Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL)
OASIS SARIF Presentation

Charles Wilson
Senior Principal Engineer, Cybersecurity Development Lifecycle Practice

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
Reference Sources

NIST Special Publication 800-181
National Initiative for Cybersecurity Education (NICE)
Cybersecurity Workforce Framework

William Horne
Stephanie Koch
Rajul Seth
Ying Wu

This publication is available free of charge from:
https://csrc.nist.gov/publication.html?id=SP-800-181

Foreword

ISO (the International Organization for Standardization) is a membership-based, international, non-profit organization. The work of standardization is carried out through national 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 committees have also been established to bring together national standards bodies of several countries on a globally relevant topic. The work of ISO is supported by staff实在太 and 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 reviewed, 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. 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).

Downloaded from SAE International by Charles Wilson, Friday, September 17, 2021
# AVPDL – Autonomous Vehicle Product Development Lifecycle

<table>
<thead>
<tr>
<th>AVPDL</th>
<th>15288 (SDLC system)</th>
<th>12207 (SDLC software)</th>
<th>26262 (safety)</th>
<th>21434 (cybersecurity)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>organization processes</strong></td>
<td>technical processes</td>
<td>technical processes</td>
<td>management of functional safety</td>
<td>overall cybersecurity management</td>
</tr>
<tr>
<td><strong>foundation phase</strong></td>
<td>N/A</td>
<td>N/A</td>
<td>supporting processes</td>
<td>project dependent cybersecurity management</td>
</tr>
<tr>
<td><strong>requirements phase</strong></td>
<td>requirements definition</td>
<td>requirements definition</td>
<td>safety requirements</td>
<td>cybersecurity requirements</td>
</tr>
<tr>
<td></td>
<td>requirements analysis</td>
<td>system requirements analysis</td>
<td>hazard analysis / risk assessment</td>
<td>cybersecurity assessment</td>
</tr>
<tr>
<td><strong>design phase</strong></td>
<td>architectural design</td>
<td>system architectural design</td>
<td>architectural design</td>
<td>cybersecurity design</td>
</tr>
<tr>
<td><strong>implementation phase</strong></td>
<td>implementation</td>
<td>implementation</td>
<td>implementation</td>
<td>development</td>
</tr>
<tr>
<td></td>
<td>integration</td>
<td>system integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>verification phase</strong></td>
<td>verification</td>
<td>system qualification testing</td>
<td>integration and verification</td>
<td>integration and verification</td>
</tr>
<tr>
<td></td>
<td>software installation</td>
<td>software installation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>software acceptance support</td>
<td>software acceptance support</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>release phase</strong></td>
<td>validation</td>
<td>validation</td>
<td>production</td>
<td>production</td>
</tr>
<tr>
<td><strong>operation phase</strong></td>
<td>operation</td>
<td>software operation</td>
<td>operation, service and decommissioning</td>
<td>continuous cybersecurity activities</td>
</tr>
<tr>
<td></td>
<td>maintenance</td>
<td>software maintenance</td>
<td>operation and maintenance</td>
<td></td>
</tr>
<tr>
<td><strong>decommissioning phase</strong></td>
<td>disposal</td>
<td>software disposal</td>
<td>decommissioning</td>
<td>decommissioning</td>
</tr>
<tr>
<td><strong>supplier processes</strong></td>
<td>agreement processes</td>
<td>agreement processes</td>
<td>supporting processes</td>
<td>distributed cybersecurity activities</td>
</tr>
</tbody>
</table>
How Standards Inform the AVCDL
Phases and Requirements

Foundation

- Training
- Roles and Responsibilities
- Toolchain Support
- Overall Requirements
- Protect the Code
- Ensure Release Integrity
- Incident Response Plan
- Decommissioning Plan
- Threat Prioritization Plan
- Deployment Plan

Requirements
- Security Requirements
  - Security Design Review
  - Attack Surface Analysis
  - Threat Modeling
  - Use Approved Tools
    - Configure Secure Build
    - Use Secure Settings
    - Reuse Secure Software
    - Code Securely
    - Deprecated Unsafe Functions
- Final Review
  - Archive

Design
- Secure Design Gate
- Design Gate

Implementation
- Implementation Gate

Verification
- Verification Gate
- Penetration Testing
  - Threat Model Review
  - ASA Review

Release
- Release Gate

Operation
- Decommissioning Process
  - Identify / Confirm Vulnerabilities
  - Assess / Prioritize Remediation
  - Root Cause Vulnerabilities
  - Secure Deployment
AVCDL on GitHub

Overview

The AVCDL is a set of identified processes, requirements of those processes, generated products, and mappings from the generated products to their corresponding certification standard (ISO/SAE 21434, UNECE WP.29 R155-7) work products; for the purpose of ensuring the creation of secure systems.
AVCDL Material

https://github.com/nutonomy/AVCDL
SARIF-relevant Processes

- **Requirements**
  - Security Requirements
  - Security Design Review
  - Attack Surface Analysis
  - Threat Modeling

- **Design**
  - Secure Design
  - Configure Secure Build
  - Use Secure Settings
  - Reuse Secure Software
  - Code Securely
  - Deprecate Unsafe Functions
  - Static Analysis
  - Dynamic Analysis
  - Fuzz Testing

- **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

- **Verification**
  - Penetration Testing
  - Threat Model Review
  - ASA Review

- **Release**
  - Final Review
  - Archive

- **Operation**
  - Identify / Confirm Vulnerabilities
  - Assess / Prioritize Remediation
  - Root Cause Vulnerabilities
  - Secure Deployment

- **Decommissioning**
  - Decommissioning Process
# SARIF Field Compatibility

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

- triaged threat candidates
- rank
- ranked threat candidates
- risk
- ranked/risked threat candidates
- slice
- uncontrolled threats
- threat report
- threat candidate ranking
- ranked threat candidate risking
- threat candidate slicing
- update dismissed candidate in source tracker

To issue tracking system
References (1 of 2)

Systems and software engineering - Software life cycle processes

Systems and software engineering - System life cycle processes

Road vehicles – Functional safety

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

NICE Cybersecurity Workforce Framework (NCWF)
References (2 of 2)

Secure Software Development Framework (SSDF)

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