Understanding Verification and Validation in an AVCDL Context

Revision

Version 5
4/14/25 2:01 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

Overview

The **AVCDL** [1] provides a lifecycle with the goal of ensuring the cybersecurity of a safety-critical, cyber-physical product. As such, it uses the non-functional goals and requirements established by the various risk groups within the organization to bound the cybersecurity efforts. A major focus within the risk realm are the technical processes of verification and validation. These are heavily referred to in the **ISO 26262** [2] safety standard. They are defined in **ISO 9000** [3] and elaborated on in **ISO/IEC/IEEE 15288 – Systems and software engineering – System life cycle processes** [4]. In this document, the relationship between these technical processes and the **AVCDL** will be explored.

Definitions

It's important to have a baseline for discussing verification and validation. **ISO 9000** and **ISO/IEC/IEEE 15288** define them as follows:

Verification

ISO 9000 – *confirmation, through the provision of objective evidence, that specified requirements have been fulfilled*

**ISO/IEC/IEEE 15288 –** *The system was built right.*

Validation

ISO 9000 – *confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled*

ISO/IEC/IEEE 15288 – *The right system was built.*

Note: Within this document the **ISO/IEC/IEEE 15288** simplified definitions will be used.
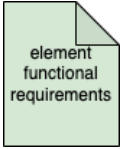
Visualization

The following diagram shows the dependencies between various **AVCDL** phase requirement products and how verification and validation are achieved.
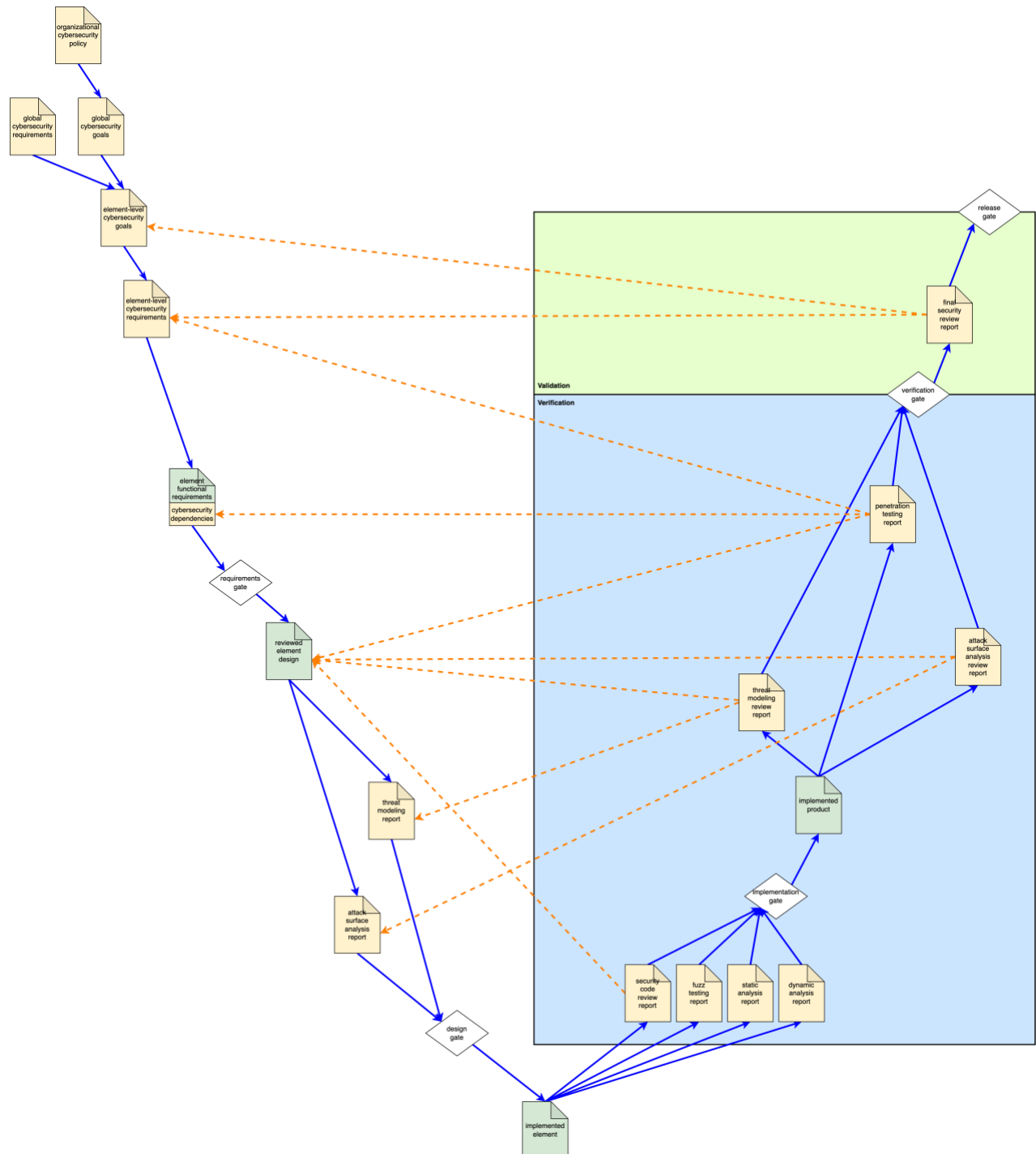
Note: This diagram is intended to provide a conceptual overview. It does not include all activities or dependencies laid out within the **AVCDL**.

Symbology

The following table covers the symbology used in this document's diagrams.

Symbol	Description
product-level cybersecurity goals	Cybersecurity artifact
element functional requirements	Non-cybersecurity artifact
requirements gate	Phase gate
	Process flow
	Verification and validation dependency

Note: There is no significance to the background color of each block (verification, validation). They differ in order to improve visual uptake.

Note: The verification and validation blocks above represent **ISO/IEC/IEEE 15288** technical processes and not **AVCDL** phases.

Verification

The following diagram shows the elements of interest within the verification technical processes.
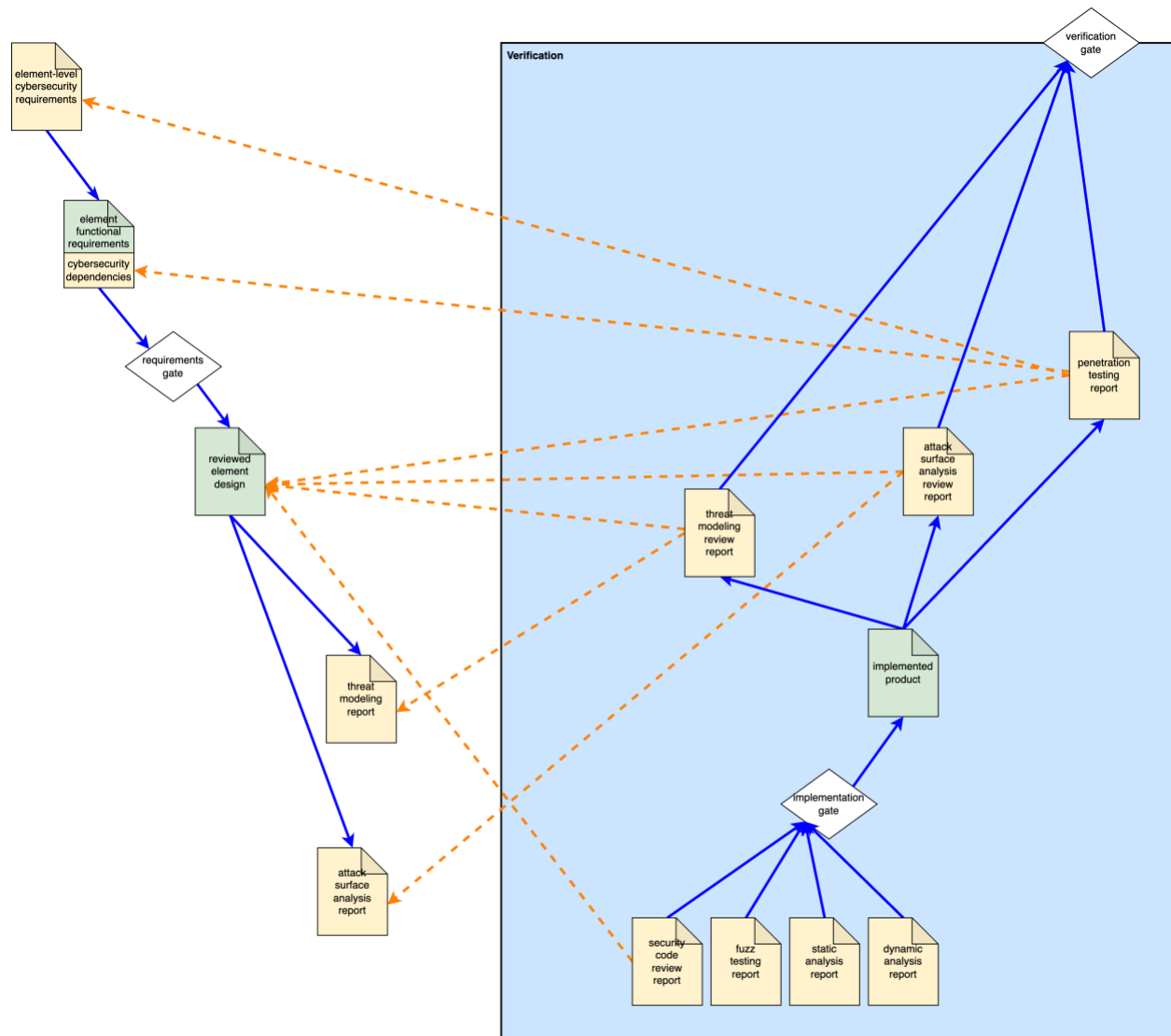

Due to the nature of cybersecurity, the verification technical processes consider **AVCDL** implementation phase activities as well as **AVCDL** verification phase ones. This is a different approach than taken in other standards.

Note: The three AVCDL artifacts: **fuzz testing report** [5], **static analysis report** [6], and **dynamic analysis report** [7] are included in the verification technical processes but do not refer back to previous artifacts. This is because they provide direct feedback to the implementation of the element being reported upon based not upon goals or requirements, but on correct cybersecurity implementation as determined by *de facto* standards.
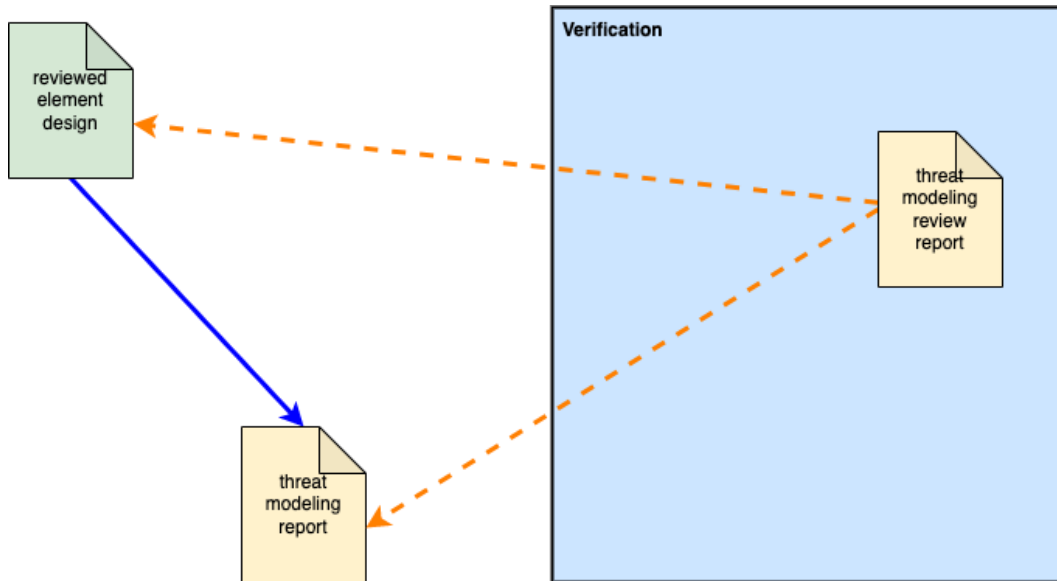
Secure Code Review

The verification basis of the **security code review report** [8] is depicted below.
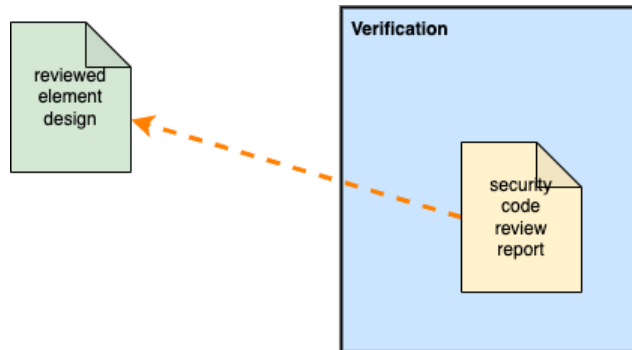
The **security code review report** uses the **reviewed element design** [9] as its basis for verification.
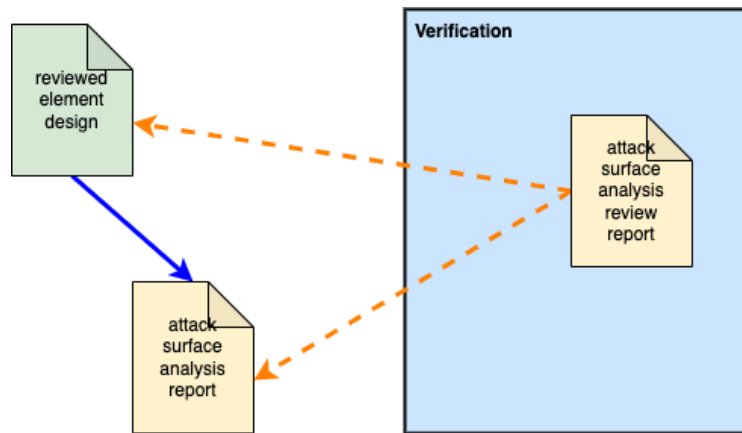
Threat Modeling Review

The verification basis of the **threat modeling review report** [10] is depicted below.

The **threat modeling review report** uses the **reviewed element design** and the **threat modeling report** [11] as its basis for verification. Since the threat model is based on the design it is used to ensure that the base threat model is accurate. The review ensures that all issues identified in the base threat modeling report have been controlled.

Attack Surface Analysis Review

The verification basis of the **attack surface analysis review report** [12] is depicted below.

The **attack surface analysis review report** uses the **reviewed element design** and the **attack surface analysis report** [13] as its basis for verification. Since the attack surface is based on the design it is used to ensure that the base attack surface analysis is accurate. The review ensures that all issues identified in the base attack surface analysis report have been addressed.

Penetration Testing

The verification basis of the **penetration testing report** [14] is depicted below.
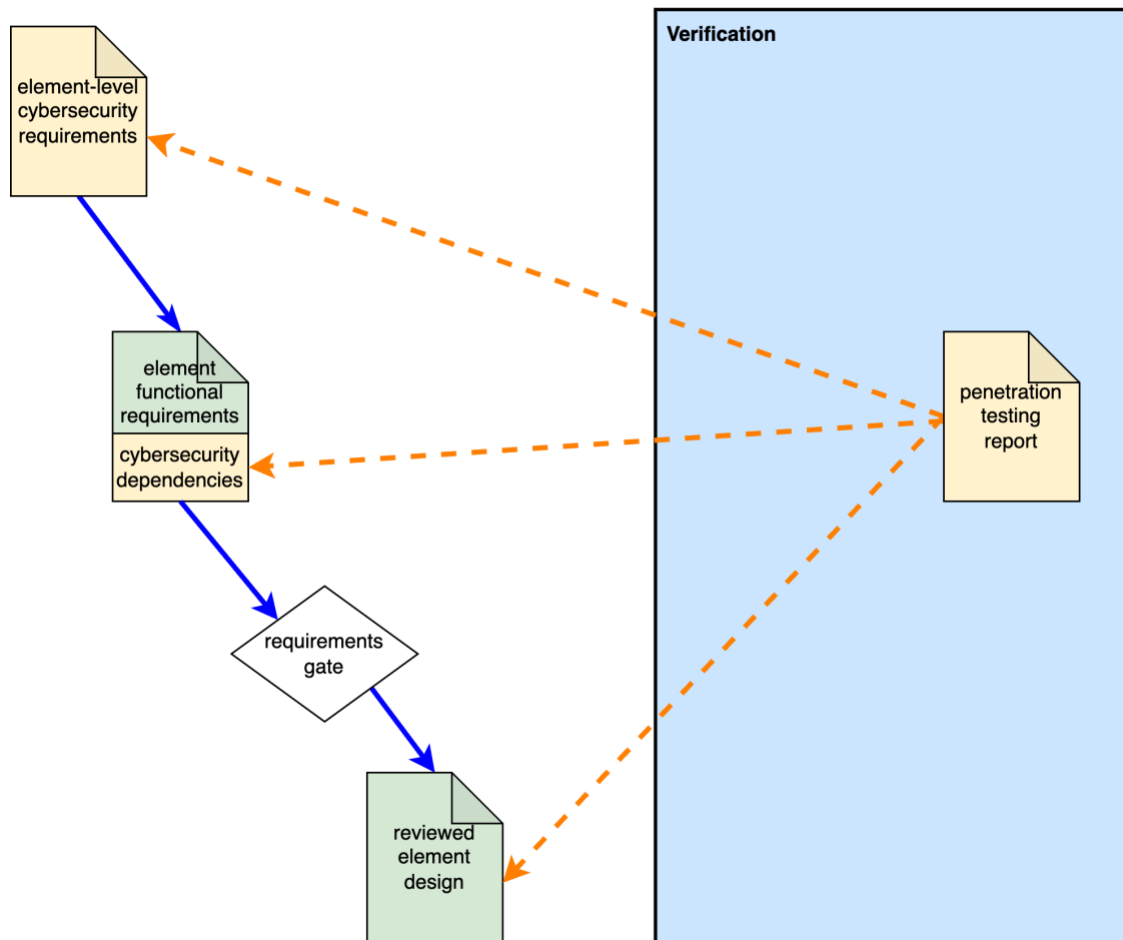
The **penetration testing report** uses the **element-level cybersecurity requirements** [15], **cybersecurity dependencies** [16] augmenting the **element functional requirements**, and the **reviewed element design** as its basis for verification. Since penetration testing is performed on an operational component (or system), all three are necessary. The review ensures that the component withstands direct attack.

Validation

The following diagram shows the elements of interest within the validation technical processes.
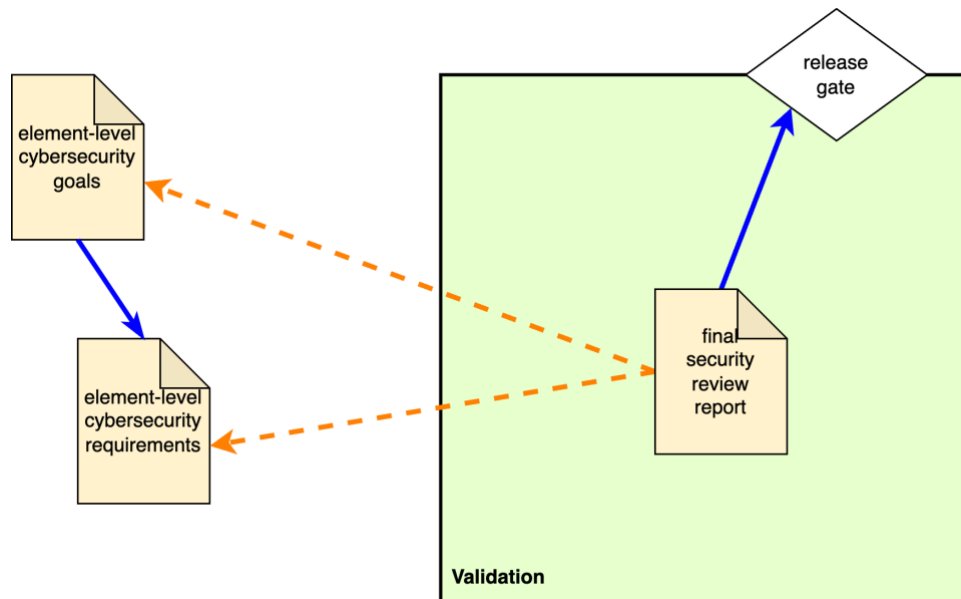
Unlike the verification technical processes, the validation technical processes occur during a single **AVCDL** phase, specifically the release phase. This phase is not named the validation phase as activities other than validation occur in it.

The validation basis of the **final security review report** [17] is depicted above. The **final security review report** uses the **element-level cybersecurity requirements** and the **element-level cybersecurity goals** [18] as its basis for validation. The review ensures that the product as implemented adheres to and achieves the product's cybersecurity goals and requirements.

References

1. **AVCDL** (primary document)
2. **ISO 26262 – Road vehicles – Functional safety**
   https://www.iso.org/standard/68383.html
3. **ISO 9000 Family – Quality Management**
   https://www.iso.org/iso-9001-quality-management.html
4. **ISO/IEC/IEEE 15288 – Systems and software engineering – System life cycles processes**
   https://www.iso.org/standard/63711.html
5. **Fuzz Testing Report** (AVCDL secondary document)
6. **Static Analysis Report** (AVCDL secondary document)
7. **Dynamic Analysis Report** (AVCDL secondary document)
8. **Secure Code Review Summary** (AVCDL secondary document)
9. **Security Design Review Report** (AVCDL secondary document)
10. **Updated Threat Model** (AVCDL secondary document)
11. **Threat Modeling Report** (AVCDL secondary document)
12. **Updated Attack Surface Analysis** (AVCDL secondary document)
13. **Attack Surface Analysis Report** (AVCDL secondary document)
14. **Penetration Testing Report** (AVCDL secondary document)
15. **Element-level Security Requirements** (AVCDL secondary document)
16. **Design Showing Security Considerations** (AVCDL secondary document)
17. **Final Security Review Report** (AVCDL secondary document)
18. **Element-level Security Goals** (AVCDL secondary document)