A Review of the Relationship Between Cyber-Physical Systems, Autonomous Vehicles and Their Trustworthiness

Craig Morrison[a], Elena Sitnikova[a], Shraga Shoval[b]

[a]University of NSW, Australian Centre for Cyber Security, ADFA Canberra, ACT, Australia
[b]Ariel University, Industrial Engineering & Management, Israel

craig.morrison@student.adfa.edu.au e.sitnikova@adfa.edu.au
shraga@ariel.ac.il

Abstract: A concentration of development in cyber-physical systems containing advanced sensors, sub-systems and machine-learning algorithms over the past decade is equipping unmanned aerial and road vehicles with autonomous decision-making capabilities. The level of autonomy depends upon the make-up and degree of sensor sophistication and the vehicle's operational application, which can range from extremely high cost military-based combat vehicles, to commercially available civilian motor vehicles and very low-cost sub $100 hobby drones. As a result, the risk of autonomous vehicles being compromised and used as an improvised threat has become more serious and therefore trust-based methods to mitigate them are needed. This paper reviews the relationship between cyber-physical systems, automated and autonomous vehicles and their trustworthiness. It examines the significant role cyber-physical systems play in building sub-system, system, and system-of-system layers found in contemporary vehicles as well as the level of human involvement in decision control loops, and the trustworthiness challenges this creates across levels of vehicle automation and autonomy. Further, the paper reviews material on methods to authenticate a vehicle's "world-view" and the veracity of information it may communicate and share with other vehicles and infrastructure. It finds that to be trustworthy, automated and autonomous vehicles will need to implement data verification frameworks and methods. It recommends that future research be conducted into the effectiveness of implementing a pervasive trustworthiness hub where information flowing between heterogeneous autonomous vehicles and infrastructure within their surrounding environment can be authenticated.

Keywords:
Cyber-physical systems, autonomy, unmanned vehicles, human in/on the loop, trustworthiness, cyber-security

Introduction

Intensive development in advanced sensors, sub-systems and machine-learning algorithms over the past decade has equipped vehicle-based cyber-physical (VCP) systems with automated and autonomous decision-making capabilities. Depending upon the level of autonomy, humans can be "in-the-loop" for decision control, play a supervisory "human-on-the loop" role for escalated decisions, or be completely "out-of-the loop" where there is no human intervention or control over a system to reliably carry out its purpose (Nothwang et al., 2016, Issitt, 2016, Weber, 2014). Such high-level systems autonomously process and interpret an array of complex inputs to form a "world-view" contextual map of the surrounding environment and an awareness of its place within it without any operational human assistance (Anderson et al., 2014). The level of autonomy depends upon the mixture and degree of sensor sophistication and the vehicle's operational application which can range from extremely high cost military-based combat vehicles, to commercially available civilian motor vehicles and very low cost, sub $100 unmanned aerial vehicle (UAV) hobby drones. However, as predicted by Moore's Law, the gap between technology cost and sophistication is falling rapidly as the volume of component mass production increases to meet market demand (Mulay, 2016). As a result, there is a significant and present risk of easily accessible, autonomous VCP systems being able to be compromised and used as improvised threats in both theatres of conflict and civilian contexts. The threats are often unidentified and they will become more serious unless trust-based methods to mitigate them are further researched and better understood (Hartmann and Giles, 2016).

The purpose and significance of this paper is to explore and understand the trustworthiness problem inherent in automated and autonomous VCP systems through a review of contemporary literature and current commercial trends. In the first section cyber-physical (CP) systems are explained within a vehicular context, their classification and application. The degree of vehicular automation and autonomy is then examined in section two where autonomous vehicles (AVs) are viewed from different human-machine interaction levels: 1) where