Decommissioning Plan

Revision

Version 4
4/22/24 4:13 PM

SME

Charles Wilson

Abstract

This document describes the process to handle the cybersecurity aspects of decommissioning safety-critical, cyber-physical systems or components therein.

Group / Owner

Security / Partner Integration Planner

Motivation

This document is motivated by the need to have formal processes to securely decommission a safety-critical, cyber-physical system for certification of compliance to standards such as **ISO/SAE 21434** and **ISO 26262**.

License

Overview

Stored within the systems of an safety-critical, cyber-physical systems may be cryptographic materials that allow for secure data storage, transmission and manipulation. These materials need to be removed from the vehicle systems at the time of decommissioning. They include:

- Credentials
- Certificates
- PII
- Logs
- Location history
- Previous destinations
- Call history
- Stored contacts

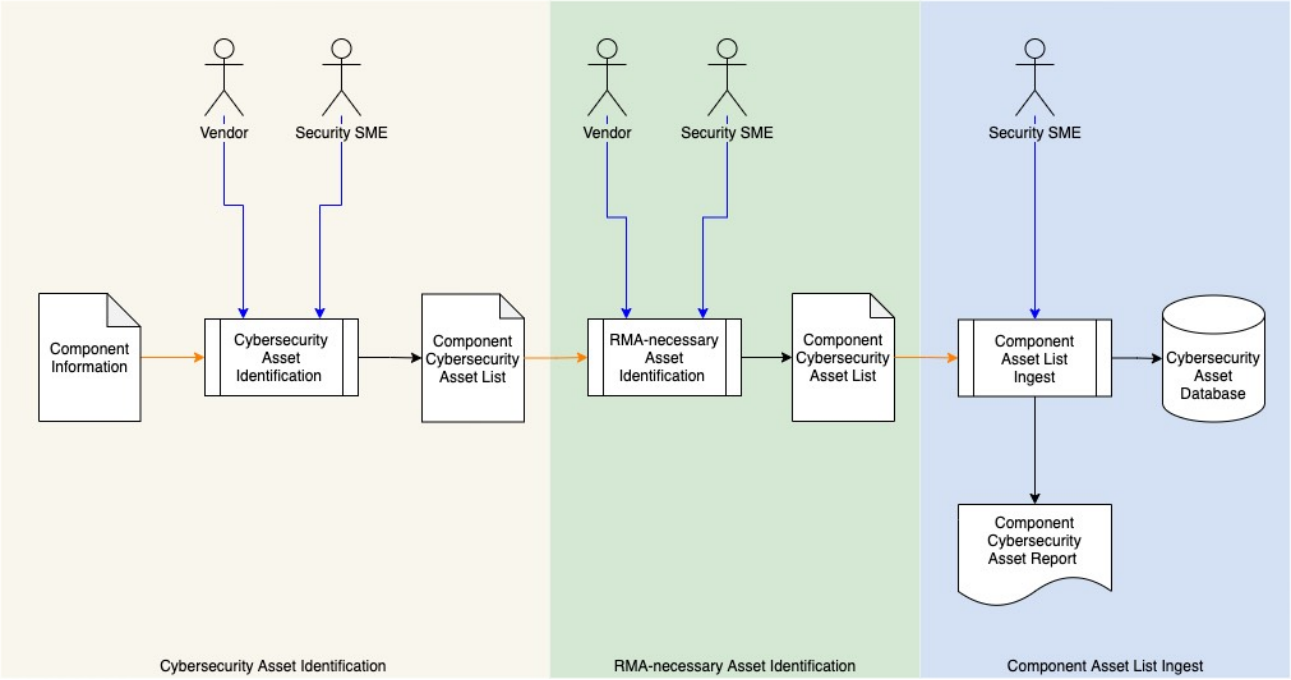
There are two modalities within the context of decommissioning:

- RMA (Return Merchandise Authorization) [1]
- EoL (End-of-Life)

Process

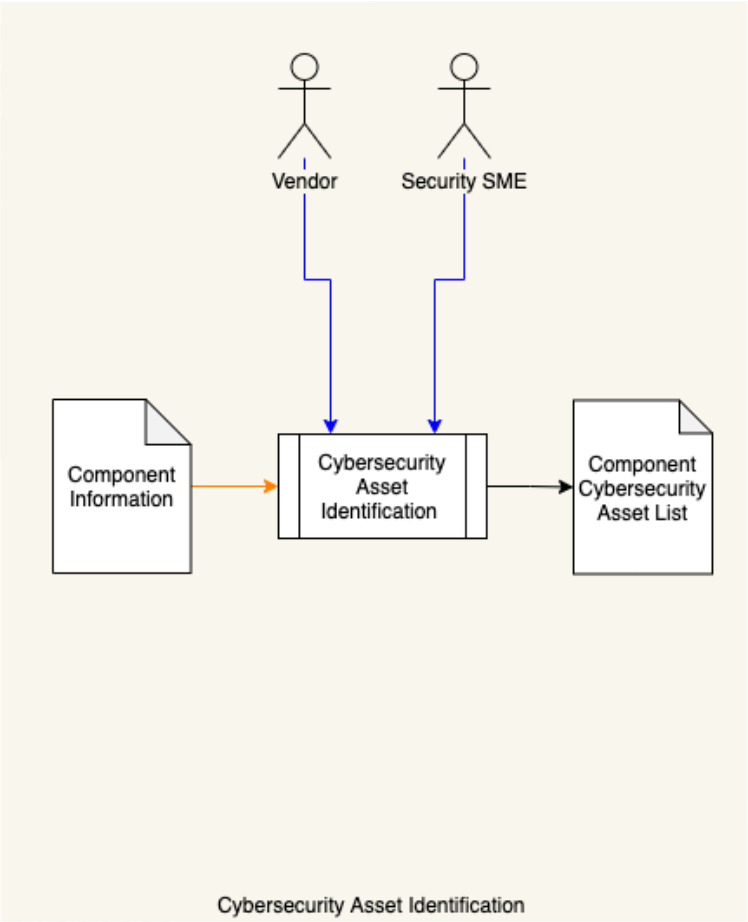
Inventory

In order to remove a vehicle or component from service (whether for repair, upgrade, or end-of-life) without risking disclosure, it is first necessary to know what cybersecurity assets reside within the system in question. The process of creating such an inventory can be visualized using the following overview:



Cybersecurity Asset Identification

Inputs	Component Information
Outputs	Component Cybersecurity Asset List
Participants	Vendor, Security SME

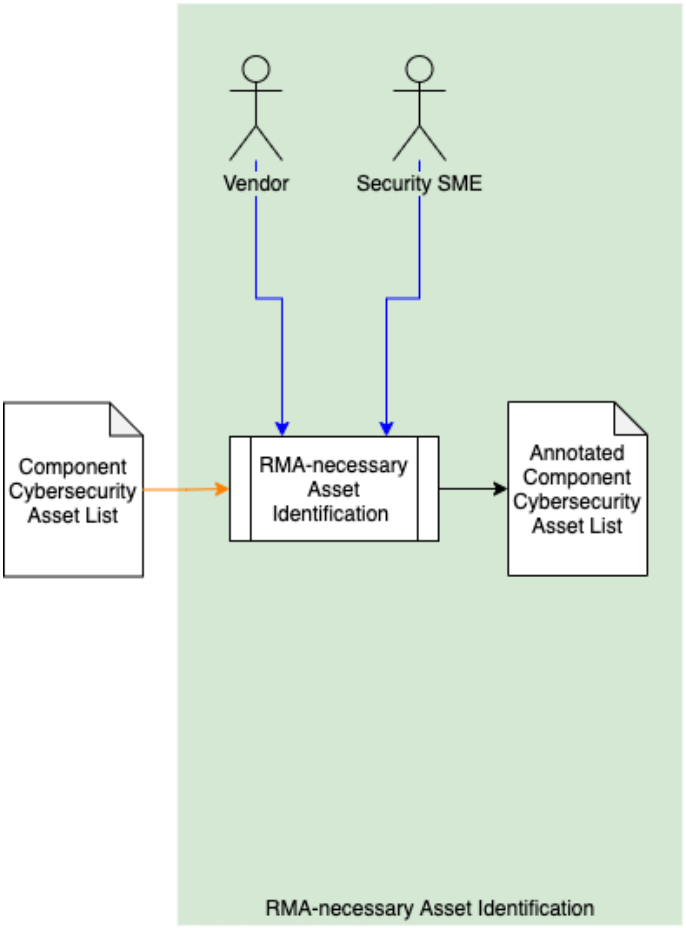


Cybersecurity Asset Identification

Using the **Component Information**, the vendor and security SME identify all cybersecurity-relevant assets within the component. These are compiled into a **Component Cybersecurity Asset List**. Additional information regarding the component necessary to later identification such as hardware and software versions, component model, etc. is also noted.

RMA-necessary Asset Identification

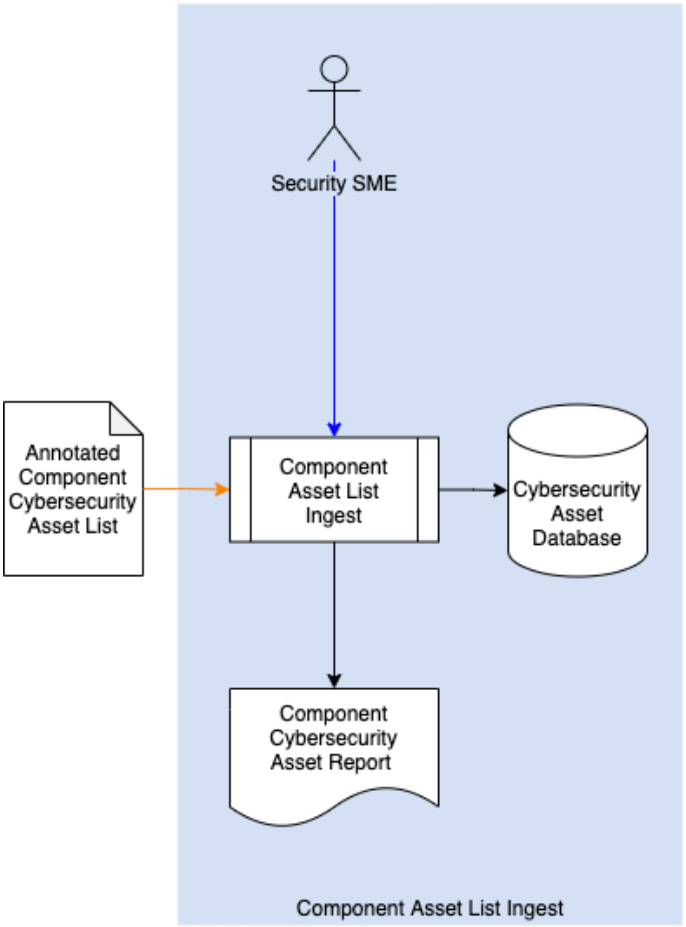
Inputs	Component Cybersecurity Asset List
Outputs	Annotated Component Cybersecurity Asset List
Participants	Vendor, Security SME



Using the **Component Cybersecurity Asset List**, the vendor and Security SME identify all assets needed by the vendor in order to diagnose issues which may occur in the component. This information is used to annotate asset list yielding an **Annotated Component Cybersecurity Asset List**. This annotation may be as simple as identification or may include characteristics of the asset needed to perform diagnostics (unencrypted data, null credentials, etc.).

Component Asset List Ingest

Inputs	Annotated Component Cybersecurity Asset List
Outputs	Cybersecurity Asset Database Component Cybersecurity Asset Report
Participants	Security SME



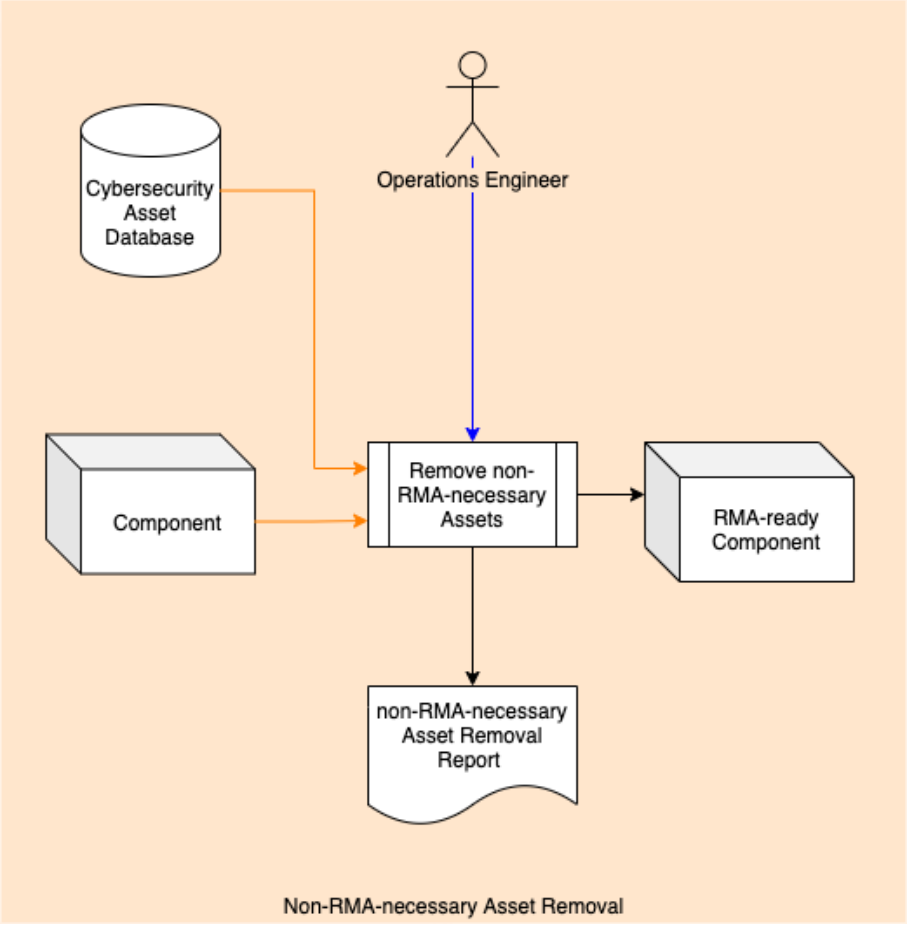
Using the **Annotated Component Cybersecurity Asset List**, the Security SME ingests data creating appropriate entries in the **Cybersecurity Asset Database**. A **Component Cybersecurity Asset Report** is also generated.

Removal from Service

As noted in the overview there are two decommissioning modalities (RMA and EoL). These will be addressed in turn.

RMA

Inputs	Cybersecurity Asset Database Component
Outputs	RMA-ready Component non-RMA-necessary Asset Removal Report
Participants	Operations Engineer

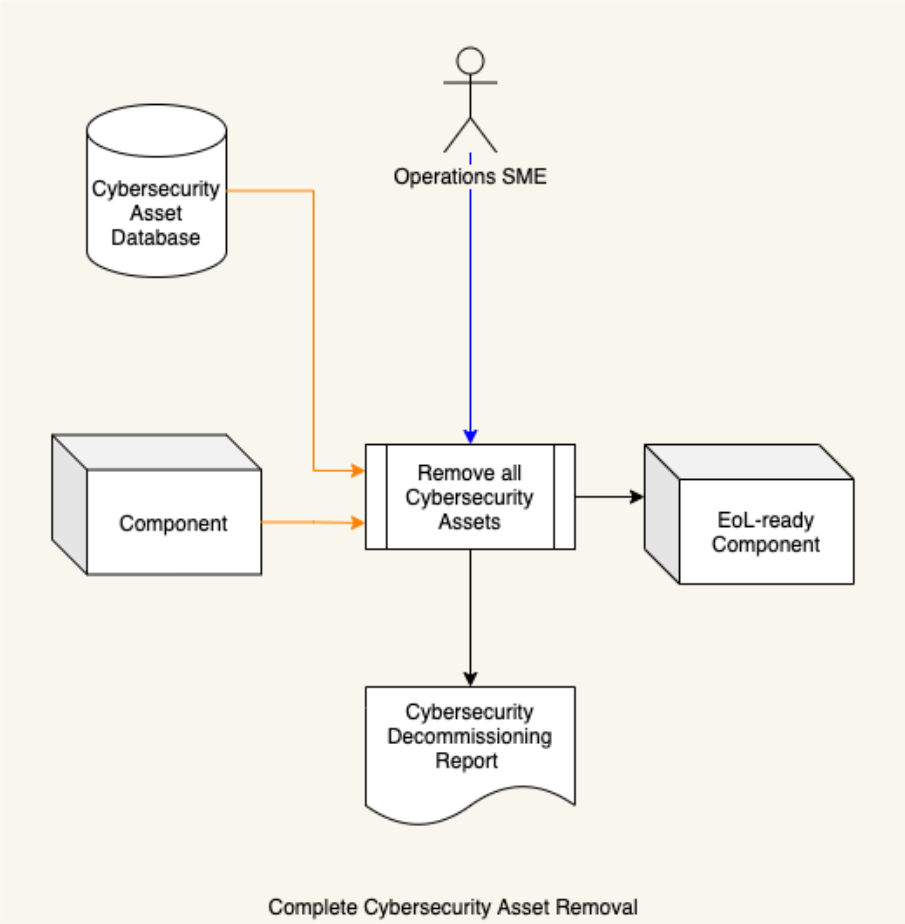


Using the **Cybersecurity Asset Database**, the operations engineer removes all non-RMA-necessary assets from the **Component**. At this time, all assets or data governed by them are modified per vendor specifications for return of the component for repair. The result will be an RMA-ready Component. Additionally, a **non-RMA-necessary Asset Removal Report** [2] is generated.

Note: When decommissioning a vehicle or component therein in order to perform an RMA activity, care must be taken to maintain as much of the information needed by the supplier of the component to be serviced as possible without disclosure of unnecessary information which may lead to a compromise of security either of a single vehicle or across the fleet.

EoL

Inputs	Cybersecurity Asset Database Component
Outputs	EoL-ready Component Cybersecurity Decommissioning Report
Participants	Operations Engineer



Complete Cybersecurity Asset Removal

Using the **Cybersecurity Asset Database**, the operations engineer removes all cybersecurity-relevant assets from the **Component**. At this time, data is wiped from the component [3]. The result will be an EoL-ready Component. Additionally, a **Cybersecurity Decommissioning Report** [2] is generated.

Note: When decommissioning a vehicle in order to permanently remove it from service, all security sensitive information must be securely removed from the vehicle as leaving it may lead to a compromise of security either of a single vehicle or across the fleet.

References

1. **Return merchandise authorization**
   https://en.wikipedia.org/wiki/Return_merchandise_authorization
2. **Decommissioning Report** (AVCDL secondary document)
3. **NIST SP 800-88 r1 – Guidelines for Media Sanitization**
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf