Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL)

Charles Wilson
Principal Engineer, Cybersecurity Development Lifecycle Practice

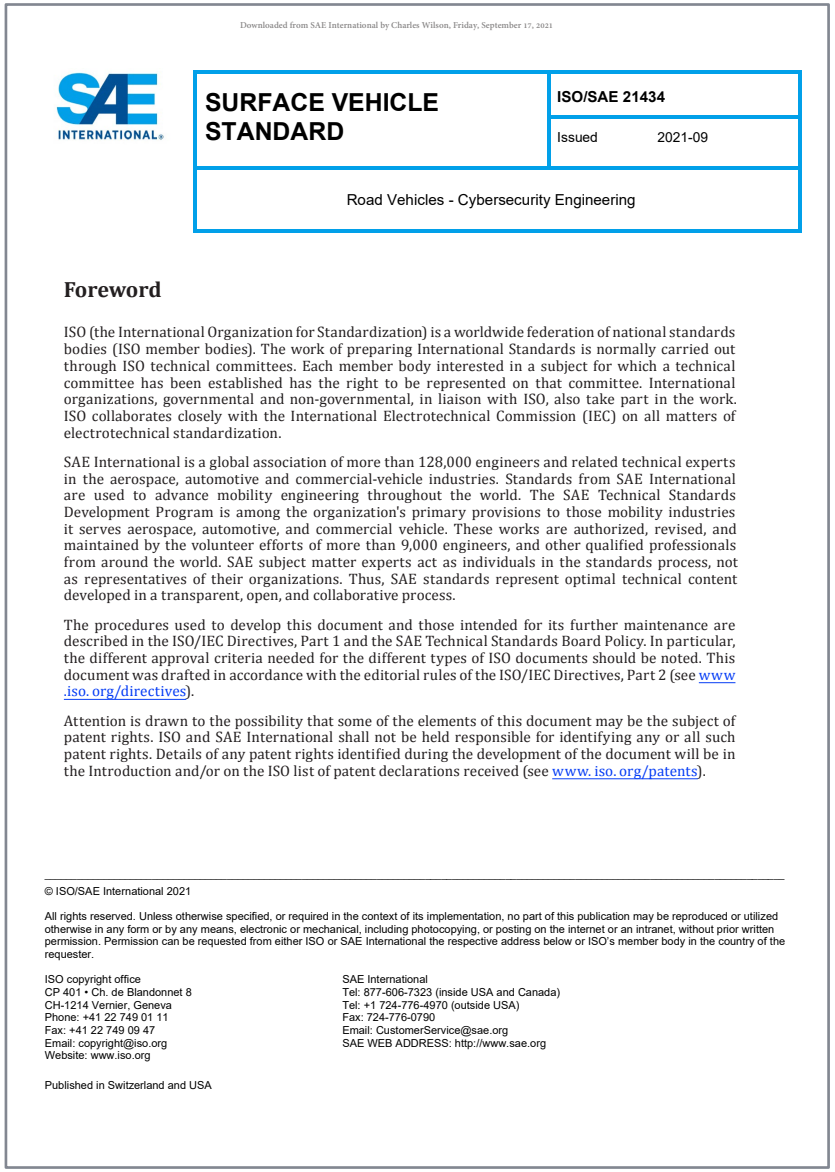
version 4
2022-02-22

Speaker Bio

Charles is a Principal Engineer at Motional responsible for developing their cybersecurity development lifecycle practice. He has over 37 years of professional experience across a broad range of domains including aerospace, publishing, software development, technical illustrations, networking, embedded wireless hardware and software, distributed image scaling, enterprise scale distributed systems, medical devices, and autonomous vehicles. He first worked on security software in 1983. He holds a BSCS (Computer Science), MSEE (Electrical and Computer Engineering), and is CSSLP certified. His masters work in 1992 was in anti-viral computer architecture. He has been threat modeling for over 10 years. Charles has participated on several ISO standards committees. His most recent activities included staffing at the FDA/MITRE/MDIC medical device threat modeling training bootcamps and working on the development ISO/SAE 21434 (Road vehicles — Cybersecurity engineering) and its related standards. He is the vice-chair of the SAE Cybersecurity Maturity Model Task Force (TEVEES18A3). He is the primary author and editor of the Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL).

ISO/SAE 21434 is Here

Road Vehicles – Cybersecurity Engineering



SAE INTERNATIONAL

SURFACE VEHICLE STANDARD	ISO/SAE 21434
	Issued 2021-09
Road Vehicles - Cybersecurity Engineering	

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

SAE International is a global association of more than 128,000 engineers and related technical experts in the aerospace, automotive and commercial-vehicle industries. Standards from SAE International are used to advance mobility engineering throughout the world. The SAE Technical Standards Development Program is among the organization's primary provisions to those mobility industries it serves aerospace, automotive, and commercial vehicle. These works are authorized, revised, and maintained by the volunteer efforts of more than 9,000 engineers, and other qualified professionals from around the world. SAE subject matter experts act as individuals in the standards process, not as representatives of their organizations. Thus, SAE standards represent optimal technical content developed in a transparent, open, and collaborative process.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1 and the SAE Technical Standards Board Policy. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

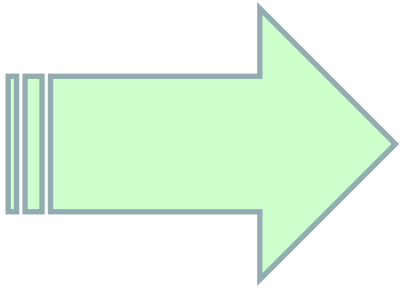
Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and SAE International shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

SAE International
Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org

Published in Switzerland and USA

How Will We Attain Compliance?



SAE INTERNATIONAL

SURFACE VEHICLE STANDARD	ISO/SAE 21434
	Issued 2021-09
Road Vehicles - Cybersecurity Engineering	

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

SAE International is a global association of more than 128,000 engineers and related technical experts in the aerospace, automotive and commercial-vehicle industries. Standards from SAE International are used to advance mobility engineering throughout the world. The SAE Technical Standards Development Program is among the organization's primary provisions to those mobility industries it serves aerospace, automotive, and commercial vehicle. These works are authorized, revised, and maintained by the volunteer efforts of more than 9,000 engineers, and other qualified professionals from around the world. SAE subject matter experts act as individuals in the standards process, not as representatives of their organizations. Thus, SAE standards represent optimal technical content developed in a transparent, open, and collaborative process.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1 and the SAE Technical Standards Board Policy. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and SAE International shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

SAE International
Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org

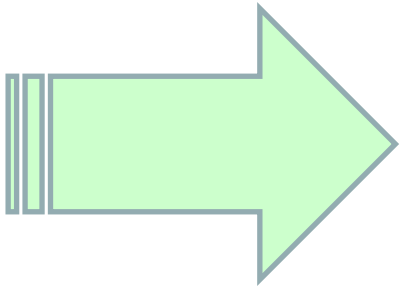
Published in Switzerland and USA

Autonomous Vehicle Cybersecurity Development Lifecycle

Autonomous Vehicle Cybersecurity Development Lifecycle
(*AVCDL*)

Charles Wilson
Principal Engineer, Cybersecurity Development Lifecycle Practice

Version 43
2/8/2022 7:00:00 PM



SAE INTERNATIONAL

SURFACE VEHICLE STANDARD	ISO/SAE 21434
	Issued 2021-09
Road Vehicles - Cybersecurity Engineering	

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

SAE International is a global association of more than 128,000 engineers and related technical experts in the aerospace, automotive and commercial-vehicle industries. Standards from SAE International are used to advance mobility engineering throughout the world. The SAE Technical Standards Development Program is among the organization's primary provisions to those mobility industries it serves aerospace, automotive, and commercial vehicle. These works are authorized, revised, and maintained by the volunteer efforts of more than 9,000 engineers, and other qualified professionals from around the world. SAE subject matter experts act as individuals in the standards process, not as representatives of their organizations. Thus, SAE standards represent optimal technical content developed in a transparent, open, and collaborative process.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1 and the SAE Technical Standards Board Policy. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

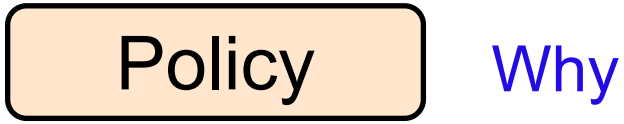
Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and SAE International shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

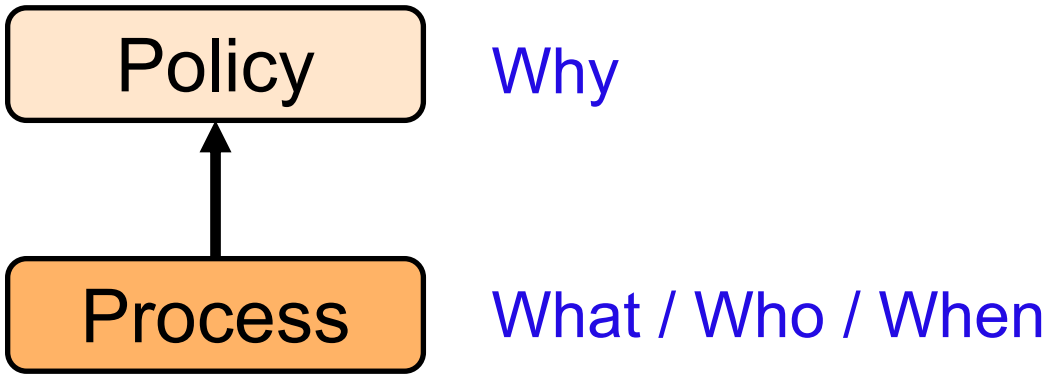
SAE International
Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE WEB ADDRESS: http://www.sae.org

Published in Switzerland and USA

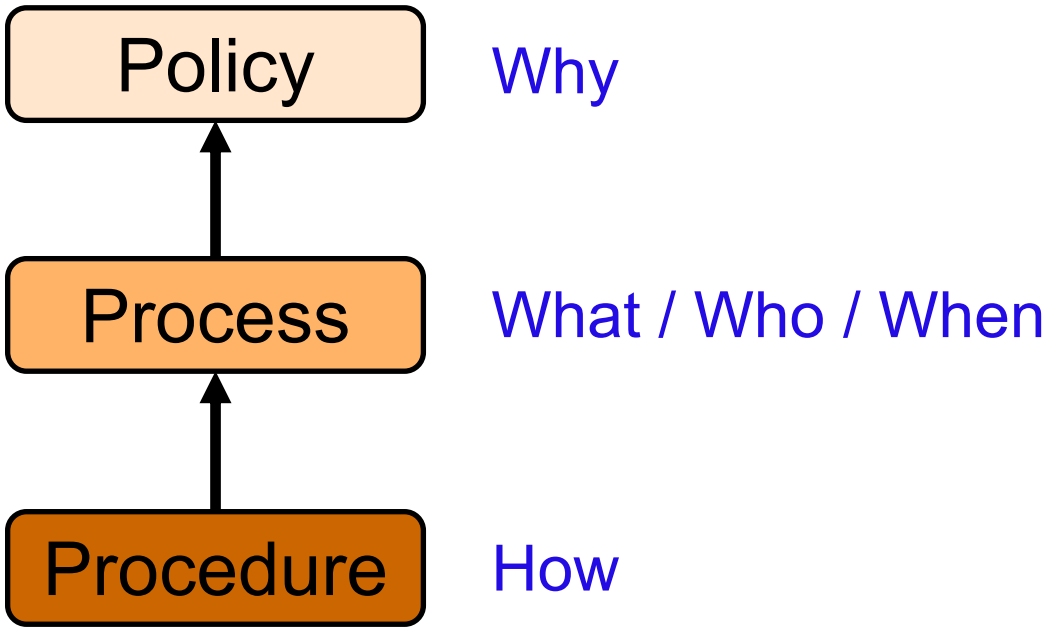
Lifecycle Basics



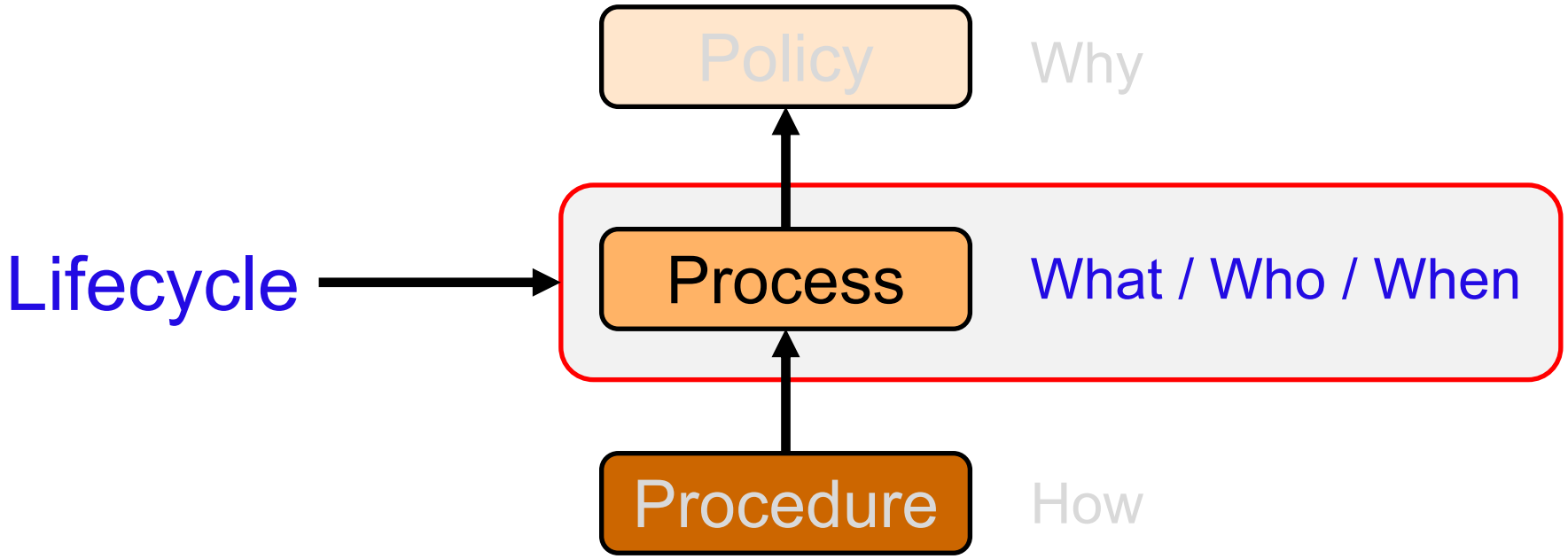
Lifecycle Basics



Lifecycle Basics



Lifecycle Basics



Lifecycles Have Assumptions

ISO 15288	System Development Life Cycle (SDLC)
ISO 12207	Software Development Life Cycle (SDLC)
ISO 26262	Road Vehicles - Functional Safety
ISO 21434	Road Vehicles - Cybersecurity Engineering
UNECE WP.29 R155	Cyber Security Management Systems (CSMS)

How the Standards Line Up

15288 (SDLC system)
technical processes
N/A
requirements definition
requirements analysis
architectural design
implementation
integration
verification
transition
validation
operation
maintenance
disposal
agreement processes

How the Standards Line Up

15288 (SDLC system)	12207 (SDLC software)
technical processes	technical processes
N/A	N/A
requirements definition	requirements definition
requirements analysis	system requirements analysis
architectural design	system architectural design
implementation	implementation
integration	system integration
verification	system qualification testing
transition	software installation
	software acceptance support
validation	
operation	software operation
maintenance	software maintenance
disposal	software disposal
agreement processes	agreement processes

How the Standards Line Up

<table>
<tr><th>15288 (SDLC system)</th><th>12207 (SDLC software)</th><th>26262 (safety)</th></tr>
<tr><td rowspan="2">technical processes</td><td rowspan="2">technical processes</td><td>management of functional safety</td></tr>
<tr><td>supporting processes</td></tr>
<tr><td>N/A</td><td>N/A</td><td>concept phase</td></tr>
<tr><td>requirements definition</td><td>requirements definition</td><td>safety requirements</td></tr>
<tr><td>requirements analysis</td><td>system requirements analysis</td><td>hazard analysis / risk assessment</td></tr>
<tr><td>architectural design</td><td>system architectural design</td><td>architectural design</td></tr>
<tr><td>implementation</td><td>implementation</td><td>implementation</td></tr>
<tr><td>integration</td><td>system integration</td><td rowspan="4">integration and verification</td></tr>
<tr><td>verification</td><td>system qualification testing</td></tr>
<tr><td rowspan="2">transition</td><td>software installation</td></tr>
<tr><td rowspan="2">software acceptance support</td></tr>
<tr><td>validation</td><td>production</td></tr>
<tr><td>operation</td><td>software operation</td><td rowspan="3">operation, service and decommissioning</td></tr>
<tr><td>maintenance</td><td>software maintenance</td></tr>
<tr><td>disposal</td><td>software disposal</td></tr>
<tr><td>agreement processes</td><td>agreement processes</td><td>supporting processes</td></tr>
</table>

How the Standards Line Up

<table>
<tr><th>15288 (SDLC system)</th><th>12207 (SDLC software)</th><th>26262 (safety)</th><th>21434 (cybersecurity)</th></tr>
<tr><td rowspan="2">technical processes</td><td rowspan="2">technical processes</td><td>management of functional safety</td><td>overall cybersecurity management</td></tr>
<tr><td>supporting processes</td><td>project dependent cybersecurity management</td></tr>
<tr><td>N/A</td><td>N/A</td><td>concept phase</td><td>concept</td></tr>
<tr><td>requirements definition</td><td>requirements definition</td><td>safety requirements</td><td>cybersecurity requirements</td></tr>
<tr><td>requirements analysis</td><td>system requirements analysis</td><td>hazard analysis / risk assessment</td><td>cybersecurity assessment</td></tr>
<tr><td>architectural design</td><td>system architectural design</td><td>architectural design</td><td>cybersecurity design</td></tr>
<tr><td>implementation</td><td>implementation</td><td>implementation</td><td>development</td></tr>
<tr><td>integration</td><td>system integration</td><td rowspan="4">integration and verification</td><td rowspan="4">integration and verification</td></tr>
<tr><td>verification</td><td>system qualification testing</td></tr>
<tr><td rowspan="2">transition</td><td>software installation</td></tr>
<tr><td rowspan="2">software acceptance support</td></tr>
<tr><td>validation</td><td>production</td><td>production</td></tr>
<tr><td>operation</td><td>software operation</td><td rowspan="3">operation, service and decommissioning</td><td>continuous cybersecurity activities</td></tr>
<tr><td>maintenance</td><td>software maintenance</td><td>operation and maintenance</td></tr>
<tr><td>disposal</td><td>software disposal</td><td>decommissioning</td></tr>
<tr><td>agreement processes</td><td>agreement processes</td><td>supporting processes</td><td>distributed cybersecurity activities</td></tr>
</table>

How the Standards Line Up

<table>
<tr><th>15288 (SDLC system)</th><th>12207 (SDLC software)</th><th>26262 (safety)</th><th>21434 (cybersecurity)</th></tr>
<tr><td rowspan="2">technical processes</td><td rowspan="2">technical processes</td><td>management of functional safety</td><td>overall cybersecurity management</td></tr>
<tr><td>supporting processes</td><td>project dependent cybersecurity management</td></tr>
<tr><td>N/A</td><td>N/A</td><td>concept phase</td><td>concept</td></tr>
<tr><td>requirements definition</td><td>requirements definition</td><td>safety requirements</td><td>cybersecurity requirements</td></tr>
<tr><td>requirements analysis</td><td>system requirements analysis</td><td>hazard analysis / risk assessment</td><td>cybersecurity assessment</td></tr>
<tr><td>architectural design</td><td>system architectural design</td><td>architectural design</td><td>cybersecurity design</td></tr>
<tr><td>implementation</td><td>implementation</td><td>implementation</td><td>development</td></tr>
<tr><td>integration</td><td>system integration</td><td rowspan="3">integration and verification</td><td rowspan="3">integration and verification</td></tr>
<tr><td>verification</td><td>system qualification testing</td></tr>
<tr><td rowspan="2">transition</td><td>software installation</td></tr>
<tr><td rowspan="2">validation</td><td rowspan="2">software acceptance support</td><td>production</td><td>production</td></tr>
<tr><td>operation</td><td>software operation</td><td rowspan="3">operation, service and decommissioning</td><td>continuous cybersecurity activities</td></tr>
<tr><td>maintenance</td><td>software maintenance</td><td>operation and maintenance</td></tr>
<tr><td>disposal</td><td>software disposal</td><td>decommissioning</td></tr>
<tr><td>agreement processes</td><td>agreement processes</td><td>supporting processes</td><td>distributed cybersecurity activities</td></tr>
</table>

AVPDL – Autonomous Vehicle Product Development Lifecycle

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

AVPDL – Autonomous Vehicle Product Development Lifecycle

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

AVPDL – Governance Processes

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	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

AVPDL – Lifecycle Phases

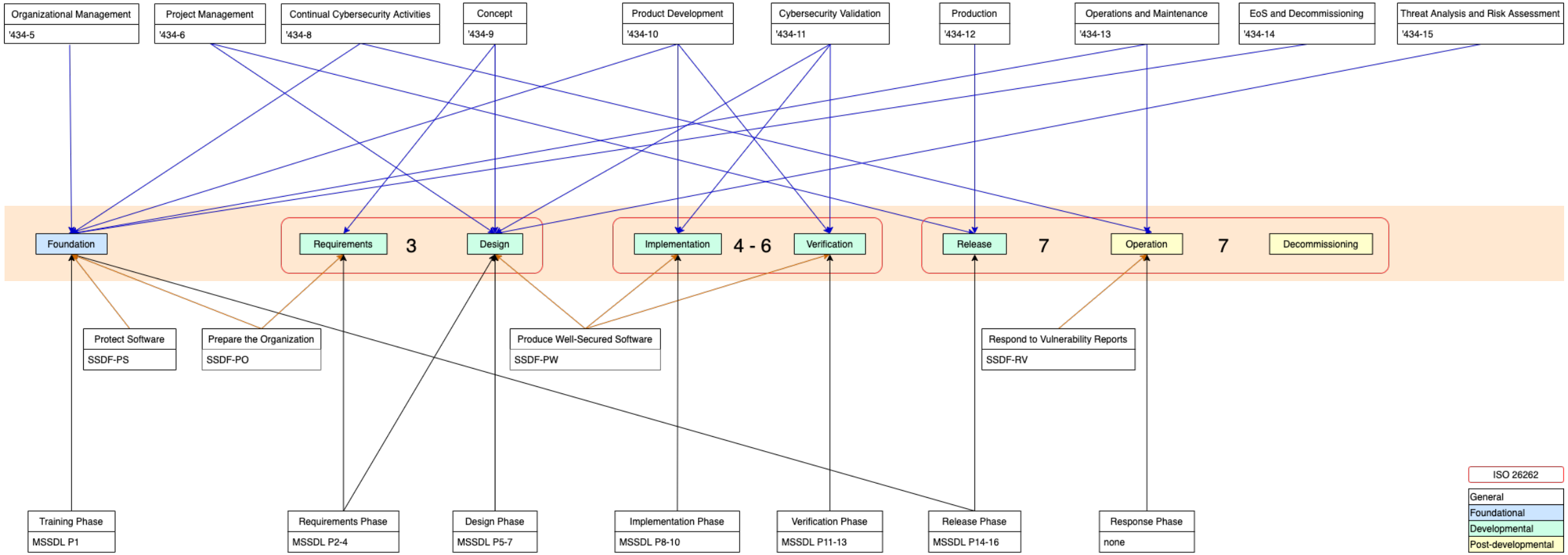
AVPDL	15288 (SDLC system)	12207 (SDLC software)	26262 (safety)	21434 (cybersecurity)
organization processes	technical processes	technical processes	management of functional safety	overall cybersecurity management
			supporting processes	project dependent cybersecurity management
foundation phase	N/A	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	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

ISO 21434 Work Products and Requirements

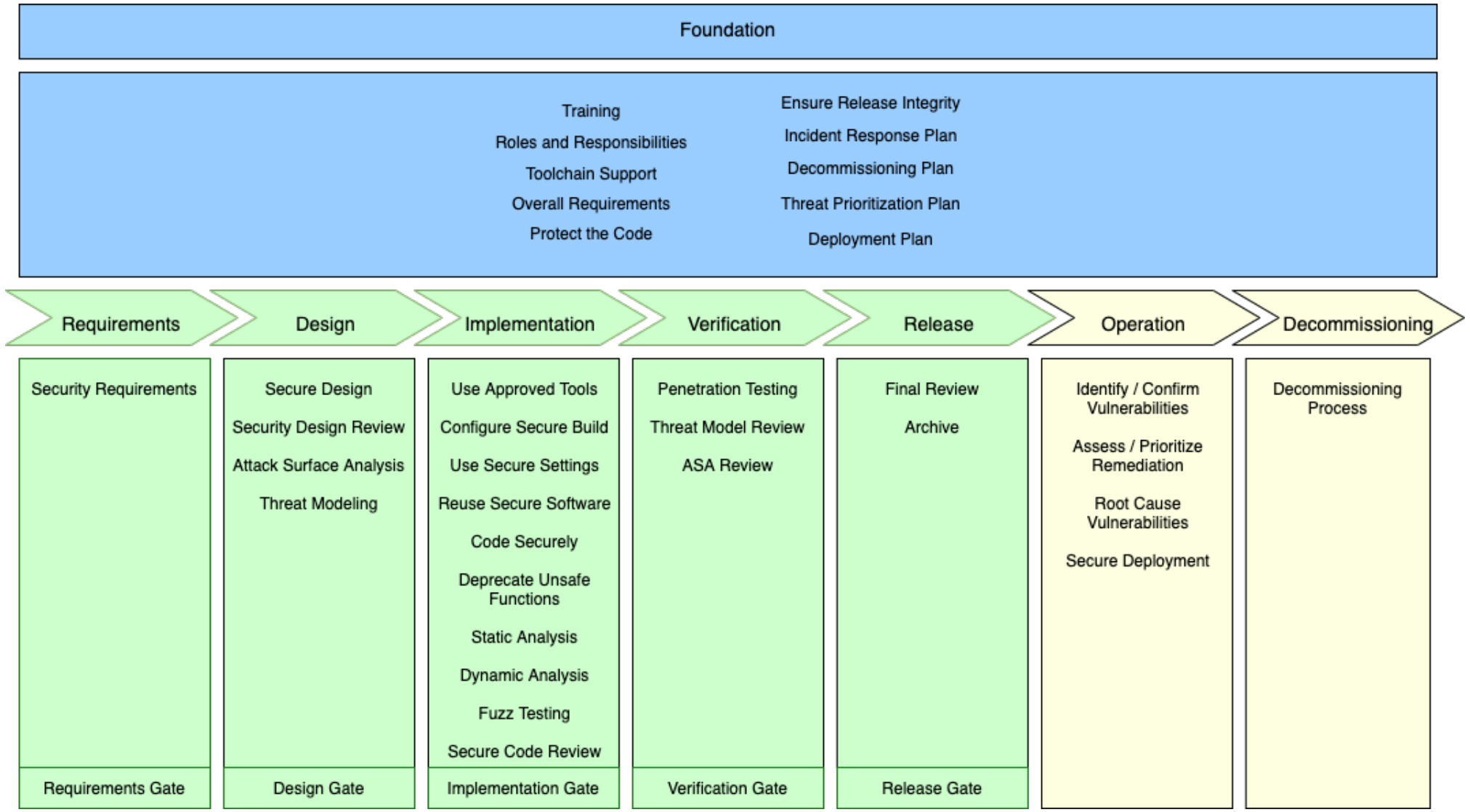
	Activity		AVCDL Phase	Work Product		Dependencies			
Contin Cyberse Activi	8.4	Cybersecurity Event Assessment	operation	WP-08-04	Cybersecurity event assessment	RQ-08-04			
	8.5	Vulnerability Analysis	operation	WP-08-05	Vulnerability analysis	RQ-08-05	RQ-08-06		
	8.6	Vulnerability Management	design	WP-08-06	Vulnerability management	RQ-08-07			
			design	WP-08-X1	Apply incident response protocols	RQ-08-08			
Concept and Product Development Phases									
Concept	9.3	Item Definition	requirements	WP-09-01	Item definition	RQ-09-01	RQ-09-02		
	9.4	Cybersecurity Goals	design	WP-09-02	Threat analysis and risk assessment	RQ-09-03	RQ-09-04		
			design	WP-09-03	Cybersecurity goals	RQ-09-05			
			design	WP-09-04	Cybersecurity claims	RQ-09-06			
			design	WP-09-05	Verification report	RQ-09-07			
	9.5	Cybersecurity Concept	design	WP-09-06	Cybersecurity concept	RQ-09-08	RQ-09-09	RQ-09-10	
			design	WP-09-07	Verification report of cybersecurity concept	RQ-09-11			
Product Development, Cybersecurity Validation	10.4.1	Refinement of Cybersecurity Requirements and Architectural Design	design	WP-10-01	Refined cybersecurity specification	RQ-10-01	RQ-10-02		
			requirements	WP-10-02	Cybersecurity requirements for post-development	RQ-10-03			
			foundation	WP-10-03	Documentation of the modelling, design, or programming languages and coding guidelines	RQ-10-04	RQ-10-05		
			verification	WP-10-04	Verification report for the refined cybersecurity specification	RQ-10-08			
	10.4.2	Integration and Verification	verification	WP-10-05	Vulnerability analysis report	RQ-10-07	RC-10-12	RQ-10-13	
			implementation	WP-10-06	Integration and verification specification	RQ-10-10			
			implementation	WP-10-07	Integration and verification reports	RQ-10-09	RQ-10-11	RC-10-12	RQ-10-13
	11.0	Cybersecurity Validation of the Item at Vehicle Level	verification	WP-11-01	Validation report	RQ-11-01	RQ-11-02		
Post-Development Phases									
Production, Operations and Maintenance, End of	12.0	Production	foundation	WP-12-01	Production control plan	RQ-12-01	RQ-12-02		
			operation	WP-12-X1	Production control plan implementation	RQ-12-03			
	13.3	Cybersecurity Incident Response	foundation	WP-13-01	Cybersecurity incident response plan	RQ-13-01			
			operation	WP-13-X1	Cybersecurity incident response plan implementation	RQ-13-02			
	13.4	Updates	operation	WP-13-X2	Update plan	RQ-13-03			
	14.3	End of Cybersecurity Support	foundation	WP-14-01	Procedures to communicate end of cybersecurity support	RQ-14-01			
	14.4	Decommissioning	foundation	WP-14-X1	Decommissioning implications	RQ-14-02			
Threat Analysis and Risk Assessment Methods									
Threat Analysis and Risk Assessment Methods	15.3	Asset Identification	design	WP-15-01	Damage scenarios	RQ-15-01			
			design	WP-15-02	Identified assets and cybersecurity properties	RQ-15-02			
	15.4	Threat Scenario Identification	design	WP-15-03	Threat scenarios	RQ-15-03			
	15.5	Impact Rating	design	WP-15-04	Impact rating, including the associated impact categories of the damage scenarios	RQ-15-04	RQ-15-05	RQ-15-06	
	15.6	Attack Path Analysis	design	WP-15-05	Identified attack paths	RQ-15-08	RQ-15-09		
	15.7	Attack Feasibility Rating	design	WP-15-06	Attack feasibility rating	RQ-15-10			
	15.8	Risk Determination	design	WP-15-07	Risk values	RQ-15-15	RQ-15-16		
	15.9	Risk Treatment Decision	design	WP-15-08	Risk treatment decision per threat scenario	RQ-15-17			

Reference Sources

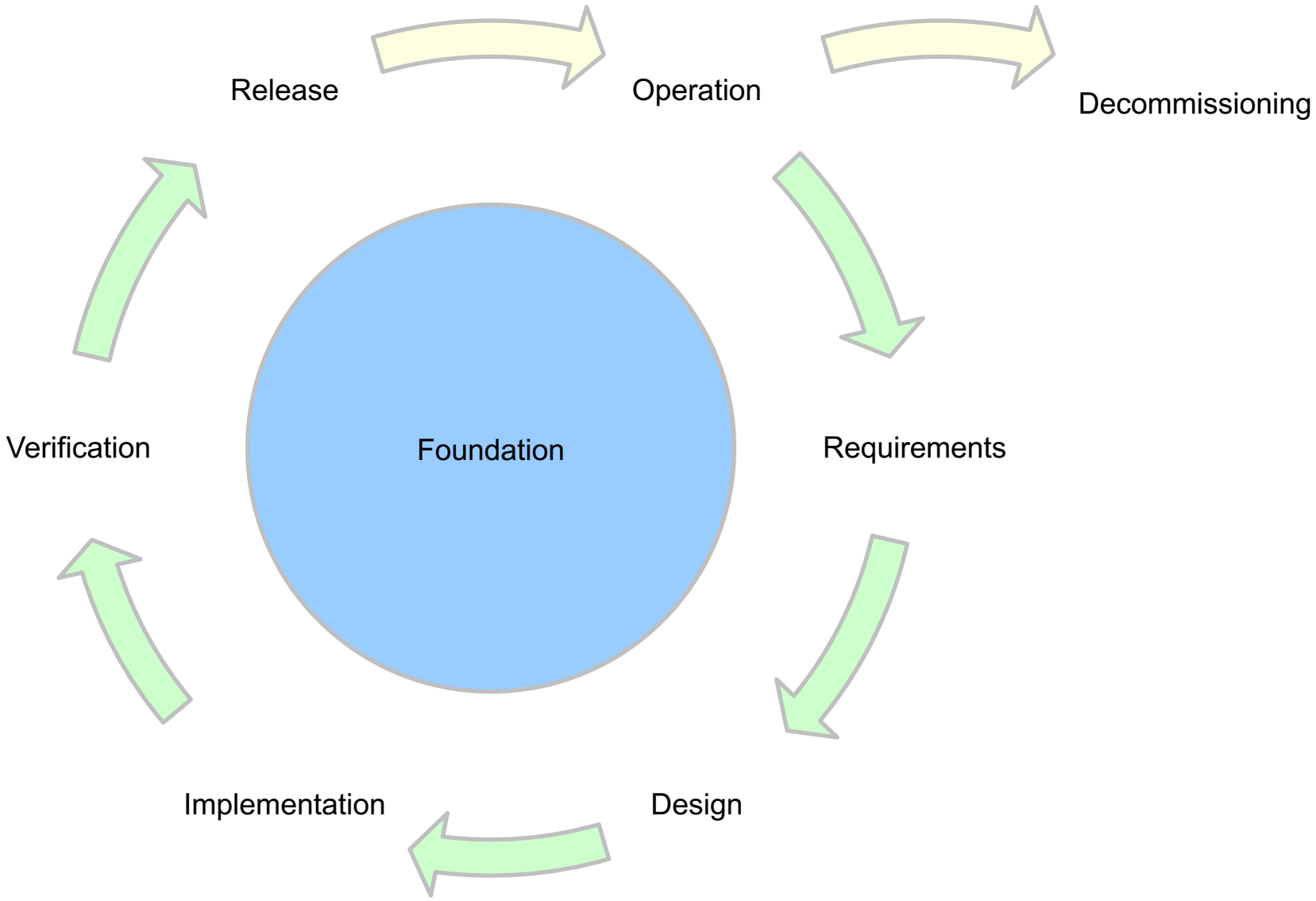
How Standards Inform the AVCDL



Phases and Requirements



Cyclic View


Release
Operation
Decommissioning
Verification
Foundation
Requirements
Implementation
Design

Compliance to Standards

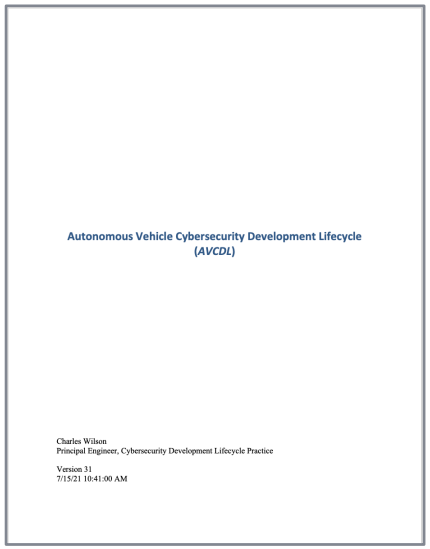
AVCDL phase	AVCDL requirement	Title	WP-05-01	WP-05-02	WP-05-03	WP-05-04	WP-05-05	WP-06-01	WP-06-02	WP-06-03	WP-06-04	WP-07-X1	WP-07-X2	WP-07-01	WP-08-01	WP-08-02	WP-08-03	WP-08-04	WP-08-05	WP-08-06	WP-08-X1	WP-09-01	WP-09-02	WP-09-03	WP-09-04	WP-09-05	WP-09-06	WP-09-07	WP-10-01	WP-10-02	WP-10-03	WP-10-04	WP-10-05	WP-10-06	WP-10-07	WP-11-01	WP-12-01	WP-12-X1	WP-13-01	WP-13-X1	WP-13-X2	WP-14-01	WP-14-X1	WP-15-01	WP-15-02	WP-15-03	WP-15-04	WP-15-05	WP-15-06	WP-15-07	WP-15-08
Foundation	1	Training																																																
	2	Roles and Responsibilities																																																
	3	Toolchain Support				X																								X																		
	4	Definition of Security Requirements																																															
	5	Protect the Code																																															
	6	Ensure Release Integrity																																			X												
	7	Incident Response Plan													X	X	X																					X											
	8	Decommissioning Plan																																							X	X							
	9	Threat Prioritization Plan																		X																													
	10	Deployment Plan																																			X					X							
Requi	1	Security Requirements Definition																				X								X																		
	2	Requirements Gate																																															
Design	1	Apply Security Requirements and Risk Information to Design																								X		X																	X					
	2	Security Design Review								X															X		X																						
	3	Attack Surface Reduction																																															
	4	Threat Modeling																					X	X	X																				X		X	X	X	X	X	X
	5	Design Gate																																															
Implementation	1	Use Approved Tools				X																																										
	2	Configure the Compilation and Build Process to Improve Executable Security																																															
	3	Use Secure Settings by Default																																															
	4	Reuse Existing, Well-Secured Software When Feasible Instead of Duplicating Functionality																																															
	5	Code Securely																																															
	6	Deprecate Unsafe Functions																																															
	7	Static Analysis																																															
	8	Dynamic Program Analysis																																															
	9	Security Code Review																																															
	10	Fuzz Testing																																															
	11	Implementation Gate																																		X													
Verification	1	Penetration Testing																																	X													
	2	Threat Model Review																													X	X	X														
	3	Attack Surface Analysis Review																													X	X	X														
	4	Verification Gate																																	X	X												
ase	1	Final Security Review									X																																						

Requirements / Roles / RACI / Dependent Inputs

				group				inputs			
AVCDL phase	requirement	Title	NCWF role	security	devops	development	risk	security	devops	development	risk
Foundation	1	Training	cyber instructor	R	I	C	I	training subjects		list of programming languages / compilers	
	2	Roles and Responsibilities	systems requirements planner	R	C	C		list of phase requirements			
	3	Toolchain Support	information systems security developer	C	R	C		list of security tools / tool security criteria	component tracking system	list of development tools	
	4	Definition of Security Requirements	systems requirements planner	R	I	I		global security goals / security taxonomy			
	5	Protect the Code	information systems security developer	C	R			secure IP handling	secure IT infrastructure		
	6	Ensure Release Integrity	information systems security developer	C	R	C		secure credential management recommendations	code signing / credential management / deployment infrastructure	credentials needed / integrity check availability	
	7	Incident Response Plan	partner integration planner	R		C		incident tracking system		triage information required	
	8	Decommissioning Plan	partner integration planner	R	C	C		secure wipe process	decommissioning / RMA process	list of data stored on systems	
	9	Threat Prioritization Plan	systems requirements planner	R		I	I				
	10	Deployment Plan	information systems security developer	C	R	C		secure deployment recommendations	deployment infrastructure / process	list material to be deployed	
	11	Fuzz Testing Plan	Vulnerability Assessment Analyst	R	C	C					
Requi	1	Security Requirements Definition	security architect	R		I		product security goals / security taxonomy		high-level design / high-level requirements	
	2	Requirements Gate	secure software assessor	R		R		all phase requirement products			
Design	1	Apply Security Requirements and Risk Information to Design	software developer	R		R		security requirements catalog		detailed functional requirements	
	2	Security Design Review	systems requirements planner	R		R	C			element detailed design	
	3	Attack Surface Reduction	security architect	R		R				functional OS interface design	
	4	Threat Modeling	security architect	R		R	R			element detailed design	
	5	Design Gate	secure software assessor	R		R	R	all phase requirement products			
Implementation	1	Use Approved Tools	software developer	C	C	R		tool selection criteria	component tracking comparison system	list of tools used	
	2	Configure the Compilation and Build Process to Improve Executable Security	information systems security developer	C	R	C		secure build setting recommendations	build system	list of adopted secure build settings	
	3	Use Secure Settings by Default	security architect	R		R		secure configuration recommendations		element detailed design	
	4	Reuse Existing, Well-Secured Software When Feasible Instead of Duplicating Functionality	software developer	C	I	R				list of libraries used	
	5	Create Source Code Adhering to Secure Coding Practice	software developer	C		R		secure coding recommendations		element implementation	
	6	Deprecate Unsafe Functions	software developer	C		R		list of unsafe functions		list of deprecated functions in use	
	7	Static Analysis	information systems security developer	C	R	C		secure static analysis setting recommendations	static analysis infrastructure / settings tracking	list of adopted security-related settings	
	8	Dynamic Program Analysis	software developer	C		R		secure dynamic analysis tool recommendations	dynamic analysis testing infrastructure	list of adopted security-related tools	
	9	Security Code Review	secure software assessor	R		C			code review infrastructure	element implementation	
	10	Fuzz Testing	Vulnerability Assessment Analyst	R	C	C		fuzz testing recommendations	fuzz testing process infrastructure	element implementation	
	11	Implementation Gate	secure software assessor	R	R	R		all phase requirement products			
Verification	1	Penetration Testing	Vulnerability Assessment Analyst	R	C	C			penetration testing process infrastructure	operational system	
	2	Threat Model Review	security architect	R		R	R			updated element detailed design	
	3	Attack Surface Analysis Review	security architect	R		R				updated functional OS interface design	
	4	Verification Gate	secure software assessor	R		R	R	all phase requirement products			
Release	1	Final Security Review	secure software assessor	R	C	C	C			final design documentation	
	2	Archive	information systems security developer		R	C			artifact storage infrastructure / tracking system	final materials for deployment	
	3	Release Gate	secure software assessor	R	R	R	R	all phase requirement products			
Operation	1	Identify and Confirm Vulnerabilities on an Ongoing Basis	Cyber Defense Forensics Analyst	R		C		incident tracking system		element detailed design	
	2	Assess and Prioritize the Remediation of all Vulnerabilities	Cyber Defense Forensics Analyst	R		C	C	incident tracking system			
	3	Analyze Vulnerabilities to Identify Their Root Causes	Cyber Defense Forensics Analyst	R		C		incident tracking system		element implementation	
	4	Secure Deployment	information systems security developer	C	R	C		secure deployment recommendations	deployment infrastructure / process	materials for deployment	
De	1	Apply Decommissioning Protocol	information systems security developer	I	R			secure wipe process	decommissioning / RMA process	list of data stored on systems	

AVCDL Document Set

Process Overview (primary)

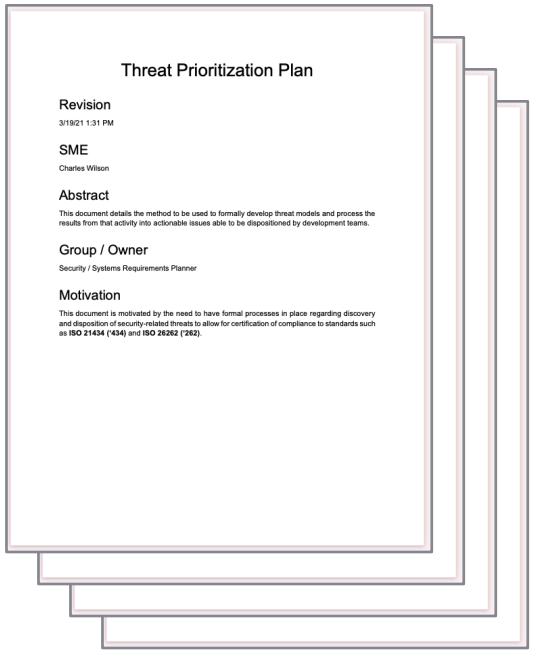


Autonomous Vehicle Cybersecurity Development Lifecycle
(*AVCDL*)

Charles Wilson
Principal Engineer, Cybersecurity Development Lifecycle Practice

Version 31
7/15/21 10:41:00 AM

Process Detail (secondary)



Threat Prioritization Plan

Revision
3/19/21 1:31 PM

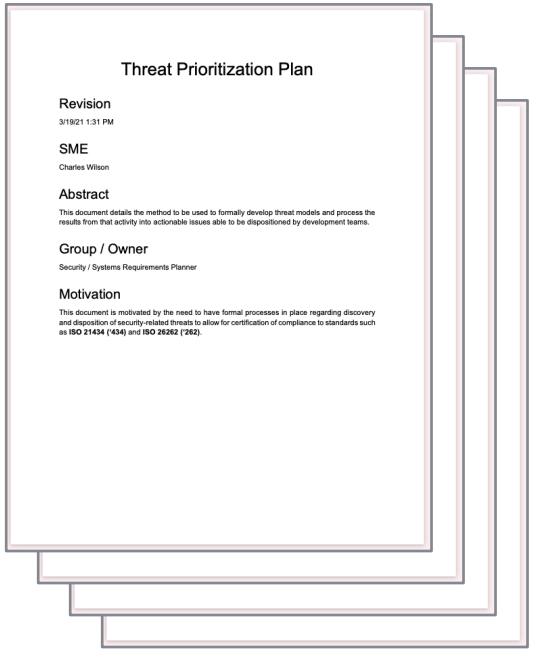
SME
Charles Wilson

Abstract
This document details the method to be used to formally develop threat models and process the results from that activity into actionable issues able to be dispositioned by development teams.

Group / Owner
Security / Systems Requirements Planner

Motivation
This document is motivated by the need to have formal processes in place regarding discovery and disposition of security-related threats to allow for certification of compliance to standards such as **ISO 21434 ('434)** and **ISO 26262 ('262)**.

Procedure (tertiary)



Threat Prioritization Plan

Revision
3/19/21 1:31 PM

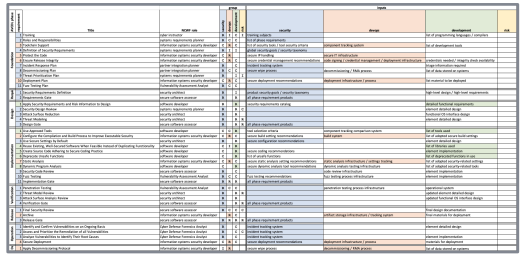
SME
Charles Wilson

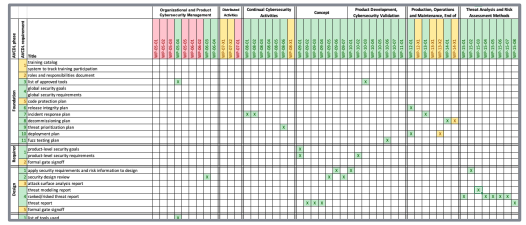
Abstract
This document details the method to be used to formally develop threat models and process the results from that activity into actionable issues able to be dispositioned by development teams.

Group / Owner
Security / Systems Requirements Planner

Motivation
This document is motivated by the need to have formal processes in place regarding discovery and disposition of security-related threats to allow for certification of compliance to standards such as **ISO 21434 ('434)** and **ISO 26262 ('262)**.

Supporting Material





What / Who / When
(company agnostic)

How
(company specific)

Phase Requirement Page Sample (1 of 2)

1 9.3.4 Threat Modeling [AVCDL-Design-4]

2 Owner

Group: Security

NCWF Role: Security Architect

3 Administration

security	devops	development	risk
R	-	R	R

4 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**.

5 Training Provided

yes

6 Phase Requirement Dependencies

[AVCDL-Foundation-9] Threat Prioritization Plan
[AVCDL-Design-1] Apply Security Requirements and Risk Information to Design

7 External Group Product Dependencies

Group	Inputs
Devops	**none**
Development	Element detailed design
Risk	**none**

Item	Section	Description
1	Title	The title of the phase requirements and its ID. Each AVCDL phase requirement has a unique ID comprised of 'AVCDL', the phase (here 'requirements') and a sequence number.
2	Owner Group / Role	The group accountable for the activity and the NCWF role. These link to a summary of the particular group's accountable phase requirements and the NIST SP 800-181 workforce job description.
3	RACI	RACI information for the various groups possibly involved in the activity
4	Description	A general description of the activity and its application
5	Training	Whether training is provided for the activity
6	Internal Dependencies	Predecessor AVCDL phase requirements
7	External Dependencies	Non-security group dependent materials

Phase Requirement Page Sample (2 of 2)

(8) AVCDL Products

- Threat Modeling Report
- Ranked / Risked Threat Report
- Threat Report

(9) 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

(10) WP.29 CSMS Requirements

[7.2.2.2(b)] The processes used for the identification of risks to vehicle types. Within these processes, the threats in Annex 5, Part A, and other relevant threats shall be considered.

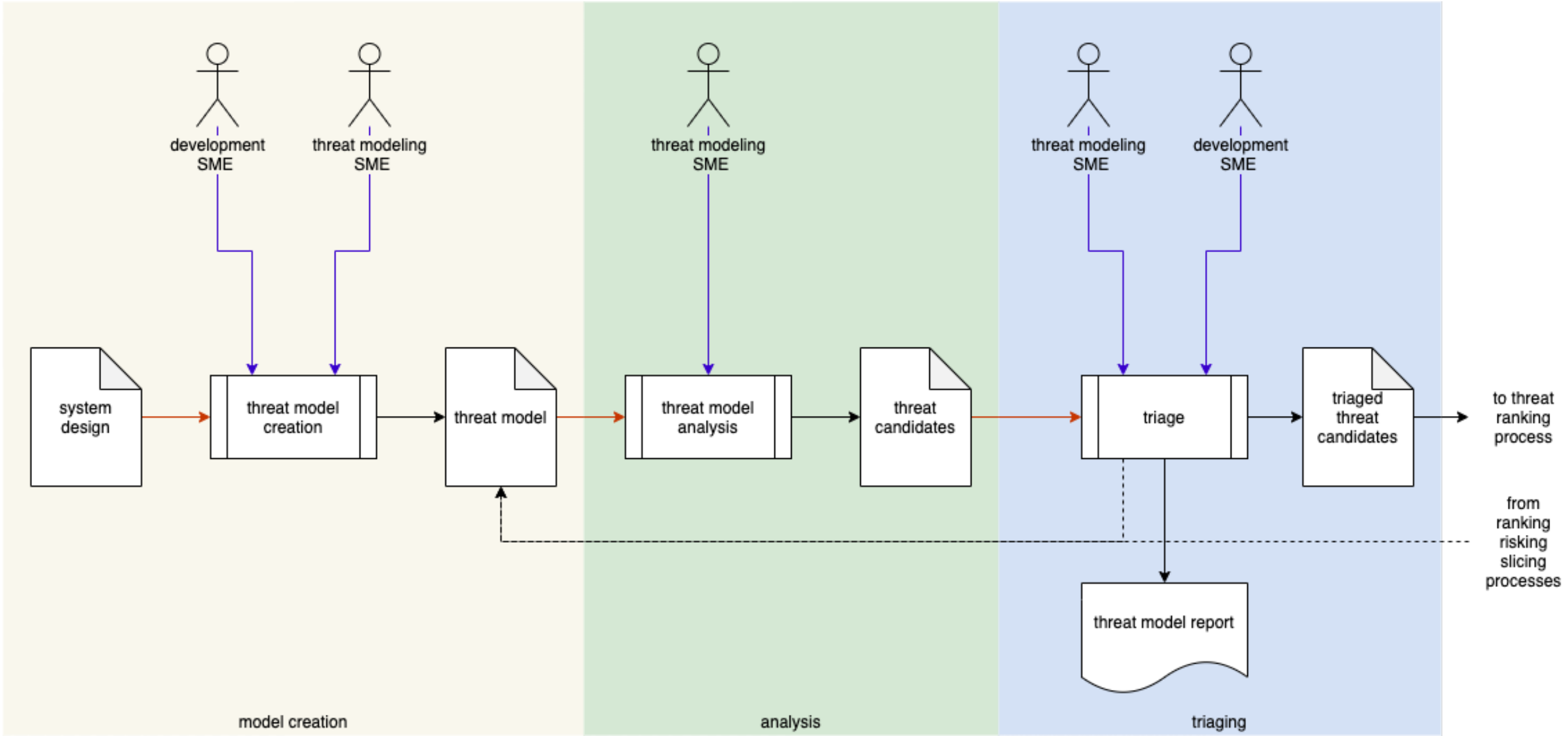
[7.2.2.2(c)] The processes used for the assessment, categorization and treatment of the risks identified.

(11) CMMC Applicable Practices

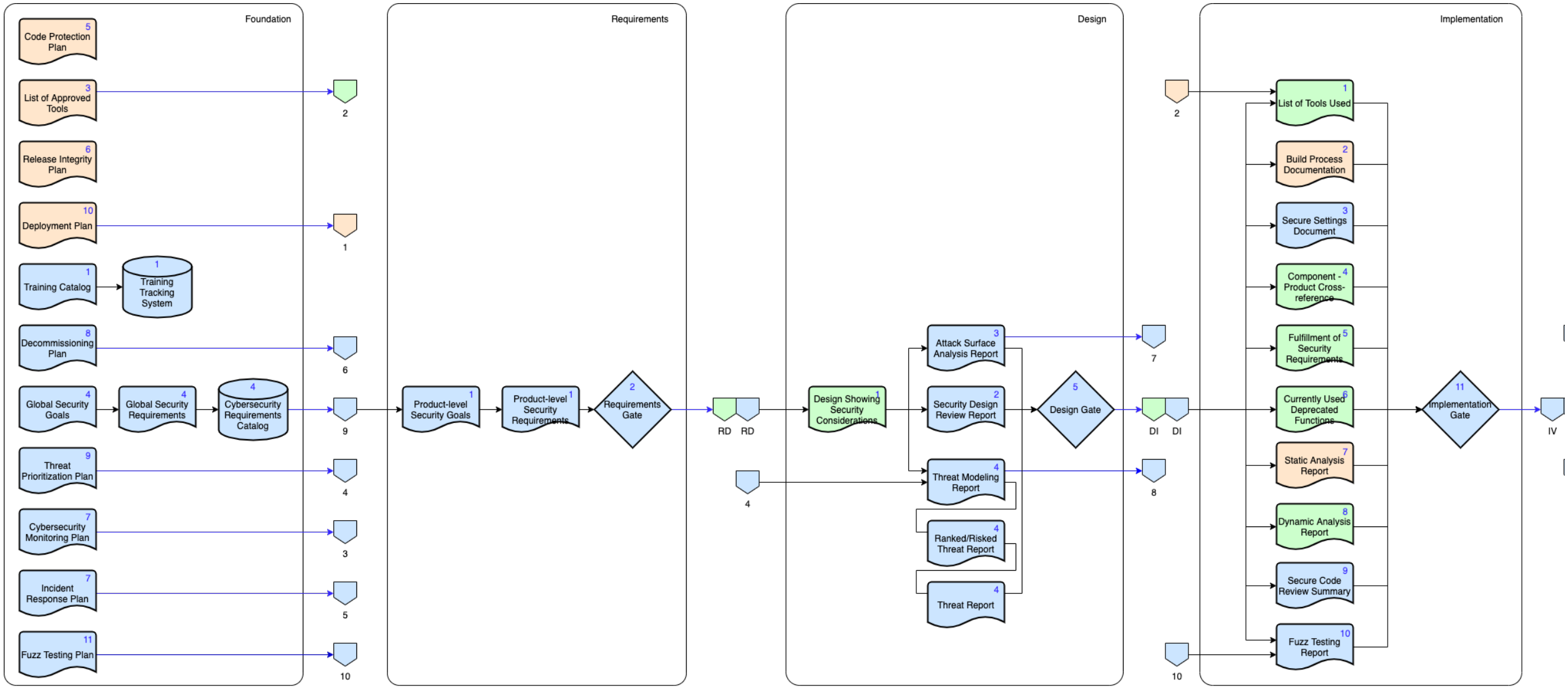
Level	Practice
1	**none**
2	RM.2.143
3	AU.3.049, AU.3.052, RM.3.144
4	**none**
5	AU.5.055

Item	Section	Description
(8)	Phase Products	Products created as a result of the activity. These are linked to secondary documents providing more specific information into the process needed to create them.
(9)	21434 Work Products	Specific **ISO 21434** work products / requirements satisfied by the activity.
(10)	WP.29 Requirements	Specific **WP.29 CSMS (R155)** requirements satisfied by the activity.
(11)	CMMC Practices	CMMC best practices applicable to the activity.

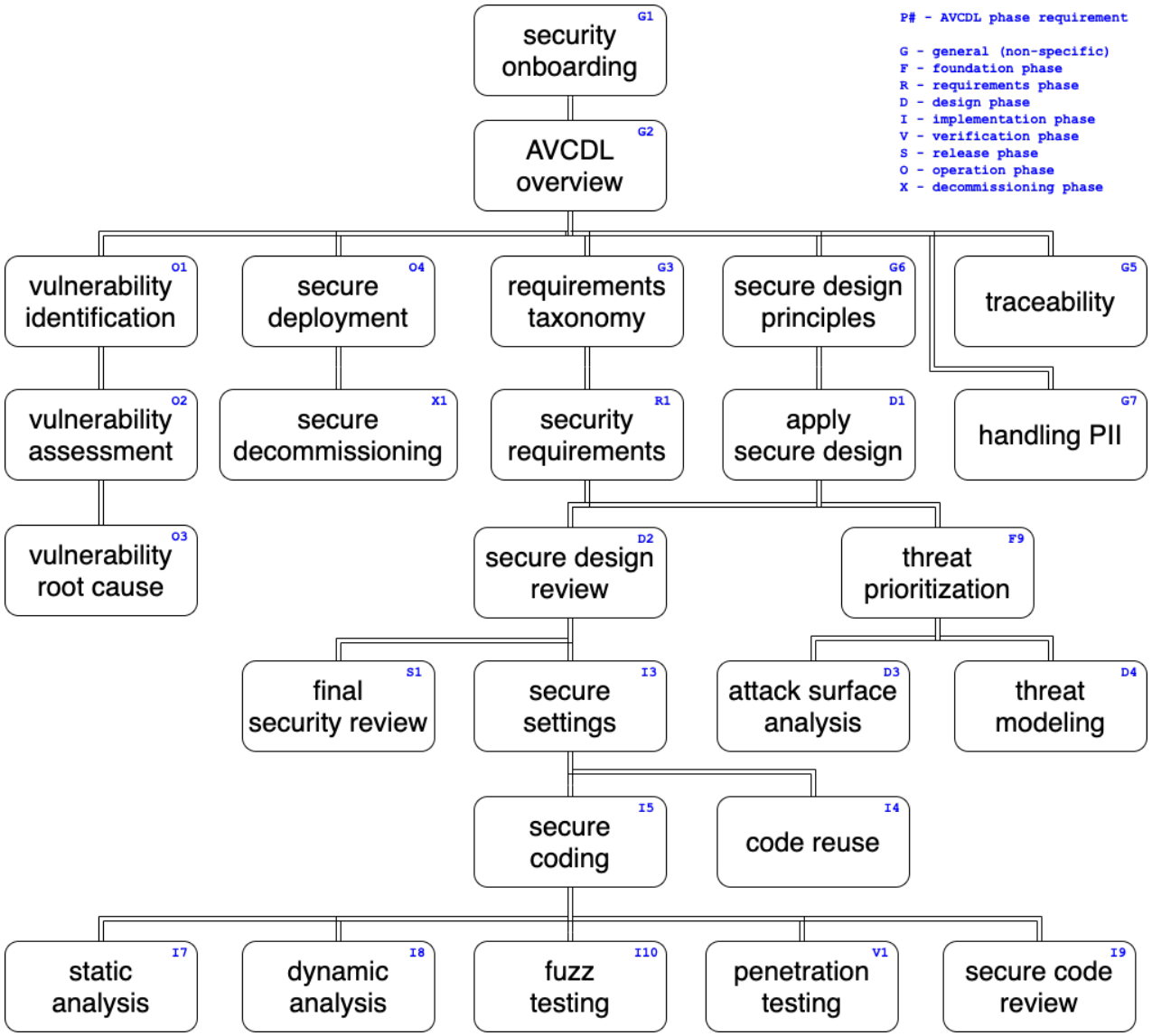
Process Flows



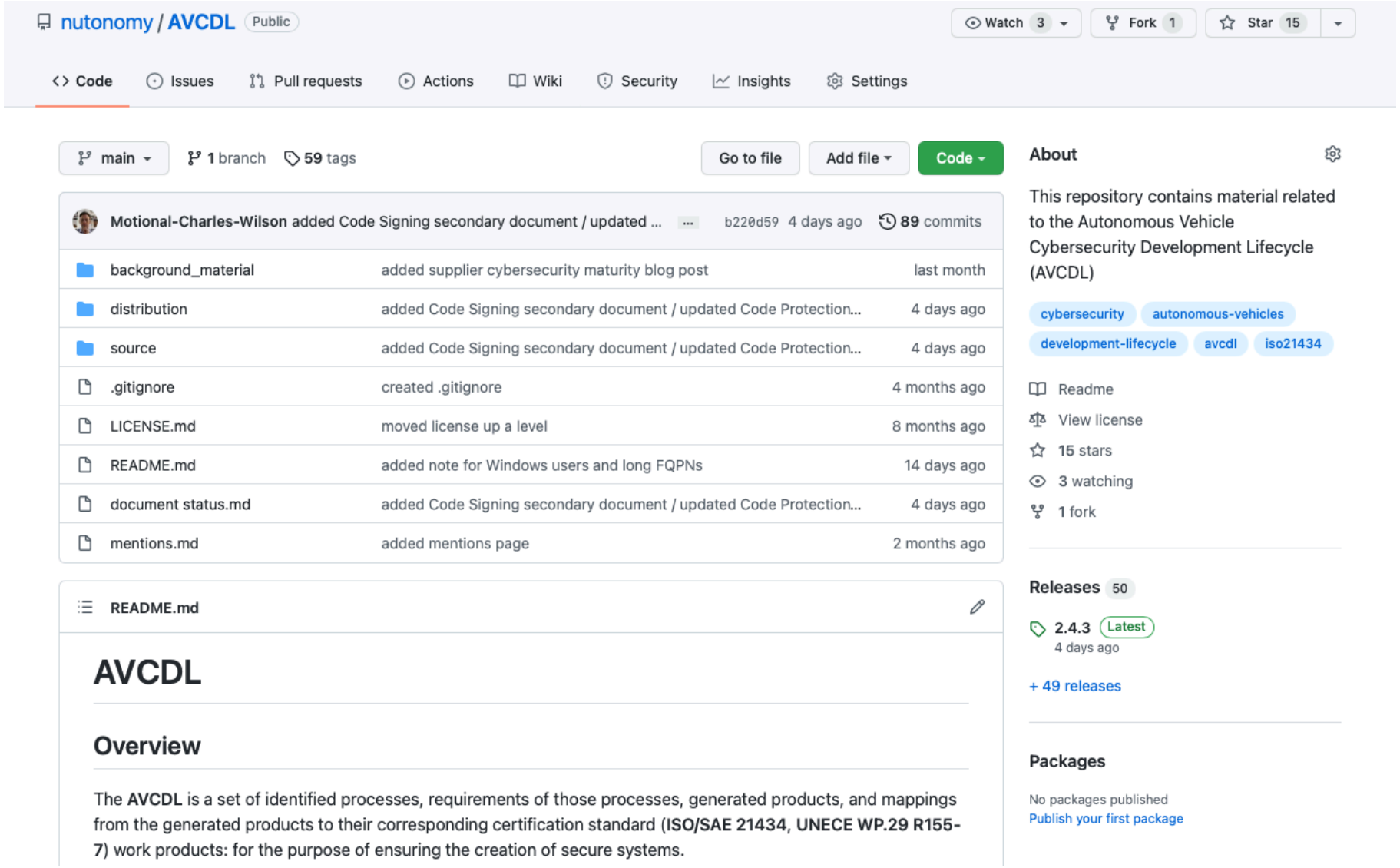
Traceability



Training


P# - AVCDL phase requirement
G - general (non-specific)
F - foundation phase
R - requirements phase
D - design phase
I - implementation phase
V - verification phase
S - release phase
O - operation phase
X - decommissioning phase
G1 security onboarding
G2 AVCDL overview
O1 vulnerability identification
O4 secure deployment
G3 requirements taxonomy
G6 secure design principles
G5 traceability
O2 vulnerability assessment
X1 secure decommissioning
R1 security requirements
D1 apply secure design
G7 handling PII
O3 vulnerability root cause
D2 secure design review
F9 threat prioritization
S1 final security review
I3 secure settings
D3 attack surface analysis
D4 threat modeling
I5 secure coding
I4 code reuse
I7 static analysis
I8 dynamic analysis
I10 fuzz testing
V1 penetration testing
I9 secure code review

AVCDL on GitHub



AVCDL Posts

README.md

AVCDL Introductory Blog Posts

The following is a blog series introducing the **AVCDL** and the concepts behind it.

Title	Description
Purpose-driven Security [PDF]	how we have chosen to apply security in a way that supports vehicle safety
Certifiably Secure: Does it Matter? [PDF]	you can make thing secure without getting outside approval, so why bother?
Policy - Process - Procedure [PDF]	coming to terms with the terms
Aligning the Organization with the AVPDL [PDF]	how do you bring the multitude of development practices together?
Traceability: Making the Case for Security [PDF]	how do you ensure follow through?
The AVCDL: Autonomous Vehicle Cybersecurity Development Lifecycle [PDF]	an overview of the AVCDL

AVCDL Document Status

The **AVCDL** documents are mostly complete. The majority of the secondary documents have been written and reviewed internally. Internally reviewed documents will be released soon after they have received certification body review.

Secondary Document Status

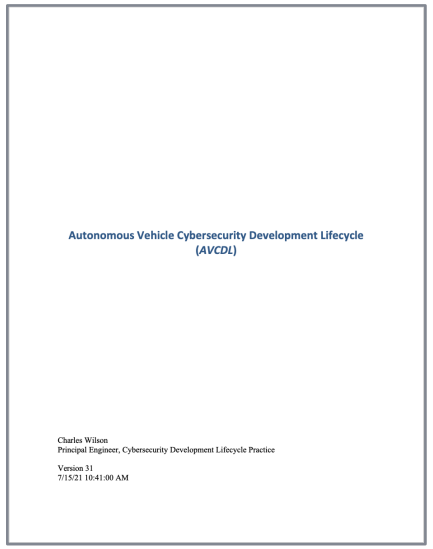
The following table shows the status of the various AVCDL elements.

Secondary (process) Document	Status
General	
security requirements taxonomy	complete
understanding the phase products dependencies graph	complete
secure design principles	complete
understanding workflow graphs	complete
AVCDL phase requirement product ISO 21434 work product fulfillment summary	complete
AVCDL phase requirement product ISO 26262 work product fulfillment summary	complete
AVCDL Phase Requirement Product UNECE WP.29 R155 Work Product Fulfillment	draft
code signing	complete

AVCDL Documents Available

https://github.com/nutonomy/AVCDL

AVCDL Documents Available – Primary Document



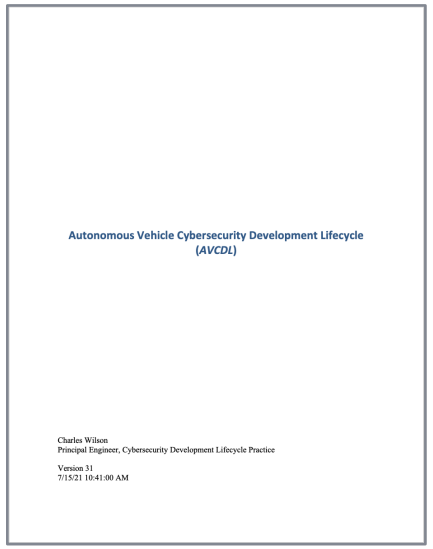
Autonomous Vehicle Cybersecurity Development Lifecycle
(*AVCDL*)

Charles Wilson
Principal Engineer, Cybersecurity Development Lifecycle Practice

Version 31
7/15/21 10:41:00 AM

https://github.com/nutonomy/AVCDL

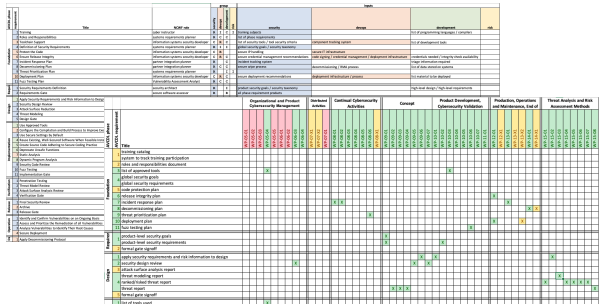
AVCDL Documents Available – Reference Material



Autonomous Vehicle Cybersecurity Development Lifecycle
(*AVCDL*)

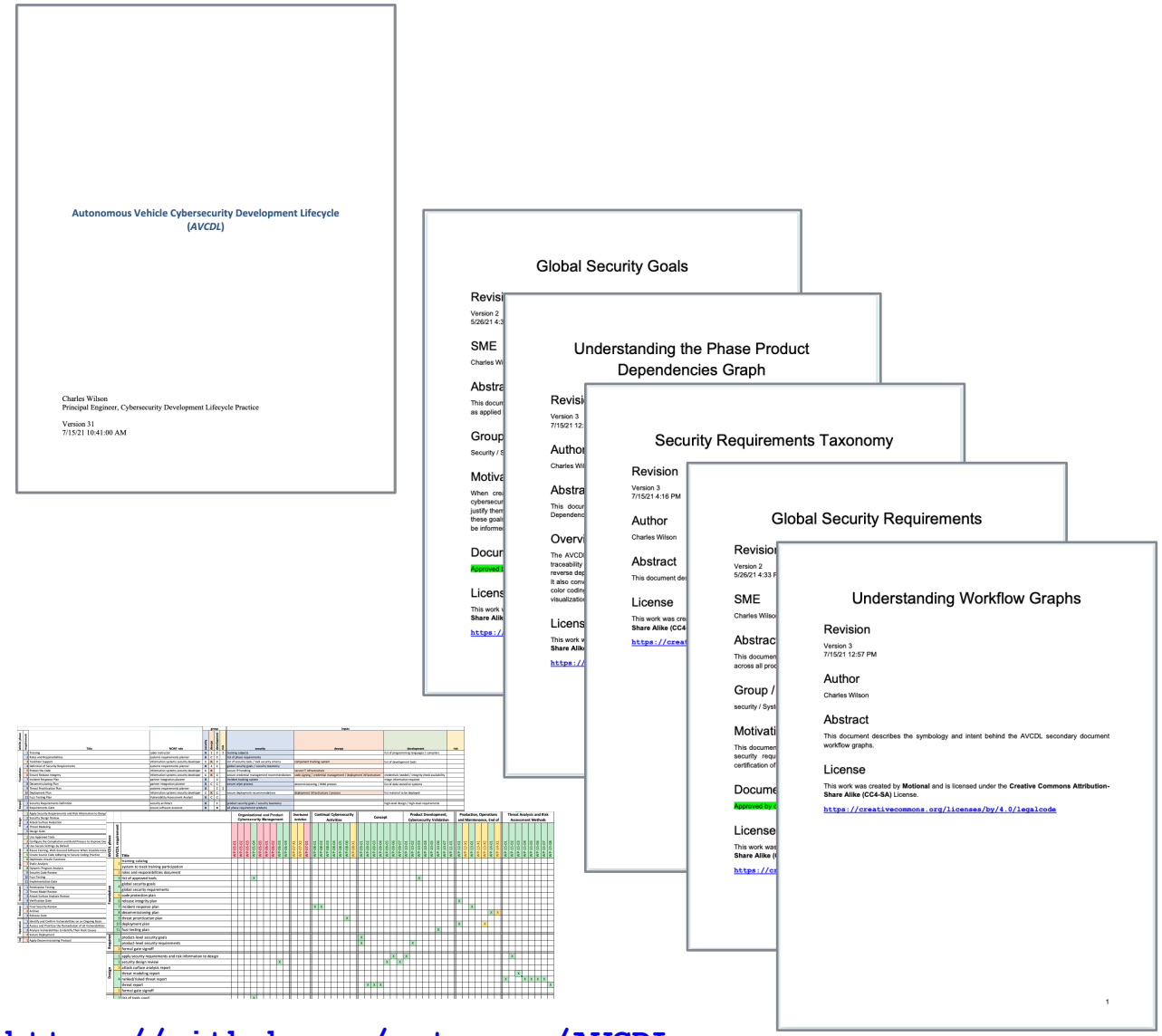
Charles Wilson
Principal Engineer, Cybersecurity Development Lifecycle Practice

Version 31
7/15/21 10:41:00 AM



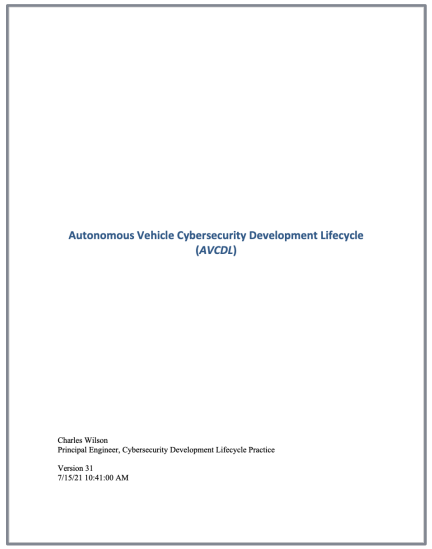
https://github.com/nutonomy/AVCDL

AVCDL Documents Available – Secondary Documents



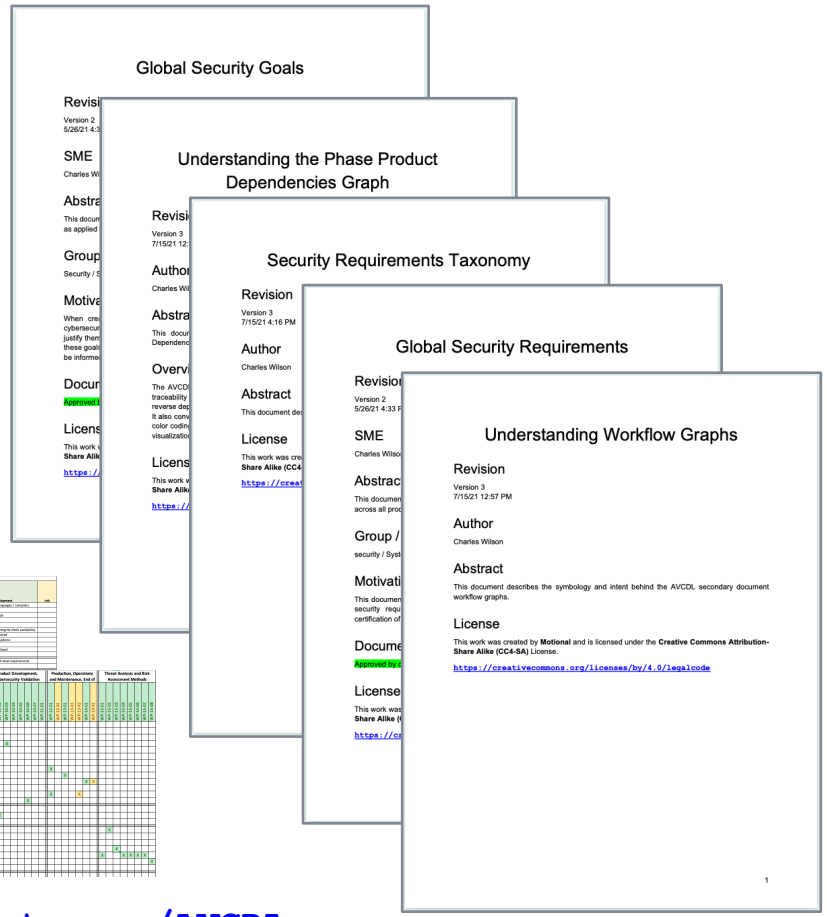
https://github.com/nutonomy/AVCDL

AVCDL Documents Available – Supplier Materials


Autonomous Vehicle Cybersecurity Development Lifecycle
(*AVCDL*)

Charles Wilson
Principal Engineer, Cybersecurity Development Lifecycle Practice

Version 31
7/15/21 10:41:00 AM


Global Security Goals

Understanding the Phase Product Dependencies Graph

Security Requirements Taxonomy

Global Security Requirements

Understanding Workflow Graphs

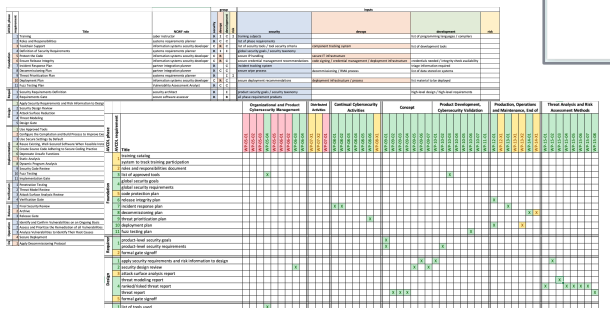
Revision
Version 3
7/15/21 12:57 PM

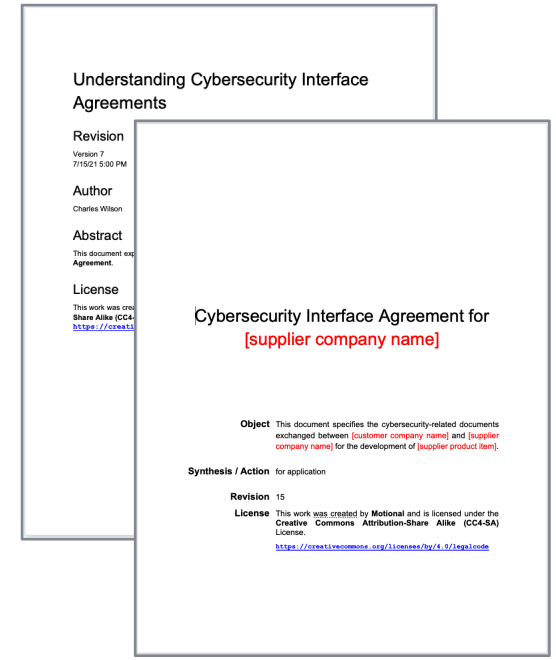
Author
Charles Wilson

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 (CC4-SA)** License.
https://creativecommons.org/licenses/by/4.0/legalcode

1




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

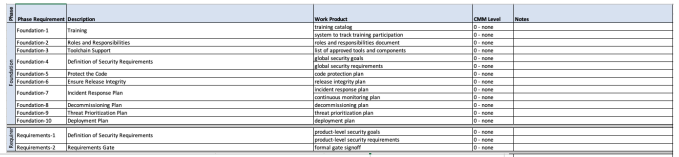
Cybersecurity Interface Agreement for
[supplier company name]

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

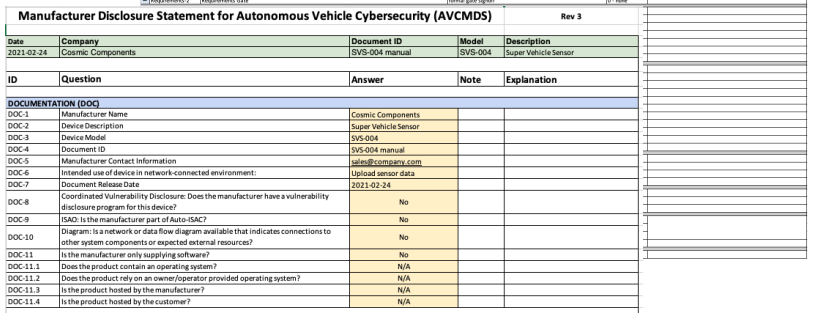
Synthesis / Action for application

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



Phase	Phase Requirement	Description	Work 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	
Product	Requirements-1	Definition of Security Requirements	decommissioning plan	0 - none	
	Requirements-2	Requirements Gate	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	

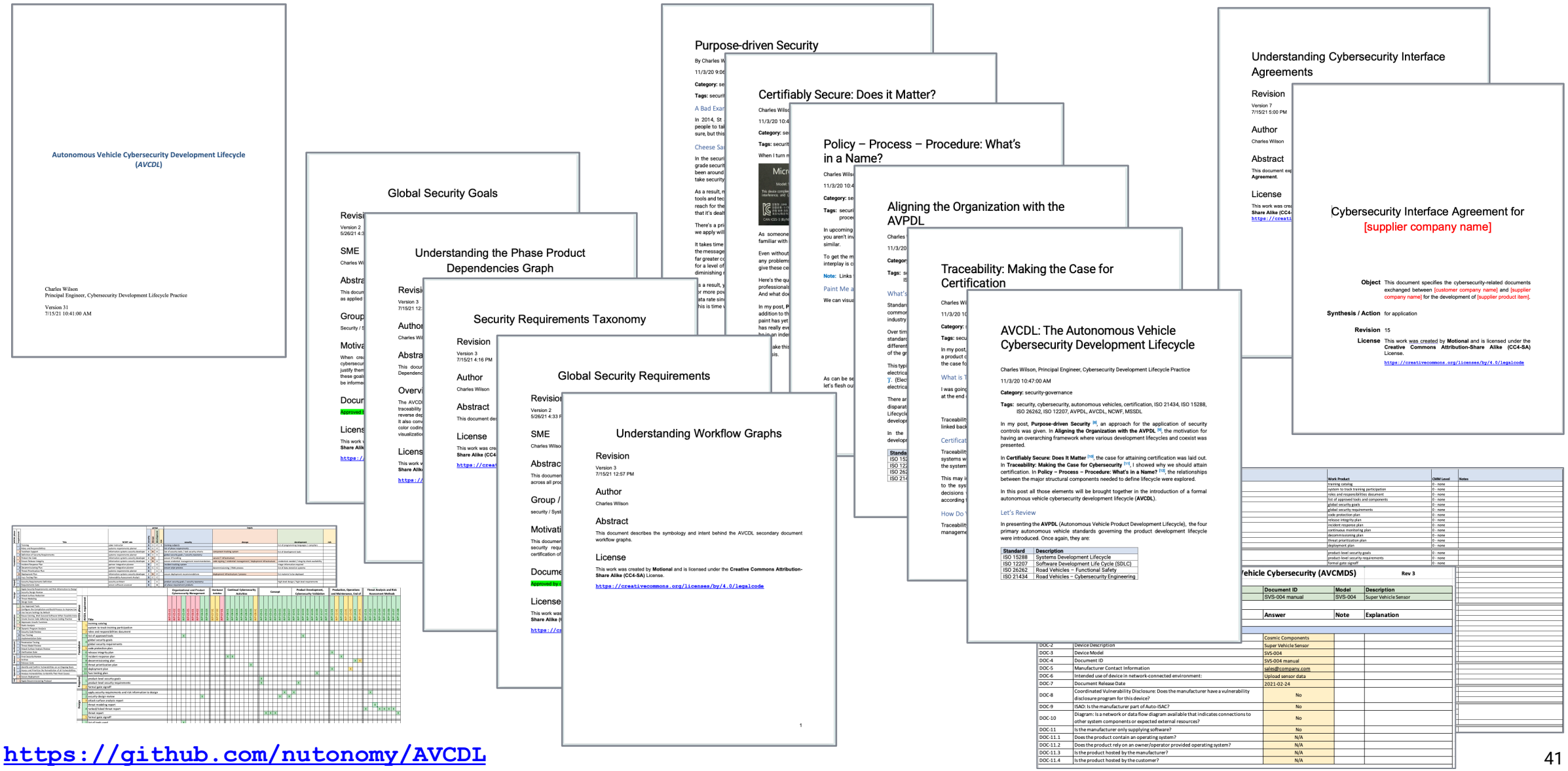

Manufacturer Disclosure Statement for Autonomous Vehicle Cybersecurity (AVCMDS) Rev 3

Date	Company	Document ID	Model	Description
2021-02-24	Cosmic Components	SVS-004 manual	SVS-004	Super Vehicle Sensor

ID	Question	Answer	Note	Explanation
DOCUMENTATION (DOC)				
DOC-1	Manufacturer Name	Cosmic Components		
DOC-2	Device Description	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		

https://github.com/nutonomy/AVCDL

AVCDL Documents Available – Introductory Blog Posts



https://github.com/nutonomy/AVCDL

References (1 of 2)

Systems and software engineering - Software life cycle processes
https://en.wikipedia.org/wiki/ISO/IEC_12207

Systems and software engineering - System life cycle 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/

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

References (2 of 2)

Secure Software Development Framework (SSDF)
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04232020.pdf

AVCDL (GitHub)
https://github.com/nutonomy/AVCDL

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

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