturity X
Cybersecurity Interface Agreement

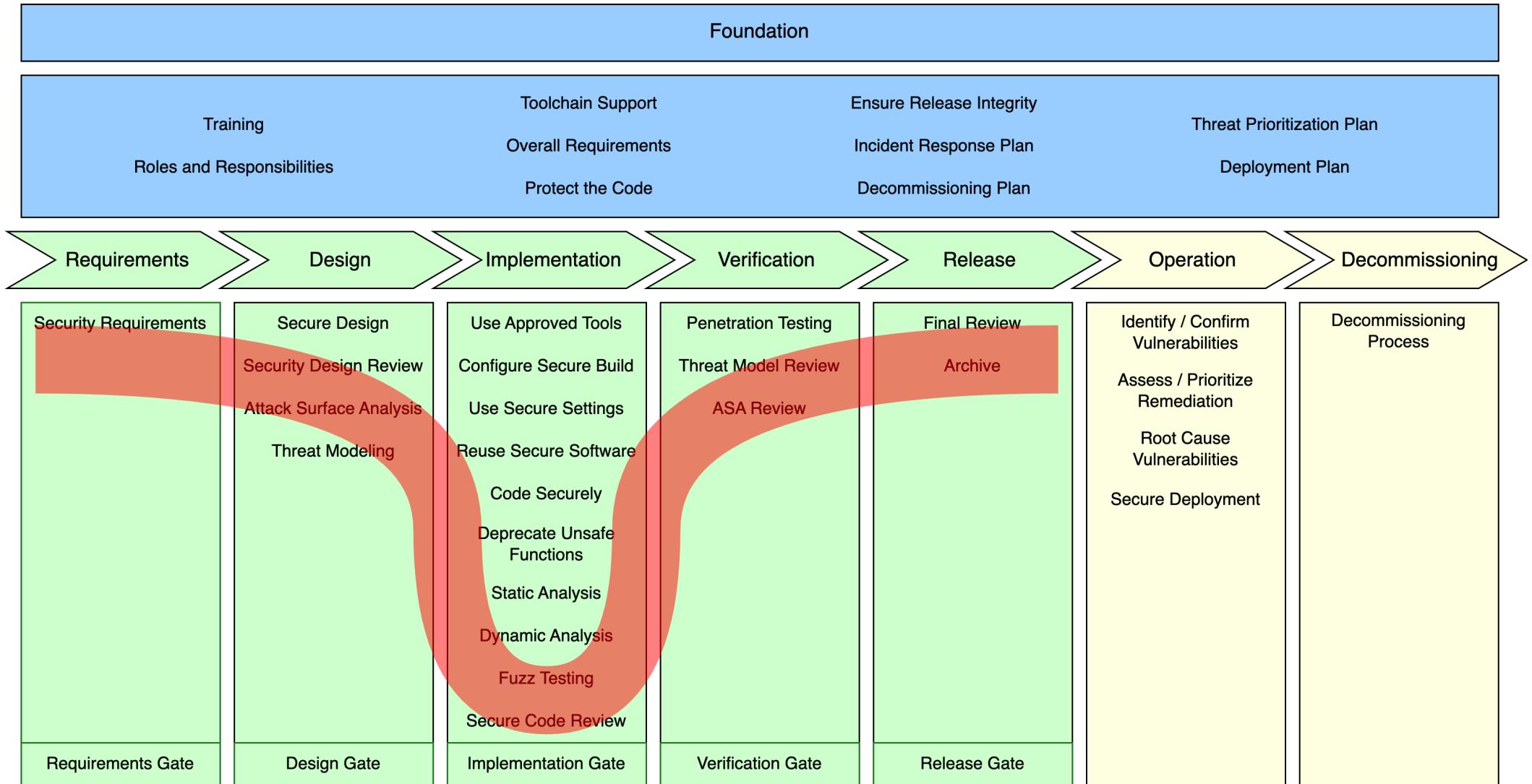
AVCDL Framework



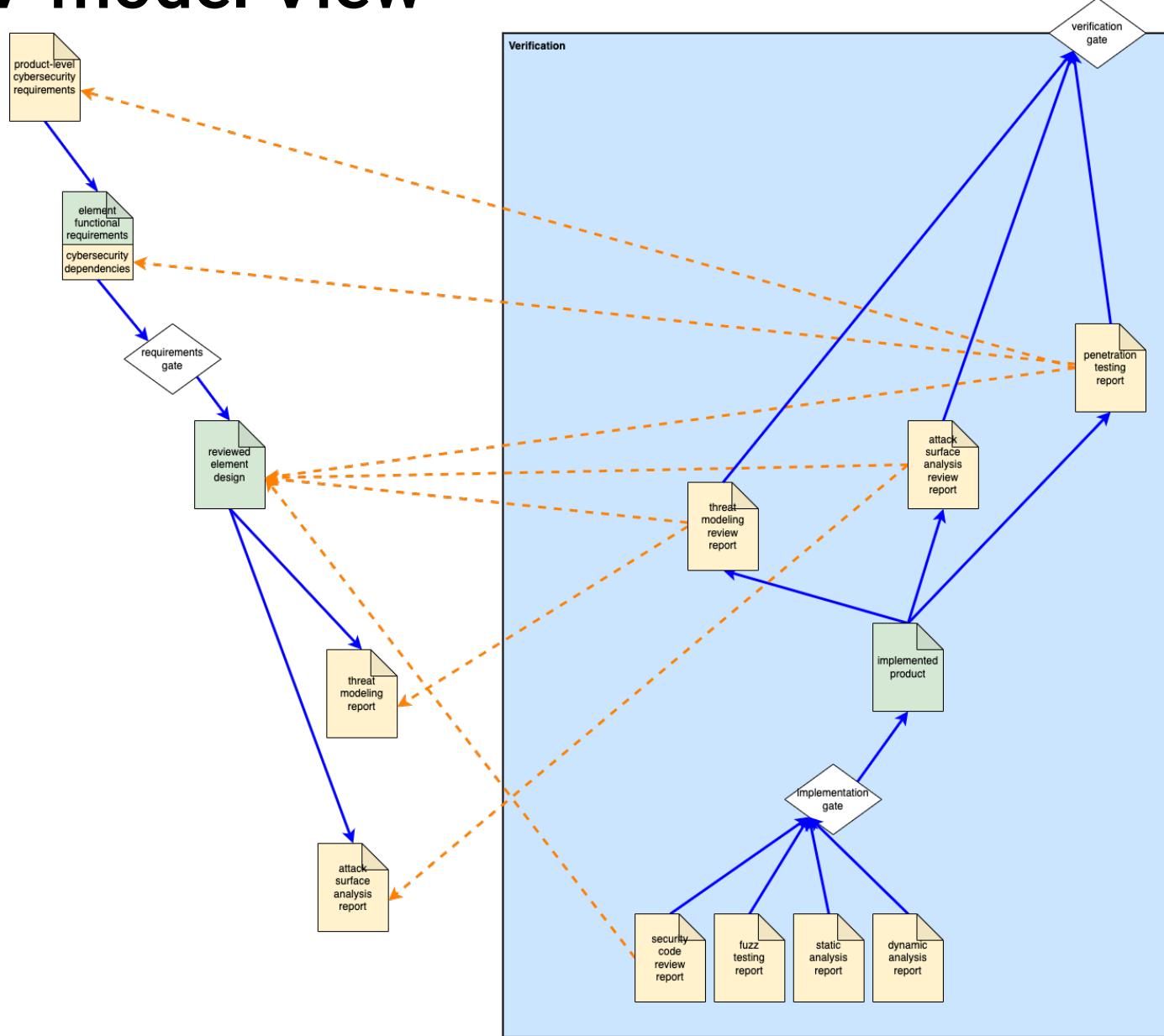
Design Deficiencies vs Implementation Defects



Distribution of Cybersecurity Activities



V-model View



Understanding Verification and Validation in an AVCDL Context

Revision

Version 3
4/25/23 4:47 PM

Author

Charles Wilson

Abstract

This document describes how verification and validation as defined in ISO 9000 relate to the structure of the AVCDL.

Audience

The audience of this document are the cybersecurity development lifecycle practice leads who will be guiding AVCDL adoption within their organization.

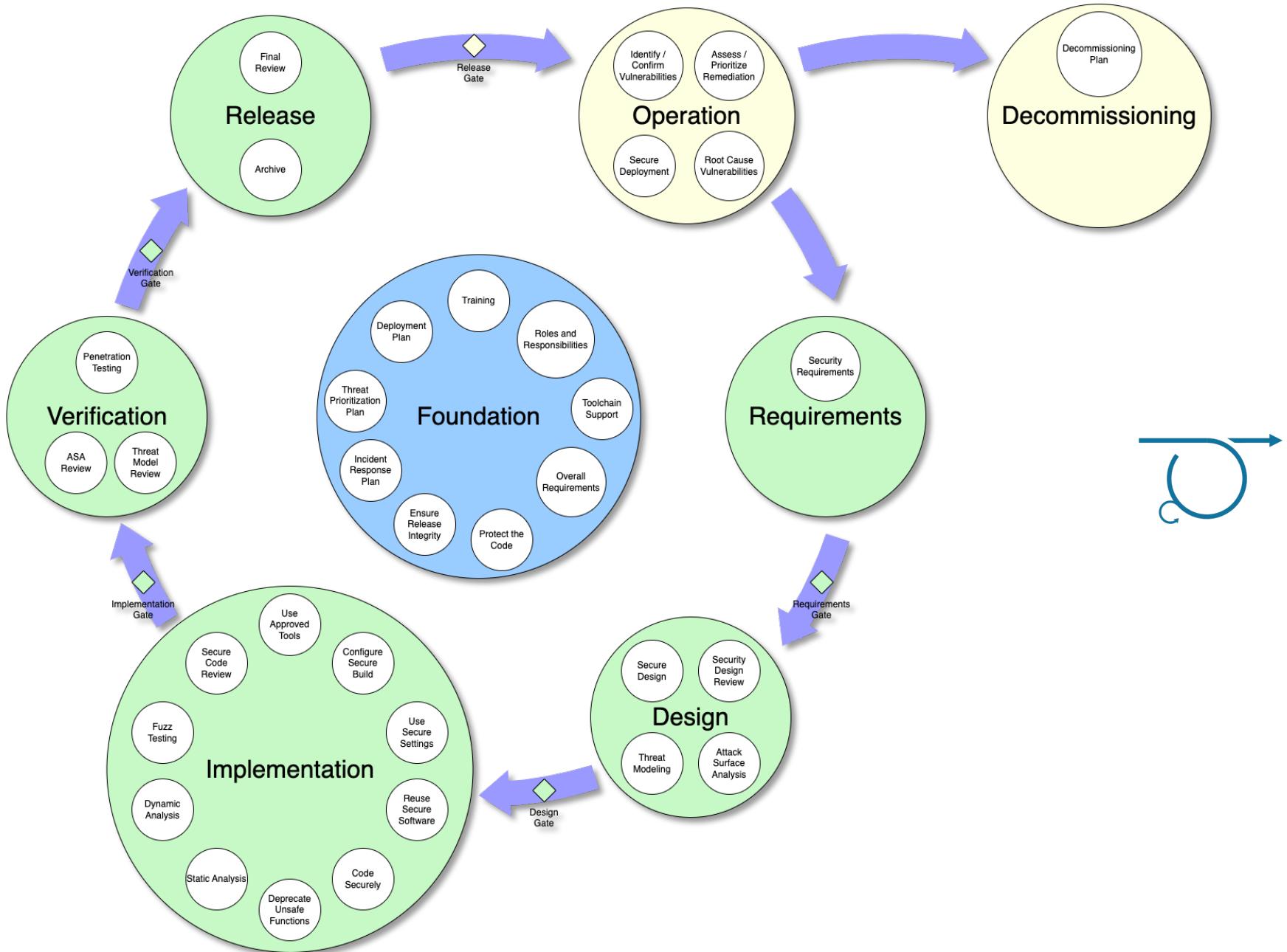
Note: This document is not subject to certification body review.

License

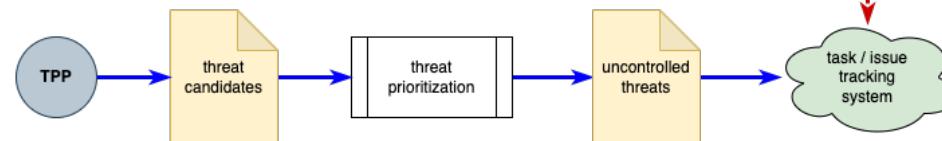
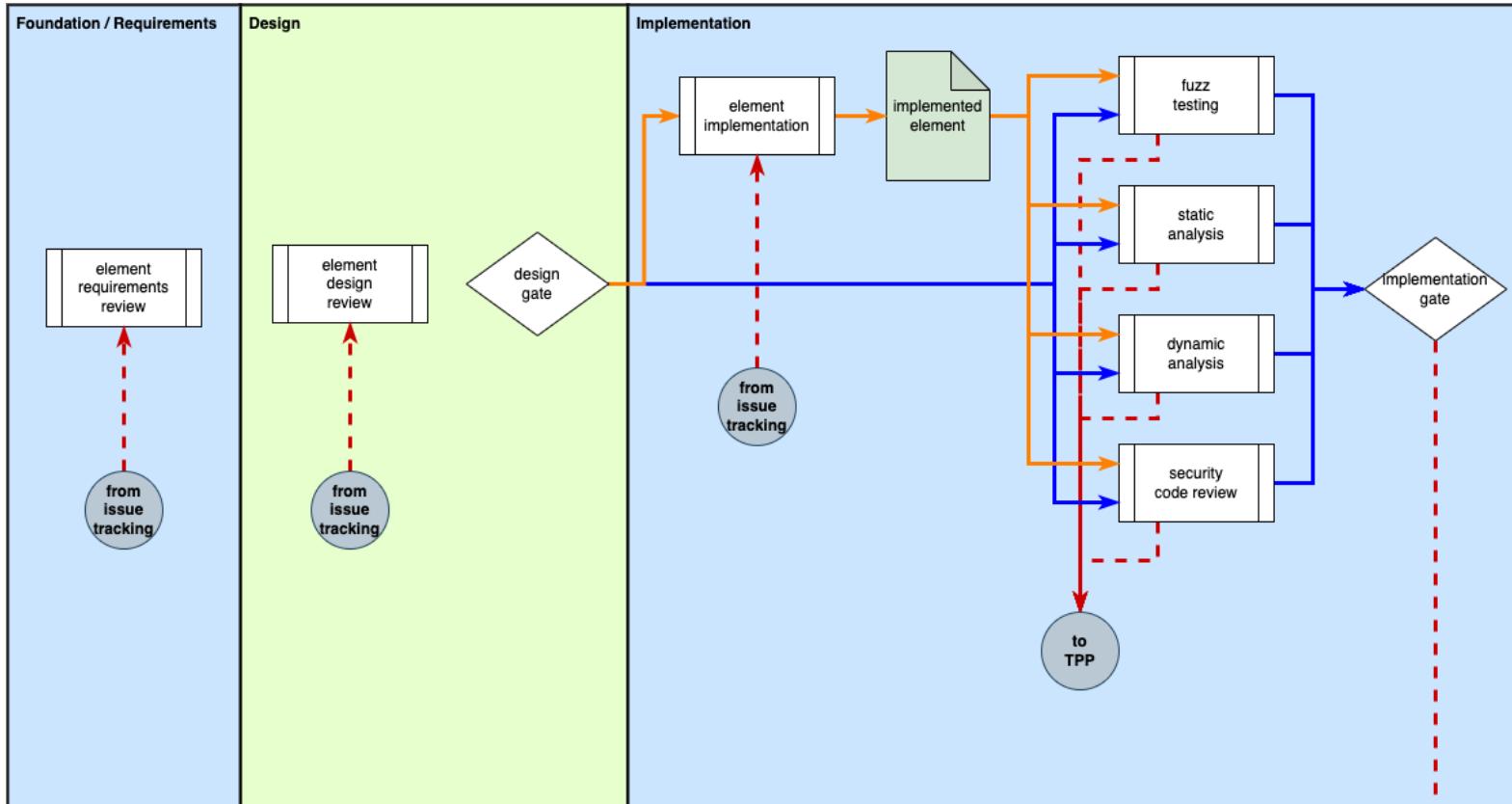
This work was created by Motional and is licensed under the Creative Commons Attribution-Share Alike (CC BY-SA-4.0) License.

<https://creativecommons.org/licenses/by/4.0/legalcode>

Cyclic View



Cyclic Feedback



Understanding Cybersecurity Risk Freshness in an AVCDL Context

Revision
Version 4
3/7/24 7:19 PM

Author
Charles Wilson

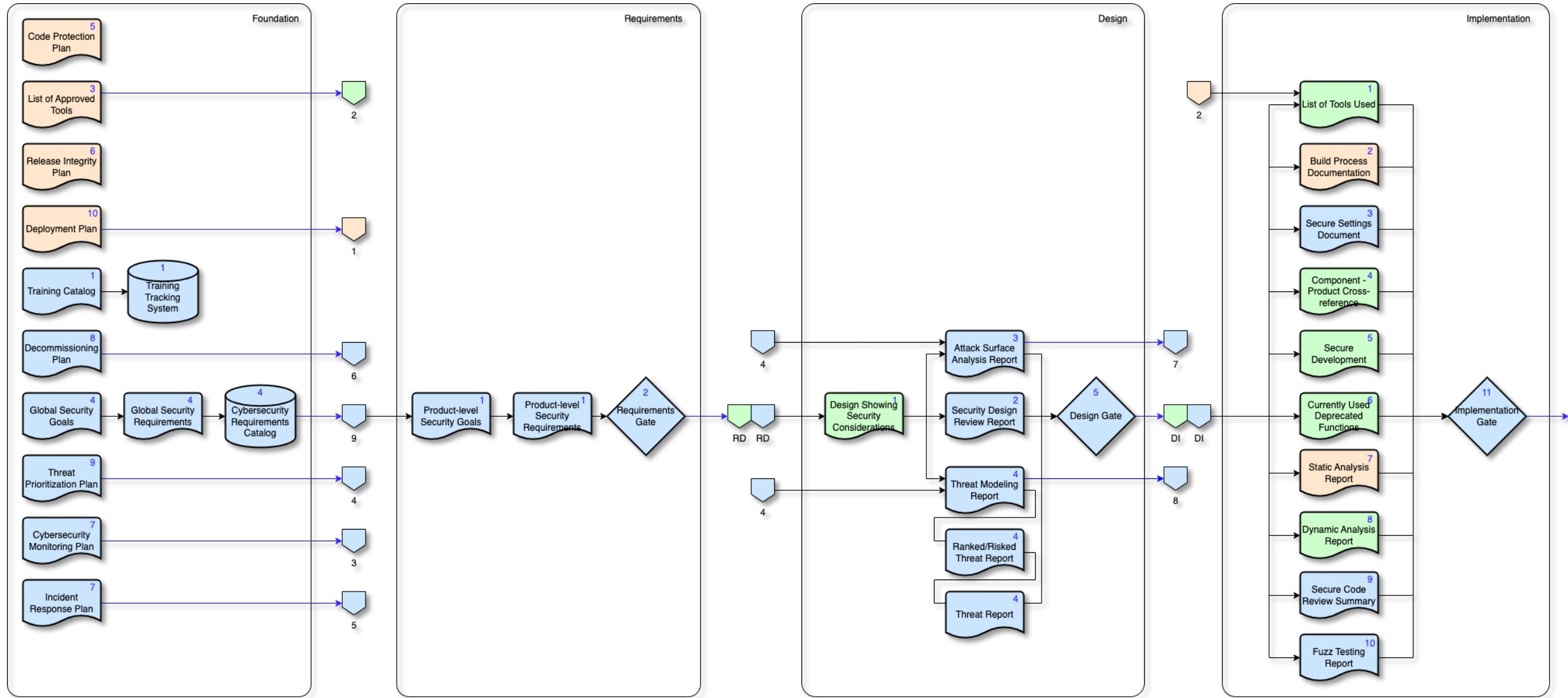
Abstract
This document describes how the freshness of cybersecurity risks is achieved within the AVCDL.

Audience
The audience of this document are the cybersecurity development lifecycle practice leads who will be guiding AVCDL adoption within their organization.

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

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>

Traceability



devops development security

phase requirement #

Details

Typical Phase Requirement

Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL)

9.3.4 Threat Modeling [AVCDL-Design-4]

Owner

Group: Security

NCWF Role: Security Architect

Administration

security	devops	development	risk
R	-	R	R

Threat modeling is an exercise which may be done at any stage of development. It realizes an abstraction of the system as a set of interacting processes managing resources passing data between them. It is on these data flows that automated threat modeling tools reason.

In that same way that security requirements should be considered at multiple levels in order to provide a complete landscape, so do threat models.

Note: Threat modeling is a team exercise, encompassing program/project managers, developers, and testers, and represents the primary security analysis task performed during the software design stage.

Note: The threat modeling AVCDL work products are generated through application of the threat prioritization plan set out in [\[AVCDL-Foundation-9\] Threat Prioritization Plan](#).

Training Provided

yes

Phase Requirement Dependencies

[AVCDL-Foundation-9] Threat Prioritization Plan

[AVCDL-Design-1] Apply Security Requirements and Risk Information to Design

External Group Product Dependencies

Group	Inputs
Devops	none
Development	Element detailed design
Risk	none

Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL)

AVCDL Products

[AVCDL-Design-4.1] Threat Modeling Report

[AVCDL-Design-4.2] Ranked / Risked Threat Report

[AVCDL-Design-4.3] Threat Report

ISO 21434 Required Work Products

[WP-09-02] Threat analysis and risk assessment

[WP-09-03] Cybersecurity goals

[WP-09-04] Cybersecurity claims

[WP-09-05] Verification report

[WP-15-01] Damage scenarios

[WP-15-03] Threat scenarios

[WP-15-04] Impact rating

[WP-15-05] Attack paths

[WP-15-06] Attack feasibility rating

[WP-15-07] Risk values

[WP-15-08] Risk treatment decision per threat scenario

WP.29 CSMS Requirements

[7.2.2.1(a)] development phase CSMS

[7.2.2.1(c)] post-production phase CSMS

[7.2.2.2(b)] risk identification

[7.2.2.2(c)] risk treatment

[7.2.2.2(d)] verification of risk management

[7.2.2.2(f)] risk assessment kept current

[7.2.2.2(g)] adaptable monitoring / response

[7.2.2.3] timely risk management

[7.3.3] critical element risk assessment

[7.3.4] type risk protection

[7.3.5] type risk countermeasures

[7.4.1] periodic monitoring report

WP.29 CSMS Supplemental

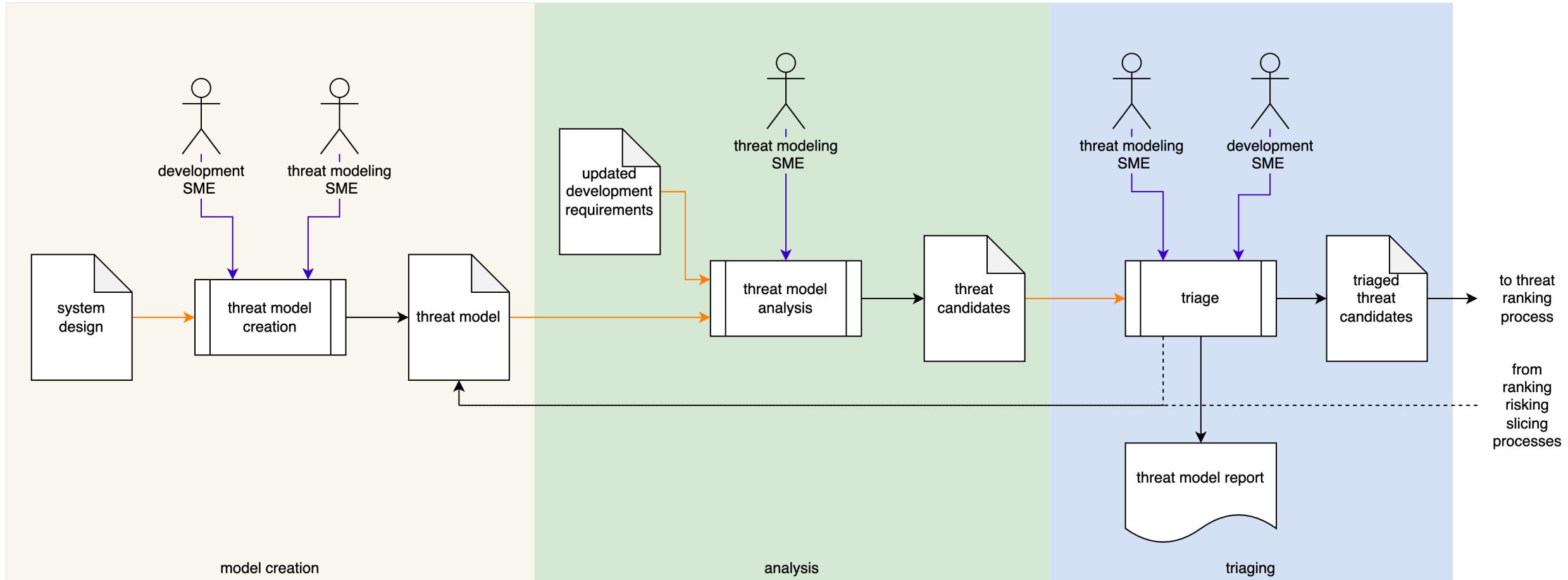
[7.2.2.1(b)] production phase CSMS

[7.3.2] management of type

CMMC Applicable Practices

Level	Practice
1	none
2	RM.2.143
3	AU.3.049, AU.3.052, RM.3.144
4	none
5	AU.5.055

Process Workflows



Document References

Manifest Generation

Revision

Version 3
3/13/24 2:14 PM

Author

Charles Wilson

Abstract

This document describes the process used to generate the vehicle manifest.

Group / Owner

DevOps / Information Systems Security Developer

Motivation

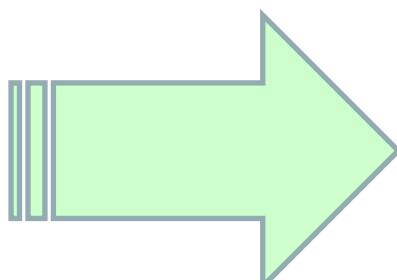
This document is motivated by the need to adopt best practices regarding creation of vehicle manifests, to allow for certification of compliance to standards such as ISO/SAE 21434 and ISO 26262.

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

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>



References

1. Software Bill of Materials (AVCDL elaboration document)
2. Component / Version – Product / Version Cross-reference Document (AVCDL secondary document)
3. Code Protection Plan (AVCDL secondary document)
4. SOFTWARE BILL OF MATERIALS
<https://www.ntia.gov/SBOM>
5. Tooling Ecosystem working with SPDX
https://docs.google.com/document/d/1A1jF1YihB-IyTQgv7E_KoSjlbwNGmu_wOXBs6siemXA/edit
6. Tooling Ecosystem working with SWID
https://docs.google.com/document/d/1oebYvHcOhtMG8Uhnd5he01_vhty7MsTj_p6fYC0wUmwM/edit
7. Software Package Data Exchange® (SPDX®)
<https://spdx.dev/wp-content/uploads/sites/41/2017/12/spdxversion2.1.pdf>
8. ISO 19770-2:2015 Information technology - IT asset management - Part 2: Software identification tag
<https://www.iso.org/standard/65666.html>
9. NIST IR 8060 Guidelines for the Creation of Interoperable Software Identification (SWID) Tags
https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST_IR_8060.pdf

AVCDL Materials

Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL)

Charles Wilson
Technical Fellow, Cybersecurity Engineering
Version 56
10/30/2023 5:34:00 PM

Global Security Goals

Revision: Version 2 5/26/21 4:3

SME: Charles Wilson

Abstract: This document is as applied.

Group / security / System

Motivation: When dealing with cybersecurity, justify these goals to be informed.

Document / Model: The AVCDL traceability reverse dependency graph. It also contains a visual representation of the dependencies.

License: This work is licensed under a Share Alike (CC-BY) license.
<https://creativecommons.org/licenses/by/4.0/legalcode>

Understanding the Phase Product Dependencies Graph

Revision: Version 3 7/15/21 1:2

Author: Charles Wilson

Abstract: This document is dependent on the Global Security Goals.

Group / security / System

Motivation: This document provides dependencies between phases.

Document / Model: The AVCDL traceability reverse dependency graph. It also contains a visual representation of the dependencies.

License: This work is licensed under a Share Alike (CC-BY) license.
<https://creativecommons.org/licenses/by/4.0/legalcode>

Security Requirements Taxonomy

Revision: Version 3 7/15/21 4:16 PM

Author: Charles Wilson

Abstract: This document defines the taxonomy of security requirements.

Group / security / System

Motivation: The AVCDL traceability reverse dependency graph. It also contains a visual representation of the dependencies.

Document / Model: The AVCDL traceability reverse dependency graph. It also contains a visual representation of the dependencies.

License: This work is licensed under a Share Alike (CC-BY) license.
<https://creativecommons.org/licenses/by/4.0/legalcode>

Global Security Requirements

Revision: Version 2 5/26/21 4:33 PM

SME: Charles Wilson

Abstract: This document describes the symbology and intent behind the AVCDL secondary document workflow graphs.

Group / security / System

Motivation: This document describes the symbology and intent behind the AVCDL secondary document workflow graphs.

Document / Model: The AVCDL traceability reverse dependency graph. It also contains a visual representation of the dependencies.

License: This work is licensed under a Share Alike (CC-BY) license.
<https://creativecommons.org/licenses/by/4.0/legalcode>

Understanding Workflow Graphs

Revision: Version 4 3/12/24 5:44 AM

Author: Charles Wilson

Abstract: This document describes the symbology and intent behind the AVCDL secondary document workflow graphs.

Group / security / System

Motivation: This document describes the symbology and intent behind the AVCDL secondary document workflow graphs.

Document / Model: The AVCDL traceability reverse dependency graph. It also contains a visual representation of the dependencies.

License: This work was created by Motional and is licensed under the Creative Commons Attribution-Share Alike (CC BY-4.0) License.
<https://creativecommons.org/licenses/by/4.0/legalcode>

Purpose-driven Security

By Charles Wilson
11/3/20 9:06

Category: security

Tags: security

A Bad Example: In 2014, Stuxnet people to take security sure, but this cheese sale.

In the security grade security been around take security. And it's a tools and a reach for the that it's deal. There's a price we apply will it takes time the message far greater cost for a level of diminishing returns.

As someone familiar with Even without any problems give these certificates. Here's the question professional. And what does it is a result, you addition to paint has yet has ever been able to make this job.

In my post, I addition to paint has yet has ever been able to make this job.

As can be seen let's flesh out

Certifiably Secure: Does it Matter?

Charles Wilson
11/3/20 10:4

Category: security

Tags: security

When I turn in my model: This device controls the CAN bus. CAN BUS (BUN).

As someone familiar with Even without any problems give these certificates. To get the message interplay is clear. Note: Links Paint Me a We can visualize

Policy – Process – Procedure: What's in a Name?

Charles Wilson
11/3/20 10:4

Category: security

Tags: security, process

In upcoming you aren't similar. To get the message interplay is clear.

Aligning the Organization with the AVPDL

Charles Wilson
11/3/20 10:4

Category: security

Tags: security

What's Standard common industry Over time standard different from the group. This type of electrical T. (Electrical) There are disparate Lifecycle development in the development Traceability linked back to the system. This may be to the right decisions according to How Do We Manage Traceability management

Traceability: Making the Case for Certification

Charles Wilson
11/3/20 10:4

Category: security

Tags: security

What is The case for certification? I was going to the end of the case for certification.

AVCDL: The Autonomous Vehicle Cybersecurity Development Lifecycle

Charles Wilson, Principal Engineer, Cybersecurity Development Lifecycle Practice
11/2/20 10:47:00 AM

Category: security-governance

Tags: security, cybersecurity, autonomous vehicles, certification, ISO 21434, ISO 15288, ISO 26262, ISO 12207, AVPDL, AVCDL, NCWF, MSSD

In my post, Purpose-driven Security [\[link\]](#), an approach for the application of security controls was given. In Aligning the Organization with the AVPDL, the motivation for having an overarching framework where various development lifecycles coexist was presented.

In Certifiably Secure Does it Matter [\[link\]](#), the case for obtaining certification was laid out. In Traceability: Making the Case for Cybersecurity [\[link\]](#), I showed why we should attain certification. In Policy – Process – Procedure: What's in a Name? [\[link\]](#), the relationships between the major structural components needed to define lifecycle were explored.

In this post all those elements will be brought together in the introduction of a formal autonomous vehicle cybersecurity development lifecycle (AVCDL).

Let's Review

In this post, the AVCDL (Autonomous Vehicle Product Development Lifecycle), the four primary autonomous vehicle standards governing the product development lifecycle were introduced. Once again, they are:

Standard	Description
ISO 15288	Systems Development Lifecycle
ISO 12207	Software Development Life Cycle (SDLC)
ISO 26262	Road Vehicles – Functional Safety
ISO 21434	Road Vehicles – Cybersecurity Engineering

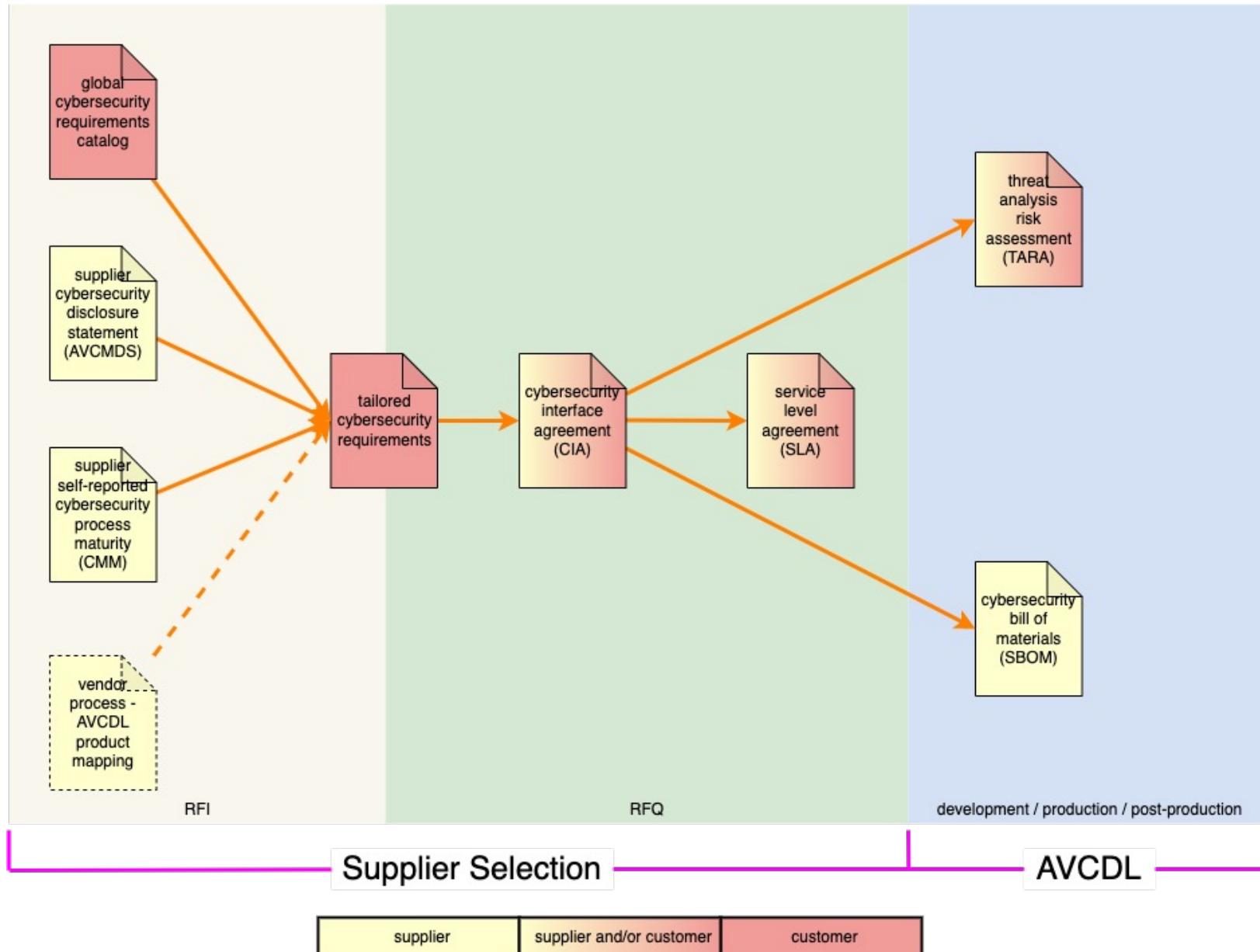
Vehicle Cybersecurity (AVCMDS) Rev 3

Document ID	Model	Description
SVS-004	SVS-004	Super Vehicle Sensor

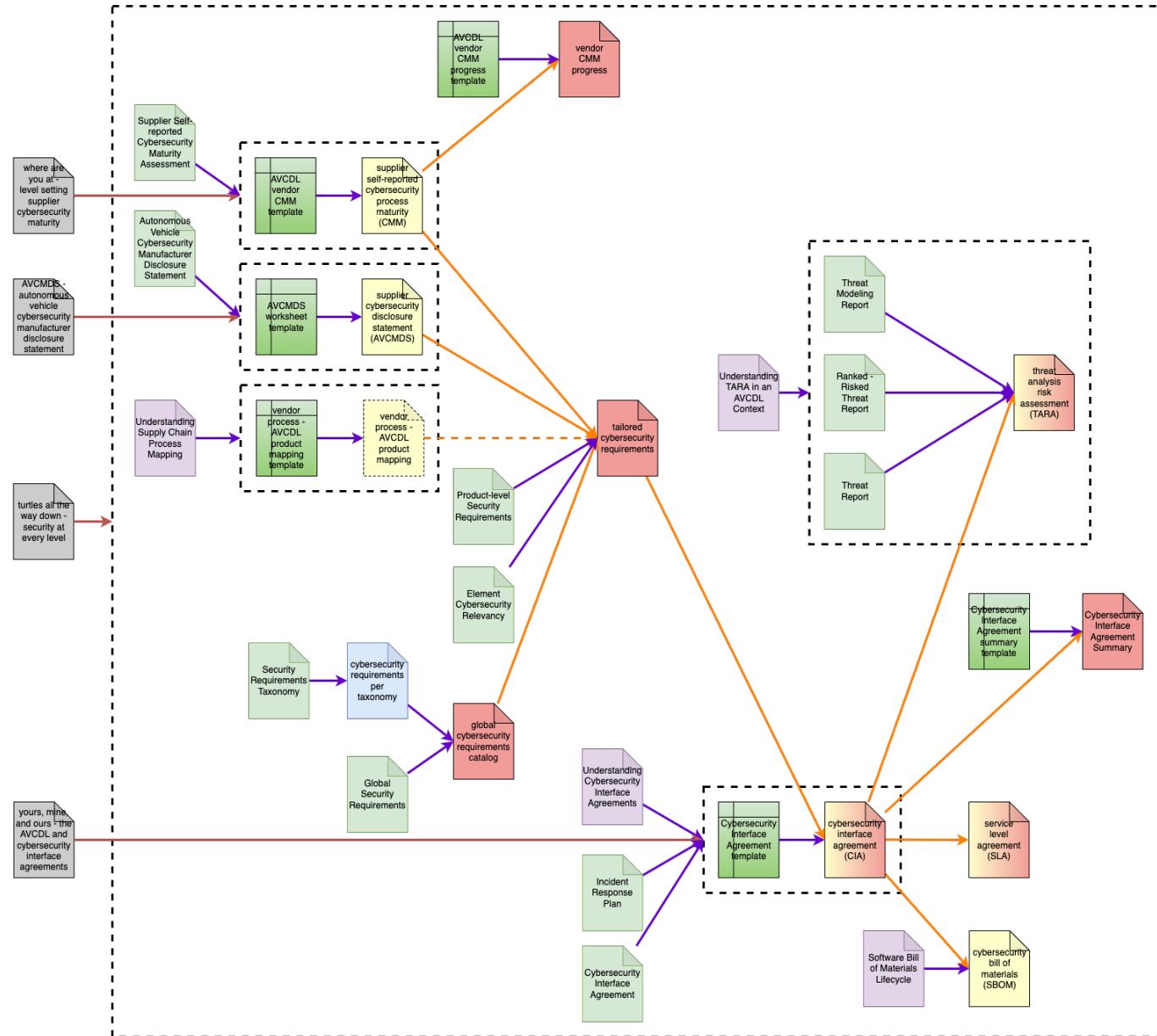
Answer	Note	Explanation
DOC-1		
DOC-2		
DOC-3	Cosmic Components	
DOC-4	Device Model	
DOC-5	SVS-004	
DOC-6	Document ID	
DOC-7	SVS-004 manual	
DOC-8	Device Description	
DOC-9	SVS-004	
DOC-10	SVS-004	
DOC-11	SVS-004	
DOC-11.1	SVS-004	
DOC-11.2	SVS-004	
DOC-11.3	SVS-004	
DOC-11.4	SVS-004	

Supply Chain

Supplier Selection

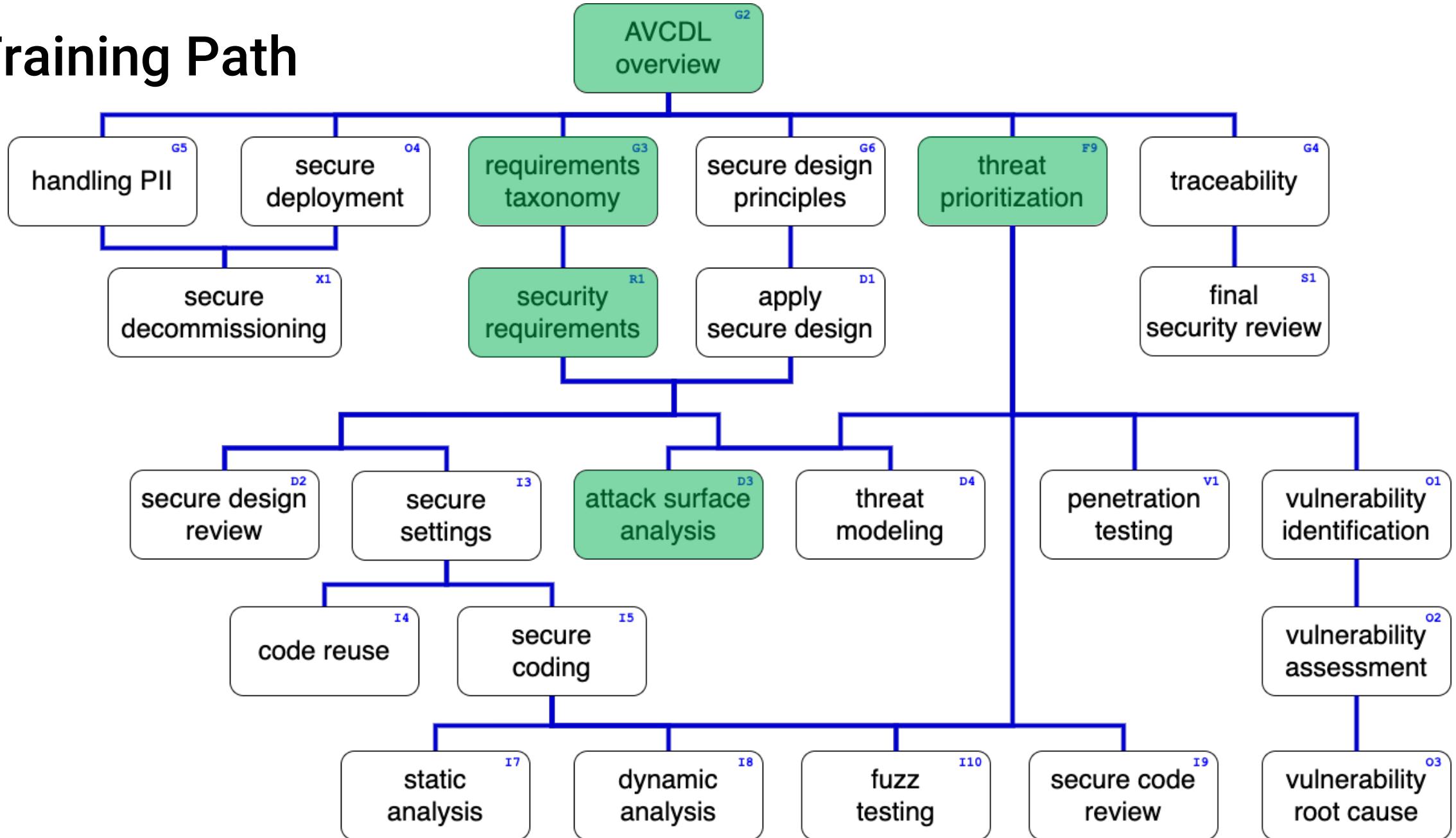


Supply Chain Guidance Documents

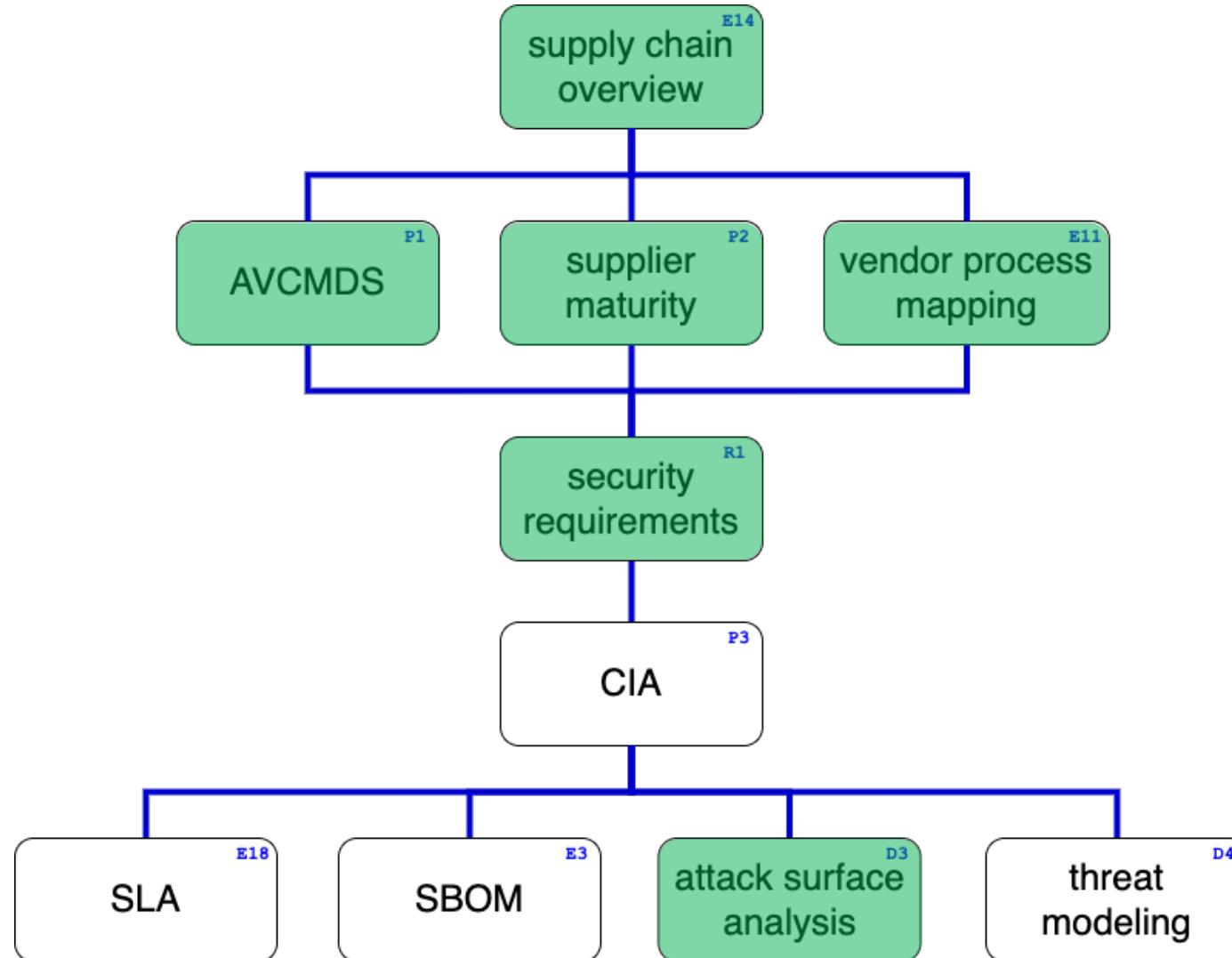


Training

Training Path



Supply Chain Training Path

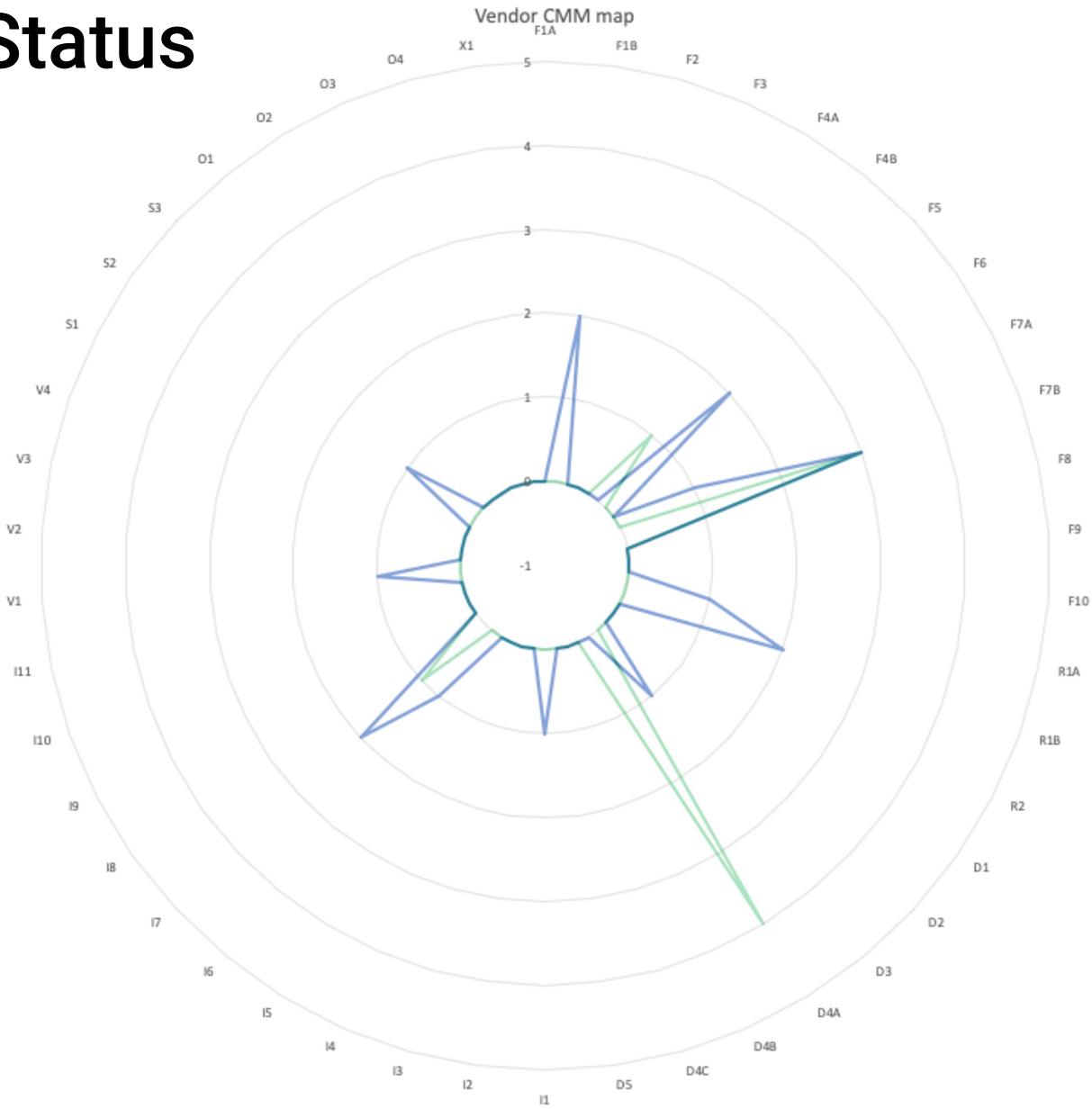


Assessment

Evaluating Your Status

Phase	Phase Requirement	Description	AVCDL Product	CMM Level	Notes
Foundation	Foundation-1	Training	training catalog	0 - none	
	Foundation-2	Roles and Responsibilities	system to track training participation	0 - none	
	Foundation-3	Toolchain Support	roles and responsibilities document	0 - none	
	Foundation-4	Definition of Security Requirements	list of approved tools and components	0 - none	
	Foundation-5	Protect the Code	global security goals	0 - none	
	Foundation-6	Ensure Release Integrity	global security requirements	0 - none	
	Foundation-7	Incident Response Plan	code protection plan	0 - none	
	Foundation-8	Decommissioning Plan	release integrity plan	0 - none	
	Foundation-9	Threat Prioritization Plan	incident response plan	0 - none	
	Foundation-10	Deployment Plan	continuous monitoring plan	0 - none	
Requirement	Requirements-1	Definition of Security Requirements	decommissioning plan	0 - none	
	Requirements-2	Requirements Gate	threat prioritization plan	0 - none	
Design	Design-1	Take Security Requirements and Risk Information into Account During Software Design	deployment plan	0 - none	
	Design-2	Review the Software Design to Verify Compliance with Security Requirements and Risk Information	product-level security goals	0 - none	
	Design-3	Attack Surface Reduction	product-level security requirements	0 - none	
	Design-4	Threat Modeling	formal gate signoff	0 - none	
	Design-5	Design Gate	design showing security considerations	0 - none	
Implementation	Implementation-1	Use Approved Tools	security design review report	0 - none	
	Implementation-2	Configure the Compilation and Build Process to Improve Executable Security	attack surface analysis report	0 - none	
	Implementation-3	Configure the Software to Have Secure Settings by Default	threat modeling report	0 - none	
	Implementation-4	Reuse Existing, Well-Secured Software When Feasible Instead of Duplicating Functionality	ranked/risked threat report	0 - none	
	Implementation-5	Create Source Code Adhering to Secure Coding Practice	threat report	0 - none	
	Implementation-6	Deprecate Unsafe Functions	formal gate signoff	0 - none	
	Implementation-7	Static Analysis	list of tools and components used	0 - none	
	Implementation-8	Dynamic Program Analysis	build process documentation	0 - none	
	Implementation-9	Security Code Review	secure setting document	0 - none	
	Implementation-10	Fuzz Testing	component/version - product/version cross-reference document	0 - none	
	Implementation-11	Implementation Gate	secure development	0 - none	
Verification	Verification-1	Penetration Testing	currently used deprecated functions document	0 - none	
	Verification-2	Threat Model Review	static analysis report	0 - none	
	Verification-3	Attack Surface Analysis Review	dynamic analysis report	0 - none	
	Verification-4	Verification Gate	secure code review summary	0 - none	
Release	Release-1	Final Security Review	fuzz testing report	0 - none	
	Release-2	Archive	formal gate signoff	0 - none	
	Release-3	Release Gate	final security review report	0 - none	
Operation	Operation-1	Identify and Confirm Vulnerabilities on an Ongoing Basis	archive manifest	0 - none	
	Operation-2	Assess and Prioritize the Remediation of all Vulnerabilities	formal gate signoff	0 - none	
	Operation-3	Analyze Vulnerabilities to Identify Their Root Causes	cybersecurity incident report	0 - none	
	Operation-4	Secure Deployment	software deployment report	0 - none	
De	Decommissioning-1	Apply Decommissioning Protocol	decommissioning report	0 - none	

Mapping Your Status



Assessing for Compliance

Motional AD Inc. (f/k/a nuTonomy Inc.)
100 Northern Ave, Suite 200
Boston, MA 02210, USA

Cybersecurity Assessment Summary – Motional AVCDL

File name: TUVSUD_CybersecurityAssessmentSummary_Motional_AVCDL_v.2.12.docx Revision: Rev 2.12 Date: June 27, 2022 Page: 1 of 5

To whom it may concern:

TÜV SÜD has conducted a conformity assessment of Motional's cybersecurity framework called "Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL)" against the standard ISO/SAE 21434:2021 [1].

This assessment refers to the conformity of the framework specifically with respect to the lifecycle aspects of the above standard; it explicitly does not include any references to the standard's implementation or interpretation. The assessment results, therefore, provide no statement on the underlying processes or the organizational implementation within Motional or any other organization.

The following clauses were not considered in this assessment, as they were considered by Motional as being outside the scope of the framework:

- Clause 5: out of scope
- Clause 6: out of scope

The results of the assessment are as follows:

Clause	Conformity within the specified scope is given (y/n)
Clause 5	N/A (Out of Scope)
Clause 6	N/A (Out of Scope)
Clause 7	Yes
Clause 8	Yes
Clause 9	Yes
Clause 10	Yes
Clause 11	Yes
Clause 12	Yes
Clause 13	Yes
Clause 14	Yes
Clause 15	Yes

TÜV SÜD America, Inc.
401 Edgewater Pl Suite 500
Wakefield, MA 01880
USA

TUVSUD_CybersecurityAssessmentSummary_Motional_AVCDL_v.2.12.docx
Rev 2.12
June 27, 2022
Page 1 of 5

Motional AD Inc. (f/k/a nuTonomy Inc.)
100 Northern Ave, Suite 200
Boston, MA 02210, USA

Cybersecurity Assessment Summary for UN R155 – Motional AVCDL

File name: TUVSUD_CybersecurityAssessmentSummary_R155_Motional_AVCDL_v.3.1.docx Revision: Rev 3.2 Date: June 13, 2023 Page: 1 of 7

To whom it may concern:

TÜV SÜD has conducted a conformity assessment of Motional's cybersecurity framework called "Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL)" against the UN Regulation R155 [1].

This assessment refers to the conformity of the framework specifically with respect to the lifecycle aspects of the above regulation; it explicitly does not include any references to the regulation's implementation or interpretation. The assessment results, therefore, provide no statement on the underlying processes or the organizational implementation within Motional or any other organization.

Requirements related to the vehicle type were additionally included in the assessment as stated below, but with no relation to a specific vehicle. The AVCDL framework was only assessed for its supporting role in fulfilling these requirements.

Several requirements were considered out of scope, as they were not applicable to the AVCDL and thus could not be assessed.

The results of the assessment are as follows:

Clause	AVCDL requirement title	Conformity within the specified scope is given (y/n)
CSMS Requirements		
7.1.1	UN regulation non-exclusion	N/A (Out of Scope)
7.2.1	compliance verification	N/A (Out of Scope)
7.2.2.1(a)	development phase CSMS	Yes
7.2.2.1(b)	production phase CSMS	Yes
7.2.2.1(c)	post-production CSMS	Yes
7.2.2.2(a)	cybersecurity management	Yes
7.2.2.2(b)	risk identification	Yes
7.2.2.2(c)	risk assessment/treatment	Yes
7.2.2.2(d)	verification of risk management	Yes
7.2.2.2(e)	cybersecurity testing	Yes
7.2.2.2(f)	risk assessment kept current	Yes
7.2.2.2(g)	adaptable monitoring/response	Yes
7.2.2.2(h)	cybersecurity controls tracking	Yes
7.2.2.3	timely risk mitigation	Yes
7.2.2.4(a)	vehicle monitoring enrollment	N/A (Out of Scope)
7.2.2.4(b)	threat extraction from vehicle logs	Yes
7.2.2.5	supplier deficiency management	Yes
Vehicle Type Requirements		
7.3.1	certificate of compliance	N/A (Out of Scope)
7.3.2	management of type	Yes
7.3.3	critical element risk assessment	Yes
7.3.4	type risk protection	Yes
7.3.5	hosted environments	Yes
7.3.6	sufficient testing	Yes
7.3.7(a)	detect/prevent cyberattacks	Yes
7.3.7(b)	vehicle cybersecurity monitoring	Yes
7.3.7(c)	provide forensic capability	Yes
7.3.8	use standard crypto modules	Yes
7.4.1	periodic monitoring report	Yes
7.4.2	approval defect reporting	N/A (Out of Scope)

Non-conformities and corrective actions have been evaluated and documented in the assessment sheet [2].

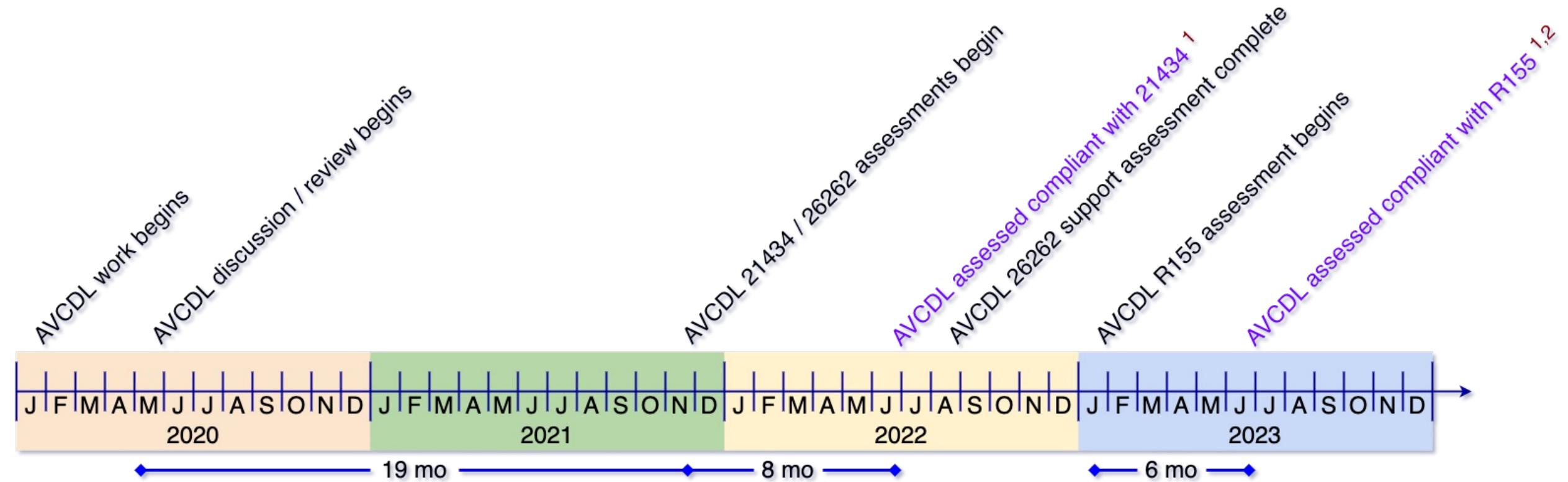
TÜV SÜD America, Inc.
401 Edgewater Pl Suite 500
Wakefield, MA 01880
USA

TUVSUD_CybersecurityAssessmentSummary_R155_Motional_AVCDL_v.3.2.docx
Rev 3.2
June 13, 2023
Page 1 of 7

TÜV SÜD America, Inc.
401 Edgewater Pl Suite 500
Wakefield, MA 01880
USA

TUVSUD_CybersecurityAssessmentSummary_R155_Motional_AVCDL_v.3.2.docx
Rev 3.2
June 13, 2023
Page 2 of 7

Assessment Timeline

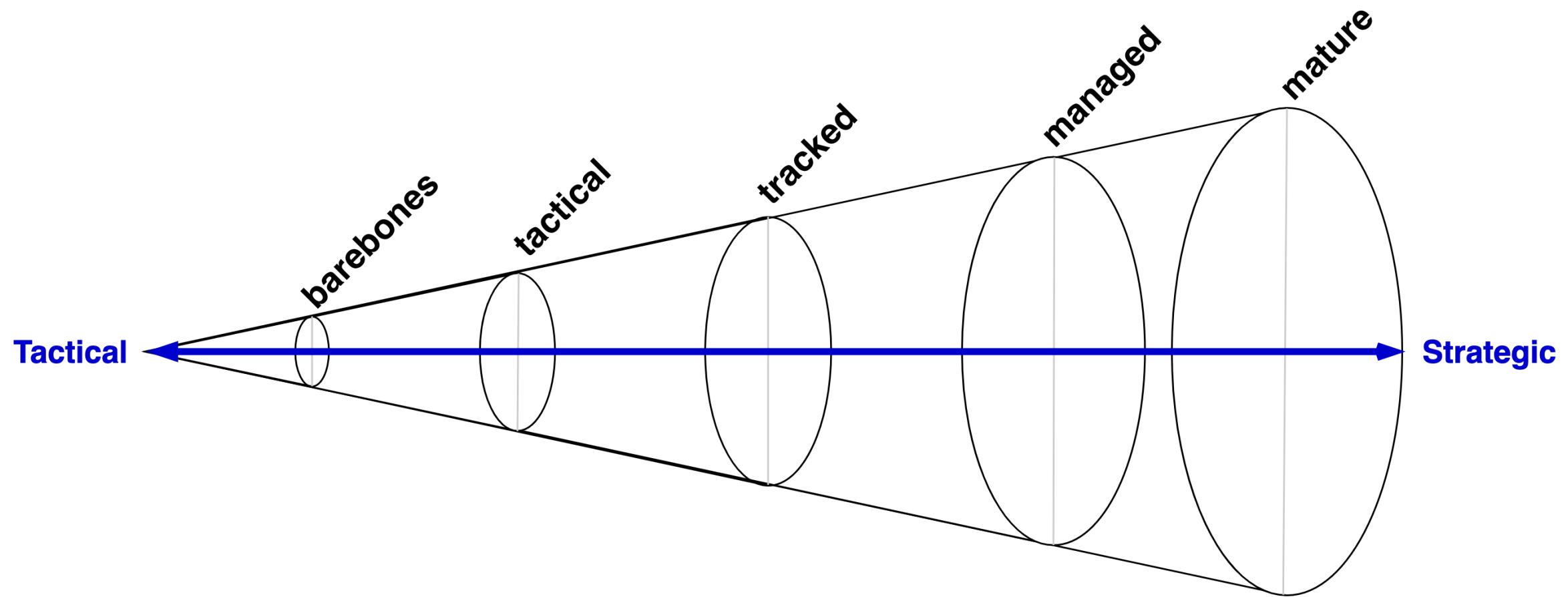


¹ excludes elements that are the responsibility of the organization

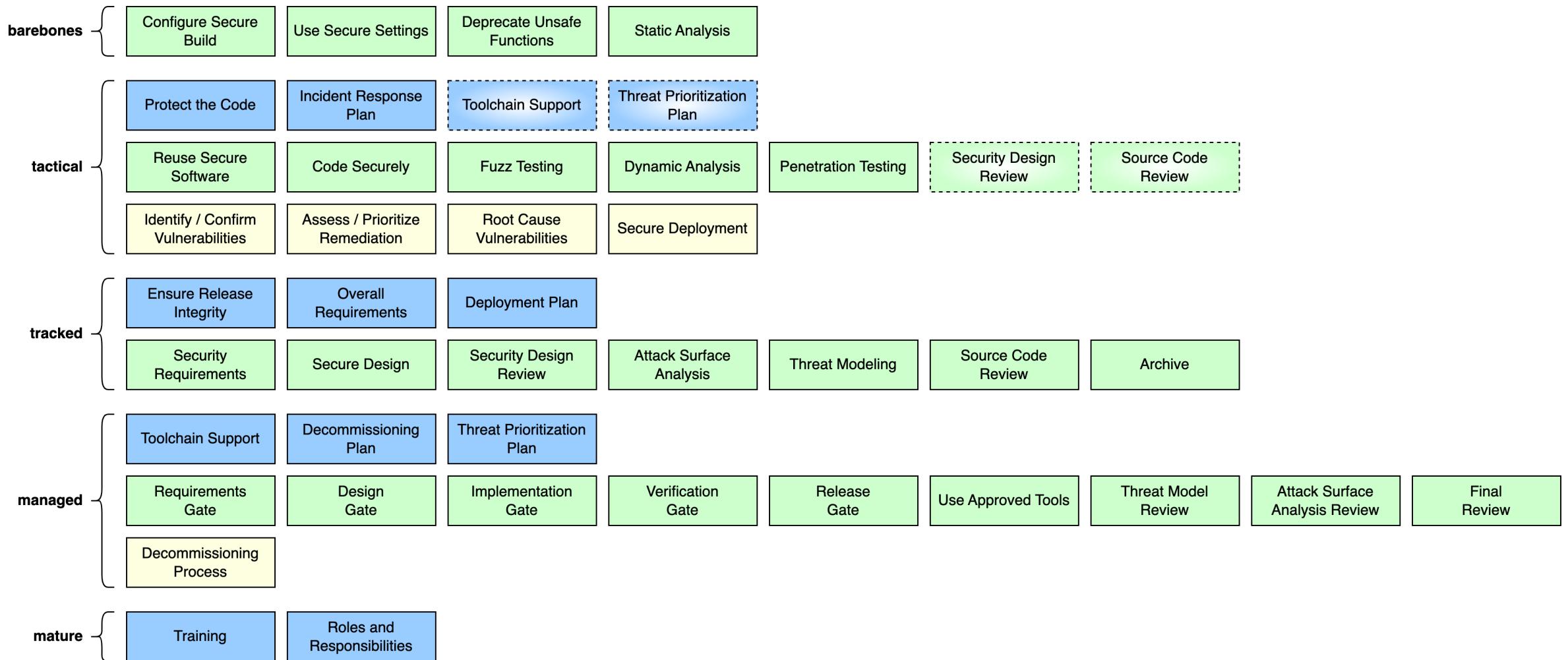
² excludes elements that are the sole responsibility of the OEM

Incremental Adoption

Incremental Adoption Spectrum



Prioritized Phase Requirements



Lessons Learned

Lessons Learned

- Learn from the past
- Be systematic and consistent
- Play well with others
- Allow realistic amounts of time
- Communicate liberally

Learning More

AVCDL on YouTube

<https://youtube.com/@AVCDL/playlists>



AVCDL

@AVCDL · 58 subscribers · 10 videos

This channel contains material regarding the AVCDL (Autonomous Vehicle Cybersecurity D... >

github.com/nutonomy/AVCDL

[Subscribe](#)

Home

Videos

Playlists

Community

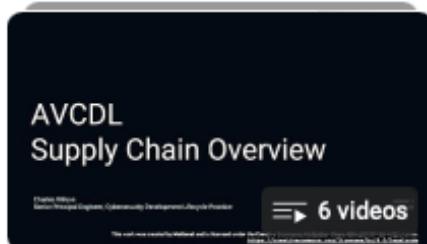


Created playlists



AVCDL

[View full playlist](#)



AVCDL supply chain

[View full playlist](#)

AVCDL on GitHub

<https://github.com/nutonomy/AVCDL>

The screenshot shows the GitHub repository page for AVCDL. The repository is owned by nutonomy and has 293 commits. The commit history lists various changes made to files like assessments, background_material, distribution, source, training, .gitignore, LICENSE.md, README.md, document_status.md, mentions.md, supply_chain.md, supply_chain.pdf, and zip_downloading.md. The repository has 13 watchers, 17 forks, and 72 stars. It includes sections for About, Releases, and a report repository link.

Code Issues Pull requests Actions Wiki Security Insights Settings

AVCDL Public

main 1 Branch 265 Tags

Go to file + <> Code

Motional-Charles-Wilson added generic process overlay to AVCDL framework diagram... 3e3a4ff · 1 hour ago 293 Commits

assessments added discussion material to the assessments readme 9 months ago

background_material added PDF version of the lifecycle construction page / linked... last week

distribution Updated Understanding Cybersecurity Risk Freshness in an ... 5 days ago

source added generic process overlay to AVCDL framework diagram... 1 hour ago

training moved GitHub screenshot from AVCDL overview training to ... 3 hours ago

.gitignore created .gitignore 3 years ago

LICENSE.md moved license up a level 3 years ago

README.md restored non-Git user ZIP archive download section last week

document_status.md added AVCDL Phase Requirement Product ISO 24089 Work ... 2 weeks ago

mentions.md updated mentions page to include Brandon Barry's Block Ha... 7 months ago

supply_chain.md created a PDF version of the supply chain material overview /... 2 weeks ago

supply_chain.pdf created a PDF version of the supply chain material overview /... 2 weeks ago

zip_downloading.md added instructions to download repository as a ZIP archive f... 2 years ago

About

This repository contains material related to the Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL)

cybersecurity autonomous-vehicles
automotive-security development-lifecycle
avcdl iso21434

Readme View license Activity Custom properties 72 stars 13 watching 17 forks Report repository

Releases 254

4.15.6 Latest 1 hour ago + 253 releases

References (1 of 2)

AVCDL (GitHub)

<https://github.com/nutonomy/AVCDL>

Incremental AVCDL Adoption (AVCDL elaboration document)

AVCDL vendor CMM template (AVCDL template document)

AVCDL Introductory Blog Post

https://github.com/nutonomy/AVCDL/tree/main/background_material/blog_posts

Systems and software engineering - Software lifecycle processes

https://en.wikipedia.org/wiki/ISO/IEC_12207

Systems and software engineering - System lifecycle processes

https://en.wikipedia.org/wiki/ISO/IEC_15288

Road vehicles – Functional safety

https://en.wikipedia.org/wiki/ISO_26262

Secure Software Development for Autonomous Vehicles

<https://www.sae.org/standards/content/iso/sae21434/>

References (2 of 2)

Microsoft Security Development Lifecycle (SDL) - simplified implementation

http://download.microsoft.com/download/F/7/D/F7D6B14F-0149-4FE8-A00F-0B9858404D85/SimplifiedImplementation_of_the SDL.doc

NHTSA Cybersecurity Best Practices for the Safety of Modern Vehicles

https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

NICE Cybersecurity Workforce Framework (NCWF)

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>

Secure Software Development Framework (SSDF)

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04232020.pdf>

UN Regulation No. 155 - Cyber security and cyber security management system

<https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security>

What is the difference between ISO 9001 and IATF 16949

<https://www.qualityze.com/difference-iso-9001-iatf-16949/>

Questions