Updated Attack Surface Analysis

Revision

Version 4
9/8/23 4:41 PM

SME

Charles Wilson

Abstract

This document describes the process used to update the attack surface analysis report.

Group / Owner

Security / Security Architect

Motivation

This document is motivated by the need to determine whether the security deficiencies identified during the design phase have been appropriately disposed. This is necessary given the nature of safety-critical, cyber-physical systems, subject to certifications such as **ISO/SAE 21434** and **ISO 26262**.

License

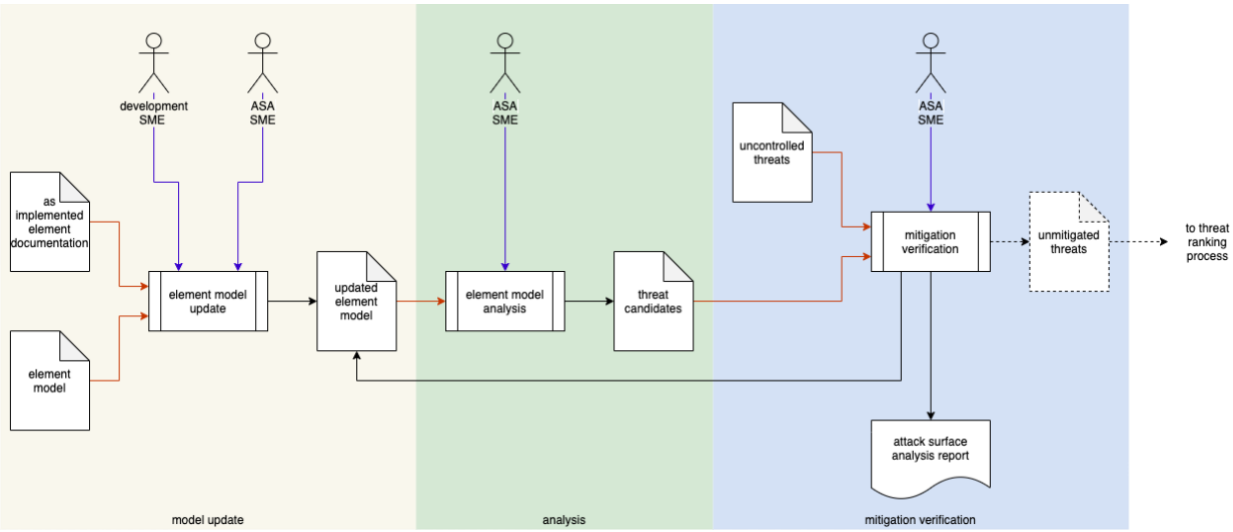
This work was created by **Motional** and is licensed under the **Creative Commons Attribution-Share Alike (CC4-SA)** License.

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

Overview

Many changes can occur between the creation/update of an element model during the design phase and the verification phase. Reviewing the model allows for the verification that issues identified for mitigation have been appropriately dealt with and that no new issues have arisen.

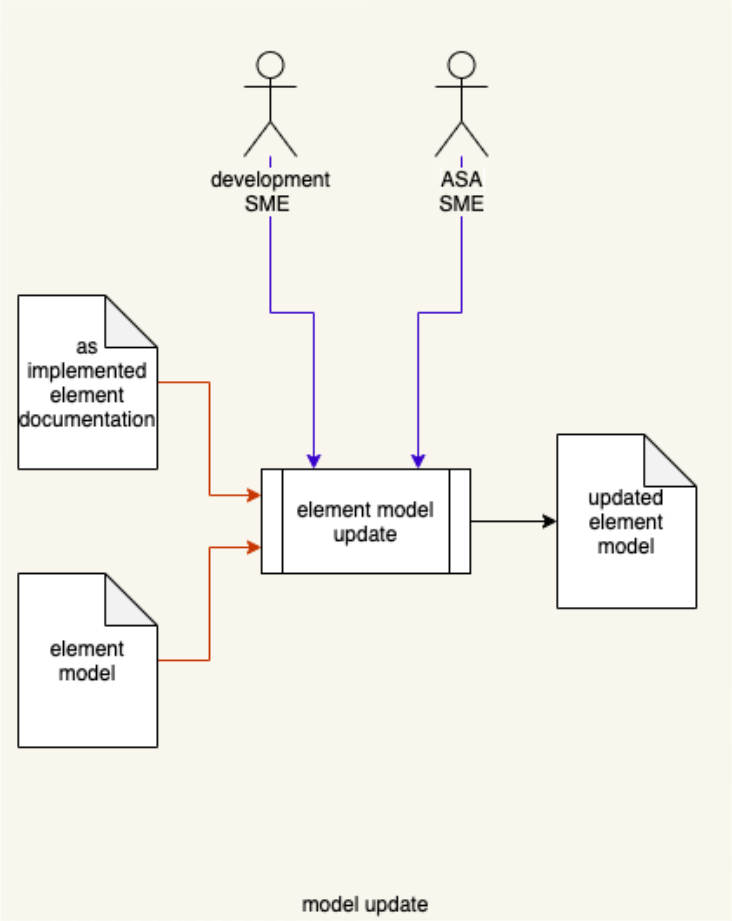
The following diagram illustrates the process to be used:



Process

Model Update

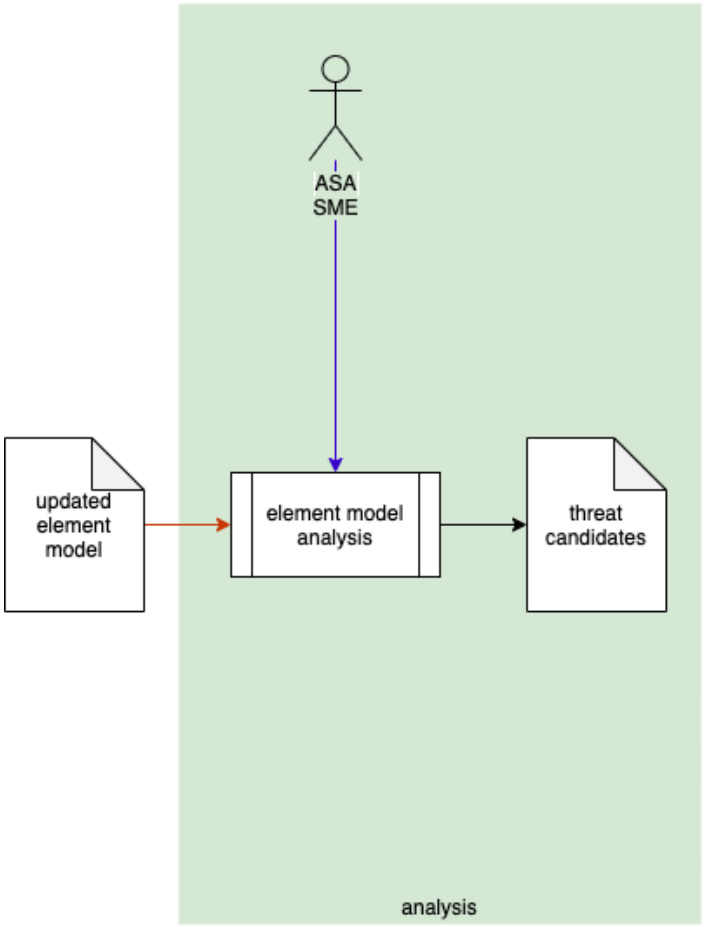
Inputs	As-implemented element documentation Element model
Outputs	Updated element model
Participants	Development SME ASA SME



The attack surface analysis (**ASA**) SME works with the development SME(s) to create an **updated element model** of the system. The **as-implemented element documentation** is used to update the model created in the design phase.

Analysis

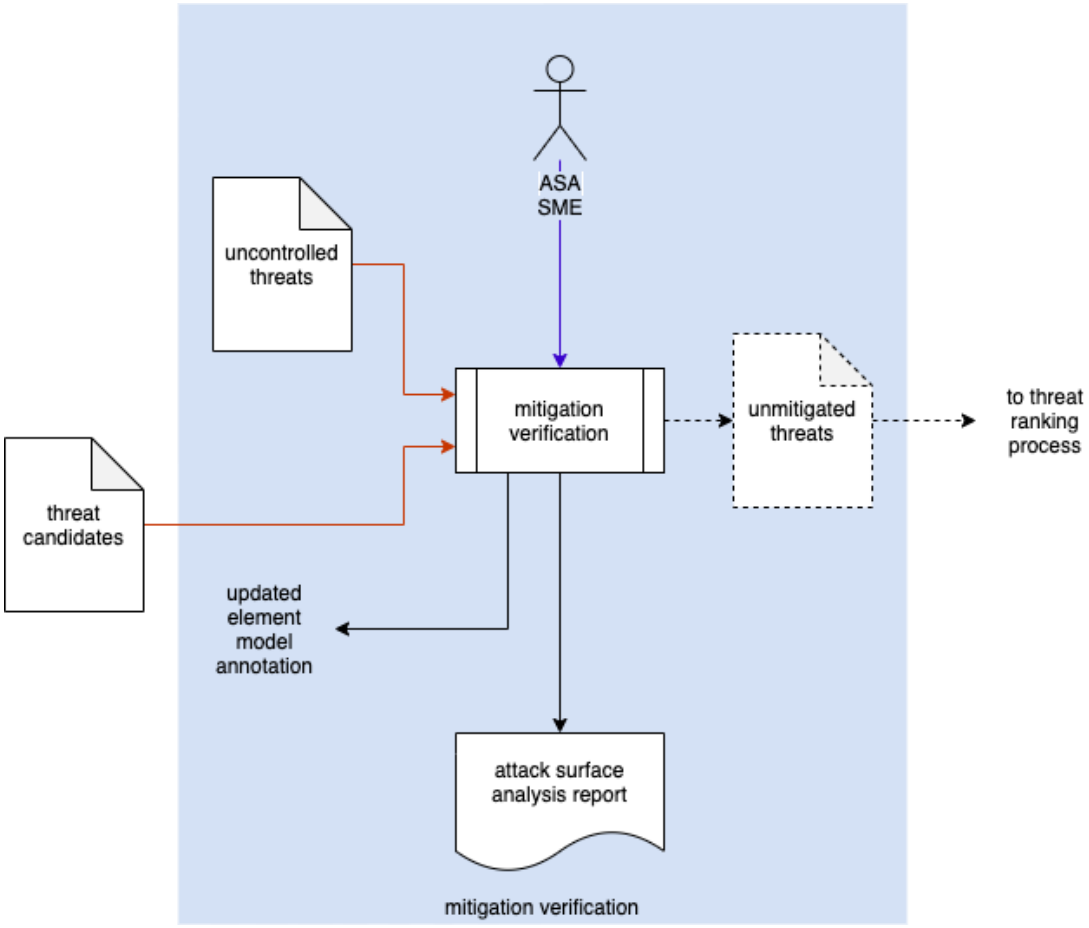
Inputs	Updated element model
Outputs	Threat candidates
Participants	ASA SME



The ASA SME takes the **updated element model** and performs a new analysis. This results in the creation of a list of **threat candidates**.

Mitigation Verification

Inputs	Threat candidates Uncontrolled threats
Outputs	Unmitigated threats
Participants	ASA SME



The ASA SME takes the **threat candidates** and the previously established **uncontrolled threats** generated in the design phase and verifies that all uncontrolled threats have been mitigated. A **attack surface analysis report** is generated. The **updated element model** is annotated with the findings of the verification. If any uncontrolled threats remain, a list of **unmitigated threats** is generated and passed along to the threat ranking process (specified in the **Threat Prioritization Plan**).

References

1. **Threat Prioritization Plan** (AVCDL secondary document)
2. **Attack Surface Analysis Report** (AVCDL secondary document)