

# Design Phase Gate

## Revision

Version 4  
9/8/23 3:43 PM

## SME

Charles Wilson

## Abstract

This document describes the process used to confirm that all work products specified within the design phase are complete, and sufficient to generate the work products required by applicable certification standards.

## Group / Owner

Security / Secure Software Assessor

## Motivation

This document is motivated by the need to have formal processes in place for the verification and sign-off of phase products necessary for the creation of certification work products required for the certification safety-critical, cyber-physical systems, such as **ISO/SAE 21434 ('434)** and **ISO 26262 ('262)**.

## License

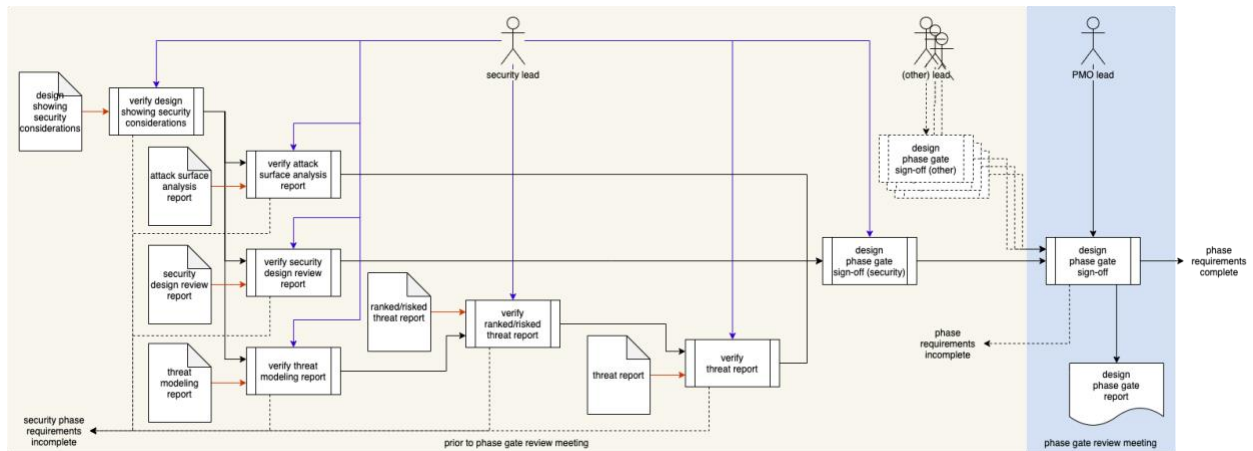
This work was created by **Motional** and is licensed under the **Creative Commons Attribution-Share Alike (CC4-SA)** License.

<https://creativecommons.org/licenses/by/4.0/legalcode>

# Overview

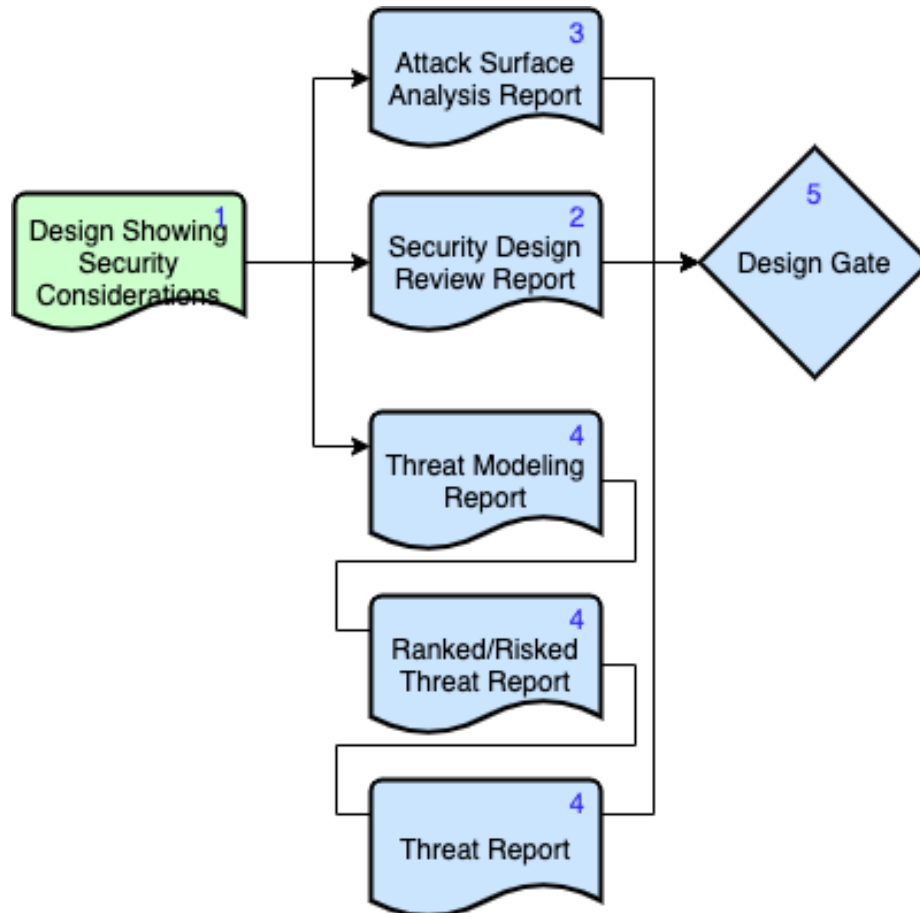
The design phase gate provides a point of process synchronization for all organizational groups to confirm that their process requirements have been fulfilled. The outcome is either a passing of the gate (transition to the design phase) or failure to pass (required products are incomplete).

The following diagram illustrates the process to be used:



# Process

The following diagram is a taken from the design phase section of the **AVCDL** product dependencies graph.



As shown by the blue numbers in the upper right corner of each element, we can see that the requirements phase gate has four gated phase requirements with six products.

**Note:** Activities stemming from non-dependent phase requirements may be undertaken in parallel.

The following phase requirement products need to be verified as completed for the gate to be signed off:

1. **Design Showing Security Considerations**
2. **Security Design Review Report**
3. **Attack Surface Analysis Report**
4. **Threat Modeling Report**
5. **Ranked / Risked Threat Report**
6. **Threat Report**

The process is broadly divided into two parts: prior to the phase gate review meeting and the meeting itself. Activities taking place prior to the meeting are conducted separately by each group with a dependency on the gate. Failure during these activities precludes the meeting taking place, as any such failure would cause the gate to be failed.

## Design Showing Security Consideration Verification

<b>Inputs</b>	Design Showing Security Consideration
<b>Outputs</b>	none
<b>Participants</b>	Security Lead

The security lead verifies that the **Design Showing Security Considerations** phase requirements product for the element under consideration are complete. If they are not complete, the gate should not be entered and the PMO should be informed.

## Secure Design Review Report Verification

<b>Inputs</b>	Secure Design Review Report
<b>Outputs</b>	none
<b>Participants</b>	Security Lead

The security lead verifies that the **Secure Design Review Report** phase requirements product for the element under consideration are complete. If they are not complete, the gate should not be entered and the PMO should be informed.

## Attack Surface Analysis Report Verification

<b>Inputs</b>	Attack Surface Analysis Report
<b>Outputs</b>	none
<b>Participants</b>	Security Lead

The security lead verifies that the **Attack Surface Analysis Report** phase requirements product for the element under consideration are complete. If they are not complete, the gate should not be entered and the PMO should be informed.

## Threat Modeling Report Verification

<b>Inputs</b>	Threat Modeling Report
<b>Outputs</b>	none
<b>Participants</b>	Security Lead

The security lead verifies that the **Threat Modeling Report** phase requirements product for the element under consideration are complete. If they are not complete, the gate should not be entered and the PMO should be informed.

## Ranked / Risked Threat Report Verification

<b>Inputs</b>	Ranked / Risked Threat Report
<b>Outputs</b>	none
<b>Participants</b>	Security Lead

The security lead verifies that the **Ranked / Risked Threat Report** phase requirements product for the element under consideration are complete. If they are not complete, the gate should not be entered and the PMO should be informed.

## Threat Report Verification

<b>Inputs</b>	Threat Report
<b>Outputs</b>	none
<b>Participants</b>	Security Lead

The security lead verifies that the **Threat Report** phase requirements product for the element under consideration are complete. If they are not complete, the gate should not be entered and the PMO should be informed.

## Design Phase Gate Signoff (Security)

<b>Inputs</b>	none
<b>Outputs</b>	none
<b>Participants</b>	Security Lead

The security lead signs off that all security-related products for this phase are complete and in good order. The PMO is informed of this.

## Design Phase Gate Signoff

<b>Inputs</b>	none
<b>Outputs</b>	Design Phase Gate Report
<b>Participants</b>	PMO Lead

If all participating groups provide signoffs the phase gate review meeting takes place. During this meeting all parties satisfy themselves that all their dependencies upon other groups are met. If there are no issues raised, the PMO lead signs off that all products for this phase are complete and in good order. Otherwise, the gate is not passed. The PMO produces the **Design Phase Gate Report** to document the gate outcome.

At a minimum, the report contains formal sign-off from each group's lead with a list of the phase products verified.

## References

1. **AVCDL** Product Dependencies (in **AVCDL** main document)
2. **Design Phase Gate Report**
3. **Design Showing Security Considerations** (**AVCDL** secondary document)
4. **Security Design Review Report** (**AVCDL** secondary document)
5. **Attack Surface Analysis Report** (**AVCDL** secondary document)
6. **Threat Modeling Report** (**AVCDL** secondary document)
7. **Ranked / Risked Threat Report** (**AVCDL** secondary document)
8. **Threat Report** (**AVCDL** secondary document)