Understanding TARA in an AVCDL Context

Revision

Version 4
3/28/22 5:19 PM

Author

Charles Wilson

Abstract

This document describes the lifecycle of a threat analysis and risk assessment (**TARA**) within the context 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.

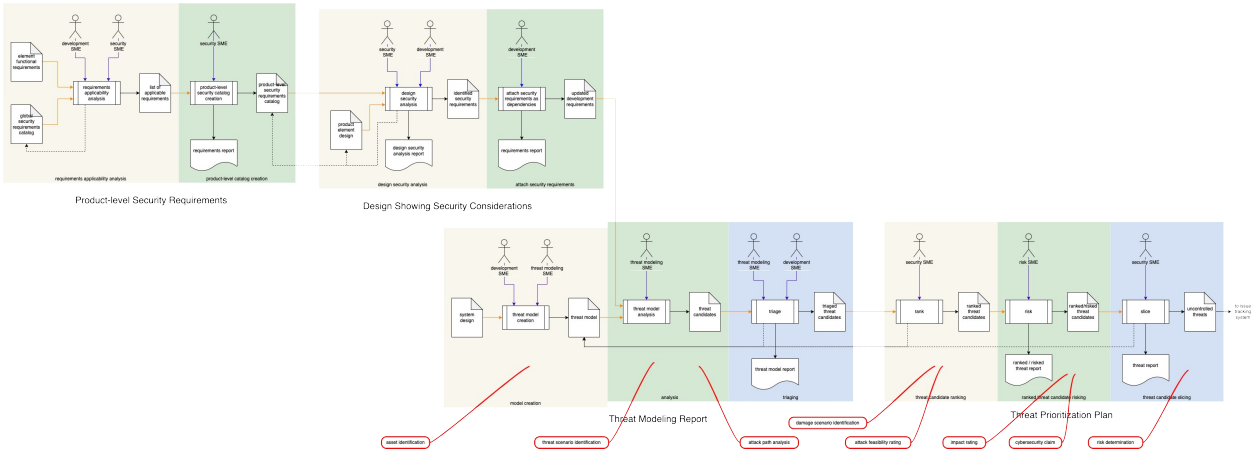
Note: This document is not subject to certification body review.

License

Overview

The TARA is an artifact described in **ISO 21434**. It is intended to be the cybersecurity equivalent of a HARA as described in **ISO 26262**. The **AVCDL** [1] does not use this terminology as the processes used to create such an artifact include those shared by multiple workflows. The **AVCDL** does, however, produce artifacts which achieve the same ends as the TARA.

The following shows processes within the **AVCDL** that have relevance within the context of the TARA.



Here the various **AVCDL** processes have be connected into a single workflow diagram. This allows us to appreciate the scope of the TARA across the **AVCDL**.

Note: Callouts in red show mapping of **ISO 21434** TARA terminology to **AVCDL** activities.

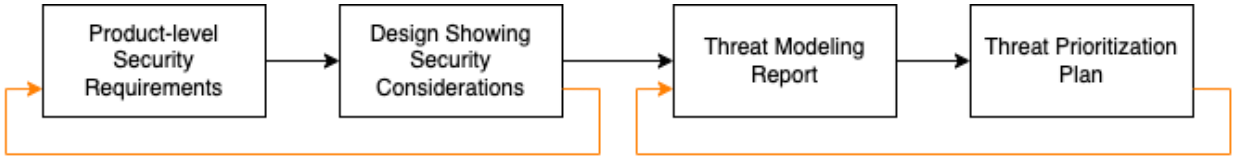
Note: It is recommended that if the reader wishes to view or work with this diagram that they refer to the source of this document in the **AVCDL** GitHub repository.

Absent are several **AVCDL** processes which are precursors to the product-level security requirements [2] creation (shown above). It is not the intent of this document to address the formal issues of traceability as those are sufficiently covered in the **AVCDL** primary document itself (both in the main body and with the traceability diagrams which follow the main text).

Briefly stated, the **Global Security Goals** [8] established based on the organizations cybersecurity policy are used to derive **Product-level Security Goals** [9]. **Global Security Requirements** [10] also based on the **Global Security Goals** and constructed based on the **Security Requirements Taxonomy** [11] are used to derive the **Product-level Security Requirements**. It is presumed, within this document, that these derivations are strictly derived and therefore do not require explicit discussion as to their foundational fulfillment.

Simplified Process Interactions Visualized

You can't really gather much from the above diagram. Let's first look at just the major process interactions.



There are four processes that provide information typically embodied in an **ISO 21434** TARA. Each of the above blocks represents the **AVCDL** secondary document by the same name. It is important to observe that the flow of information is not entirely in one direction. During both the design review [3] and threat prioritization [5] processes, additional information is fed back into the preceding process.

Note: Since the feedback shown above feeds back into review processes, it is assumed that these reviews are undertaken again should such feedback occur.

Information Management

The information used in the creation of the numerous artifacts within the various processes listed above necessitates the use of a diversity of storage mechanisms and embodiments. Description and exploration of these is outside the scope of this document. It is, however, presumed that both machine and human-readable format and embodiments will be necessary to fulfill both developmental and regulatory needs.

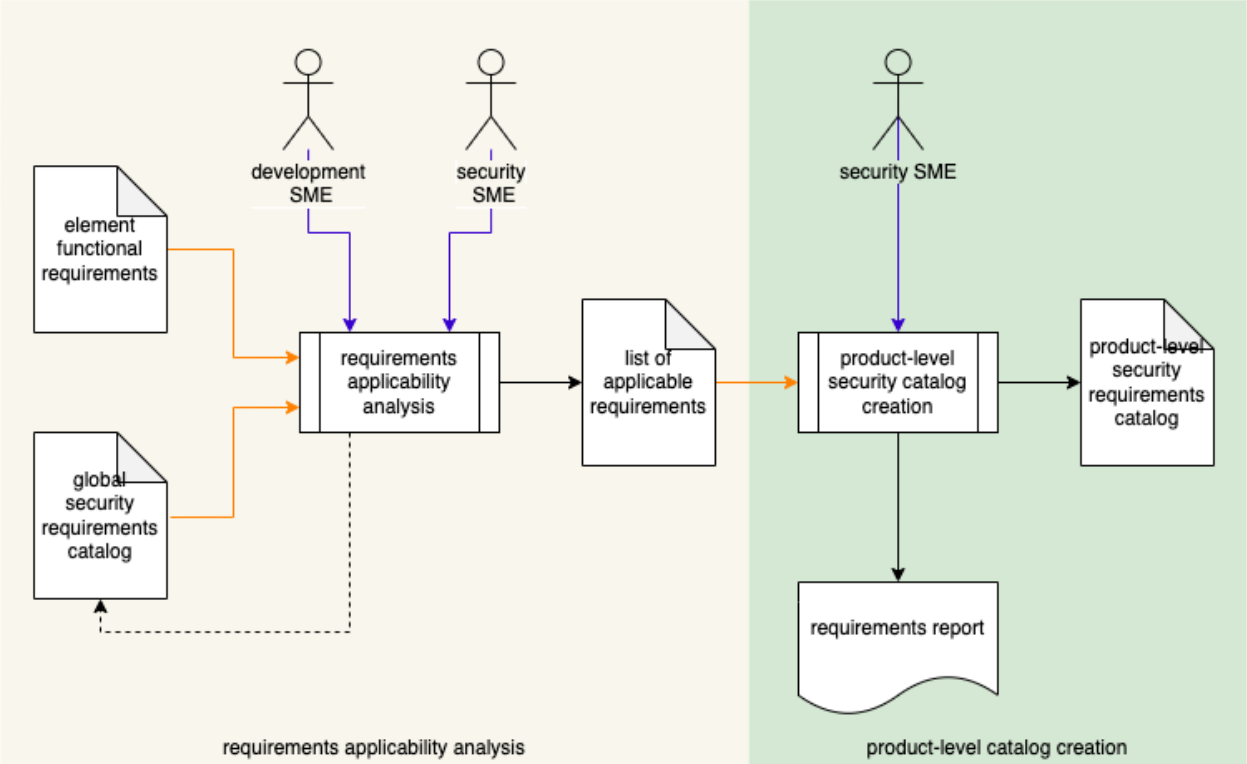
AVCDL Process Interaction

In this section, we'll look at the interactions from each of the four **AVCDL** processes impacting the **ISO 21434** TARA.

Note: This is not a reiteration of the material within these processes, but rather an elaboration on their TARA-relevant aspects.

Product-level Security Requirements [2]

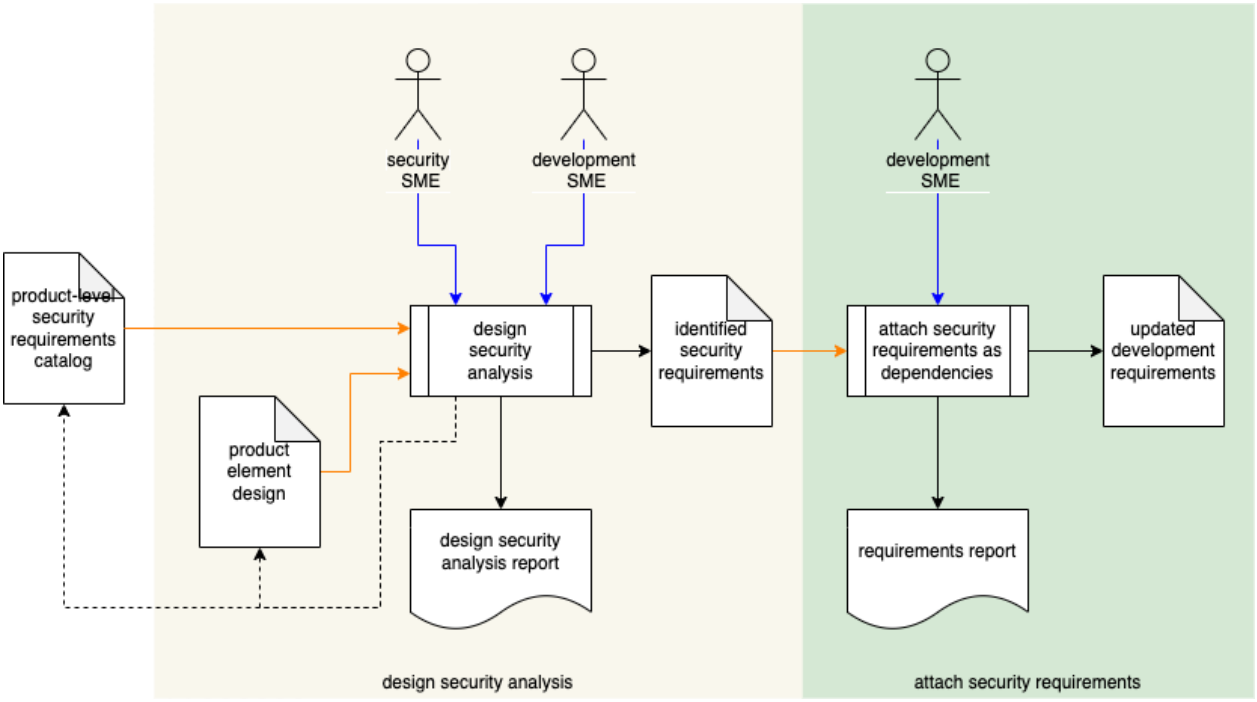
The first process impacting the TARA is that of **Product-level Security Requirements**. This process creates a **product-level security requirements catalog** from the **global security requirements catalog** based on the **element functional requirements**.



As mentioned in the overview, this process is based on and bound to additional work (called out in that section).

Design Showing Security Considerations [3]

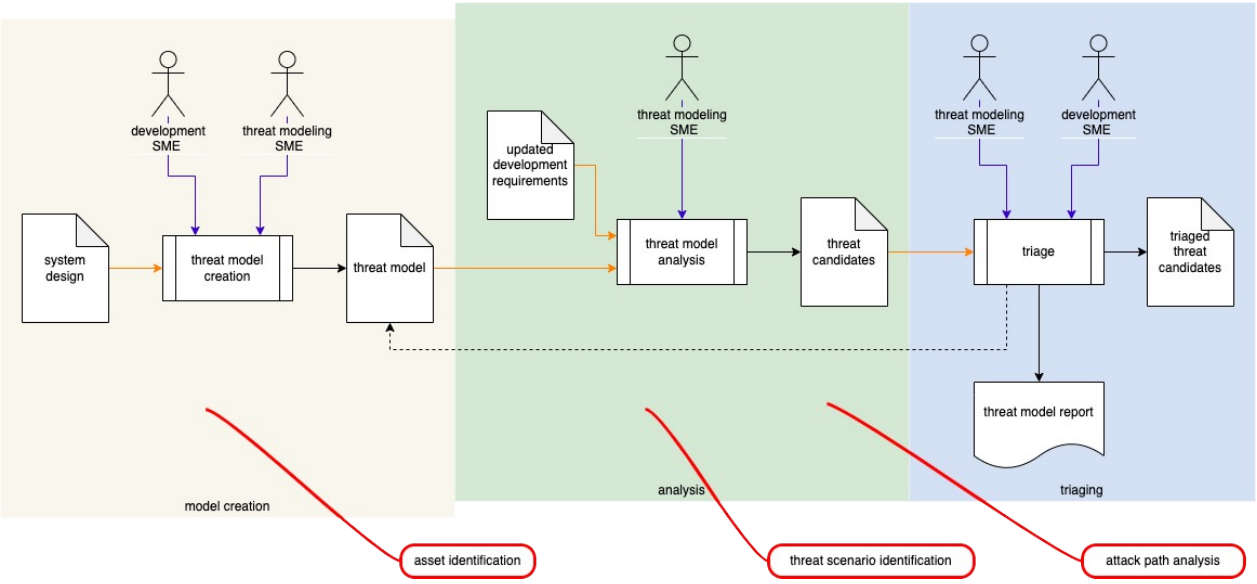
The **Design Showing Security Consideration** process is responsible for review of the product element's design and binding of the appropriate product-level security requirements to the element's functional requirements.



The **updated development requirements** artifact will be used in the threat modeling process.

Threat Modeling Report [4]

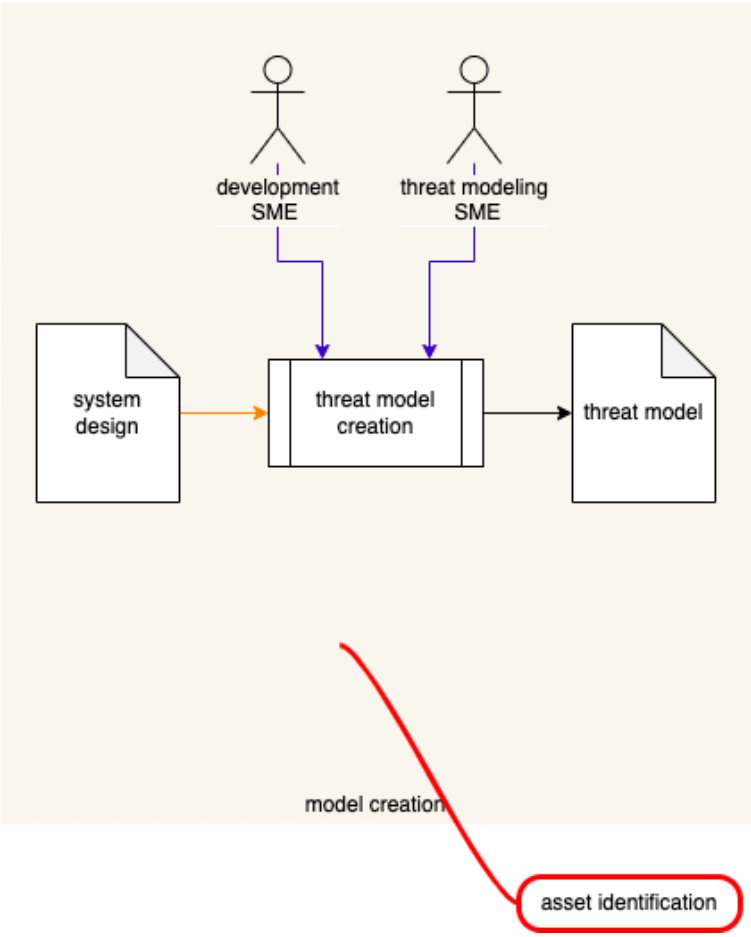
The **Threat Modeling Report** process is where we see the first direct reference to elements identified in the TARA as necessary.



We will look at each of the activities and explain the correspondence between the **AVCDL** and TARA.

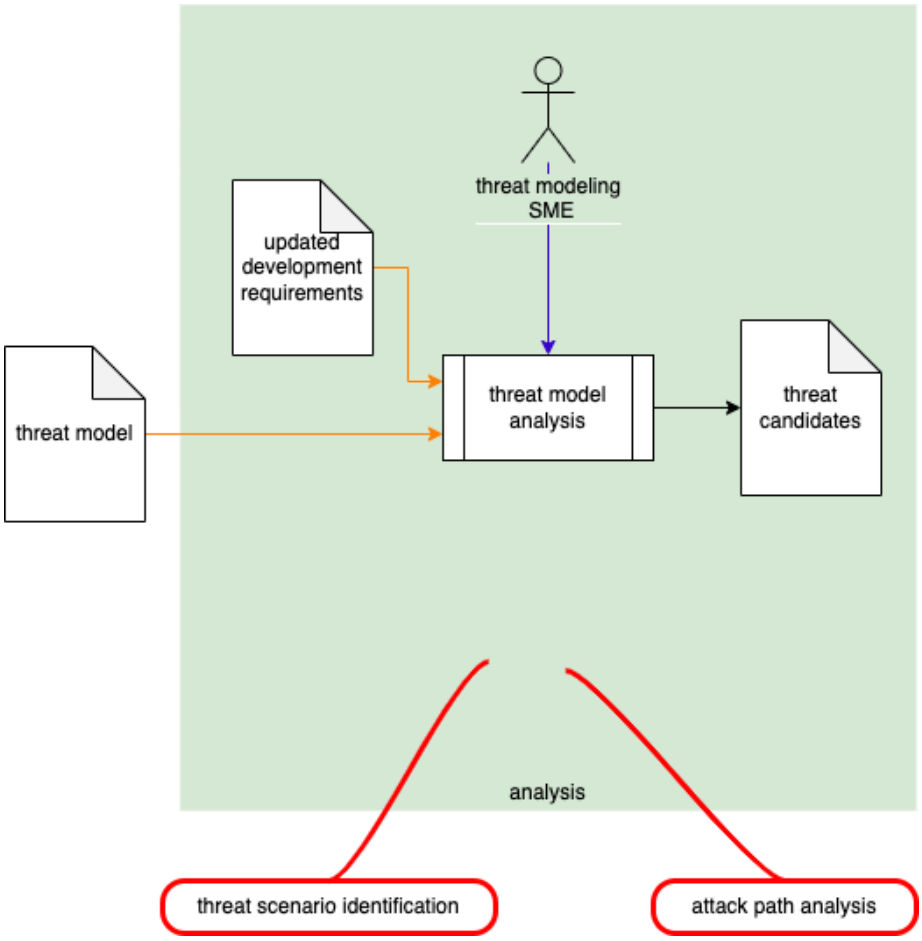
Model Creation:

Asset Identification



TARA **asset identification** is performed during the **model creation** activity. During that activity a model of the element under consideration is created. By its very nature, this requires that assets, data flows and trust boundaries be identified.

Analysis:
Threat Scenario Identification and **Attack Path Analysis**

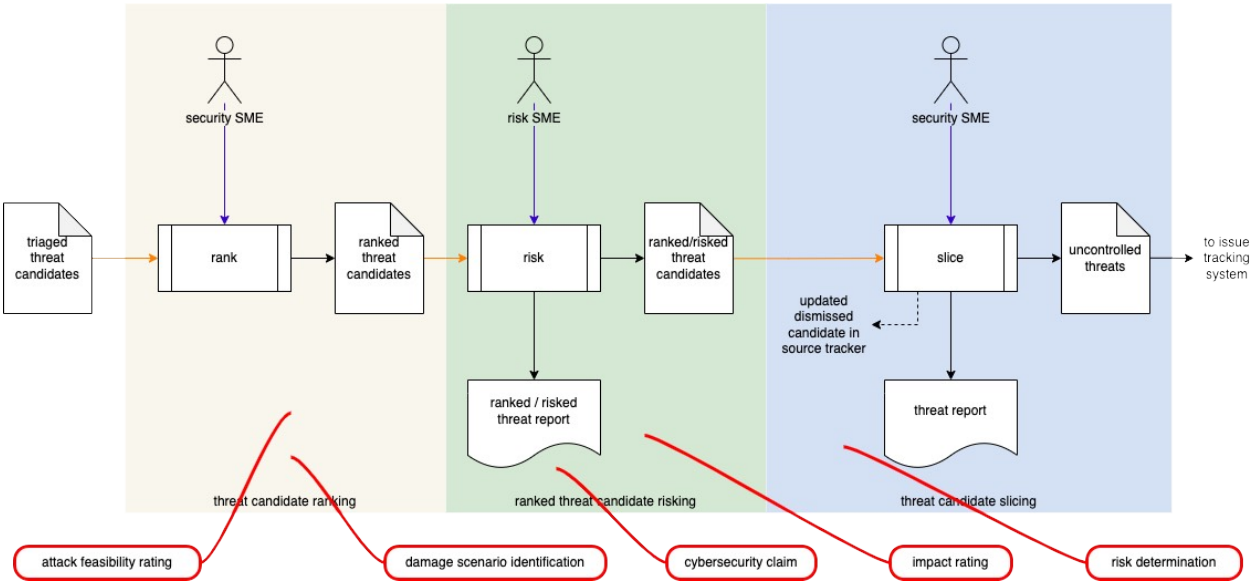


During the **analysis** activity, as the model is reasoned upon in the context of the appropriate security requirements, threat candidates are evoked. At this point we have the equivalent of an **attack path analysis** being performed. Description of these threat candidates detail the **threat scenario** that contextualizes them.

Note: As discussed in ISO 21434 clause 15.6.2 note 1, there is no single methodology by which an attack path analysis is conducted. Such an analysis is the natural consequence of the performance of a threat modeling activity (**Threat Modeling Report** [4]). The information contained in that report is further elaborated upon in the ranking activity (**Ranked / Risked Threat Report** [6]) which is part of the general threat prioritization process (**Threat Prioritization Process** [5]).

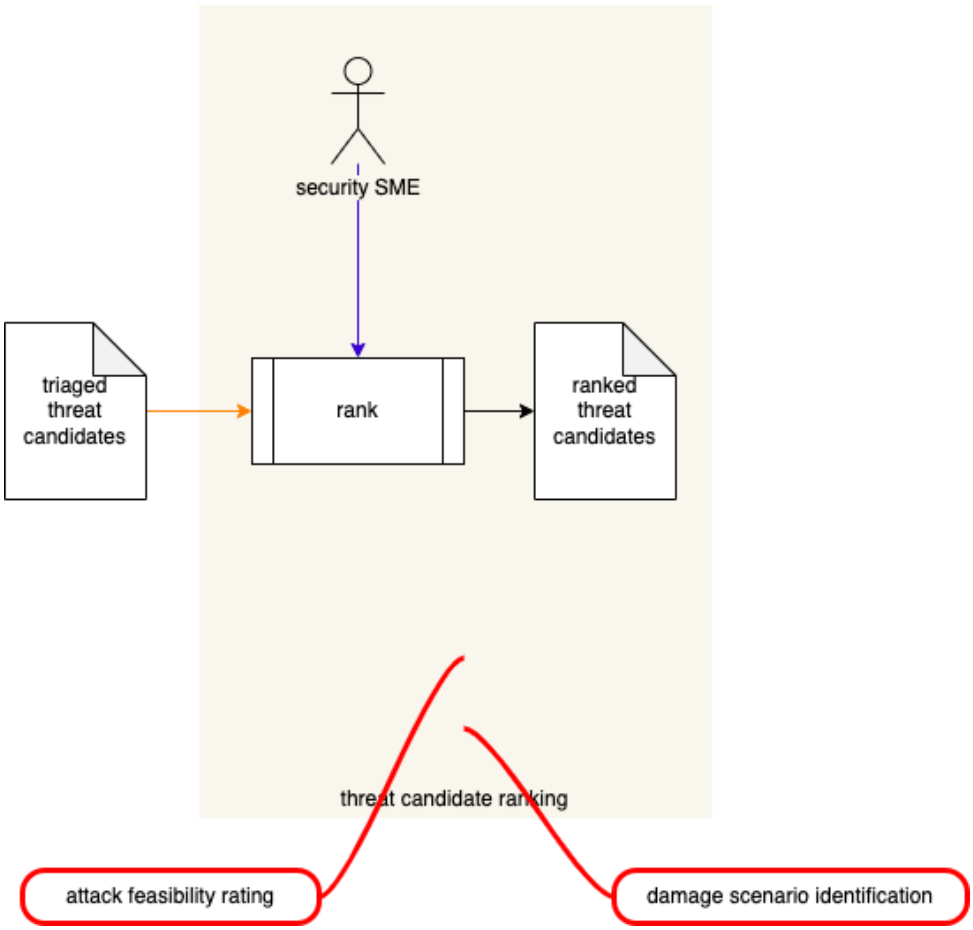
Threat Prioritization Plan [5]

The **Threat Prioritization Plan** process provides consistent mechanism for treatment of issues. These issues may come from threat modeling, attack surface analysis, incident reports, or other sources.



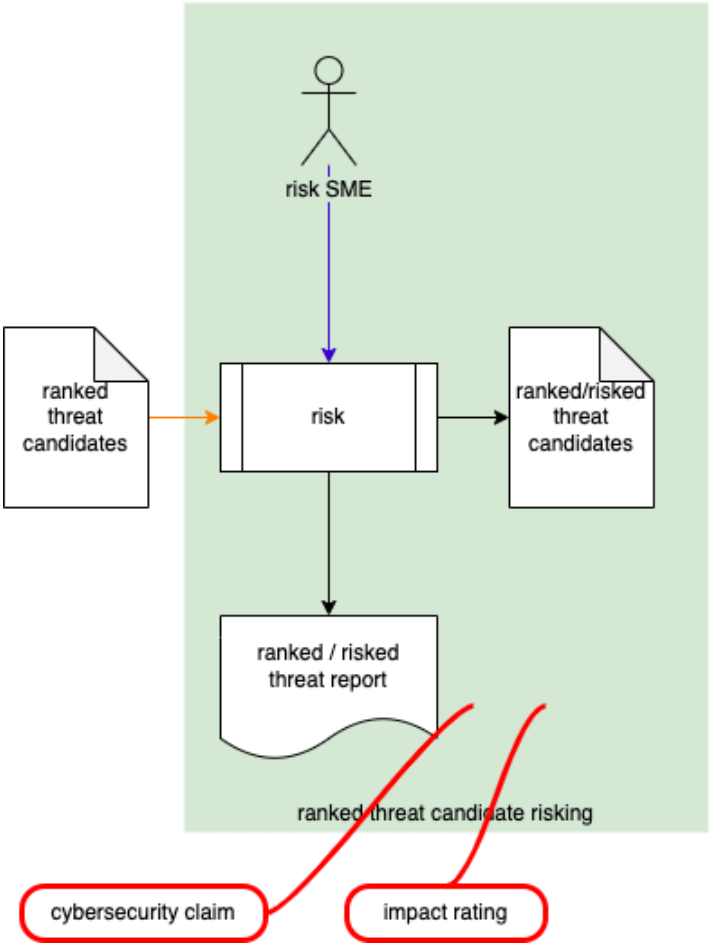
We will now consider the activities in this process.

Threat Candidate Ranking:
Attack Feasibility Rating and **Damage Scenario Identification**



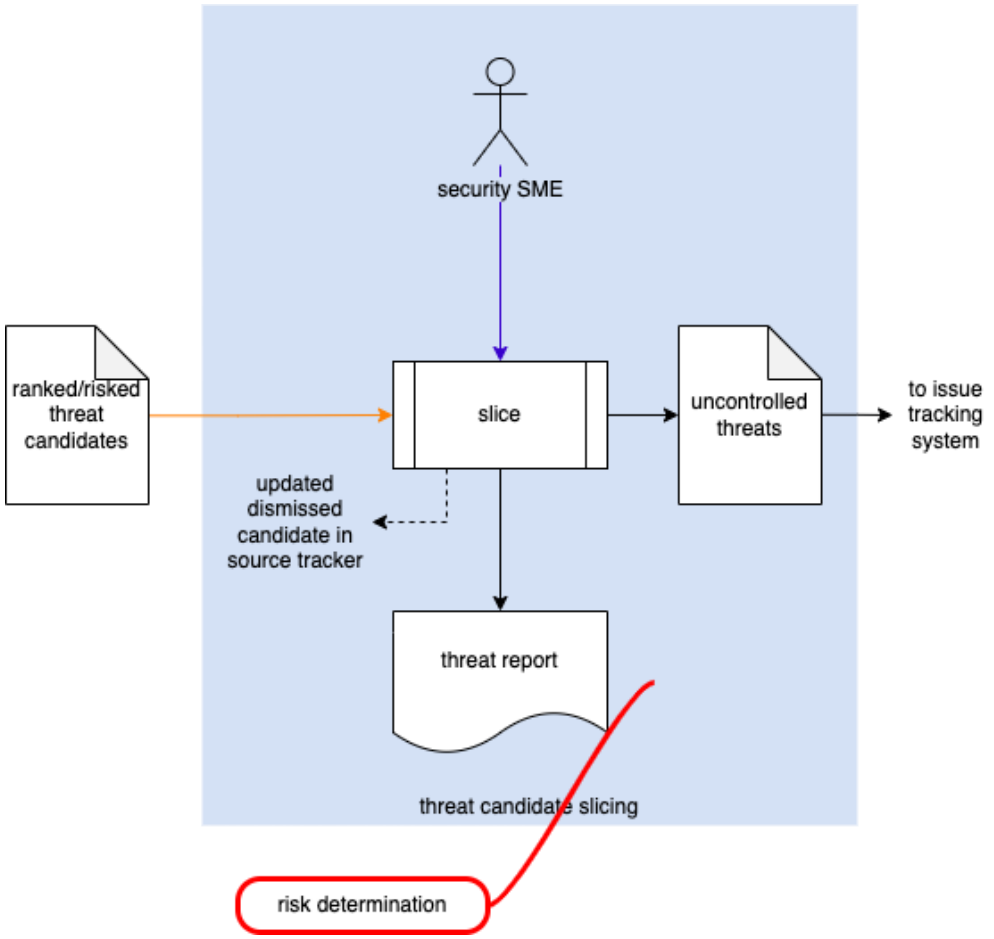
During the **threat candidate ranking** activity, the **triaged threat candidates** are ranked. This is the TARA equivalent of determining an **attack feasibility rating**. At this time a **damage scenario** representing the worst case resulting from the threat being exploited is identified.

Ranked Threat Candidate Risking:
Impact Rating and **Cybersecurity Claim**



During the **ranked threat candidate risking** activity (**Ranked / Risked Threat Report**), the **ranked threat candidates** are risked based on the damage scenario identified during the **threat candidate ranking** activity. This is the TARA equivalent of determining an **impact rating**. The ranked/risked threat candidates contain the justification of value determination which is a **cybersecurity claim**.

Threat Candidate Slicing:
Risk Determination



During the **threat candidate slicing** activity, the **ranked / risked threat candidates** are determined to be either controlled or uncontrolled. This is the TARA equivalent of determining a **risk determination**.

From here, **uncontrolled threats** are transferred to the issue tracking system for standard disposition.

References

1. **Autonomous Vehicle Cybersecurity Development Lifecycle** (AVCDL primary document)
2. **Product-level Security Requirements** (AVCDL secondary document)
3. **Design Showing Security Considerations** (AVCDL secondary document)
4. **Threat Modeling Report** (AVCDL secondary document)
5. **Threat Prioritization Plan** (AVCDL secondary document)
6. **Ranked / Risked Threat Report** (AVCDL secondary document)
7. **Threat Report** (AVCDL secondary document)
8. **Global Security Goals** (AVCDL secondary document)
9. **Product-level Security Goals** (AVCDL secondary document)
10. **Global Security Requirements** (AVCDL secondary document)
11. **Security Requirements Taxonomy** (AVCDL elaboration document)