Product-level Security Goals

Revision

Version 4
5/3/22 1:29 PM

SME

Charles Wilson

Abstract

This document describes the product-level security goals.

Group / Owner

Security / Security Architect

Motivation

When creating a safety-critical cyber-physical system, it is insufficient to have arbitrary cybersecurity requirements. Those requirements need to be motivated by overarching goals which justify them. In turn these goals must derive from cybersecurity concepts. Finally, the global security goals are refined and applied at the product level.

License

Overview

Product-level security goals need to both consider the global security goals and add constraints necessary to the specifics of the product under consideration.

Product-level security goals provide the justification and traceability for product-level security requirements.

The following goals were adapted from the UN working group on autonomous vehicle cybersecurity[1].

Product Goals

Product goals drive the creation of product cybersecurity requirements.

1. The storage and transmission of data should be secure and should be controlled.
2. The vehicle and its backend supporting systems should be designed to be resilient to cyberattacks.
3. The vehicle and its backend support systems should be designed with the capability to detect cyberattacks and respond appropriately.

References

1. UNECE trans WP.29 GRVA 2019 2 - **World Forum for Harmonization of Vehicle Regulations: Proposal for a Recommendation on Cyber Security**
   https://unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf