Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL) OASIS SARIF Presentation

Charles Wilson
Senior Principal Engineer, Cybersecurity Development Lifecycle Practice

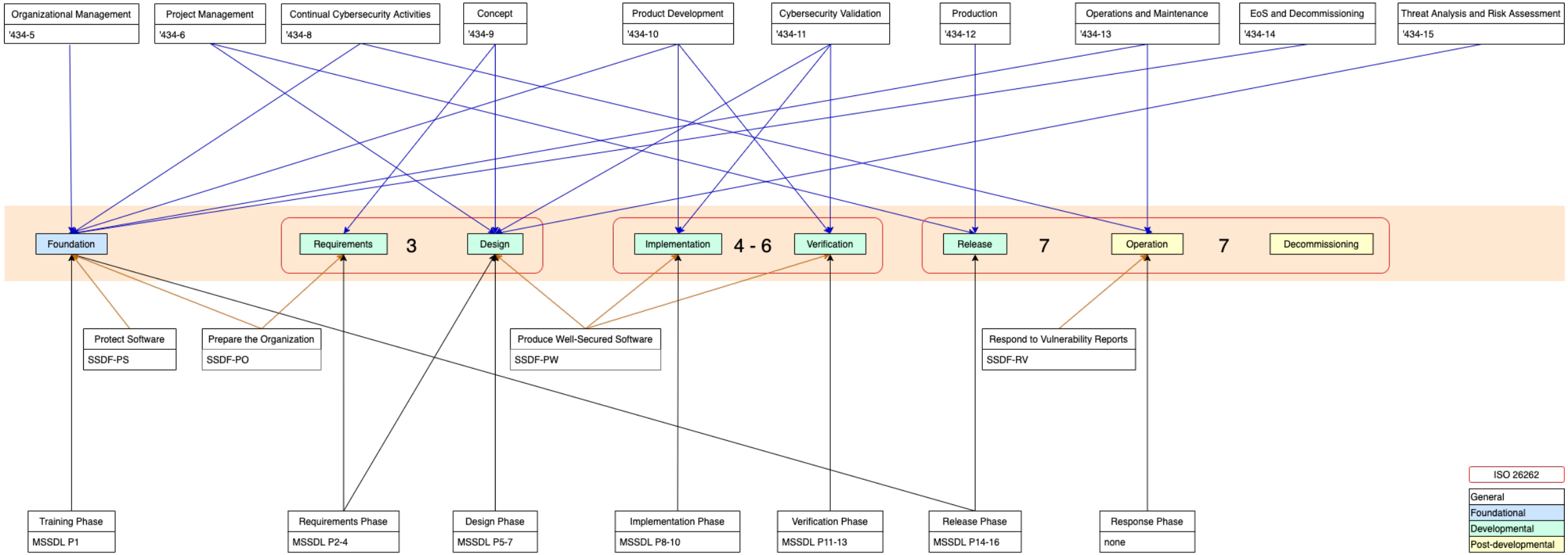
version 1
2022-11-10

Reference Sources

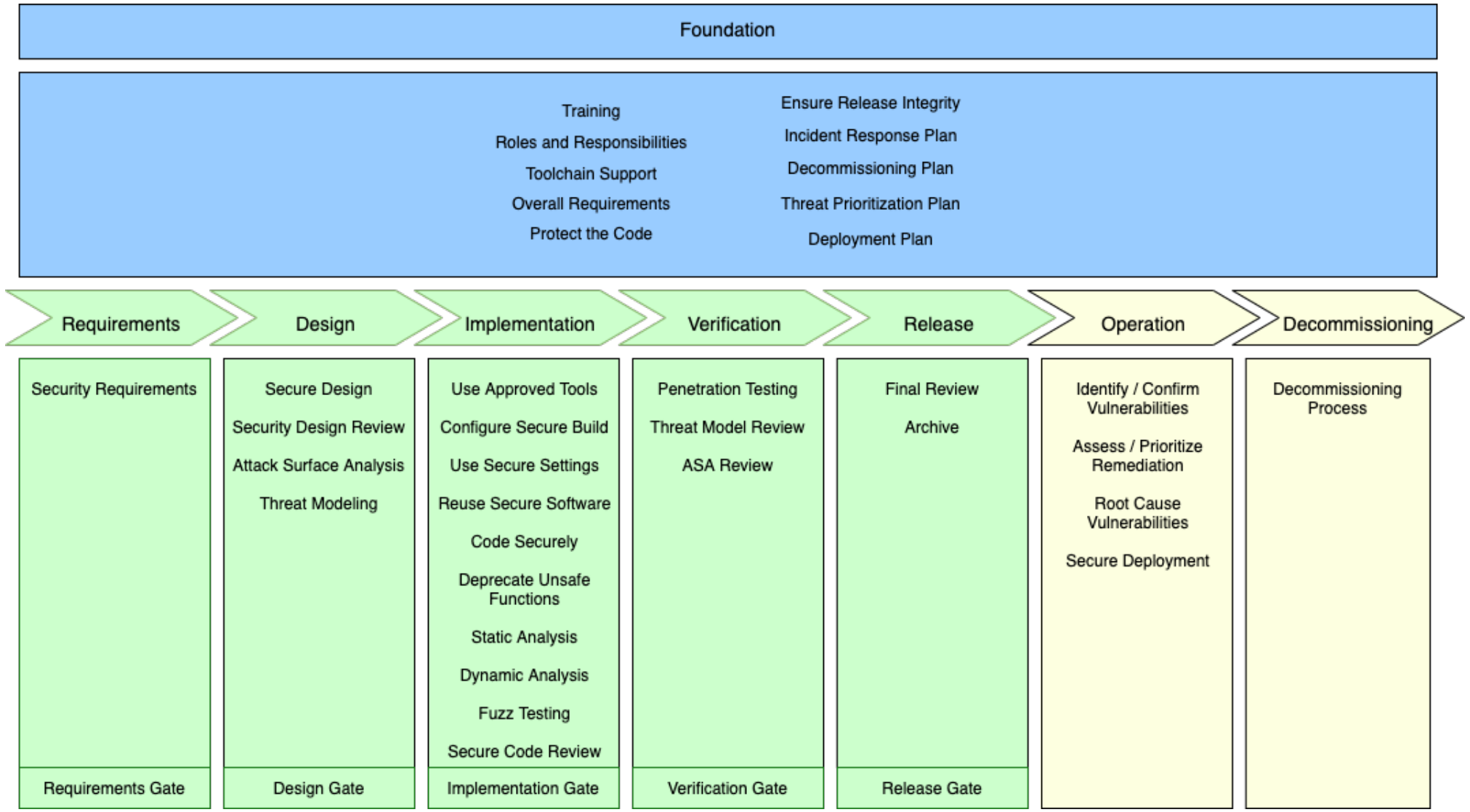
AVPDL – Autonomous Vehicle Product Development Lifecycle

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

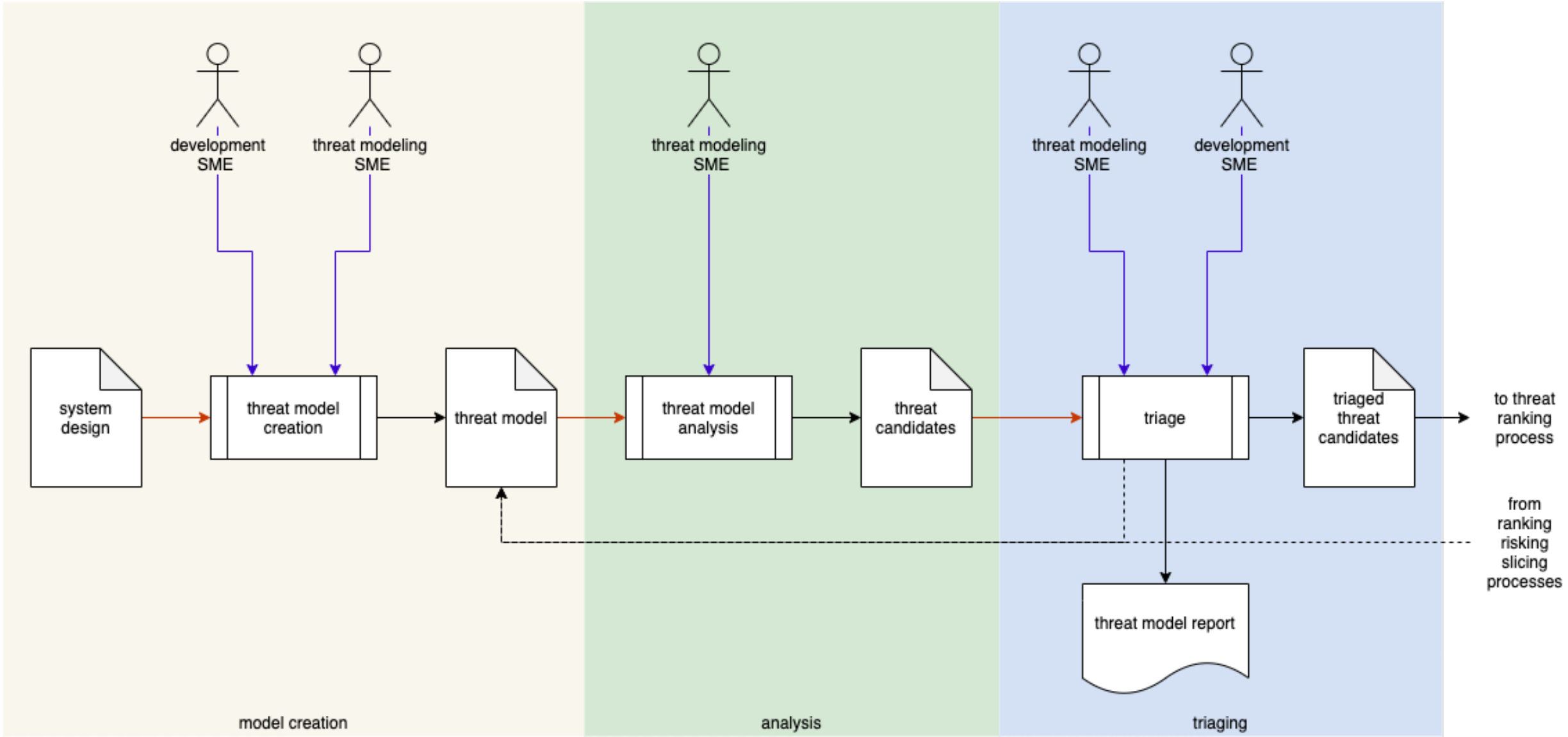
How Standards Inform the AVCDL



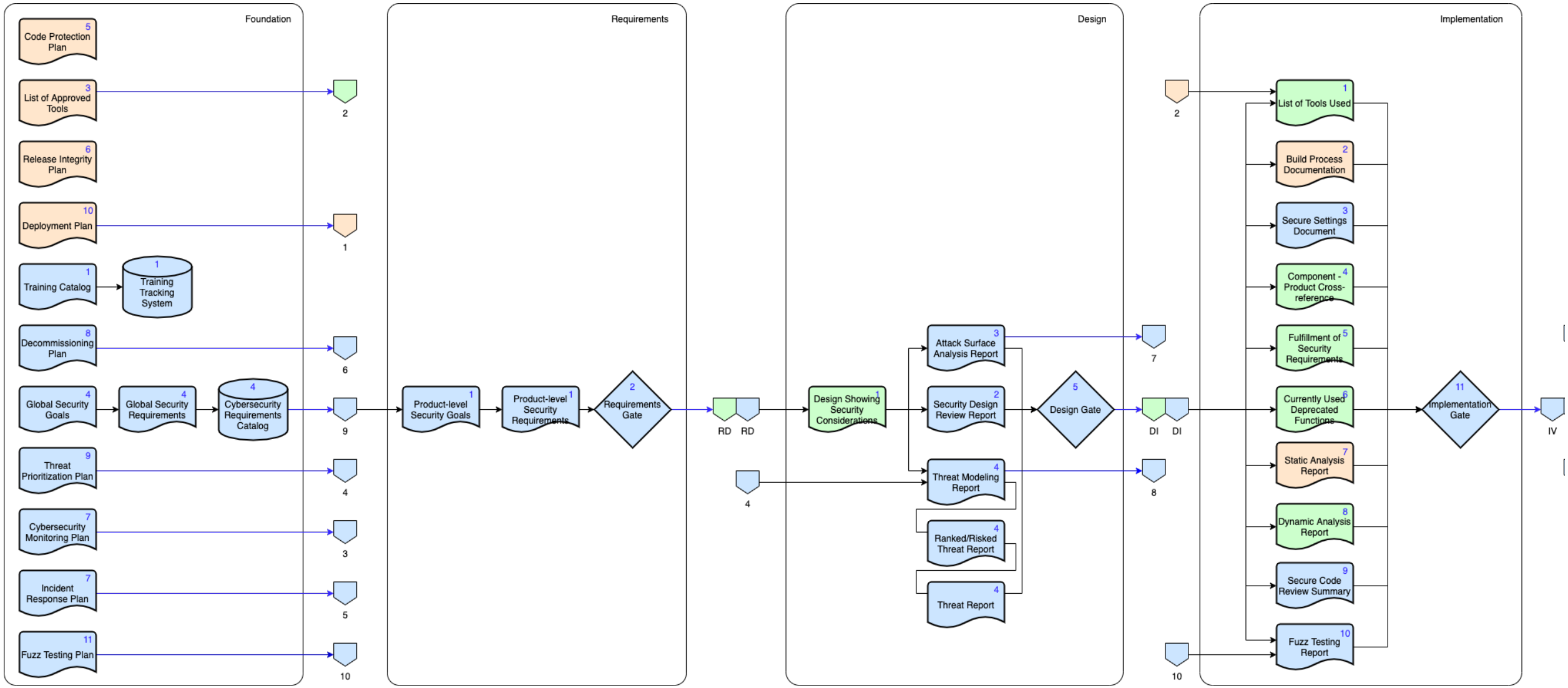
Phases and Requirements



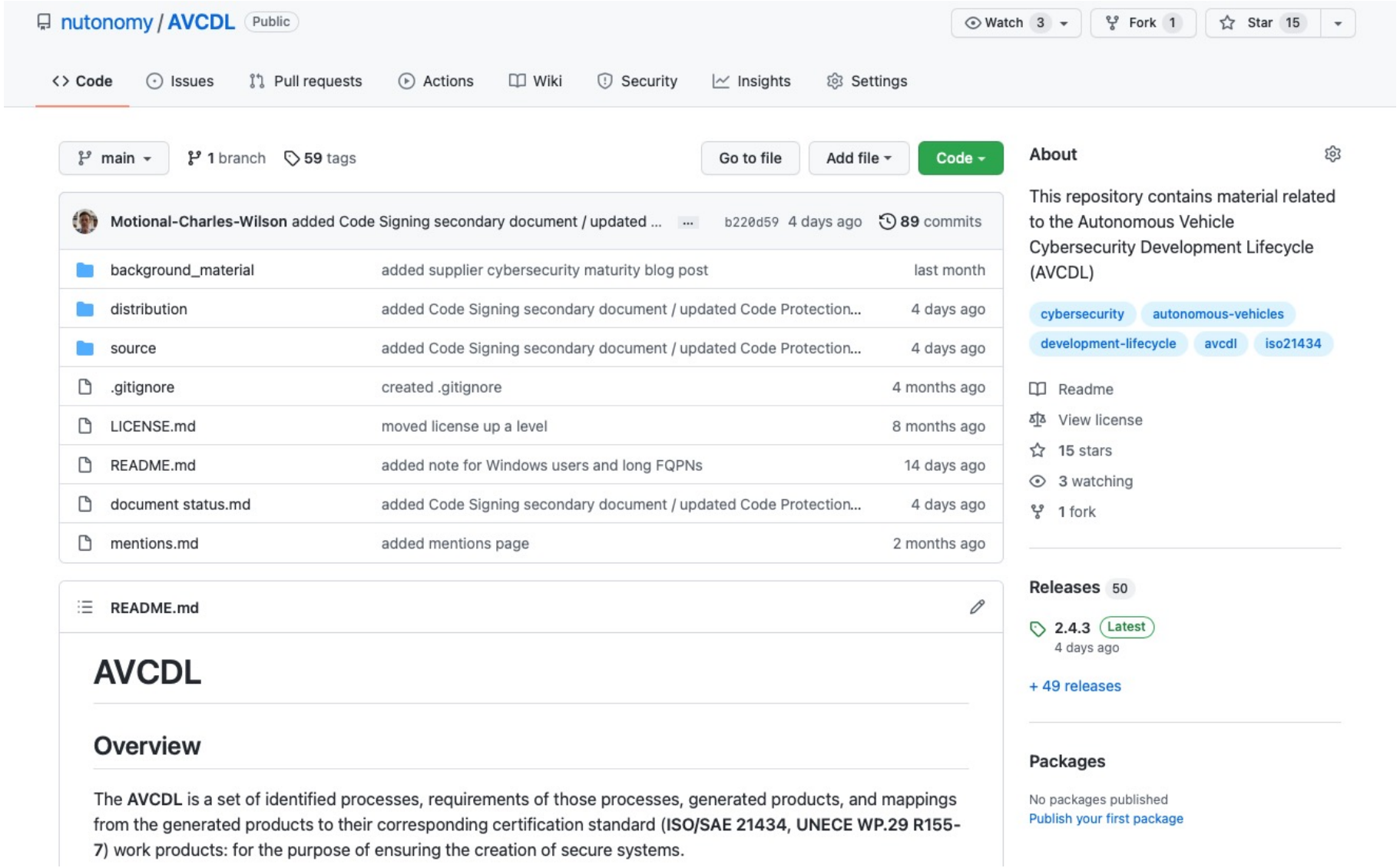
Process Flows



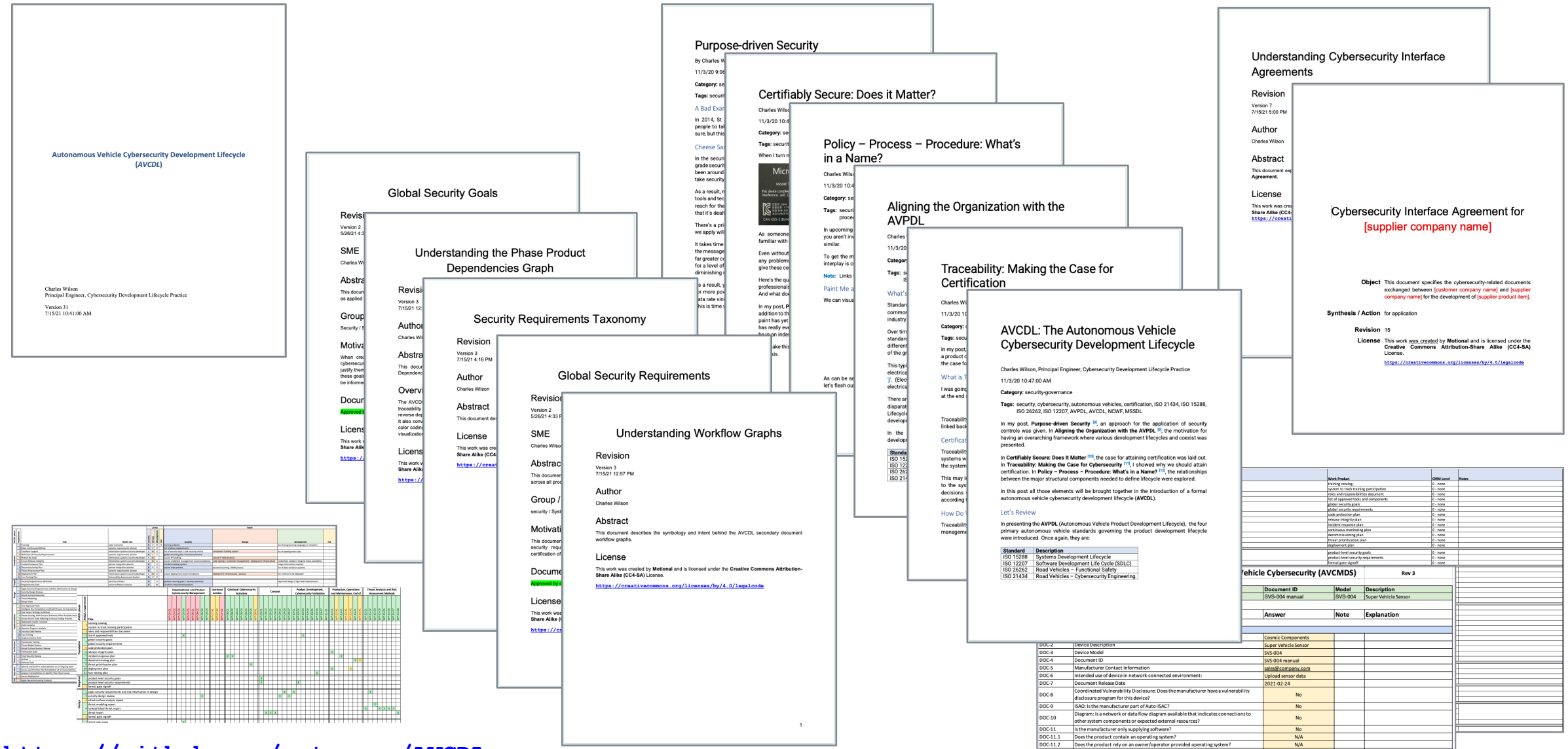
Traceability



AVCDL on GitHub

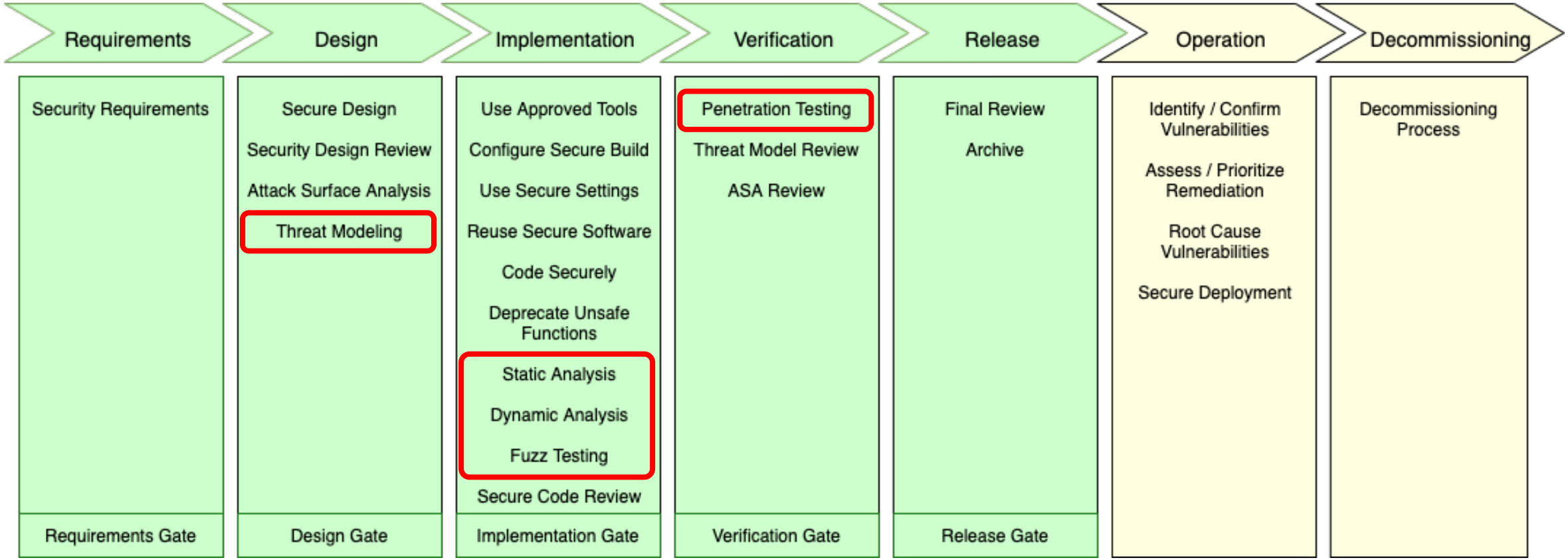


AVCDL Material



https://github.com/nutonomy/AVCDL

SARIF-relevant Processes



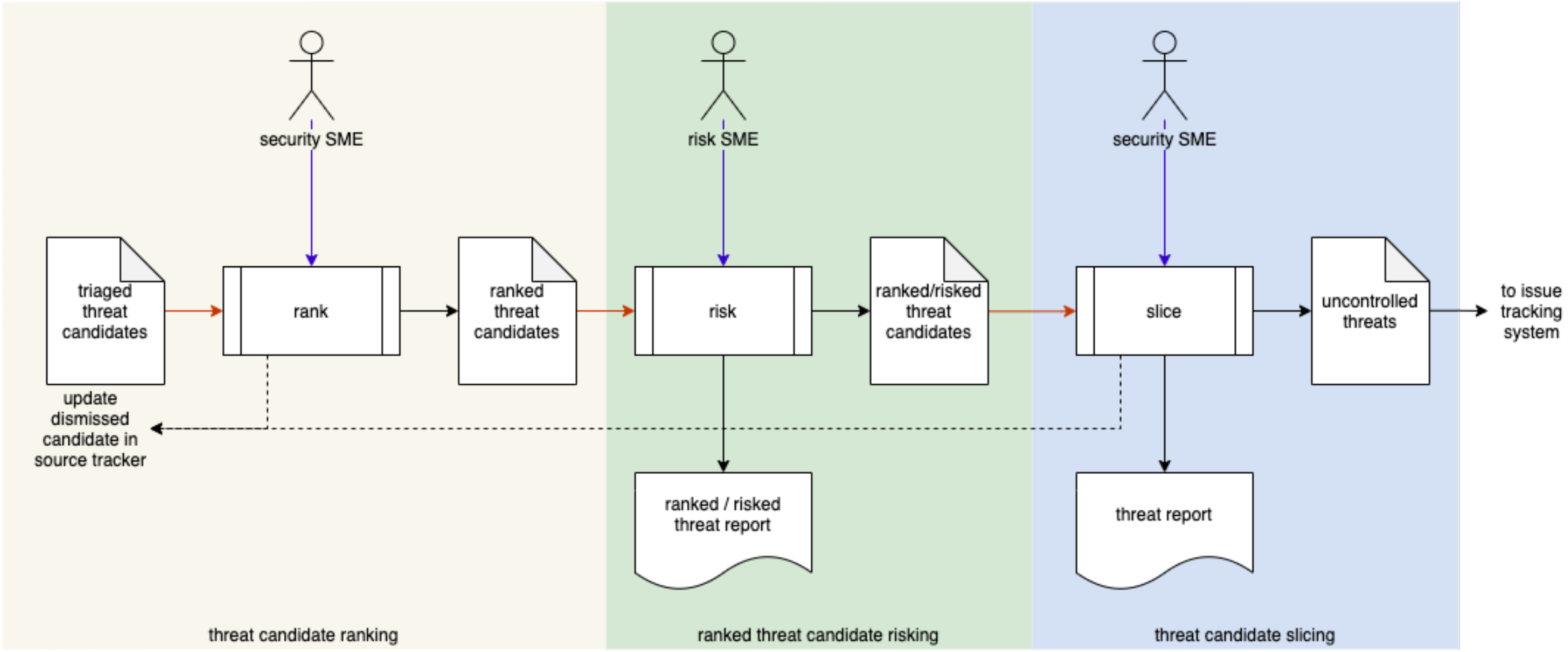
SARIF Field Compatibility

Process	SARIF element				
	Context	Run	Test	Finding	
				Location	Issue
Static Analysis	Common	Common	Checker	File / Line	Violation
Threat Modeling			Rule	Graph Edge	Violation
Fuzz Testing			Checker	File / Line	Fault
Dynamic Analysis			Checker	(variable resolution location)	Failure
Penetration Testing			Test	Test Step	Failure

Why Extend SARIF? (Static ➔ Systematic)

- Body of Knowledge (standard and practitioners)
- Automation
- Consistency
- Scale
- Supply Chain (data interchange)
- Single Source of Truth

Consistency – Threat Prioritization Process



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