Original Article

JDMS

Journal of Defense Modeling and Simulation: Applications, Methodology, Technology
1–13
© The Author(s) 2015
DOI: 10.1177/1548512915575803
dms.sagepub.com
SAGE

A study on cyber-security of autonomous and unmanned vehicles

Eray Yağdereli, Cemal Gemci and A Ziya Aktaş

Abstract

Technological developments towards vehicle automation have been taking place for years. Satellite navigation, cruise control and anti-lock braking systems (ABS) are well-known examples of automation technology used in everyday cars. The trend of automation technology being used in vehicles is expected to move closer to full autonomy through technological advancements in robotics and artificial intelligence. As a result, our daily lives will become more and more dependent on digitally-controlled devices and vehicle systems (partially or highly automated). On the other hand, computing and digital systems also have a tendency to become more fragile and susceptible to faults and failures because of cyber-attacks and software and hardware defects, as well as accidental defects introduced by developers. Therefore, autonomous vehicle systems must be developed to bear such dangers in mind and must be equipped with defensive capabilities and measures such that they can be able to respond automatically and dynamically to both accidental and deliberate defects and attacks. In this study, autonomous and unmanned vehicle systems are examined for their cyber-security vulnerabilities. Threats and attacks exploiting these vulnerabilities are identified and classified. Development guidelines and a mitigation strategy to be used in the development of autonomous and unmanned vehicle systems are proposed and discussed in the final section.

Keywords

Autonomy, autonomous vehicles, communication security, cyber-security metrics, infrastructure vulnerability, instrument landing system, intelligent transportation systems, unmanned aerial vehicle (UAV), unmanned sea/surface vehicle (USV)

1. Introduction

In recent years, the successful applications of unmanned systems in the battlefield, space, the deep sea and other dangerous and distant environments have attracted much research interest. Unmanned systems include deep space probes, spacecraft, unmanned aerial vehicles (UAV), unmanned ground vehicles (UGV), unmanned sea/surface vehicles (USV), unmanned underwater vehicles (UUV), unmanned munitions and unmanned sensors. Autonomy has been defined in many studies, but the definition proposed by the autonomy levels for unmanned systems (ALFUS) working group of the National Institute of Standards and Technology (NIST) is the most comprehensive and standardized.[1] Thus, the autonomy of an unmanned system (UMS) may be defined as follows:

> "a UMS's own ability of sensing, perceiving, analyzing, communicating, planning, decision making, and acting, to achieve its goals as assigned by its human operator(s) through designed human-robot interaction (HRI). Autonomy is characterized into levels by factors including mission complexity, environmental difficulty, and level of HRI to accomplish the mission."[2]

From this definition, one may conclude that "autonomy" is the unmanned system's capability of being independent of an operator and being self-managed. One, then, can define autonomous vehicles as machines which can operate themselves without human input or supervision. Unmanned vehicles can be defined as vehicles which are

Computer Engineering Department, Başkent University, Turkey

Corresponding author:
A Ziya Aktaş, Computer Engineering Department, Başkent University, Bağlıca Kampusu, Eskişehir Yolu 20. Km. 06530 Ankara, Turkey.
Email: zaktas@baskent.edu.tr

either controlled remotely or operated autonomously. Autonomous vehicles can also operate semi-autonomously: a human operator retains control of vehicle, while some control functions of vehicle function are autonomous. Although it is early for the application of fully autonomous and unmanned technologies for public usage in our daily lives, technological advancements in robotics and artificial intelligence are increasingly opening up a wide range of potential applications for them.

Autonomous and unmanned vehicle technology has already achieved a high degree of development. Most modern cars incorporate features which allow them to operate semi-autonomously such as self-parking and adaptive cruise control, while unmanned aerial systems (unmanned air vehicles (UAVs) in military terms) have already been employed for military purposes for the last three decades.[3] It is expected that commercial and public applications of these developments in autonomous technologies will make self-driving cars, unmanned aerial vehicles, flying machines and other robotic devices part of our daily lives within a few decades.

Since autonomous vehicles can potentially carry out tasks more safely and efficiently than humans, they are being employed and will be employed for a wide range of hazardous or labor intensive activities by military, industry and some government agencies. For example, autonomous and unmanned vehicles already have been used to survey tunnels, take samples in volcanoes, explore the deep ocean, perform reconnaissance over hostile regions and even to carry out scientific research on Mars.[4]

However, one of the biggest impediments to widespread usage of autonomic vehicle systems in our daily lives is the public safety and public acceptance of leaving human lives in control of autonomous machines/vehicles. For example, today's category IIIc commercial aircraft are able to take off and land themselves automatically. It is good to know that the aircraft has automatic landing capability if something happens to the pilots, but who wants to travel with an airline whose aircrafts take off and land by themselves instead of pilots? Especially when we take into account ever increasing cyber-threats and some notorious aircraft accidents caused by pilots depending blindly on auto pilot systems such as the Asiana flight 214 accident (on 6 July 2013).[5]

Autonomous vehicles, especially the ones that will be used in areas concerning human life, such as transportation, must be developed with capabilities to handle and decide as human operators, especially when they are under cyber-attack or have failing hardware onboard.

In the following sections, first, emerging autonomous unmanned vehicle usage areas are overviewed. Secondly, potential cyber-security vulnerabilities, threats and attacks are examined. Finally, some design guidelines and mitigation strategies for securing autonomous unmanned vehicles are proposed and discussed.

2. Autonomous vehicle categories

Visions of unmanned and autonomous machines are not new. Experiments with unmanned aircraft began in World War I, and a radio controlled car was demonstrated in the streets of New York in 1925.[6] Self-driving trains have been in use on metro systems since the 1960s. Recent years have seen considerable progress towards the goal of autonomous and unmanned vehicles, which are using increasingly sophisticated artificial intelligence and robotics capabilities. These technological advances are very promising especially in two major categories of autonomous and unmanned vehicles: (i) autonomous cars and (ii) unmanned aerial systems (UAS). Advances in autonomous cars probably will introduce the biggest change to vehicles since the motorcar replaced the horse and cart.

2.1. Autonomous cars and other highway vehicles

A fully autonomous car can be defined as a car that is able to perceive its environment, decide what route to take to its destination and drive it. The development of this technology could allow significant changes to travel; everyone in the car could be a passenger, or the car could even drive with no occupants at all.[7]

Incremental steps towards vehicle automation have already been taking place for years. Anti-lock braking systems (ABS), automatically activated safety mechanisms, have been mandatory on new European Union (EU) passenger cars since 2007.[8] Assisted-driving functions such as satellite navigation and cruise control have almost become standard equipment in even economy class cars. Modern cars contain many electronic control units (ECUs), computers which control everything from a car's engine to onboard entertainment systems. ''Drive-by-wire'' technology, which replaces traditionally mechanical connections with electrical systems (analogous to aviation's ''fly-by-wire''), has also become increasingly common.[9] The trend of automation is expected to continue, and through the innovation of new features, everyday cars are likely to progressively move closer to full autonomy. In Table 1, autonomous features of cars and other highway vehicles such as lorries, buses, etc., which are mostly referred to as advanced driver assistance systems (ADASs), are summarized.[10]

Over the next five to ten years, ADASs such as the ones listed in Table 1 are likely to become more standard, and cars are expected to become increasingly digitized. Their computerized functions are likely to be better integrated, with a view to developing fully autonomous capabilities.[10] The development of autonomous navigation systems will be a significant contribution in moving towards this goal. This will mean that a car should not only avoid dangerous situations and maintain a direct route to the destination,

Table 1. Levels of autonomy in highway vehicles.

Levels of Autonomy	Existing Examples	
1. Driver only	The vehicle is entirely under human control but may have some automated systems.	Cruise control; electronic stability control; anti-lock brakes .
2. Driver assistance	The steering and/or acceleration are automated but the driver must control the other functions.	Adaptive cruise control: distance to car in front maintained; Pparking assistant: steering is automated, driver controls accelerator and brakes.
3. Partial autonomy	The driver does not control steering or acceleration but is expected to be attentive at all times and take back control instantaneously when required.	Adaptive cruise control with lane keeping.; Ttraffic jams assistance.
4. High autonomy	Vehicles are able to operate autonomously for some portions of the journey. Transfer of control back to the human driver when a warning happens. Similar to cruise control systems employed today's cars.	Oxford's Robot car project and, early prototypes of Google's Driverless Car which allows a human driver to take control of the car by stepping on the brake or turning the wheel.
5. Full autonomy	The vehicle is capable of driving unaided for the entire journey with no human intervention, potentially without a human in the car.	Driverless cars, which have no steering wheel, gas pedal, or brakes; 100% autonomous.

but also be able to choose different routes to its final destination based on factors such as traffic conditions.[11] This would require a far more complex awareness of road protocols such as how to behave at traffic lights and junctions, and how and when to change lanes. It is hard to predict how long these things could take, and they may take time, but autonomous driving is likely to become progressively more advanced and common place.

As cars become increasingly built around digital systems, there could be a need for common information and communication technology (ICT) protocols and frameworks.[12]

Wirelesses networking among the vehicles and in the vehicle itself come in two forms:

- inter-vehicle networking around the vicinity of the vehicle, in the local area, known as vehicle to vehicle (V2V); and
- networking between a vehicle and its infrastructure system, known as vehicle to infrastructure (V2I).

The collective term for these two networking technologies is V2X. V2X can be used to prevent collisions by rapidly sharing data such as a car's speed, location and activity. For example, a vehicle could transmit a warning signal if the brakes are used in an emergency, giving a fast warning to drivers that they need to stop soon. Major computing companies have already made a movement to integrating their systems with cars. Last year, Apple announced plans for integrating its mobile operating system, iOS, into cars, and in January 2014, Google announced a partnership with major car manufacturers to develop its Android operating system for cars.[12]

2.2. Civilian aircraft

Although many serious obstacles still remain for the full implementation of completely autonomous cars, such as adequate regulations, international standards for digital infrastructure (traffic lights and road signs could transmit electronic signals) to assist driving and achieving reliable safety standards as those in the field of aviation, modern, large aircraft have been using automatic landing systems for years. Major airports such as Paris–Charles de Gaulle Airport are allowing only auto-landing aircraft, and in this way they remain operational for almost every day of the year.

The instrument landing system (ILS) is a ground-based instrument approach aid system based on two radio beams which together provide pilots with both vertical and horizontal guidance during an approach to land. As tabulated in Table 2, there are three categories of ILS equipment depending on the visibility range and height, from category I which is the least precise to category IIIc which operates under zero visibility (automatic landing).[13]

Aircraft approaching a runway are guided by their onboard ILS receivers. Many modern, large aircraft can route these signals into their autopilot to approach and land automatically. Under category III visibility conditions, which is visibility less than 210 meters, no manual landing is allowed and auto-landing is mandatory.[13] The role of the pilot in this condition is that if a safe landing is in doubt,

Table 2. Instrument landing system (ILS) categories for precision instrument approach and landing.

Approach Category	Decision Height (DH) or Alert Height	Runaway Visual Range (RVR)	Visibility Minimum
I	200 ft. (61 m)	550 m or 1.800 ft., increased to 800 m for single crew operations (no passenger)	800 m (1.600 ft. or 1.200 ft. in Canada)
II	100 ft. (30 m)	1.200 fteet (370 m)	NA
IIIa	No DH	700 feet (210 m)	NA
IIIb	No DH	150 feet (46 m)	NA
IIIc	No DH	No RVR	NA

he will abort the landing and try the same (go-around) or different landing approach or divert to an alternate airport. In short, in most western international airports, commercial aircraft are landing autonomously with human (pilot) supervision.

2.2.1. Lessons to be learned from auto-landing systems. Even though auto-landing systems are not very new technological achievements, there is inspiring design features developed for their safety systems which should be employed today against cyber-attacks in autonomous vehicle systems. It is essential that any failure of the ILS must be detected in a timely manner and the pilot must be warned immediately to provide flight safety. To achieve this, the onboard ILS control system monitors continually and assesses the vital characteristics of the transmissions. If any significant deviation beyond strict limits is detected, ILS is automatically switched off and a ''failure flag'' indication is activated to warn the pilot about the failure. This safety measure can be used by autonomous vehicle systems in case of cyber-attacks against them.

2.3. Trains

Self-driving trains have been in use on metro systems since the 1960s, and can now be found in cities all around the world.[14] Many have a driver or guard onboard to operate some functions, or as a safety precaution, but metro systems are increasingly being run without any onboard staff.[15]

The use of autonomous technology has not been employed in over ground, cross-country trains, as these operate in less controlled environments and travel at faster speeds. Accordingly, it would be easier for a pedestrian or an obstacle to get onto the train tracks, and much more powerful sensors for detecting obstacles would be needed in order for an adequate stopping distance to be achieved. Meanwhile, the stopping distance of a train is much longer than a car, i.e. it could be close to a mile. This remains an area of development for the future. There have been a few autonomous train systems deployed in recent years, including one in Ohio that carried coal from a mine to a power plant. However, this train was in a relatively secluded area with minimum hazards.[16]

Since metro systems are controlled by separate networks of their own, they are less sensitive to cyber-attacks provided that the local area network cabling of their control system is physically protected and wireless technology is not used. Otherwise, control network communication must be encrypted and a network intrusion detection system must be employed.

2.4. USVs

USVs are defined as vessels primarily guided by automated onboard decision systems but controlled by a remote operator in a shore side control station. They have also been called autonomous surface craft (ASC). As the name implies, they remove the operators from the platform and allow new modes of operations. As global positioning systems (GPS) have become more compact, effective and affordable, USVs have become more capable. Affordable, long-range and higher bandwidth wireless data systems have also been a key to the rapid growth of USVs for many applications. Today USVs have been developed and demonstrated by academic labs, corporations and government users. Missions demonstrated include science, bathymetric mapping, defense and general robotics research.[17]

Scientific research is another area for both surface and underwater vessels. In the Catlin Sea view survey project, remotely operated autonomous underwater vehicles (AUVs) are employed to explore the mesospheric zone, in excess of 30–100 meters in depth. The AUVs can spend hours exploring coral reefs without the limits of human physiology, collecting samples from this depth, carrying equipment to divers or even running reconnaissance.[18,19] They also feature an ultra-short baseline (USBL) geopositioning system to capture accurate GPS fixes underwater and use depth, temperature, heading, tilt and altitude (distance from the bottom) sensors. There are US government projects for the development of autonomous submarines that could be used to search for illegal drug smuggling submarines, which are becoming increasingly common.[20,21]

A USV's position at the air–sea interface allows them to relay radio frequency transmissions in air and acoustic transmissions undersea. Thus, they are a key piece in the vision of the networked battle space of the US Navy.[22,23] In recent years, demonstrations have been conducted using USVs to support moving long baseline navigation of UUVs.[24] While some military applications have moved USVs into complex networks and behaviors, other applications have focused on more traditional requirements and capabilities such as harbor security or mine sweeping. These applications achieve the goal of removing humans from harm's way.[17]

There are many research activities in progress today to develop autonomous, unmanned cargo ships. One of the projects is maritime unmanned navigation through intelligence in networks (MUNIN). It is a collaborative research project, co-funded by the European Commission under its seventh framework program. MUNIN aims to develop and verify a concept for an autonomous ship, since maritime transport within the EU faces challenges such as significant increases in transport volumes, growing environmental requirements and a shortage of seafarers in the future.[25] The concept of the autonomous ship brings along the potential to overcome these challenges. It allows far more efficient and competitive ship operation and increases the environmental performance of vessels. Furthermore, the shore-based approach offers ''seafaring'' the possibility to become more socially sustainable by reducing the time seafarers spend away from their families.[17,25]

Since USVs have to use long distance wireless communication channels (broadcast) by their nature, control and sensor links employed for operation of these vessels have to be encrypted as the primary protection against cyber-attacks (confidentiality and integrity will be provided by encryption, but jamming attacks cannot be prevented by encryption).[21]

2.5. UAS

A UAV is defined as a space-traversing vehicle that flies without a human crew onboard and can be remotely controlled or can fly autonomously.[26] More than three decades ago, UAVs started to be used for military purposes especially for reconnaissance and surveillance purposes. Since then, the popularity of UAVs or UASs (UASs were initiated by the US Department of Defense in 2005 from the perspective of a system) has kept growing at an unprecedented rate. Although now UAVs are used mostly in military applications (intelligence, surveillance and reconnaissance missions and combat operations—strike missions, suppression and/or destruction of the enemy and its facilities), their future potential civil applications are enormous (e.g. border patrol, forest fire monitoring and firefighting, nonmilitary security work such as surveillance of industrial sites, road/rail infrastructure, mineral exploration, coastal surveillance, pipeline surveillance, spraying of fertilizers, insecticides, aerial photography, land mapping, environmental monitoring, transportation and gathering scientific data).[26] To date, there are over 1000 UAS models being developed in over 50 countries with the aim to serve as indispensable assistants for human operators in a broad range of military and civil applications.[27]

UASs' future is absolutely unlimited and their size, specification and purposes are limited almost only by the extent of the developers' imaginations. Some usage of UAS in daily life may seem like a futuristic and perhaps even unrealistic prospect, but it should be noted that, the world's largest e-commerce company Amazon.com Inc. unveiled their plan on public TV (CBS's ''60 Minutes'' news program) that they are testing UASs to get packages into customers' hands in 30 minutes or less using UAVs.[28] Meanwhile the US Congress passed a law in 2012 and asked the Federal Aviation Administration (FAA) to develop a plan to integrate drones into US airspace by September 2015.[29]

Since long-range wireless environment and satellite communications have been used for control and data transfer, communication data links have to be secured against cyber-attacks, by using encryption and resistant modulation techniques against jamming.

3. Types of cyber-attacks

A useful taxonomy defined by the International telecommunication union (ITU) telecommunication standardization sector (ITU-T) in recommendation X.800 classifies cyber-attacks into two categories: passive attacks and active attacks.[30] A passive attack attempts to learn or make use of information from the system, but it does not affect system resources. An active attack attempts to alter system resources or affect their operations.

3.1. Passive attacks

Passive attacks are difficult to detect, as they involve no alteration or introduction of data. All passive attacks enumerated in the taxonomy are attacks on confidentiality.

3.1.1. Eavesdropping. An attacker acquires data by passive interception of data traffic in an eavesdropping attack. If encryption is used, cracking the encryption and decrypting the information traffic is still counted as a passive eavesdropping attack.

3.1.2. Traffic analysis. In a traffic analysis attack, an attacker is able to deduct certain properties about information transactions based on the participants, duration, timing, bandwidth and other properties that are difficult to disguise in a communication allowing an attacker to examine a network by observing its transmissions.

3.2. Active attacks

In active attacks, the attacker is more intrusive. Active attacks are divided into the following categories.

3.2.1. Masquerade. In a masquerade attack, an attacker fraudulently impersonates an authorized entity to gain access to information resources. A ''man-in-the-middle'' attack involves a double masquerade—the attacker convinces the sender that he is the authorized recipient, and convinces the recipient that he is the intended sender. Man-in-the middle attacks on Wi-Fi networks using a counterfeit access point are common. Successful masquerades can compromise all aspects of security.

3.2.2. Replay. An attacker is able to rebroadcast a previous message and elicit a reaction in a replay attack. This reaction either allows the attacker to force the information system into a vulnerable state (e.g. a system reset) or to collect information to enable further attacks (such as wired equivalent privacy (WEP) encrypted packets). Replays are most directly a compromise of integrity, but they also compromise authentication, access control and non-repudiation. Selected replay attacks can also impinge on availability and confidentiality.

3.2.3. Message modification. Modification of transmitted packets by delaying, inserting, reordering or deleting en-route changes a message. In a wireless network, ''man-in-the-middle'' attacks are the most direct route to message modification. Message modification is a violation of integrity but can potentially affect all aspects of security.

3.2.4. Denial-of-service. Denial-of-service (DoS) occurs when an attacker compromises the availability of an information system. Most common types of DoS are to disable one of the communications partners or to jam the communication channel itself.

4. Potential vulnerabilities of autonomous vehicles

As vehicles become increasingly computerized and networked, they gain more autonomous capabilities and cyber-threats are likely to be a more prominent concern. This is a risk that is ever growing in our increasingly digitized society. Malicious software interfering with an autonomous vehicle could have serious implications for safety and might cause accidents which can pose a physical danger to its users or passengers. There is a potential for cyber-terrorism too. For example, a large-scale immobilization of cars on public roads could throw a country into chaos.

4.1. Vulnerabilities of modern cars

A long time ago, several studies have described potential vulnerabilities and the fragility of the automotive system structure in the academic context.[31–35] In some recent studies, researchers demonstrated experimentally by using real automobiles and real automotive components both in the lab and on road tests that once an adversary accessed the internal network, he or she can completely take control of wide range of automotive functions including disabling the brakes, selectively braking individual wheels on demand, stopping the engine, locking the doors, etc. meanwhile ignoring completely the driver's input.[36,37] In a study, it has also been shown that composite attacks that leverage individual weaknesses, including an attack that embeds malicious code in a car's telematics unit and that will completely erase any evidence of its presence after a crash, are possible.[36] In another research study, the authors demonstrated that the internal vehicle network can be accessed via a broad range of remote means (attack vectors) such as Bluetooth, 3G cellular radio used by telematics units and wireless communications channels, in addition to indirect physical access through the onboard diagnostics (OBD-II) port. Vulnerabilities reported by previous research can then be exploited and automobiles can be controlled remotely without any direct physical access.[38]

The main reason of these vulnerabilities is the controller area network (CAN) standard which was developed in 1988 and updated in 1991 and in 2003.[39] There are a variety of protocols that can be implemented on the vehicle bus, but starting in 2008 all cars sold in the US were required to implement the CAN bus (ISO 11898) for diagnostics.[39] As a result, CAN (roughly speaking, a link-layer data protocol) has become the dominant communication network for in-car networks (e.g. used by BMW, Ford, GM, Honda, Volkswagen, etc.). ECUs are networked together in one or more buses based on the CAN standard. ECUs communicate with one another by sending CAN packets.

The CAN bus structure and protocol was developed when there were no cellular or wireless communication technologies and automobiles were not network connected. Therefore, the CAN protocol has very weak security features against external adversaries as well as against internal ones. However, today, automotive systems have broad connectivity; millions of cars on the roads today can be directly addressed via cellular phones and via the Internet. Making it worse, today in a modern car there is a broad range of functionality, including the engine, drivetrain, brakes, lighting and entertainment being controlled by a heterogeneous combination of digital components (ECU) which are including tens of millions of lines of code[5] and interconnected by the CAN protocol which provides very weak security means and features. Important weaknesses of the CAN protocol can be listed as follows:[36]

- **Broadcast Nature**. Since CAN packets are both physically and logically broadcasted to all nodes, a malicious component on the network can easily snoop on all communications or send packets to any other node on the network.
- **Fragility to DoS**. The CAN protocol is extremely vulnerable to DoS attacks. In addition to simple packet flooding attacks, CAN's priority-based arbitration scheme allows a node to assert a "dominant" state on the bus indefinitely and cause all other CAN nodes to back off.
- **No Authenticator Fields**. CAN packets contain no authenticator fields (or even any source identifier fields) meaning that any component can indistinguishably send a packet to any other component. This means that any compromised component can be used to control all of the other components on that bus, provided those components themselves do not implement defenses.
- **Tester Capabilities**. Modern automobiles are complex and thus diagnosing their problems requires significant tester devices (also called a maintenance device (MD)) which uses the CAN bus for providing diagnostic access to service technicians.

4.2. Vulnerabilities of UAVs

Unfortunately, the cyber-threats that are mentioned earlier are not unique to automotive systems. A similar attack took place on a military UAV system on 4 December 2011. An American Lockheed Martin RQ-170 Sentinel UAV was captured by Iranian forces near the city of Kashmir in northeastern Iran. The Iranian government announced that the UAV was brought down by its cyberwarfare unit which took control of the aircraft and safely landed it. The US government initially denied the claims but later President Obama acknowledged that the downed UAV was a US drone and requested Iran to return it.[40] According to an Iranian engineer's assertion in a *Christian Science Monitor* article, the drone was captured by jamming both satellite and land-originated control signals to the UAV, followed up by a GPS spoofing attack that fed the UAV false GPS data to make it land in Iran at what the drone thought was its home base in Afghanistan.[41]

4.3. Classification of vulnerabilities and threats

Traditional cyber-vulnerability issues applicable for autonomous unmanned systems can be summarized as in Table 3.[42]

DoS is the major type of threat in traditional wireless communications. In a DoS attack, a network can be made unavailable by malicious coding and spamming of packets with false messages that absorb all the available bandwidth. An attacker may use malware to infect the network with malicious software, or use greedy means to gain more throughput than other users. By exploiting the vulnerabilities given in Table 3, many **c**yber-threats can be accomplished. Important cyber-threats are listed in Table 4.[43]

5. Metrics for cyber-security

Since system security cannot be absolute, quantifiable security metrics are needed. Metrics are useful even if they are not perfect; for example, relative metrics can aid in critical design decisions.[44] Historically, approaches to security metrics come from several different points of view:[45]

Table 3. Traditional autonomous unmanned systems vulnerabilities.

SNo.	Vulnerability
1	Inadequate policies, procedures, and culture developing and maintaining autonomous vehicle software
2	Inadequately designed networks with insufficient defense-in-depth
3	Remote access without appropriate access control
4	Separate auditable administration mechanisms
5	Inadequately secured wireless communication
6	Use of a non-dedicated communications channel for command and control
7	Lack of easy tools to detect/report anomalous activity
8	Installation of inappropriate applications on critical host computers
9	Inadequately scrutinized control system software
10	Unauthenticated command and control data

Table 4. Cyber-threats generated by exploitation of vulnerabilities.

Vulnerabilities	Resulting cyber- threat / intrusion
Introduce incorrect input signals (spoofing)	With access to the digital communications network, it becomes possible to trick a controller into an incorrect action by generating erroneous process information. Signal types that may be affected are set points, command functions, interlocks, general data transfers, and system status information. Various defensive mechanisms can be applied to protect the controller at several layers including signal validation.
Generate incorrect output values or commands	In a manner similar to incorrect inputs, erroneous output values can be sent to network connected actuators and other controllers. Various defensive mechanisms can be applied to protect against erroneous outputs including command validation.
Insert messages to indicate incorrect operational status of parts of the system	Messages can be posted for other controllers or corporate networked computers to read that incorrectly indicate the operational status. Such tactics can be used to spoof a maintenance action or force an unnecessary shutdown.
Collect operational information (data, set points)	Simply by tapping into digital data streams, it is possible to determine operating parameters and states that can be used detrimentally by an adversary for more complex cyber-attacks.
Interrupt or corrupt communications between control system components	Rather than directly introducing erroneous process signals for controllers to act on, one can interfere with communications and disrupt the stability of the process. The following failure types may be created depending on the network type and configuration:
	. Corruption . Incorrect Sequence . Unacceptable Delay . Masquerade . Excessive Jitter . Broadcast Storm (Denial-of-Service of Service) . Babbling Idiot (Commission Fault) . Inconsistency (Byzantine Generals' Problem) . Unintended Repetition . Loss . Insertion . Addressing . Collision
Sender/Receiver related errors	. Buffer Overflow . Incorrect Ordering . Encoding/Decoding . Data Out of Range . Message Too Early
Segmented-network r-elated errors	. Very Long Delays in Bridges and Routers . Very Long Times to Initiate Communications . Complete Blockage

a) as a means to assess how well financial consequences of a security problem are minimized or avoided, that is, the business impact;

b) to indicate how successfully the control system avoids problems that jeopardize desired operation or behavior of the system, that is, to quantify the effectiveness of operations;

c) as a measure of how well quality assurance goals are met, that is, how effectively security flaws are detected; and

d) as a means to document how well the control system satisfies/complies with security requirements.

Quantifiable security metrics are needed to assess trustworthy behavior of the autonomous unmanned vehicle especially in view of reliability, security and resiliency (the ability of the autonomous unmanned vehicle to recover from a failure or disruption to the desired operation). Financial impacts, program planning, productivity and quality assurance, though important, are not the primary aim of the kinds of measurements that need to be made to assess trustworthiness.

Frequencies of security incidents must be measured and recorded. Time between incidents must be measured, and the number of occurrence must be recorded. Carefully chosen measurements will not only provide an indication of the system security level, but will also help to identify where improvements to trustworthiness need to be made.

In practice, security metrics can be grouped under three categories: design-based metrics, policy-based metrics and performance-based metrics.[45]

5.1. Design-based metrics

Measuring the design and implementation of the system rather than its performance or operation is an upfront method. Two notable documents define design-based metrics:

a) Trusted Computer System Evaluation (TCSE, which is widely known as Orange Book) was created by the US Department of Defense in 1985 to evaluate operating systems until the Common Criteria, an international standard, was created in

1999.[46] The Common criteria security evaluation follows an international standard, ISO/IEC 15408.

b) DO-178B software considerations in airborne systems and equipment certification was produced by the Radio Technical Commission for Aeronautics Federal Advisory Committee.[47] This document defines five levels (A–E) of critical software, with level ''A'' being the most critical level and therefore requiring the most effort to achieve compliance.

5.2. Performance-based metrics

These metrics indicate how often the security system was successful in repelling an attack and conversely how often the security system did not succeed in repelling an attack. These metrics are difficult to employ, since it is not possible to determine with certainty each time an attack is attempted, and it is even less possible to know with certainty when an attack is successful, because if the attack was detected, it should have been possible to defeat the attempt. The absolute performance-based metric would be to measure the number of vulnerabilities present in a system, but there is always the possibility that unknown vulnerabilities exist, so this metric is of limited real value.[45]

5.3. Ideal-based metrics

New metrics need to be established based on the inabilities of the design-based metric to establish a measure, and performance-based metrics having little success due to their cumbersomeness in practice. The ideal-based metrics are agreements on the attributes of an ideal cyber-security system and then assessing how closely the considered system approaches the ideal.[48] Using the known approaches defined in the next section and the ideal-based metrics, one can make a positive statement-of-measure for cyber-security protection.

6. Mitigation strategies, modeling and simulation

As summarized in section 4.1, experiments carried out on transportation vehicles have shown that security mechanisms provided by car manufacturers are unfortunately, basic, outdated and inadequate.

6.1. Using reliable distributed programming tools and techniques

For continuous availability of autonomous unmanned vehicles, mitigating strategies must be founded on the anticipation of unexpected failures of hardware/software or cyber-attacks. The methods and techniques developed for building reliable and distributed applications over the last two decades are very valuable for developing secure, reliable and resilient software for the control and handling of autonomous unmanned vehicles.[49]

6.2. Including cyber-security requirements in the requirement analysis phase

The traditional paradigm of software development defined by the IEEE 830-1998 standard requires security requirements to be included in the software requirements' document but these are often neglected.[50] Cyber-security requirements and concerns must be determined and included in the autonomous vehicle systems' requirements document and not after the design of the system. At the very beginning of control system design of autonomous vehicles, a more comprehensive analysis must be done and consistency and availability together with resilience must be the first design priorities and indispensable features under any circumstances. Cyber-security requirements should be defined according to the following key concepts:[51]

- **Confidentiality** is the property of protecting information from unauthorized entities, systems or individuals.
- **Data integrity/consistency** is the property of maintaining the accuracy of data from a source to its destination.
- **Authentication** is the property of validating that parties involved in a transaction are who they claim to be.
- **Availability** is the property of providing information at all times when it is needed.
- **Non-repudiation** is the property of ensuring that a party to a contract cannot deny the authenticity of their signature on a document.

6.3. Using multi-agent system architecture

Autonomous unmanned vehicles are generally suitable to ''multi-agent system'' architecture, since they are composed of multiple subsystems or in other words are systems of systems. For example, an autonomous car system generally has many computer-controlled subsystems such as radar, a lidar GPS receiver, video cameras, an onboard computer (mission computer), a communication subsystem, etc. Using software agents as in distributed real-time systems can enable secure and robust real-time status updates for identifying remotely accessible devices vulnerable to overload, cyber-attack, etc.[52–54] It will also provide distributed intelligent adaptive control[55] and the identification of damage and failure mechanisms.

6.4. Redundancy

Redundancy is a means to prevent a single point of failure.[56] Redundancy of control systems in autonomous vehicles should be a foundational concept of these vehicles so that (1) no single failure results in loss of control of the vehicle and (2) losing control of any single component or one communication channel because of cyber-attack, hardware or software failure must not result in loss of the minimum control of the vehicle, i.e. the vehicle should be able to park in a safe manner or return to the harbor or airbase.

6.5. Diversity

Diversity is a way to prevent that no single attack vector can compromise all the replicas (the added redundancy). Implementation of diversity is accomplished by voting logic as in the ''Byzantine general'' problem.[45] The primary protection that redundant voting systems offer is defense against single component failure. A secondary benefit of redundant voting, which offers defense against cyber-attack, is the requirement that messages must be matched by the defined majority (e.g. two out of three). An errant message in only one channel (whether arising from malicious or accidental causes) is therefore disregarded using this voting method. An attacker must get control of at least two components.

6.6. Defense-in-depth

The obvious course of action against a cyber-attack is to block the pathway used for unauthorized intrusion. However, to follow a defense-in-depth philosophy, it has to be known that the communication blockage was ineffective and subsequent defense mechanisms are required to recognize that an intrusion is in progress and ultimately to know what signals or instructions are reasonable and allowable at the individual subsystem/controller level.[57]

6.7. Authentication

Authentication mechanisms prevent humans and devices from impersonating another entity in the system. Access control prevents unauthorized access to the system: it prevents outsiders (unauthenticated principals) from gaining access to the network, while imposing and enforcing proper restrictions on what insiders (authenticated principals) can do. Accountability can be maintained by keeping audit logs of the actions by authenticated entities. Secure communication between two honest entities is achieved with the help of message authentication codes or digital signatures (they can detect when messages have been tampered with by a third party). Message freshness can also be guaranteed by the use of timestamps (which require secure time-synchronization protocols) or by challenge and response mechanisms.[58]

The separation of privilege principle should be used as a design guideline to limit the amount to privileges that a corrupted entity can have.

6.8. Using micro-kernel

Embedded software running on digital units of autonomous vehicles should use micro-kernel and all device drivers and non-essential modules should be removed from the kernel.[59] This will enhance security in two ways. The first way is by eliminating device driver software from having supervisory rights; the second kernel will then be tested more thoroughly and security weaknesses will be discovered and solved before deployment.

7. Summary and conclusions

By the end of 2015, the FAA will have prepared and submitted a plan (five year roadmap) describing the activities of the FAA's Unmanned Aircraft Program Office, and its efforts to safely integrate civil UASs (less than 55 pounds) into the US national airspace system.[29] At the same time the EU's project will be finished and the first commercial unmanned cargo ship (USV) will be produced.[25] Meanwhile, in the US, four states have already passed a bill for allowing testing of driverless cars on public roads.[60] Today, Google's driverless car has already been tested more than five hundred thousand miles on public roads and major car manufacturers such as Audi, BMW, Mercedes Benz, Nissan, etc. are testing their prototype driverless cars.[61] As explained in section 4.1, the CAN bus used in today's cars provides very limited security measures to be used against cyber-intrusion threats from remote or local locations (through their maintenance ports).[36,37]

If the CAN standard which is an already aged protocol (developed in 1988[39]) is not going to be augmented against security threats, in the presence of today's hostile cyber-environment, unfortunately we will most likely see many abuse incidents for autonomous cars.

US armed forces and many other nations' military organizations have started secured communication development projects to provide their military UAVs' and USVs' secure encrypted, jamming resistant communication channels.

For small UAVs and USVs to be used by the public, a similar threat to autonomous cars is valid. Since they are using the open skies as their communication media, some kind of encryption must be utilized against cyber-intrusions and threats. The most plausible and low cost solution for this problem is the usage of certificates as used for secure transactions on the Internet. In addition to this, controller bus standards used in these vehicles must be overviewed from the security point of view and they must be updated accordingly.

For DoS attacks and electronic jamming in wireless communications, the use of electronic counter measure (ECM) techniques and jamming resistant modulations seems to be the most effective solution.

Funding

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

8. References

1. Wang YC and Guo LJ. Evaluation methods for the autonomy of unmanned systems. *Chinese Sci Bulletin* 2012; 57(26): 3409–3418.
2. Huang HM, Albus J, Messinan E, et al. Specifying autonomy levels for unmanned systems: interim report. In: *Proceedings of the 2004 SPIE defense and security symposium conference* (eds GR Gerhart, CM Shoemaker and DW Gage), Orlando, Florida, 12–14 April 2004.
3. Rafael Y. *Guidance of unmanned aerial vehicles*. New York: CRC Press, 2011, pp. 2–6.
4. Yeomans, Gillian. Autonomous vehicles handing over control: opportunities and risks for insurance, https://www.lloyds.com/ ~ /media /lloyds/reports/emerging%20risk%20reports/autonomous%20vehicles%20final.pdf (2014, accessed 12 September 2014).
5. Kreindler and Kreindler LLP. Possible causes of the Asiana flight 214 crash, http://www.kreindler.com/Possible-Causes-of-the-Asiana-Flight-214-Crash.shtml (2013, accessed 12 September 2014).
6. Yeomans 2014, 5–6.
7. Barker J, et al. Technical and legal challenges: an overview of the state of the art in autonomous vehicle technology and policy, http://www.law.washington.edu/ Clinics/Technology /Reports/Autonomous Vehicles.pdf (2013, accessed 12 September 2014).
8. The European Parliament the Council of the European Union. *Directive 2007/46/EC of the European parliament and of the council of 5 September 2007*, last modified 1 July 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02007L0046–20140701&rid=1 (2007, accessed 12 September 2014).
9. Kallenbach R. Drive by wire—what will be its impact on future vehicles, http://www.sae.org/congress/learning/techmon-kallenbach.pdf (2003, accessed 12 September 2014).
10. Chandrika N. Autonomous road vehicles—post note PN 443, http://www.parliament.uk/business/publications/research/briefing-papers/POST-PN-443/autonomous-road-vehicles (2014, accessed 12 September 2014).
11. Campbell M, et al. Autonomous driving in urban environments: approaches, lessons and challenges. *Philo Trans Royal Soc A* 2010; 368: 4649–4672.
12. Shulman M. V2V advancements in the last 12 months, http://umtri.umich.edu/content/2014.GlobalSymposium.Shulman.pdf (2014, accessed 13 September 2014).
13. Smith LH. Interim criteria for precision approach obstacle assessment category I–III ILS req, https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afs/afs400/afs420/policies_guidance/memo_TILS/media/Interim_Criteria_for_Precision_Approach_Obstacle_Assessment_Category_II-III_ILS_Req.pdf (2011, accessed 12 September 2014).
14. Driverless metros poised to expand. *Railway Gazette*, http://www.railwaygazette.com/news/single-view/view/driverless-metros-poised-to-expand.html (2000, accessed 13 September 2014).
15. Driverless train technology and the London underground: the great debate, http://www.railway-technology.com/features/ feature driverless-train-technology/ (2012, accessed 13 September 2014).
16. Lavrinc D. It's not a lack of technology that's keeping trains from going driverless, http://www.wired.com/autopia/2013/04/why-arent-trains-autonomous/ (2013, accessed 13 September 2014).
17. Manley JE Unmanned surface vehicles, 15 years of development. In: *Proceedings of the oceans 2008, MTS/IEEE*, 2008, Quebec City, Canada, 2008.
18. Catlin Sea view survey project, http://catlinseaviewsurvey.com/ (2014, accessed 10 September 2014).
19. Hagen PE, Fossum TG and Hansen RE. Applications of AUVs with SAS. In: *Proceedings of the oceans 2008, MTS/IEEE*, Quebec City, Canada, 2008.
20. Kushner D. Drug-sub culture, *The New York Times*, 23 April 2009, http://www.nytimes.com/2009/04/26/magazine/26drugs-t. html?pagewanted=all&_r=2& (2009, accessed 10 September 2014).
21. Carter M. Network integrated robotics at SPAWAR systems center pacific. In: *2nd annual C4ISR, cyber security, robotic platforms and sensors conference*. San Diego, CA: May 2009.
22. Ferreira H, et al. Swordfish: an autonomous surface vehicle for network centric operations. In: *Proceedings of the oceans Europe'07 conference, IEEE OES*, Aberdeen, Scotland, June 2007.
23. US Navy. The Navy unmanned surface vehicle (USV) master plan, July 2007, www.navy.mil/navy data/technology/usvmppr.pdf (23 July 2007, accessed 29 September 2014).
24. Curcio, J. et al. Experiments in moving baseline navigation using autonomous surface craft. In: *Proceedings of oceans 2005, MTS/IEEE*, Washington, DC, September, 2005.
25. MUNIN project brochure, http://www.unmanned-ship.org/munin/wp-content/uploads/2013/01/MUNIN-Brochure.pdf (2013, accessed 14 September 2014).
26. Yanushevsky, Rafael. *Guidance of Unmanned Aerial Vehicles*. Pp. 3–10. Boca Raton, FL: CRC Press, 2011.
27. Guowei C, Dias J and Seneviratne L. A survey of small-scale unmanned aerial vehicles: recent advances and future development trends. *Unmanned Systems* 2014; 2(2): 1–25.

28. Bloomberg Inc. Amazon unveils futuristic plan: delivery by drone, http://www.bloomberg.com/news/2013–12–02/amazon-testing-octocopters-for-delivery-ceo-tells-60-minutes-.html (2014, accessed 14 September 2014).
29. Conference report on HR 658, FAA reauthorızation and reform act of 2012, conference report (H Rept 112–381), Congressional record volume 158, number 16 (Wednesday, 1 February 2012), pp. H230–H304, http://fas.org/sgp/news/2012/02/faa-uas.html (2012, accessed 14 September 2014).
30. International telecommunications union. ITU-T3 recommendation X.800, Security architecture for OSI, Geneva, Switzerland, 1991.
31. Larson UE and Nilsson DK. Securing vehicles against cyber attacks. In: *CSIIRW'08: proceedings of the 4th annual workshop on cyber security and information intelligence research*. New York, NY, 2008.
32. Thorn PR and MacCarley CA. A spy under the hood: controlling risk and automotive EDR. *Risk Manage* 2008; 55: 22–25.
33. Wolf M, Weimerskirch MA and Paar C. Security in automotive bus systems. In: *Proceedings of the workshop on embedded security in cars*. Bochum, Germany: 2004.
34. Wolf M, Weimerskirch A and Wollinger T. State of the art: embedding security in vehicles. *EURASIP J Embedded Systems* 2007 http://jes.eurasipjournals.com/content/pdf/1687-3963-2007-074706.pdf doi:10.1155/2007/74706 (2007, accessed 23 Sept 2014).
35. Zhao Y. Telematics: safe and fun driving. *Intelligent Systems, IEEE* 2002; 17(1): 10–14.
36. Koscher K, et al. Experimental security analysis of a modern automobile. In: *IEEE symposium on security and privacy* (eds D Evans and G Vigna). Berkeley, CA: May 2010.
37. Miller C and Valasek C. Adventures in automotive networks and control units.
38. Checkoway S, et al. Comprehensive experimental analyses of automotive attack surfaces. In: *Proceedings of USENIX security*. San Francisco, CA: 2011.
39. ISO 11898–1:2003. Road vehicles—Controller area network.
40. Wikipedia, Iran–US RQ-170 incident, https://en.wikipedia.org/wiki/Iran%E2%80%93U.S._RQ-170_incident (2011, accessed 28 September 2014).
41. Peterson S and Payam F. Exclusive: Iran hijacked US drone, *The Christian Science Monitor*, 15 December 2011, ''http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer'' (2011, accessed 12 September 2014)
42. North American electric reliability council, control systems security working group, Top 10 vulnerabilities of control systems and their associated mitigations 2006, US Department of Energy, National SCADA test bed program, 16 March 2006, http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NERC_2007_Top_10.pdf (2006, accessed 12 September 2014).
43. Kisner R, et al. Design practices for communications and workstations in highly integrated control rooms, NUREG/CR-6991, September 2009.
44. Sanders B, et al. Making sound cyber security decisions through a quantitative metrics approach. In: *1st international workshop on resilience assessment of critical infrastructures* Urbana-Champaign IL: 25 April 2011.
45. Kisner R, et al. Cybersecurity through real-time distributed control systems, ORNL/TM-2010/30, February 2010.
46. Common criteria for information technology security evaluation—part 1: introduction and general model; part 2: security function requirements; part 3: security assurance requirements, ISO/IEC 15408, Version 2.0, 1999.
47. Wikipedia, DO-178B, Software considerations in airborne systems and equipment certification, http://en.wikipedia.org/wiki/DO-178B (992, accessed 23 September 2014).
48. Boyer W and McQueen M. Ideal based cyber security technical metrics for control systems. In: *CRITIS'07 2nd international workshop on critical information infrastructures security*, Benalmadena-Costa (Malaga), Spain 3–5 October 2007.
49. Birman KP. *Guide to reliable distributed systems, building high-assurance applications and cloud-hosted services*. London: Springer–Verlag, 2012, pp. 476–522.
50. IEEE 830–1998. IEEE recommended practice for software requirements specifications.
51. Stallings W. *Cryptography and network security principles and practice*. 5th ed. New York: Pearson, 2011, pp. 10–27.
52. Potok TE, Elmore MT, Reed JW, et al. VIPAR: advanced information agents discovering knowledge in an open and changing environment. In: *7th world mulitconference on systemics, cybernetics and informatics specification session on agent-based computing*, Orlando, FL, 27–30 July 2003, pp. 28–33.
53. Potok TE, Phillips L, Pollock R, et al. Suitability of agent-based systems for command and control in fault-tolerant, safety-critical responsive decision networks. In: *ISCA 16th international conference on parallel and distributed computer systems (PDCS)*, Reno, NV, 13–25 August 2003, pp. 283–290.
54. Conte de Leon D, Alves–Foss J, Krings A, et al. Modeling complex control systems to identify remotely accessible devices vulnerable to cyber attack. In: *ACM workshop on scientific aspects of cyber terrorism, (SACT)*, Washington, DC, November 2002.
55. Taylor C, Krings A, Harrison WS, et al. Considering attack complexity: layered intrusion tolerance. In: *DSN 2002 workshop on intrusion tolerance*, June 2002.
56. Amin S, Cardenas A and Sastry S. Safe and secure networked control systems under denial-of-service attacks. Hybrid systems: computation and control, Lecture notes in computer science, April 2009.
57. Stallings, William. *Cryptography and Network Security Principles and Practice, Fifth Edition*. Pp. 22–34. New York: Pearson, 2011
58. Birman, Kevin P. *Guide to Reliable Distributed Systems, Building High-Assurance Applications and Cloud-Hosted Services*. Pp. 551–568. London: Springer-Verlag, 2012.
59. Weimerskirch A. Automotive and industrial data security. In: *Cybersecurity for; cyber-physical systems workshop*, Gaithersburg, MD, USA, 23–24 April 2012.
60. Barker, J. et al. Technical and Legal Challenges: An Overview of the State of the Art in Autonomous Vehicle

Technology and Policy. http://www.law. washington edu/ Clinics/Technology /Reports/Autonomous Vehicles.pdf (2013, accessed 12 September 2013)

61. Rand Corporation. Autonomous vehicle technology how to realize its social benefits, http://www.rand.org/content/dam/rand/pubs/research_briefs/RB9700/RB9755/RAND_RB9755 .pdf (2013, accessed 15 September 2014).

Author biographies

A Ziya Aktaş obtained his BS and MS at Middle East Technical University (METU), in Ankara. He received his PhD at Lehigh University, US. He visited Vienna Technical University and Purdue University, Indiana, US. He served as the first chairman of the Department of Computer Engineering at METU for years. He is the author of a software engineering book published by Prentice Hall in the US. He is a member of Association for Computing Machinery (ACM). His recent interest areas are software engineering, cloud computing, Information System (IS) modeling, data mining, knowledge management and engineering.

Cemal Gemci obtained his BS at the military academy and his MS at METU in Ankara. He received his PhD at Gazi University, Ankara. He served for Turkish Armed Forces (TAF) as the information technology department manager for years. He is a visitor lecturer at Başkent University, Ankara. His recent interest areas are artificial intelligence, machine learning, cyber-security, cloud computing, knowledge management and engineering.

Eray Yağdereli received his BS and MS at METU in Ankara. He also received his MS in industrial engineering at Selçuk University in Konya. He worked in the Turkish Air Force (TurAF) as a system programmer and data base administrator for years. He also served at the North Atlantic Treaty Organization (NATO) as a programmer. He was serving as the branch chief in communication and information systems division at TurAF headquarters when he retired in 2014 at the rank of colonel. His recent interest areas are computer and network security, cryptography, distributed computing and machine learning.