Global Security Goals

Revision

Version 4
5/3/22 1:31 PM

SME

Charles Wilson

Abstract

This document describes the cybersecurity goals on an organizational, process and product level as applied to the development of an autonomous vehicle.

Group / Owner

Security / Systems Requirements Planner

Motivation

When creating a safety-critical cyber-physical system, it is insufficient to have arbitrary cybersecurity requirements. Requirements need to be motivated by overarching goals which justify them. In turn these goals must derive from cybersecurity concepts. Organizations support these goals through the creation of policies. Finally, the development lifecycle processes need to be informed by cybersecurity.

License

Overview

The following goals were taken from the UN working group on autonomous vehicle cybersecurity[1]. They provide a set of cybersecurity principles, styled here as goals. They have been split into organizational, process and product goals as the ways in which each set is implemented differs greatly.

Goals

Organizational Goals

Organizational goals drive the creation of policies needed to ensure proper governance of cybersecurity-related efforts.

1. Organizational security should be owned, governed and promoted at the highest organizational level.
2. Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain.
3. Organizations should implement cyber security monitoring and incident response to ensure systems are secure over their lifetime.
4. All organizations, including sub-contractors, suppliers and potential third parties, should work together to enhance the security of the system.

Process Goals

Process goals drive the creation of lifecycle management processes.

1. The vehicle should be designed using a defense-in-depth approach.
2. The vehicle manufacturer should design the vehicle architecture to reduce the likelihood that compromise of assets within one architectural element would result in propagation of the attack to other architectural elements.
3. The security of software should be managed throughout its lifetime.
4. The vehicle manufacturer should assess security functions with testing procedures.

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 should be designed to be resilient to cyberattacks.
3. The vehicle 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://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf**