SAE IAS 2024

There and Back Again

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

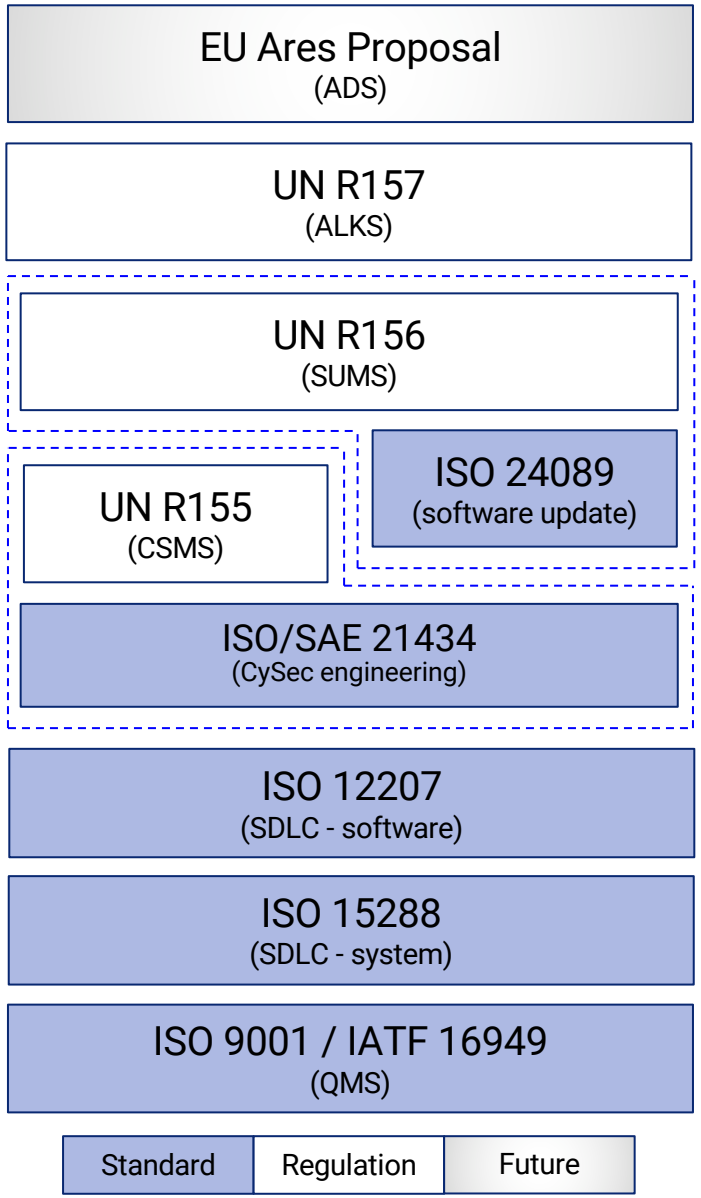
Charles Wilson
Technical Fellow, Cybersecurity Engineering
Motional

version 5
2024-04-01

Introduction

Standards and Regulations

Standards and Regulations Ecosystem



Automated Driving Systems will require conformance to R155 and R156

Auto Lane Keeping Systems must conform to R155 and R156

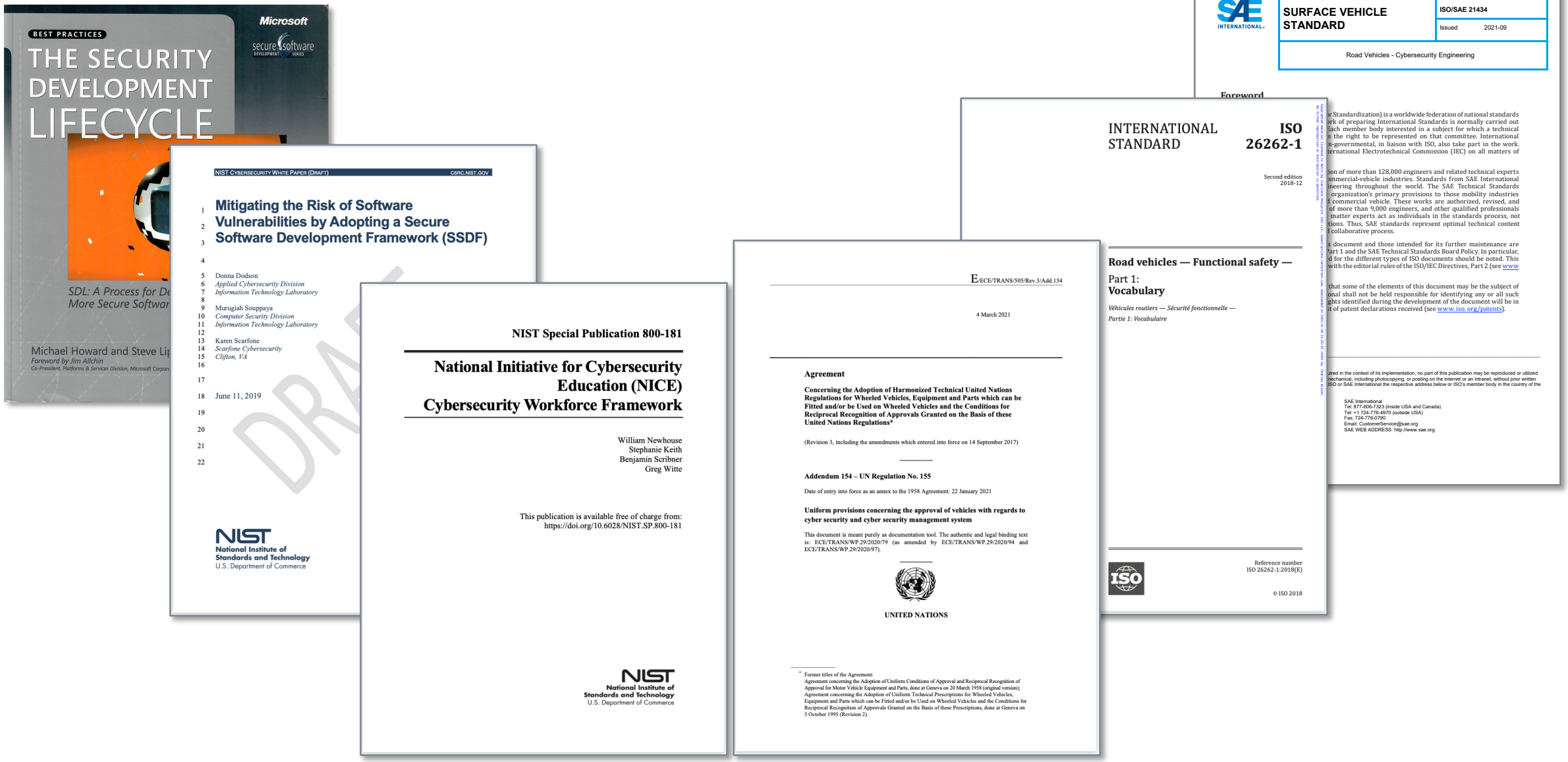
Software Update Management Systems aligned with 24089 and 21434

Cybersecurity Management Systems aligned with 21434

System and software development lifecycles

A certified QMS is the basis for compliance

Reference Sources



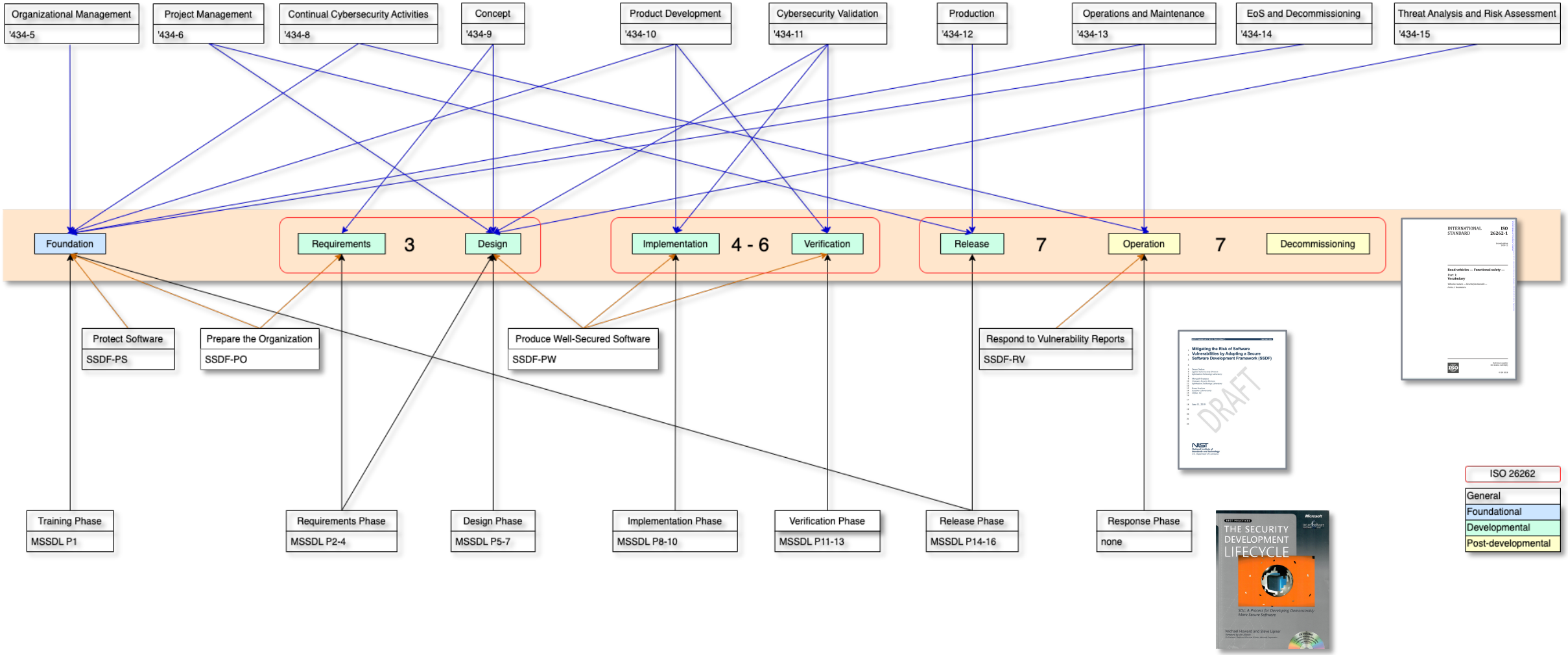
How the Standards Line Up

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

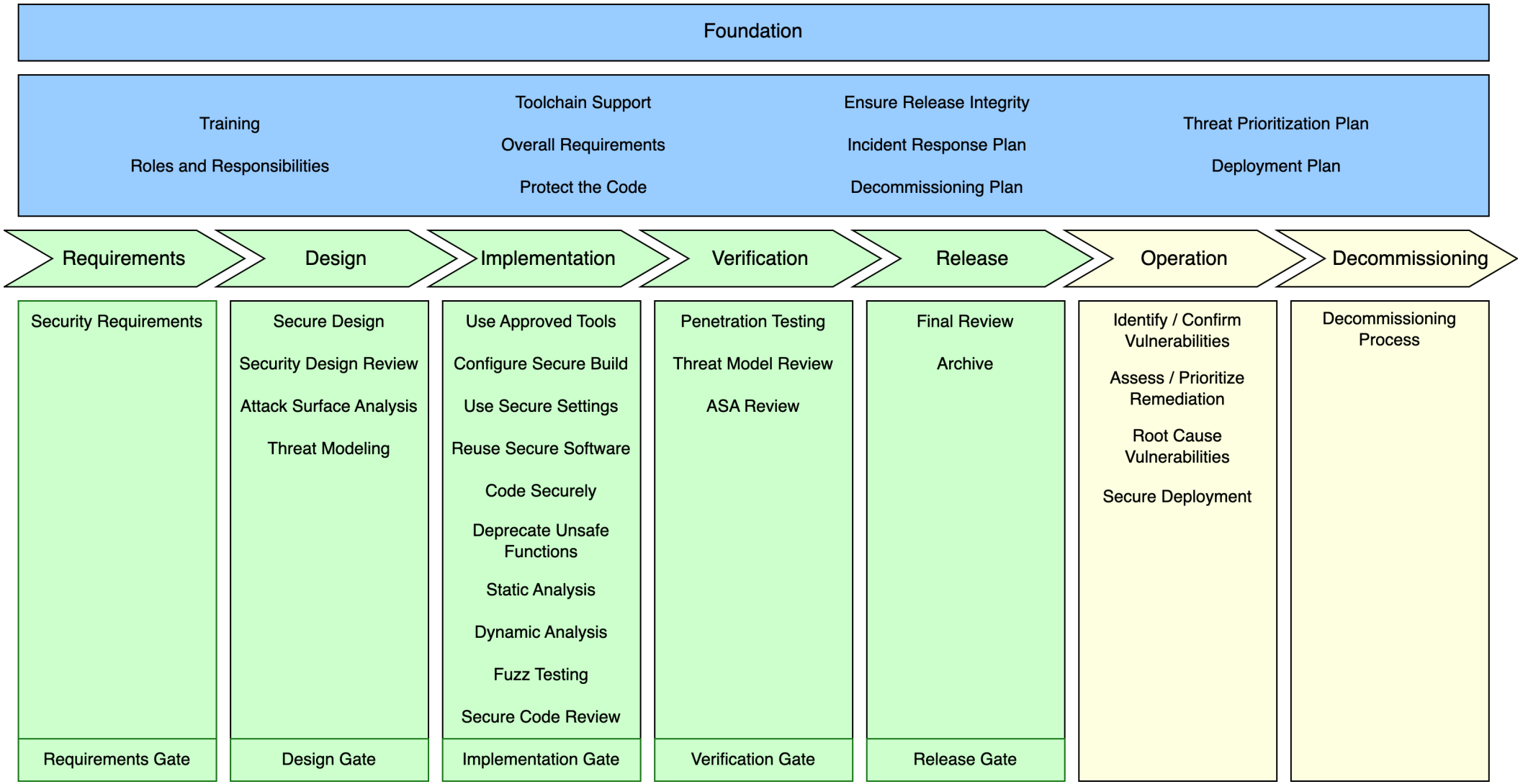
How Sources Inform the AVCDL



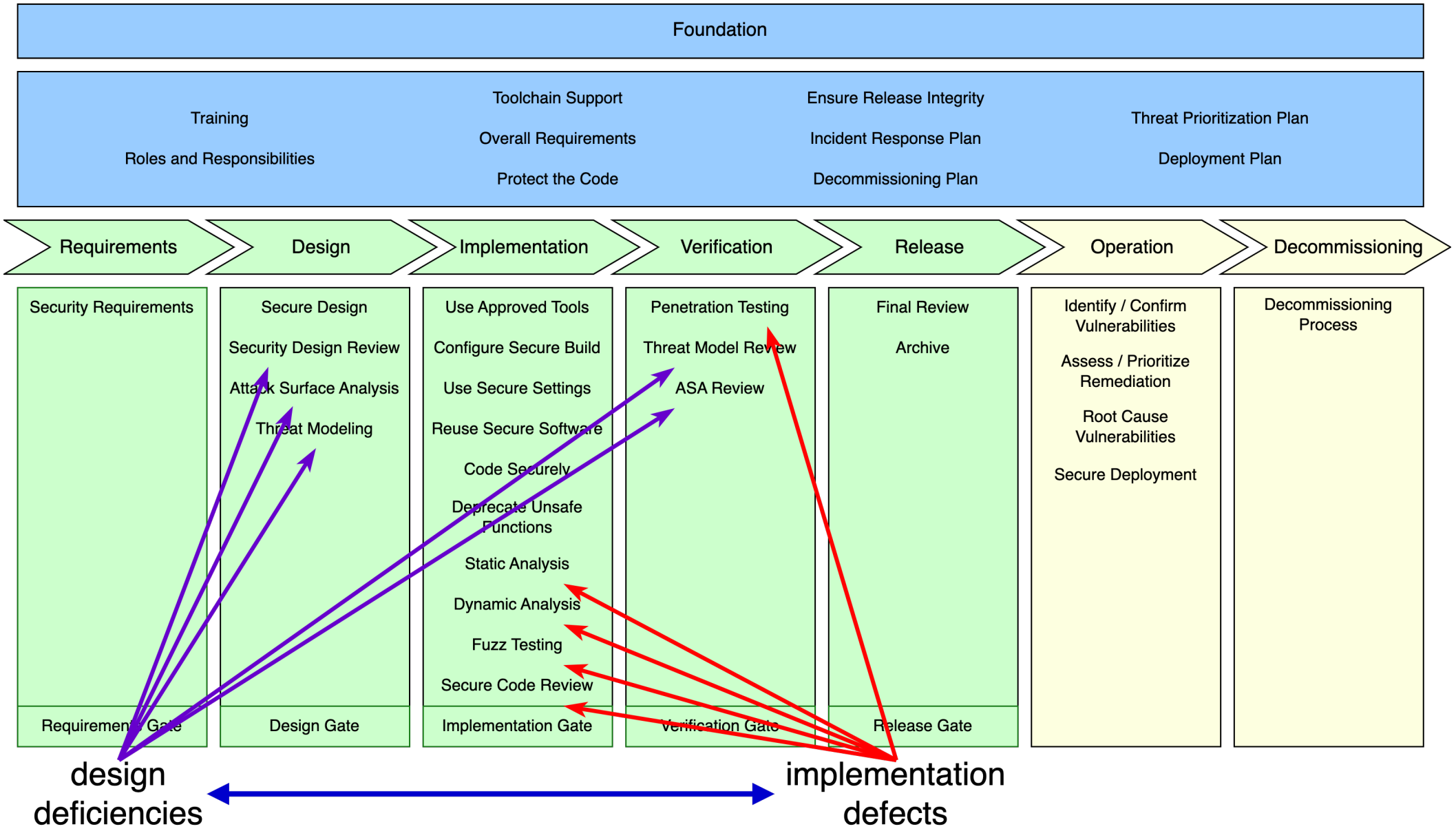
ISO/SAE 21434 – AVCDL Mapping

				Foundation														Requirements			Design					Implementation											Verification				Release			Operation				Decc	Supplier		
				1		2	3	4		5	6	7		8	9	10		1		2	1	2	3	4		5	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	1	2	3	1	2	3	4	1	1	2	3
				1	2	1	1	1	2	1	1	1	2	1	1	1		1	2	1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	X	X	1	1	1	1	1	1	1
				training catalog	system to track training participation	roles and responsibilities document	list of approved tools and components	global security goals	global security requirements	code protection plan	release integrity plan	cybersecurity monitoring plan	incident response plan	decommissioning plan	threat prioritization plan	deployment plan		product-level security goals	product-level security requirements	requirements phase gate	design showing security considerations	security design review report	attack surface analysis report	threat modeling report	ranked/risked threat report	threat report	design phase gate	list of tools and components used	build process documentation	secure setting document	component/version - product/version cross-reference document	secure development	currently used deprecated functions document	static analysis report	dynamic analysis report	secure code review summary	fuzz testing report	implementation phase gate	penetration testing report	updated threat model	updated attack surface analysis	verification phase gate	final security review report	archive manifest	release phase gate	cybersecurity incident report		software deployment report	decommissioning report	AVCMDS	Supplier Self-reported Maturity	Cybersecurity Interface Agreement
Distrubuted Cybersecurity Activities	WP-07-X1	RQ-07-01	evaluate supplier cybersecurity capability																																											X	X	
	WP-07-X2	RQ-07-03	supplier cybersecurity quote																																													
	WP-07-01	RQ-07-04	supplier cybersecurity interface agreement																																													X
		RQ-07-06	supplier vulnerability activities																																													X
		RQ-07-07	extra-security CIA conflict																																													X
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																																X				
	WP-08-04	RQ-08-04	cybersecurity event assessment										X																																X				
	WP-08-05	RQ-08-05	identified weakness analysis										X																																	X	X			
		RQ-08-06	weakness rejection rationale										X																																	X	X			
	WP-08-06	RQ-08-07	vulnerability management										X		X									X																				X	X	X		
	WP-08-X1	RQ-08-08	apply incident response protocols										X																																X	X	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																								

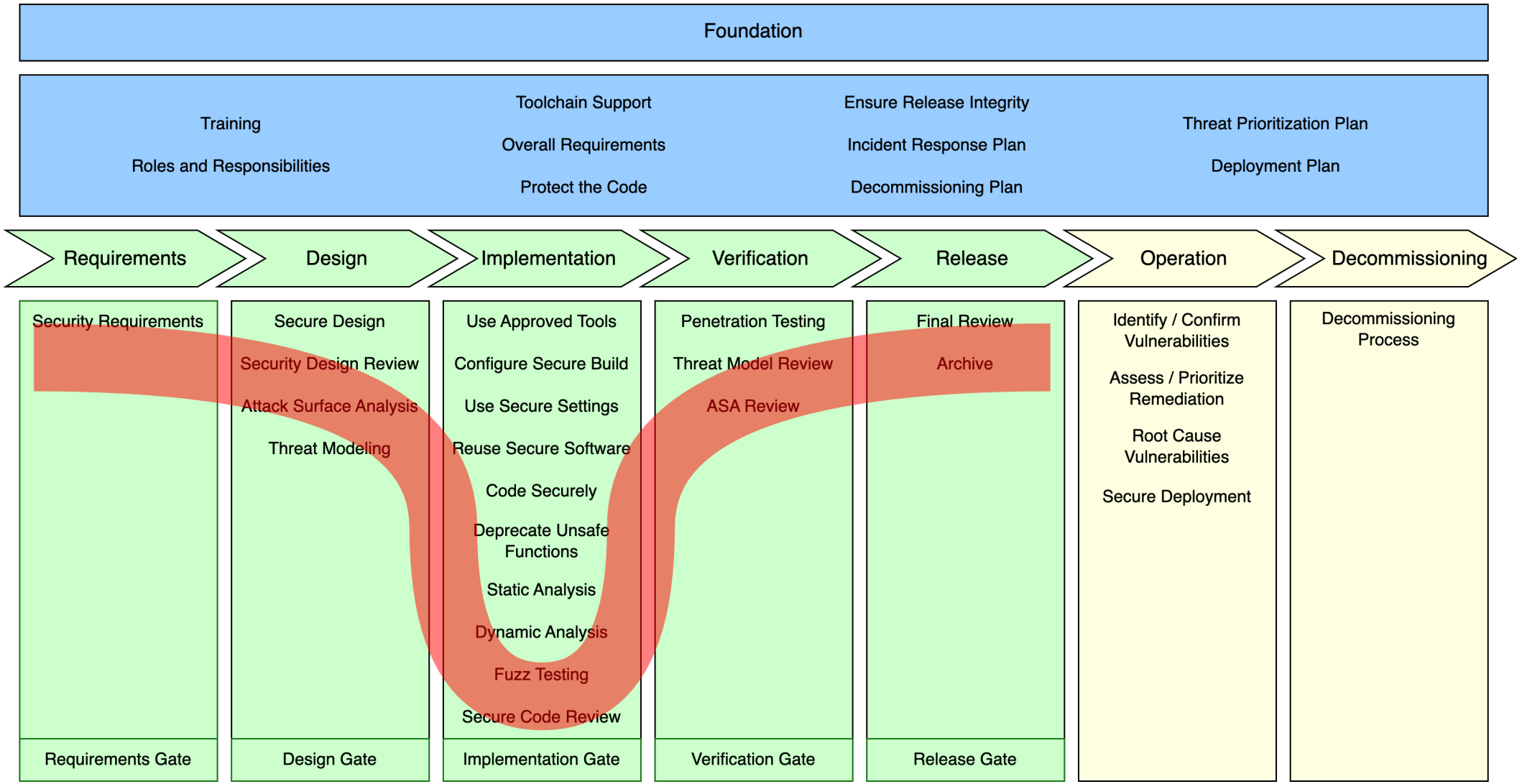
AVCDL Framework



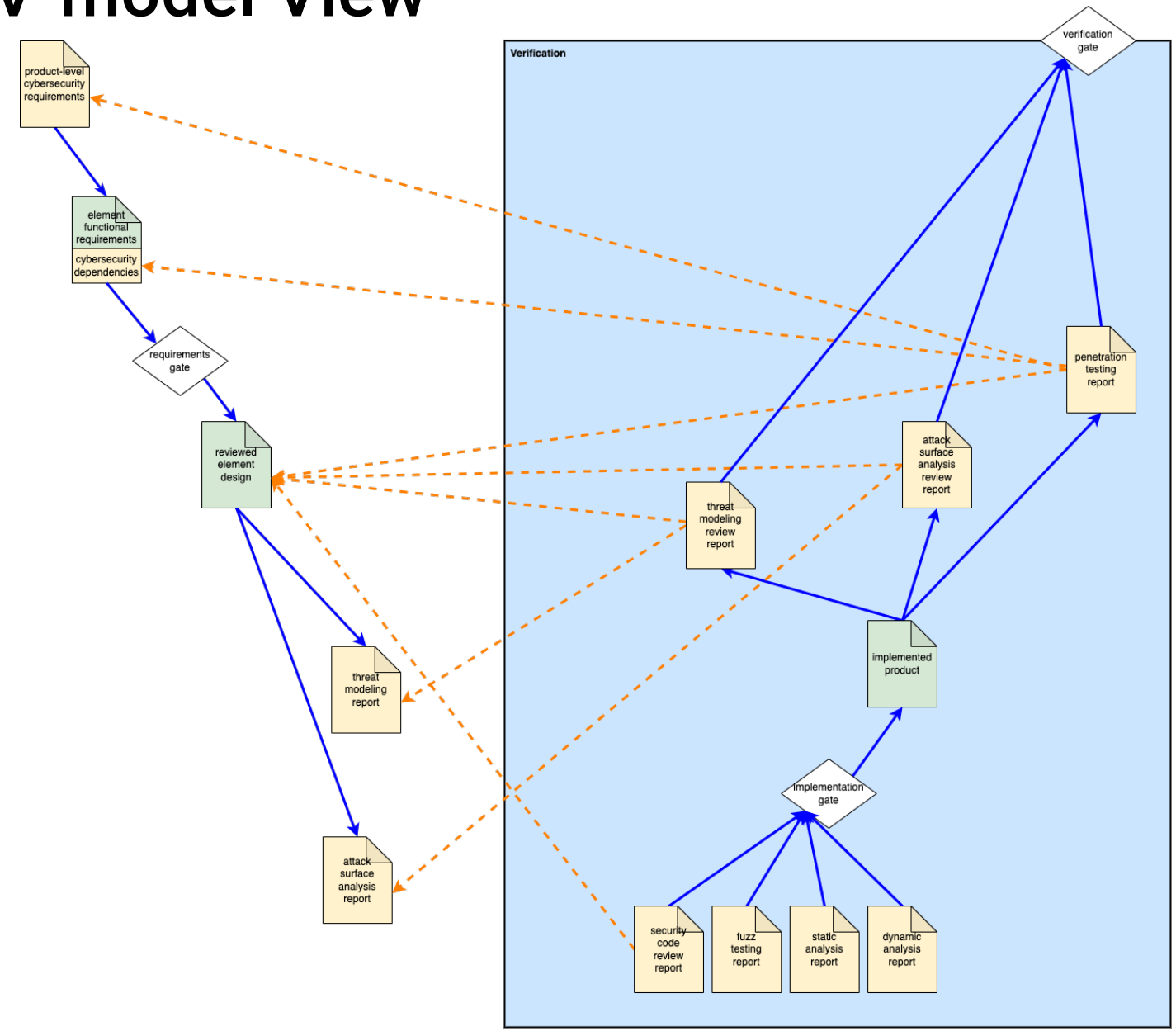
Design Deficiencies vs Implementation Defects



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**.

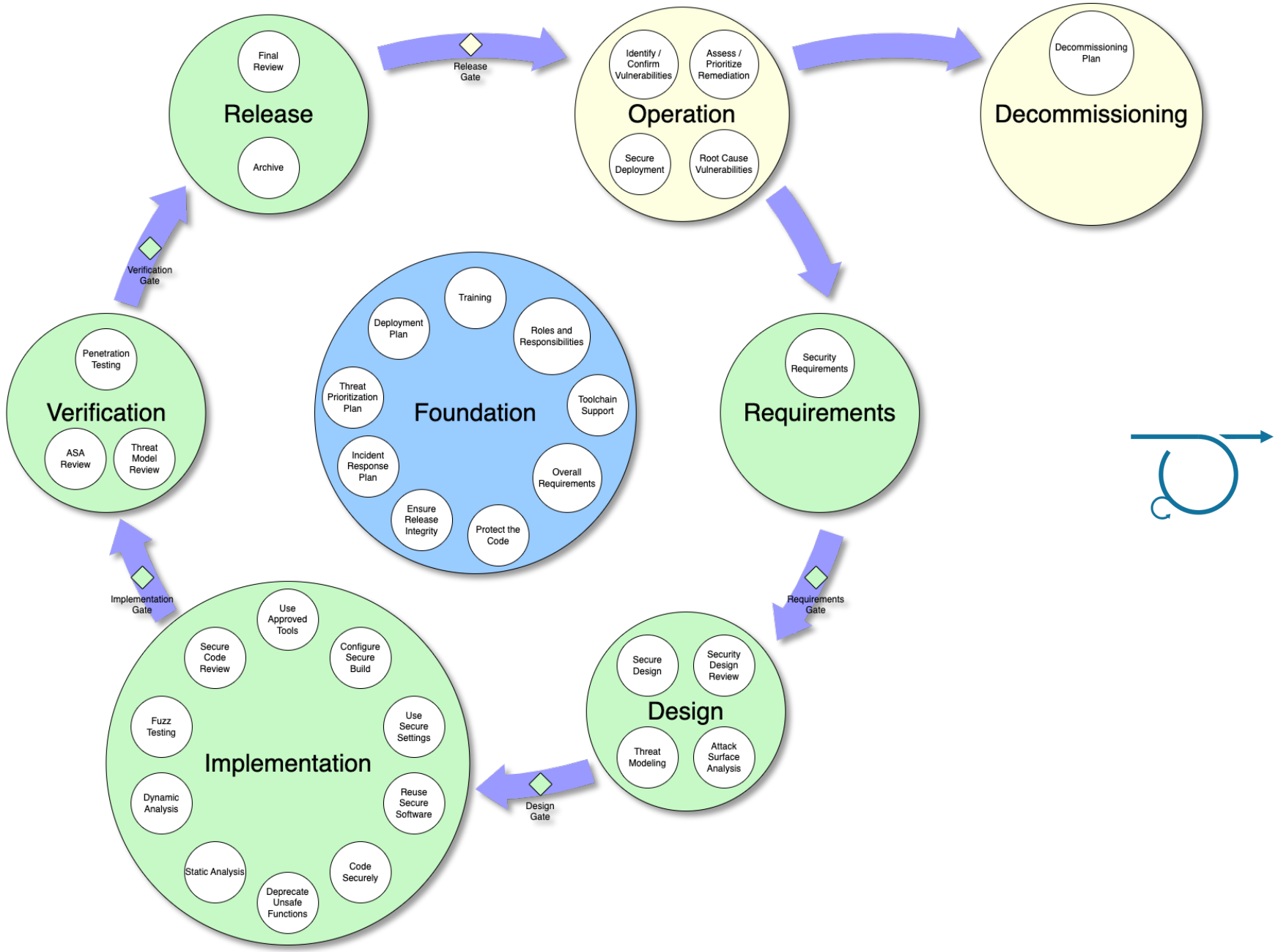
Audience

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

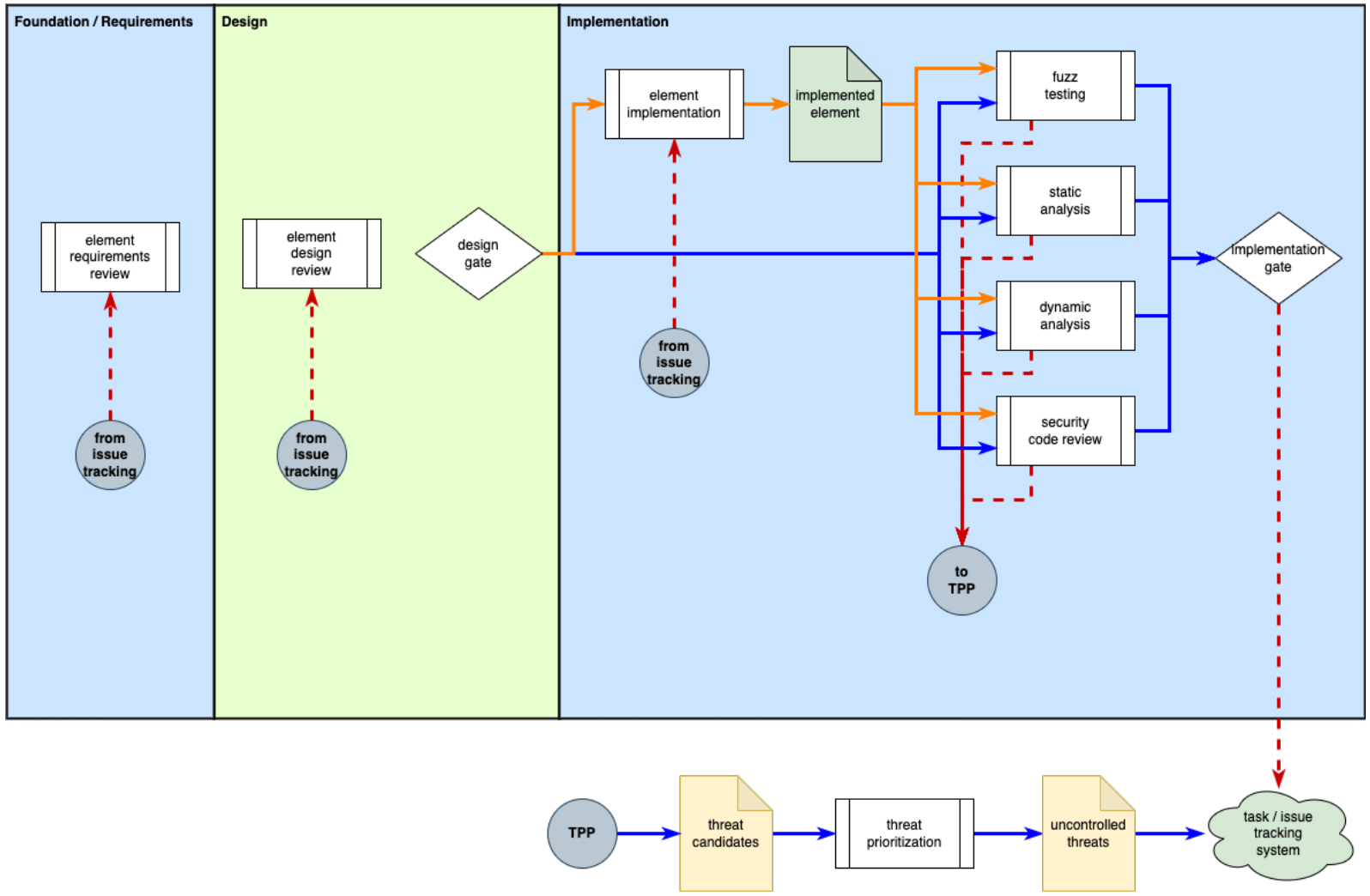
Note: This document is not subject to certification body review.

License

Cyclic View


Release
Final Review
Archive
Release Gate
Operation
Identify / Confirm Vulnerabilities
Assess / Prioritize Remediation
Secure Deployment
Root Cause Vulnerabilities
Decommissioning
Decommissioning Plan
Requirements
Security Requirements
Requirements Gate
Design
Secure Design
Security Design Review
Threat Modeling
Attack Surface Analysis
Design Gate
Implementation
Use Approved Tools
Configure Secure Build
Use Secure Settings
Reuse Secure Software
Code Securely
Deprecate Unsafe Functions
Static Analysis
Dynamic Analysis
Fuzz Testing
Secure Code Review
Implementation Gate
Verification
Penetration Testing
ASA Review
Threat Model Review
Verification Gate
Foundation
Training
Roles and Responsibilities
Toolchain Support
Overall Requirements
Protect the Code
Ensure Release Integrity
Incident Response Plan
Threat Prioritization Plan
Deployment Plan

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**.

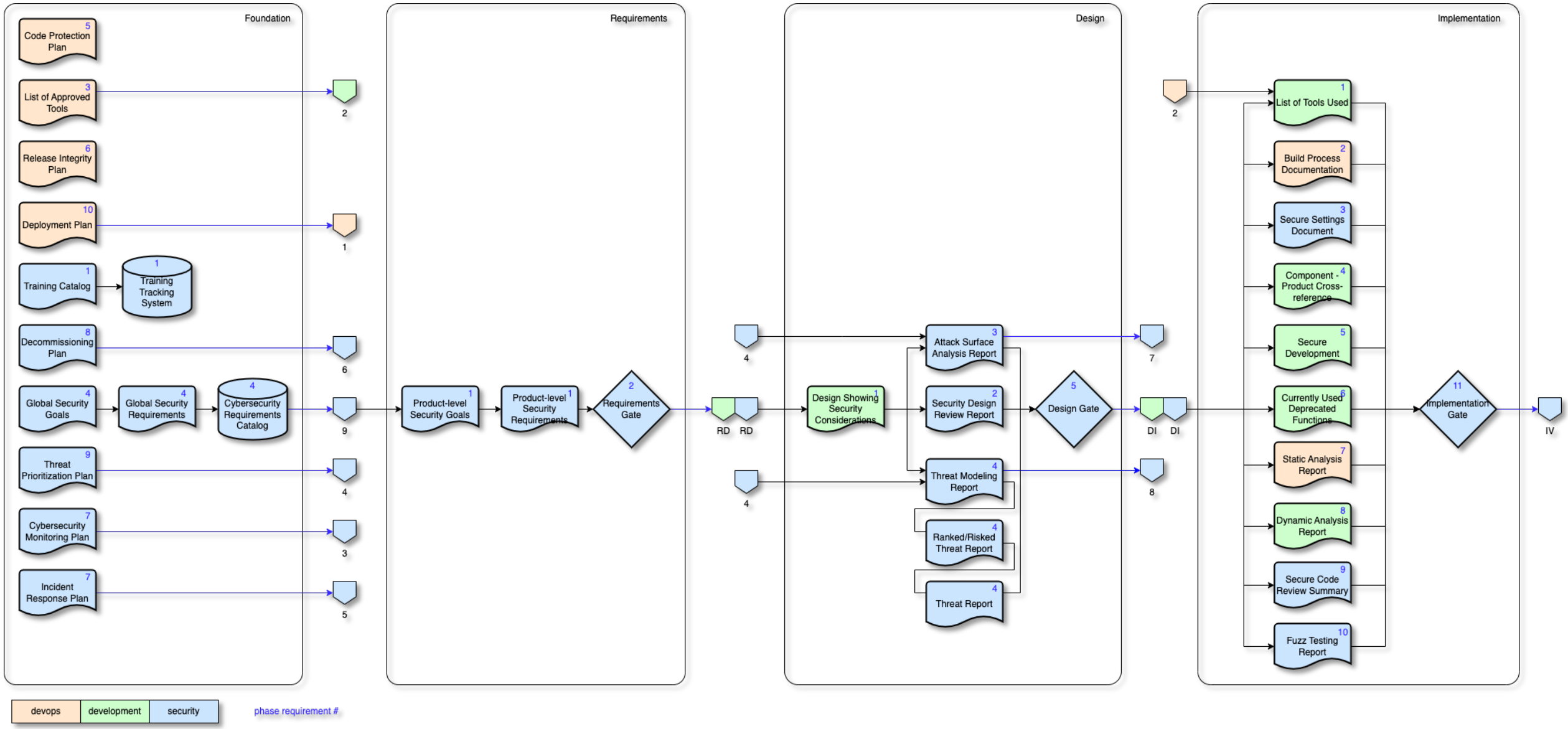
Audience

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

Traceability



Details

Typical Phase Requirement

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 to 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**

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

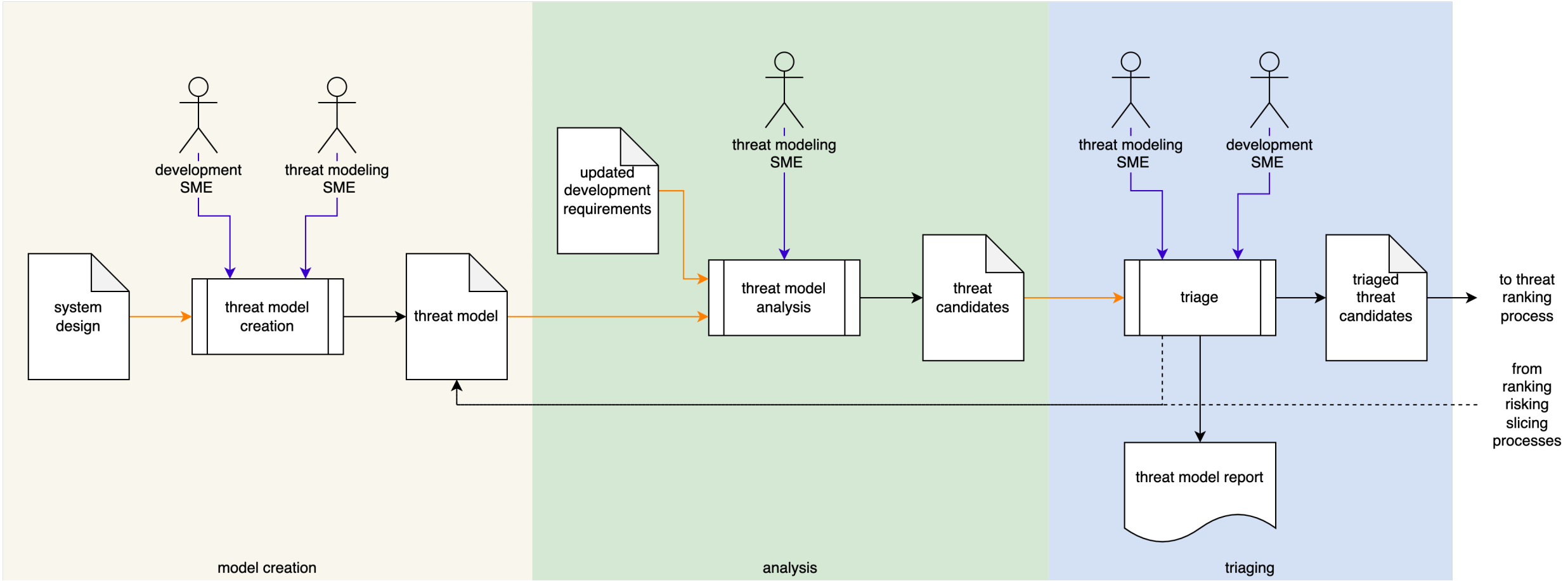
WP.29 CSMS Supplemental

[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

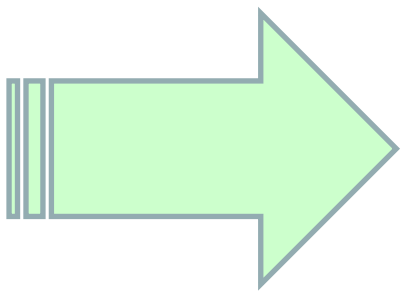
DevOps / Information Systems Security Developer

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.

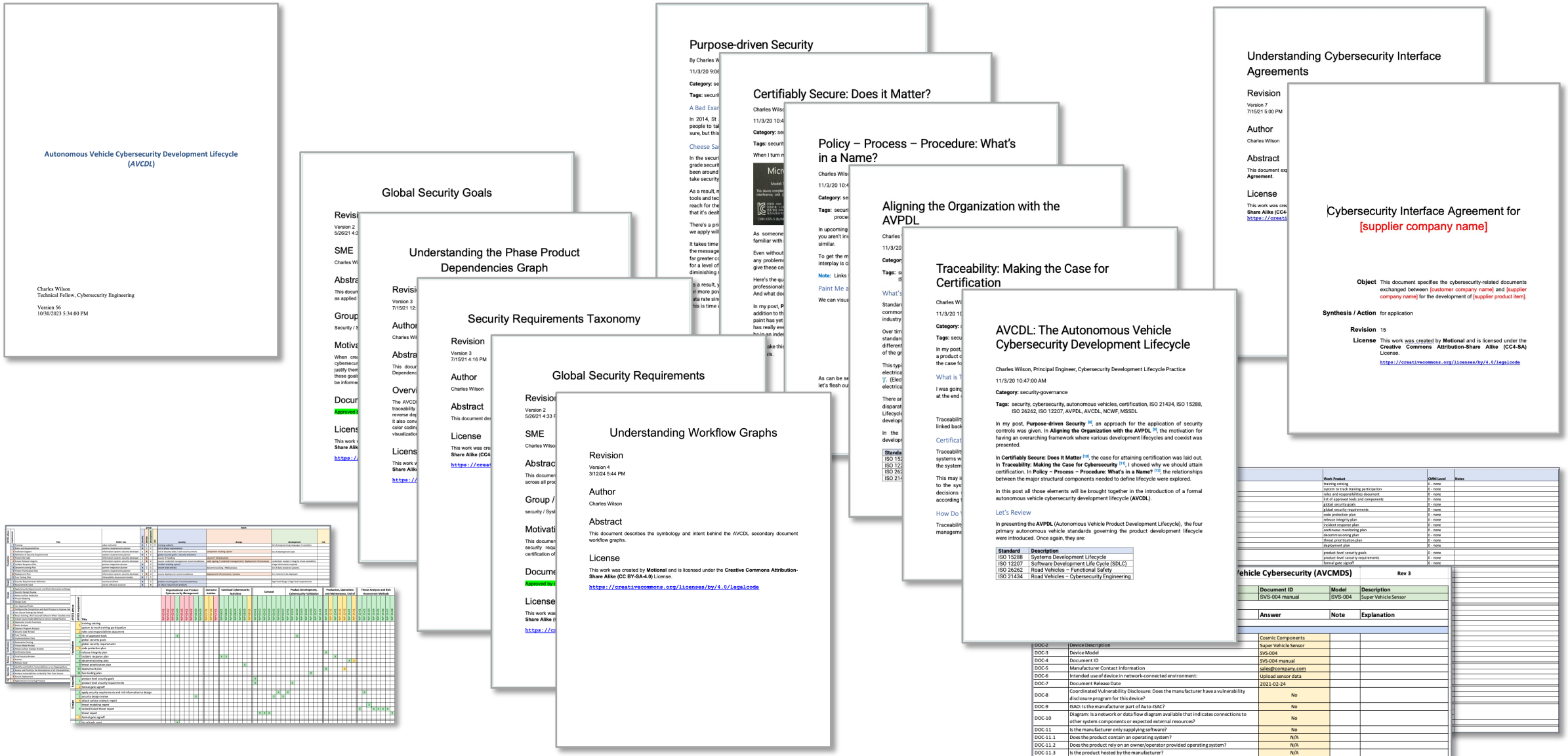
License



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/1A1jFIYihB-IyT0gv7E_KoSjLbwNGmu_wOXBs6siemXA/edit
6. **Tooling Ecosystem working with SWID**
   https://docs.google.com/document/d/1oebYvHcOhtMG8Uhnd5he0l_vhty7MsTjp6fYCOwUmwM/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

Understanding the Phase Product Dependencies Graph

Security Requirements Taxonomy

Global Security Requirements

Understanding Workflow Graphs

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

Author
Charles Wilson

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

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

Purpose-driven Security

Certifiably Secure: Does it Matter?

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

Aligning the Organization with the AVPDL

Traceability: Making the Case for Certification

AVCDL: The Autonomous Vehicle Cybersecurity Development Lifecycle

Charles Wilson, Principal Engineer, Cybersecurity Development Lifecycle Practice

11/3/20 10:47:00 AM

Category: security-governance

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

In my post, **Purpose-driven Security** [9], an approach for the application of security controls was given. In **Aligning the Organization with the AVPDL** [8], the motivation for having an overarching framework where various development lifecycles and coexist was presented.

In **Certifiably Secure: Does It Matter** [10], the case for attaining certification was laid out. In **Traceability: Making the Case for Cybersecurity** [11], I showed why we should attain certification. In **Policy – Process – Procedure: What's in a Name?** [12], 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 presenting the **AVPDL** (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

Understanding Cybersecurity Interface Agreements

Revision
Version 7
7/15/21 5:00 PM

Author
Charles Wilson

Abstract
This document exp
Agreement.

License
This work was cre
Share Alike (CC4-
https://creati

Cybersecurity Interface Agreement for
[supplier company name]

Object This document specifies the cybersecurity-related documents exchanged between [customer company name] and [supplier company name] for the development of [supplier product item].

Synthesis / Action for application

Revision 15

License This work was created by **Motional** and is licensed under the **Creative Commons Attribution-Share Alike (CC4-SA)** License.
https://creativecommons.org/licenses/by/4.0/legalcode

Work Product	CMM Level	Notes
training catalog	0 - none	
system to track training participation	0 - none	
roles and responsibilities document	0 - none	
list of approved tools and components	0 - none	
global security goals	0 - none	
global security requirements	0 - none	
code protection plan	0 - none	
release integrity plan	0 - none	
incident response plan	0 - none	
continuous monitoring plan	0 - none	
decommissioning plan	0 - none	
threat prioritization plan	0 - none	
deployment plan	0 - none	
product-level security goals	0 - none	
product-level security requirements	0 - none	
formal gate signoff	0 - none	

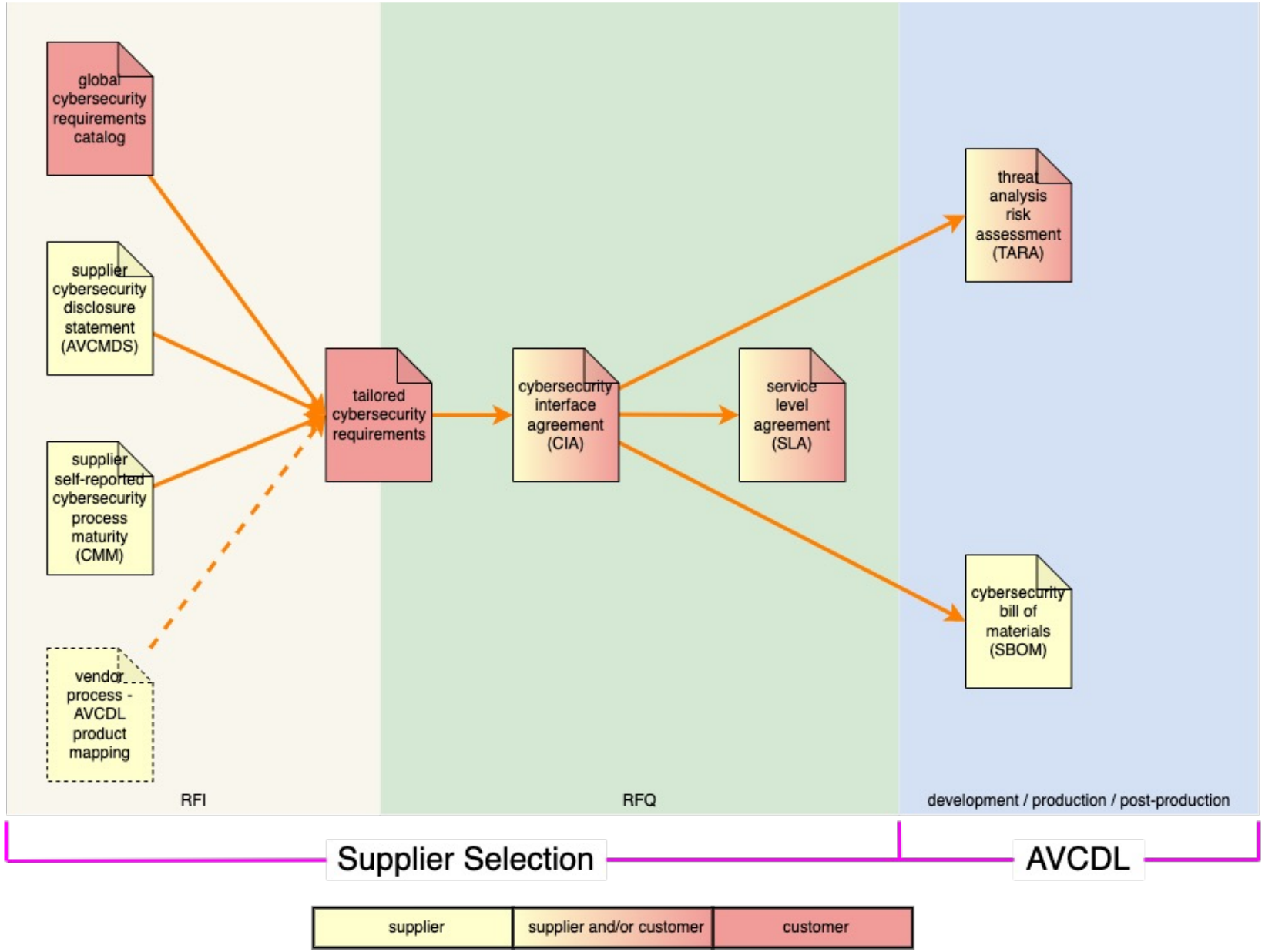
Vehicle Cybersecurity (AVCMDS) Rev 3

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

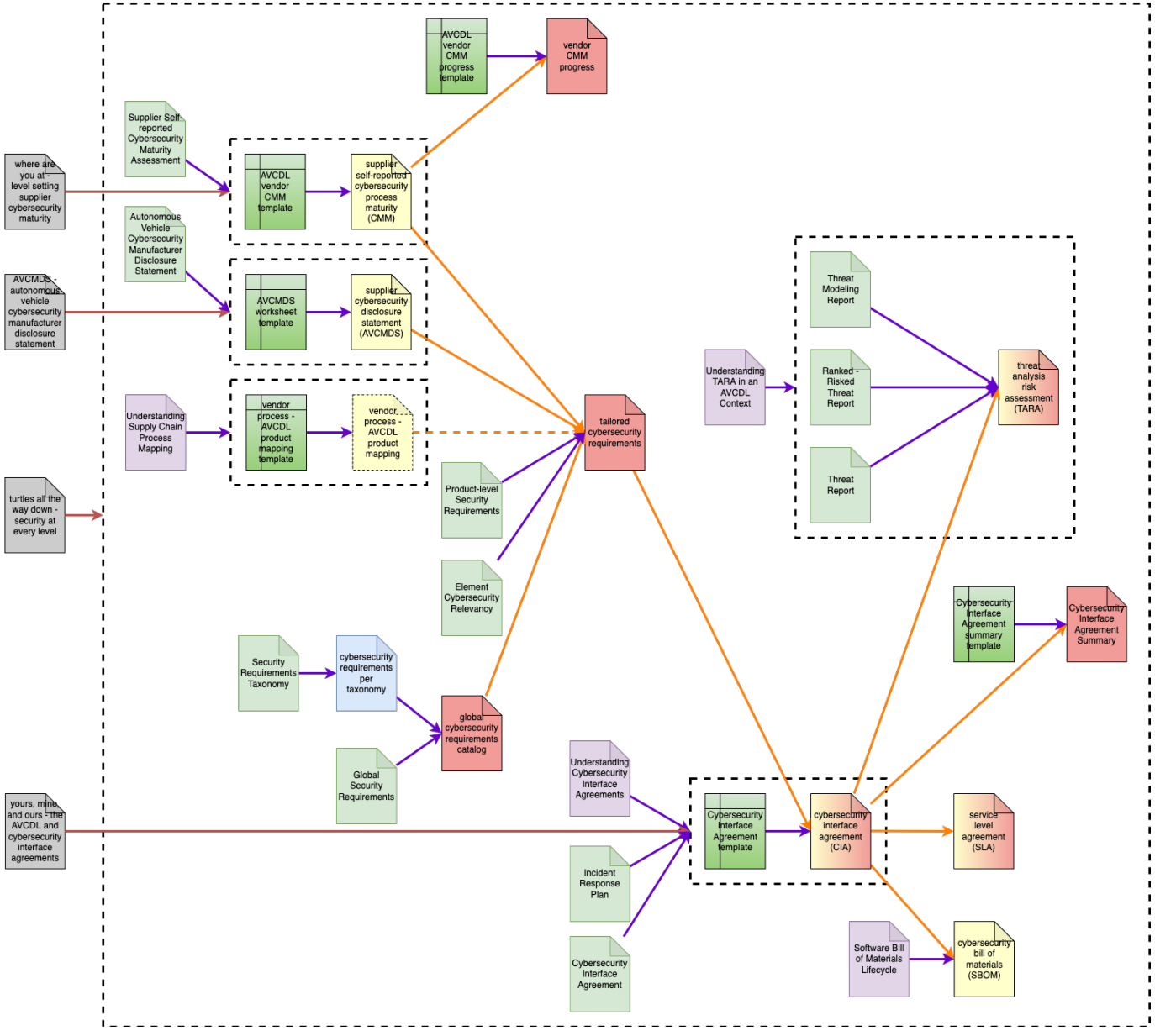
	Answer	Note	Explanation
Cosmic Components			
Super Vehicle Sensor			
DOC-3 Device Model	SVS-004		
DOC-4 Document ID	SVS-004 manual		
DOC-5 Manufacturer Contact Information	sales@company.com		
DOC-6 Intended use of device in network-connected environment:	Upload sensor data		
DOC-7 Document Release Date	2021-02-24		
DOC-8 Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	No		
DOC-9 ISAO: Is the manufacturer part of Auto-ISAC?	No		
DOC-10 Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?	No		
DOC-11 Is the manufacturer only supplying software?	No		
DOC-11.1 Does the product contain an operating system?	N/A		
DOC-11.2 Does the product rely on an owner/operator provided operating system?	N/A		
DOC-11.3 Is the product hosted by the manufacturer?	N/A		
DOC-11.4 Is the product hosted by the customer?	N/A		

Supply Chain

Supplier Selection

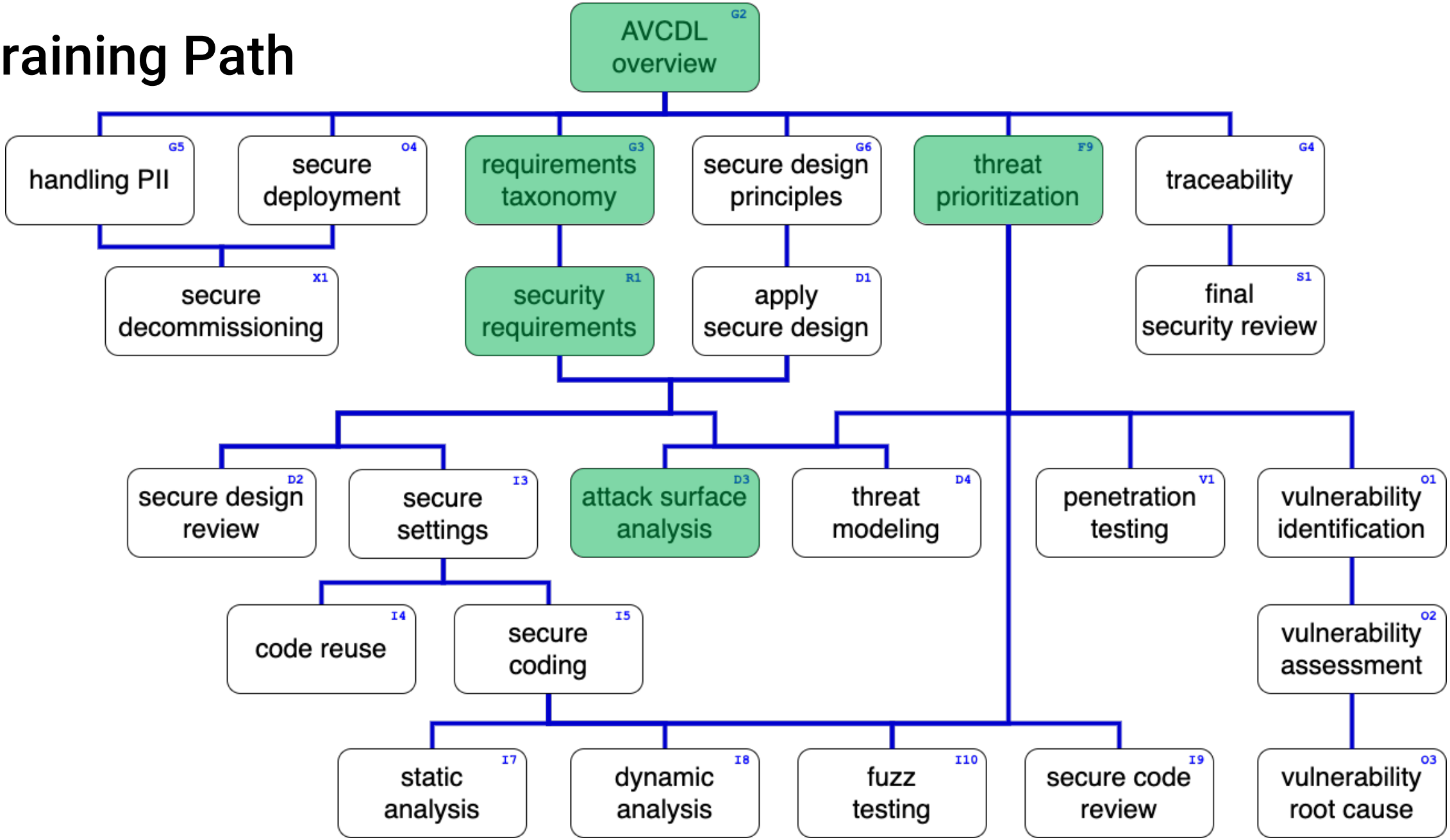


Supply Chain Guidance Documents

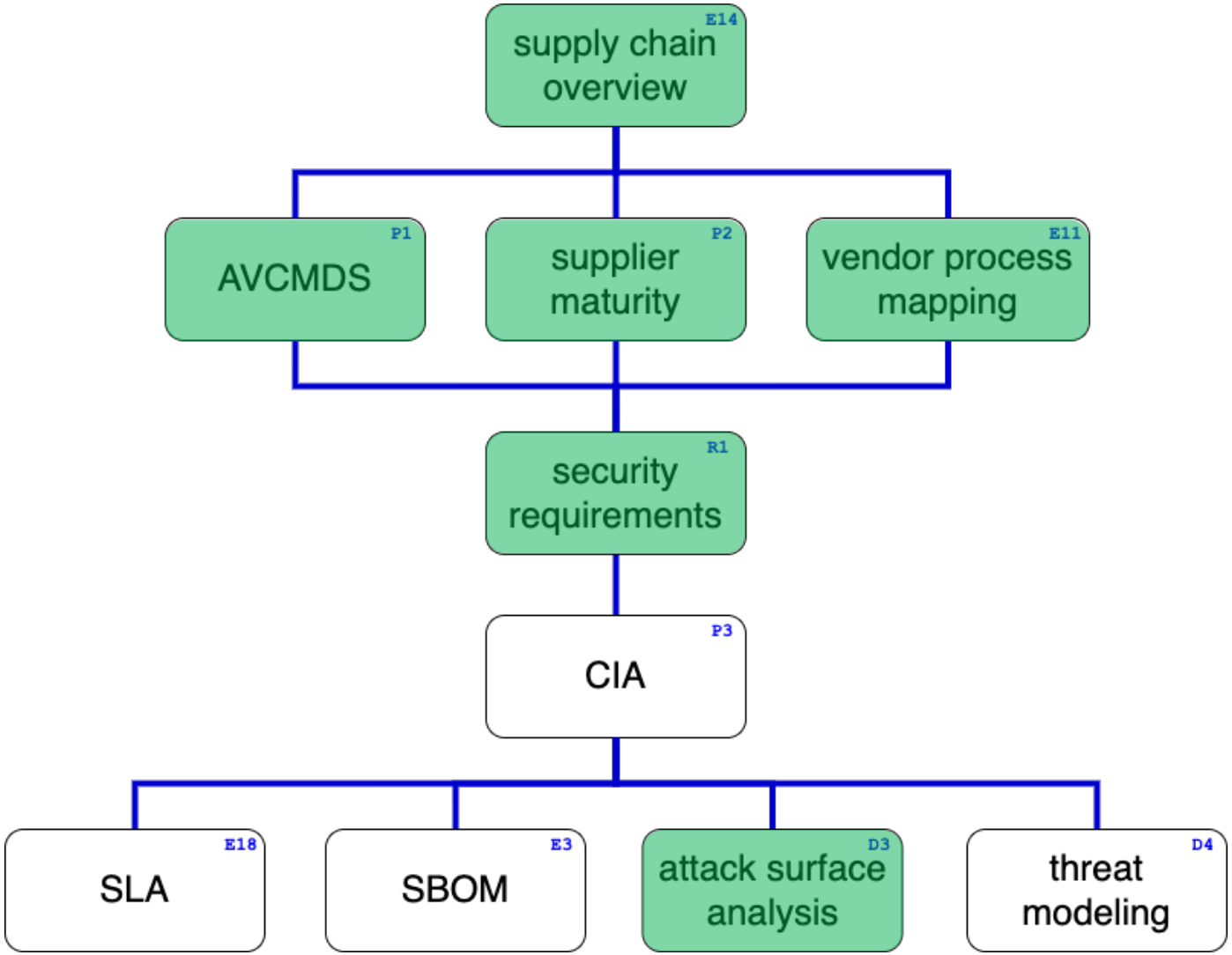


Training

Training Path



Supply Chain Training Path

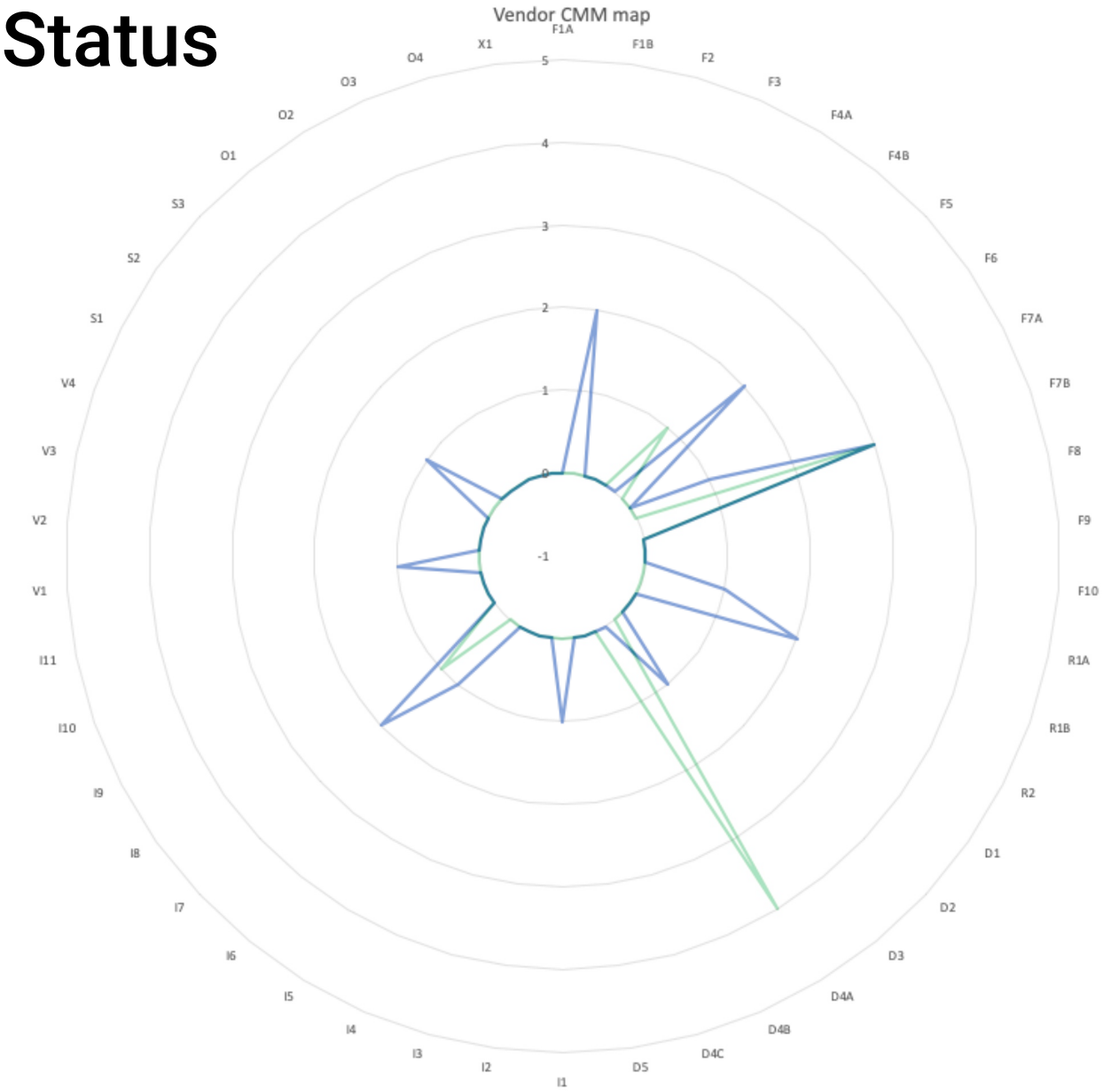


Assessment

Evaluating Your Status

Phase	Phase Requirement	Description	AVCDL Product	CMM Level	Notes
Foundation	Foundation-1	Training	training catalog	0 - none	
			system to track training participation	0 - none	
	Foundation-2	Roles and Responsibilities	roles and responsibilities document	0 - none	
	Foundation-3	Toolchain Support	list of approved tools and components	0 - none	
	Foundation-4	Definition of Security Requirements	global security goals	0 - none	
			global security requirements	0 - none	
	Foundation-5	Protect the Code	code protection plan	0 - none	
	Foundation-6	Ensure Release Integrity	release integrity plan	0 - none	
	Foundation-7	Incident Response Plan	incident response plan	0 - none	
			continuous monitoring plan	0 - none	
	Foundation-8	Decommissioning Plan	decommissioning plan	0 - none	
	Foundation-9	Threat Prioritization Plan	threat prioritization plan	0 - none	
	Foundation-10	Deployment Plan	deployment plan	0 - none	
Requirer	Requirements-1	Definition of Security Requirements	product-level security goals	0 - none	
			product-level security requirements	0 - none	
	Requirements-2	Requirements Gate	formal gate signoff	0 - none	
Design	Design-1	Take Security Requirements and Risk Information into Account During Software Design	design showing security considerations	0 - none	
	Design-2	Review the Software Design to Verify Compliance with Security Requirements and Risk Information	security design review report	0 - none	
	Design-3	Attack Surface Reduction	attack surface analysis report	0 - none	
	Design-4	Threat Modeling	threat modeling report	0 - none	
			ranked/risked threat report	0 - none	
			threat report	0 - none	
	Design-5	Design Gate	formal gate signoff	0 - none	
Implementation	Implementation-1	Use Approved Tools	list of tools and components used	0 - none	
	Implementation-2	Configure the Compilation and Build Process to Improve Executable Security	build process documentation	0 - none	
	Implementation-3	Configure the Software to Have Secure Settings by Default	secure setting document	0 - none	
	Implementation-4	Reuse Existing, Well-Secured Software When Feasible Instead of Duplicating Functionality	component/version - product/version cross-reference document	0 - none	
	Implementation-5	Create Source Code Adhering to Secure Coding Practice	secure development	0 - none	
	Implementation-6	Deprecate Unsafe Functions	currently used deprecated functions document	0 - none	
	Implementation-7	Static Analysis	static analysis report	0 - none	
	Implementation-8	Dynamic Program Analysis	dynamic analysis report	0 - none	
	Implementation-9	Security Code Review	secure code review summary	0 - none	
	Implementation-10	Fuzz Testing	fuzz testing report	0 - none	
	Implementation-11	Implementation Gate	formal gate signoff	0 - none	
Verification	Verification-1	Penetration Testing	penetration testing report	0 - none	
	Verification-2	Threat Model Review	updated threat model	0 - none	
	Verification-3	Attack Surface Analysis Review	updated attack surface analysis	0 - none	
	Verification-4	Verification Gate	formal gate signoff	0 - none	
Release	Release-1	Final Security Review	final security review report	0 - none	
	Release-2	Archive	archive manifest	0 - none	
	Release-3	Release Gate	formal gate signoff	0 - none	
Operation	Operation-1	Identify and Confirm Vulnerabilities on an Ongoing Basis	cybersecurity incident report	0 - none	
	Operation-2	Assess and Prioritize the Remediation of all Vulnerabilities		0 - none	
	Operation-3	Analyze Vulnerabilities to Identify Their Root Causes		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	Revision	Date	Page
TUVSUD_CybersecurityAssessmentSummary_Motional_AVCDL_v.2.12.docx	Rev 2.12	June 27, 2022	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

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	Revision	Date	Page
TUVSUD_CybersecurityAssessmentSummary_R155_Motional_AVCDL_v.3.1.docx	Rev 3.2	June 13, 2023	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.

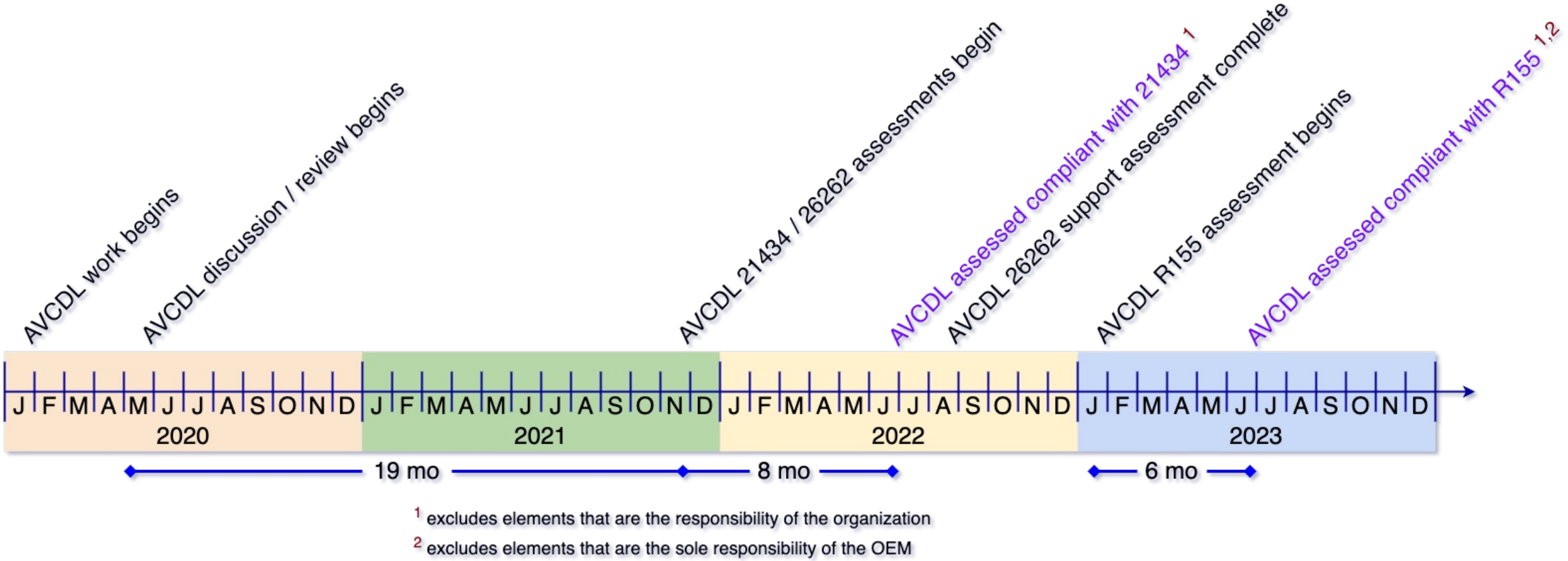
Several requirements were considered out of scope, as they were not applicable to the AVCDL and thus could not be assessed.

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].

Assessment Timeline

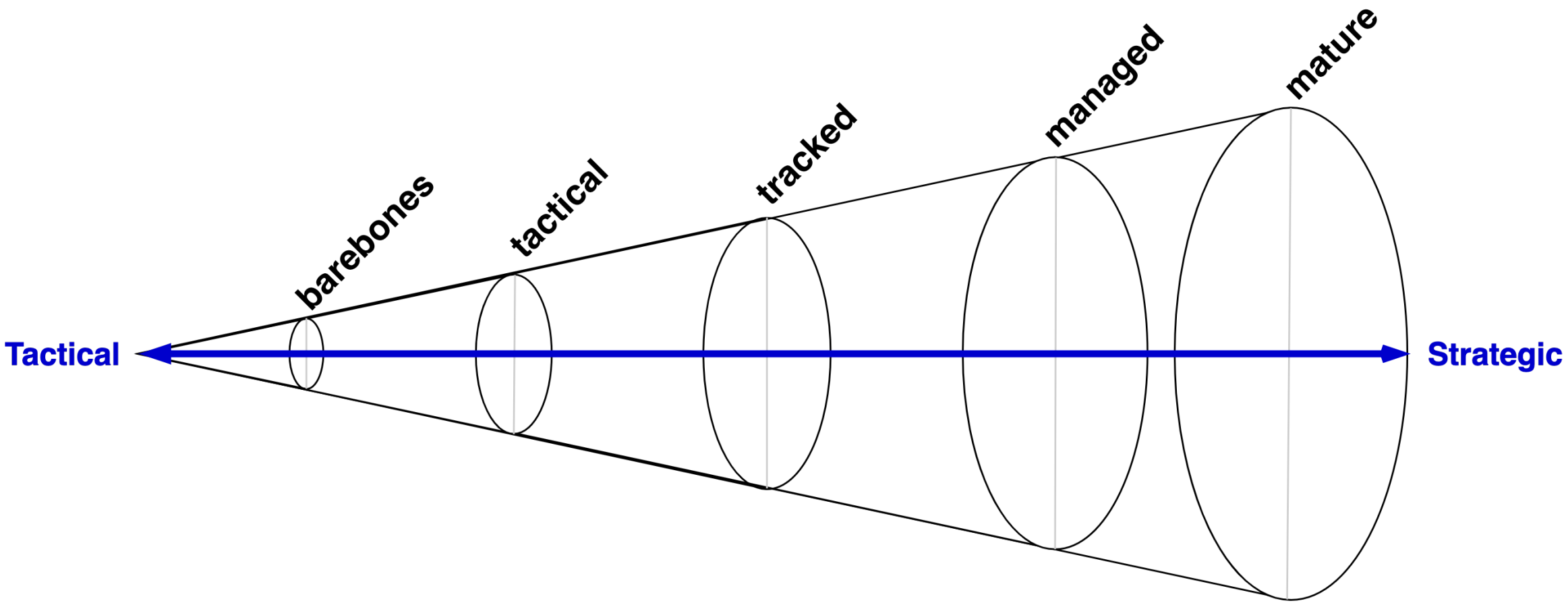


[1] excludes elements that are the responsibility of the organization

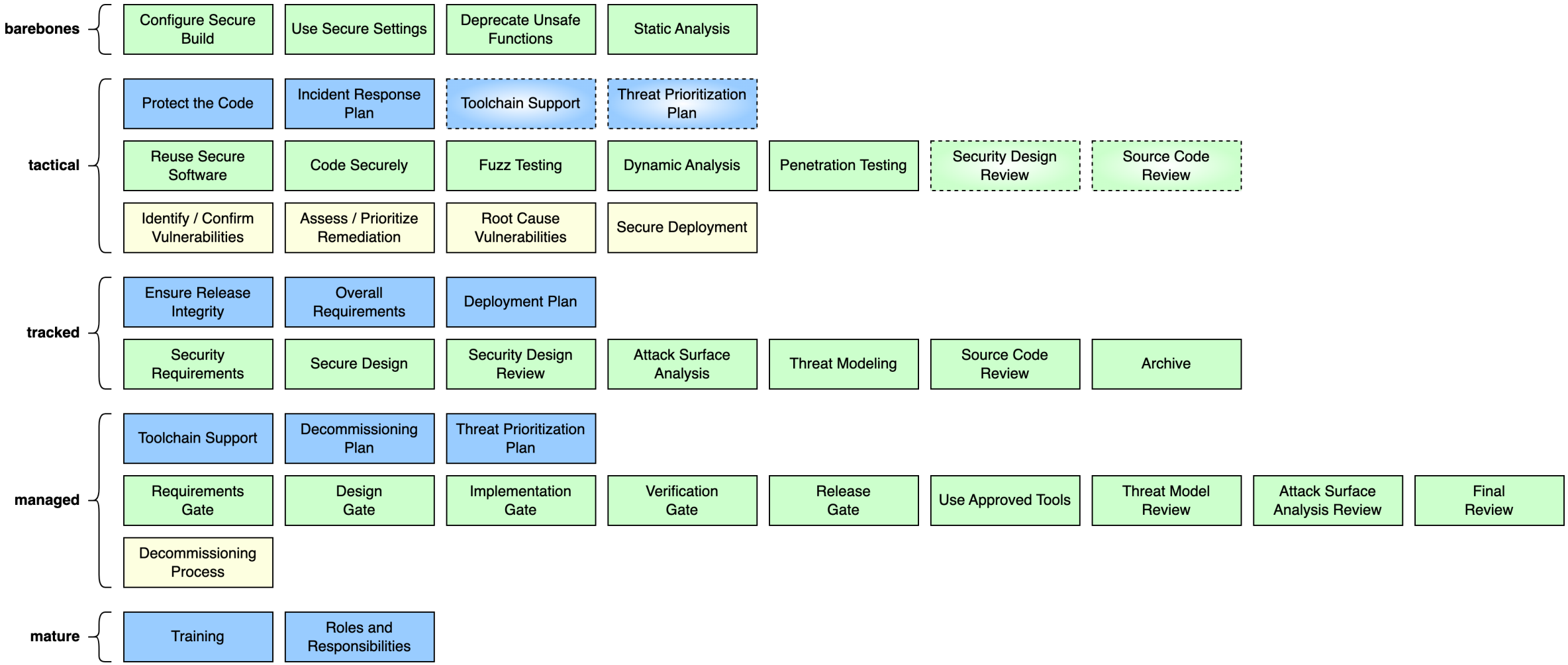
[2] excludes elements that are the sole responsibility of the OEM

Incremental Adoption

Incremental Adoption Spectrum



Prioritized Phase Requirements



Lessons Learned

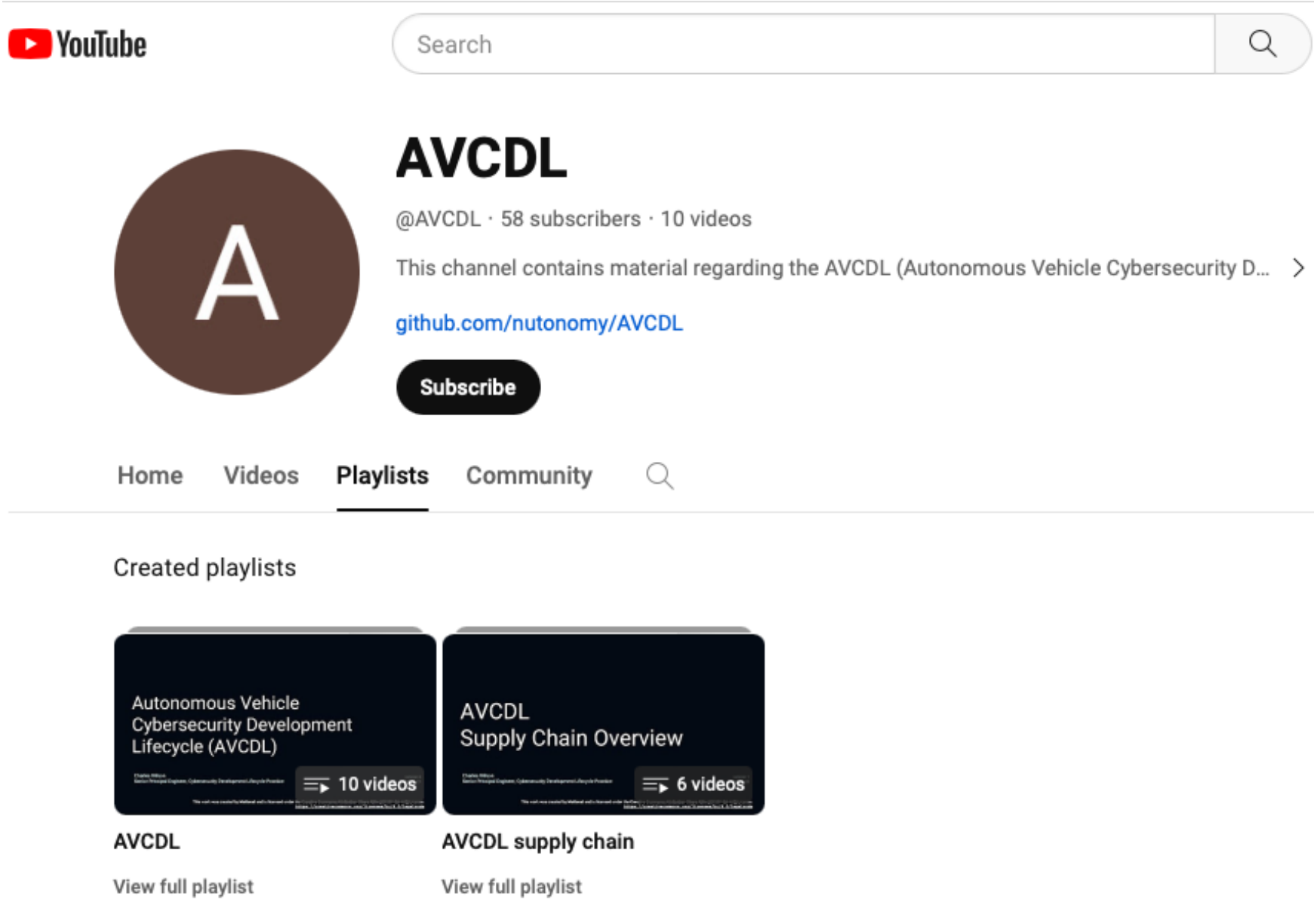
Lessons Learned

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

Learning More

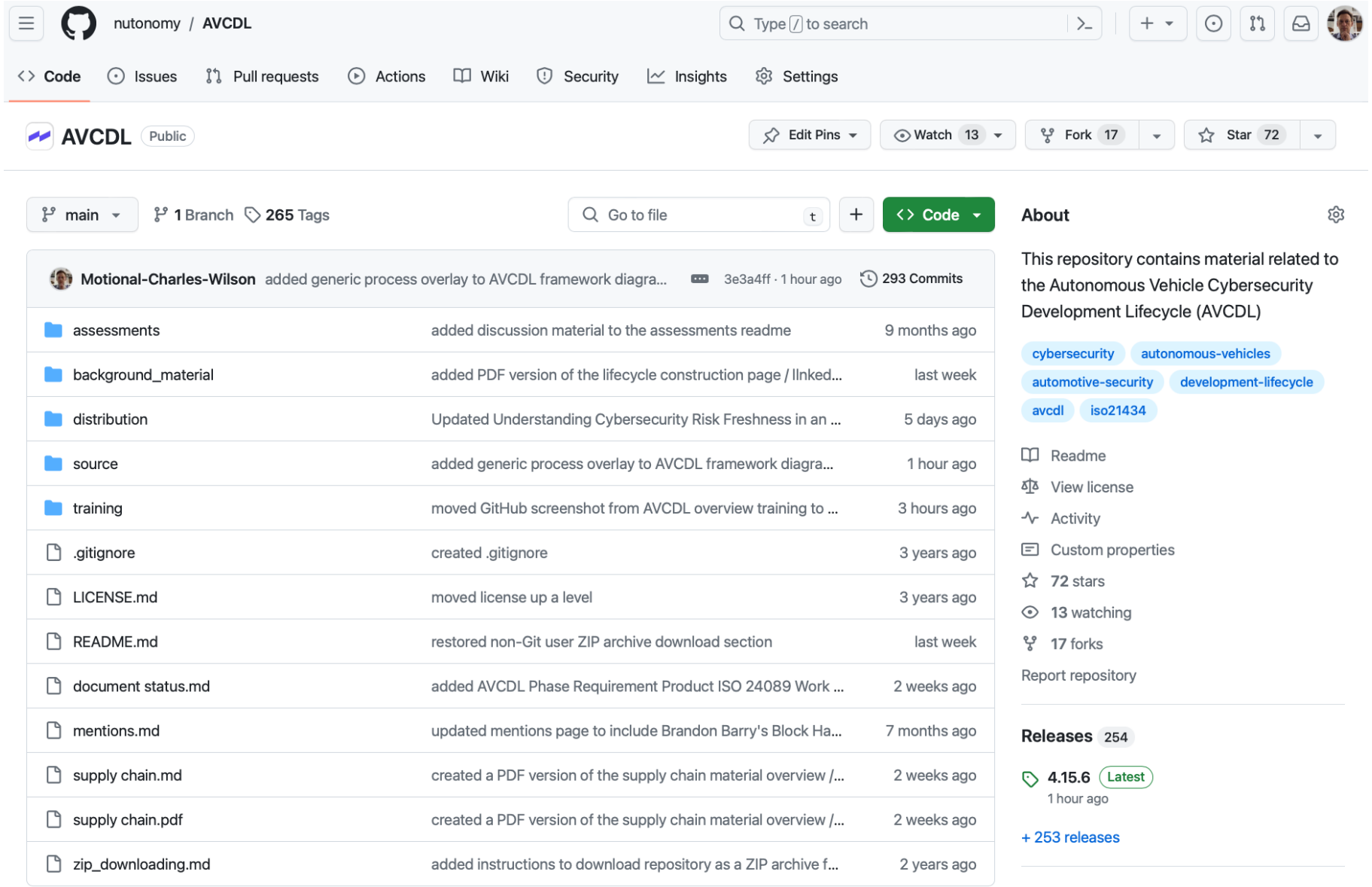
AVCDL on YouTube

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



AVCDL on GitHub

https://github.com/nutonomy/AVCDL



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/Simplified Implementation 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