AUTONOMOUS CARS AND DRIVERLESS LETHAL AUTONOMY

Nyagudi Musandu Nyagudi, Independent Researcher
Abstract

“The small picture” - make an advanced autonomous/driverless car. Lots of algorithms, sensors, computers and other gizmos. Now get it to take you to work, park itself and seamlessly run your family errands around the city. Taking grandma to the doctor for the medical check-up, getting the children from school, etc. With Radar, Lidar and other sensors, the car steering with ease through the traffic, no driver to pay, that is another plus, fuel/energy efficiency, yet another plus. It is a bold new world and the sky is the limit. Without the resolution of “small picture” issues there is no functioning autonomous/self-driving car, and without resolution of “THE BIG PICTURE” issues such as Driverless Lethal Autonomy there is no successful, viable and/or safe autonomous car.

Key-words:

Terrorism, Guerilla Warfare, Assassination, Counter-insurgency, Dual-use, Arms Control, Automotive Industry, Security, Informatics, Information Systems, Embedded Systems, Hacking, Cyber-security, beyond geo-fencing, car-jacking, car bomb, trucking...
bomb, humanitarian algorithms, epidemiology, security screening, autonomous, self-driving, driverless, ied, sniper,

**The Problem**

Be sure where there are computers, there is chaos and where there is chaos the “gremlins” on-board and a host of other off-board/on-board circumstantial saboteurs lie in wait – hazards and adversity too. They are not about to give anyone an easy drive through town. Unfortunately in this bold new and over-hyped world, there are no easy answers – here are some facts and propositions.

**Driverless Lethal Autonomy Interacts with the World**

There is a Probability of an Inevitable Collision State [Fraichard *et al*, 2010]. It is stated as a theorem but is more of a Technological Law in the realm of the emerging world of autonomous cars, such as what the Moore's Law is to computer chips. The Inevitable Collision State “…is the State in which whatever control trajectory sequence is applied by a robotic system, a collision shall eventually occur”. Given the unpredictable nature of an open environment, almost all states of motion are inevitable collision states – even more chaos, for the sci-tech world to contend with.
Building a fully functional and robust autonomous car, that is non-cooperative in type, can be achieved by way of eliminating vehicle autonomy that utilizes V2X [Vehicle to X(vehicle or infrastructure)] communications. Though efficiency of such autonomous cars may be compromised, it is a design concept that shall be much easier to implement, as there are likely to be no data privacy challenges, additionally cars cannot “discuss” who or how to kill in the event of an accident. The advantage of this design concept would be that vehicles shall not make co-operative or abusive decisions of who dies, gets injured or survives in the event of a road accident.

The elimination of occupant identification and V2X communications capabilities from autonomous cars, shall remove many of the ethical and moral query types in the realm of pre-crash control. Algorithms shall determine essential crash survival mechanics, to win-win or no win situations. Goodall gives an Equation that is vital and analytic but not rigourous in nature – describing autonomous vehicle crash dynamics, in this paper a survival parameter is added as \((k(an))\). It proposes that:

\[
f(A) = \sum_{a \in A} s(a) P(a | A) \frac{k(an)}{A}
\]

\(A \rightarrow \) set of possible outcomes of \((a)\) for a single trajectory choice
s → a function representing the severity of a specific crash outcome

a → a specific outcome

P → the conditional probability of an outcome occurring in trajectory of choice

\( f(A) \) → objective function that would be optimized by the autonomous car pre-crash control algorithms.

\( k(an) \) → it is possible to calculate occupant survival/safety based upon unique autonomous car occupant identification and location. Each and every car occupant is assigned a survival parameter.

The outcomes could be death, inconvenience, property damage and/or injury given the trajectory taken by the autonomous car.

With this knowledge how can one capitalize on such an ominous prediction to make autonomous car service a better experience? And what if the car “decides” on who gets injured or killed in the Inevitable Collision State? - Driverless Lethal Autonomy.

This new variable of the equation, introduces new parameters such as occupant identification. For the new survival parameter\( (k(an)) \) each and every occupant is allocated a unique empirically established parameter.
In due course each occupant would like to possess the greatest $k(n)$ parameter as the driverless cars shall attempt to cooperate to ensure that the occupant survives an accident. A problem arises in identifying the potential decision clincher. For each and every person $k(n)$ is a unique real variable.

E.g. $k(n)$ implies $k(a_1), k(a_2), k(a_3),...,k(an)$

As $k(n) \to \infty$, $s(a) \to 0$, and as $k(n) \to 0$, $s(a) \to \infty$.

$k(n)$ depends on factors such as:

- vehicle performance: speed/velocity
- vehicle protection: mass of materials, volume of materials, density of materials, and their engineering configurations into the car.
- analytically assigned weight to car occupants e.g. preferred survivors

From a casual analysis of the equation, comparative determination of all factors relating to the equation could only be achieved by way of some form of V2X communications under pre-crash inevitable collision state conditions.

In effect the systems of the autonomous cars are not making ethical/moral decisions...
and conducting the execution of the same, they are simply executing decisions to get/obtain actualization of pre-incident survival projections for car occupants. These pre-incident survival projection parameters may unwittingly be established by way of embrace of V2X communications systems. Their setting, utilization and manipulation is done by vehicle manufacturers, owners, occupants, Government, cyber-criminals/hackers or other interested third parties. The ethics and morals of the foregoing parties are utilized in making the Driverless Lethal Autonomy decisions.

To limit the scenarios of these autonomous car decisions, cars would be designed to prevent unauthorized actions, e.g.:

- (un)loading
- movement
- (dis)embarkation

An autonomous car would be required to possess technology that allows it to differentiate a polluted open environment from internal contamination to allow people to use it to escape from hazardous areas. This is not a particularly easy technological feat, given that interior sensor suites may sense the open environment.
For the enlightened and affluent guerilla/terrorist organization, or even a conventional army in distress, nothing could be more timely than the driverless car. Just dispatch it with the payload and destruction is delivered to the target. The armed gangster hauling away cash and bullion from a heist, would love to have an extra pair of hands away from the steering wheel, and an extra firearm deterring law enforcement officers who are in pursuit.

The only viable response is the emerging military concept of anti-access(A2)/area denial(AD) on a micro-scale. Preventing a driverless car from accessing target areas or by technically limiting their functions and potential payload in some circumstances.

The A2 concept would not be limited to restricting an autonomous car from accessing targeted areas, but would also be utilized in preventing the following:

1. Loading of lethal payload into the vehicle
2. Barring unwanted or suspect persons from utilizing or car-jacking the vehicles
3. Preventing effective navigation to or at targeted areas.
These functions shall go beyond the realm of what is known as geo-fencing. The current range of autonomous cars, go nowhere near these feasible technical aspirations. Most of their software is geared towards “safe” navigation. Artificial Intelligence systems on-board these cars, are yet to be provisioned to tackle the concept of an autonomous car in a hostile high or low intensity conflict area.

In the realm of autonomous car concepts, issues such as defensive driving have been thrust aside – the sensor technology types and computing systems, that may be expected to deliver such clarity and capabilities are nowhere near being sketched on to the drawing board.

A more complex scenario, e.g. autonomous cars that can discern the intentions of potential transgressors against its occupants – this could be an attacker squatting and pretending to be an injured person at a pedestrian crossing, while armed with a concealed pistol and waiting to ambush helpful autonomous car users.

The managed fleet type driveless car would require a wide range of passenger and/or load inspection technologies e.g.
1. Scanning technologies that can detect hazardous materials

2. Ability to conduct biometric verifications on its occupants and to determine if they are wanted by the Police for criminal offenses.

These payload discovery services would ensure that no hazardous substance transports or wanted persons abuse autonomous car public service fleets. The concept of payload discovery would be a challenge to many passengers, who have become used to transport on-demand, under complete confidentiality with no questions asked or security checks conducted. Privacy advocates would rightly argue against the networking of any such capabilities to Governments.

The most prominent image of an autonomous car to date, is those of the type with rotating LIDAR (Light Detection and Ranging) device on its roof. Picture what would happen if the system is struck off the roof or inadvertently damaged when the vehicle is moving on a road with many curves at a speed of 100kph+?

Could a hired autonomous car be in a position to “determine” if a passenger has boarded it under duress? e.g. a hostage being transported from point to point? Who
would be culpable for the crime? The manufacturer of the car? The fleet owner or the criminals? It would be exceedingly difficult for manufacturers to claim a defense of ignorance, while at the same time engaged in creating a sophisticated computing system on wheels without adequate provisioning.

A public expectation that ought to be imposed on the driverless car manufacturers, is that their product should be in a position to discern the disposition and intentions of not only those within the car, but to also assess those external to the car in the open environment, including persons who hire cars on the behalf of others. This is within the realm of possibilities for the human driver and artificial intelligence based driverless cars ought not to be “excused” or given an “easy-get-away-card” from responsibility by regulators. “Fine judgment” systems are required.

Robust and rigorous systems are a prerequisite if autonomous cars are not to become dependent on their own separate/specialized public infrastructure, resulting in additional public expenditure that is not of benefit other vehicles.
Driver monitoring [Ridella et al, 2015] implies that an autonomous car could go beyond reading the physiological parameters of its occupants – it could also act accordingly. Take the driver home, to hospital, etc. and summon the necessary assistance upon arrival at its destination. A driverless car without this capability may as well deliver a patient with ebola haemorrhagic fever or small pox to a well attended international public gathering or facility like an international airport.

At this point in time, it may be futile to speculate on how a driverless car would go about achieving such a technical feat, as that of identifying and isolating persons with highly infectious diseases. Suffice it to say that the technologies already exist and could be configured in very many ways. The main problem in this realm is that there could be manufacturer/service provider liability issues if a car detects a false positive or false negative and acts accordingly albeit wrongly.

Cyber-security plays a role in systems that would under take physiological measurements in cars. Cyber-criminals could steal highly confidential data or alter the physiological readings by on-board systems to achieve an undesired effect. The result would be an unwarranted response by the car, e.g. re-routing to a wrong
destination. No full duplex data-communications system is known to be 100% secure.

From the foregoing, it is evident that driverless cars shall pose a major challenge to public security as a vector for projecting lethal force by way of weapon delivery, if the technology is not constrained initially at design and construction levels. It is also safe to assume that even if such a vehicle is constrained from abuse as a weapon/attack delivery platform, it shall still be vulnerable to expert saboteurs.

Designers of the civilian autonomous car, should ensure that:

1. Physical access to the cars can be denied to individuals with abusive intentions
2. Unauthorized logical access is also denied – prevent an occupant or external entity from undertaking unauthorized human-computer interface functions
3. That there is sufficient counter-deception technology to prevent abuse of the non-combatant status of a civilian autonomous car for the purpose of weapon / payload delivery or as an attack vector of any kind
4. That foreseeable sabotage of components and logistics systems that autonomous cars depend on, are prevented by use of appropriate diagnostic and/or
surveillance technologies.

NB.: But the privately owned civilian autonomous car cannot be 100% harmless or pacifist especially in the United States of America where the Second Amendment of the Constitution empowers citizens to fight to defend the Nation and its values. There is a similar provision in Article 3(1) of the Constitution of the Republic of Kenya 2010, it states that, “Every person has an obligation to respect, uphold and defend this Constitution”. Obviously the Constitution cannot be defended with a teaspoon, it may be necessary for the local militia to use their civilian autonomous cars to fight off a “Zombie Apocalypse”, or the preppers may use it while fleeing some technical “Armageddon”.

An autonomous car may also be equipped with intelligent systems, that allow it to move away from an insecure area, where it may be abused for criminal activity. To achieve this it may be necessary to equip autonomous cars with wider tactical situational awareness capabilities.

In developing super sophisticated cars, there some inherent risks, e.g.
1. Malfunctions

2. Abuse

3. Market rejection

4. A car may become obsolete in short order due to the fast rate of technological innovations

5. Quality problems may be very difficult to trace or detect due to the underlying complexity of the systems

6. Inappropriate technologies for different market contexts

Some of these risks can be off-set by way of private or public insurance arrangements. Given the scope and scale of the market, litigation/regulation along these lines would force most manufacturers into financial difficulty – e.g. the Volkswagen Diesel Engines Emissions Affair of 2015 [Plungs and Hull, 2015].

Autonomous cars may come with an extra: Autonomous transportation/logistics support. There may be an autonomous car – cargo mode. The ability of a vehicle to book and utilize other forms of local/international transport, e.g. ships, aeroplanes, trains, etc. without human intervention, for deployment to an area where it is readily
Informatics is the ineluctable enabler that actualizes these diverse requirements in the “Era of Driverless Autonomy”.

Informatics would be driven by data-streams from the car's logistical centre, infrastructure and sensors. Sensor resolution is critical in defensive autonomous driving. Low sensor resolution shall result in non-responsiveness to threats (false negatives), while high sensor resolution with poor quality intelligence would cause many false positives. Sensor type also determines the resolution level.

Autonomous defensive driving problems are of the following nature, e.g. there is an autonomous car that automatically brakes when it detects a car ahead. But there is a problem if would-be attackers utilize this technological determination to slow down a moving autonomous car, prior to attacking its occupants.

A fully autonomous car will be challenged with the difficult decision of whether to avail its occupants to potential (un)intentional harm by “outsiders” in the open environment or to use its physical attributes as a weapon where there is no immediate possible get-away, e.g. by running over individuals (an Artificial Intelligence...
decision in the realm of Lethal Autonomy).

Getting an autonomous car to “understand” arson, rioting and other forms of disorder shall be a mammoth task. But one previous difficulty that shall be solved, is the source/origin and direction of gunfire(or random projectiles) in an area, this shall be done by way of radar(active sensing) and/or sonar(passive sensing) technologies, already available on many autonomous cars.

Many of the buyers of brand-new BMW and Mercedes Benz cars are of the VIP and VVIP(very very important persons) lifestyle bracket. In the luxury autonomous car range, and probably for all other autonomous cars, one does not expect an autonomous car to make random stops for each and every pedestrian crossing or walking on the road. Such an approach to technology would pose a considerable security vulnerability that avails occupants to external attacks/ambush.

It would not be in the interest of the public for manufacturers to develop highly physically vulnerable “intelligent” cars or too aggressive an autonomous car that runs over every human on its path. Fine judgment is yet to be encoded into computing
systems in many respects. A “submissive” autonomous car shall also be the darling of the urban jay walker. But a “jay walker” could be a sick, injured or disabled person crossing a road.

Radar and LIDAR technologies used in many autonomous car navigation technologies are active electromagnetic spectrum emitters. These could also be used by an attacker to trigger an improvised explosive device against an autonomous car. This is true to the extent that every car shall have its own unique encoded electromagnetic spectrum emissions.

A growing number of jurisdictions [ Nevada, 2015, etc. ] are enacting autonomous car legislation. Some of the following are likely to be universal legal requirements:

1. An autonomous car shall be required to autonomously determine its legal jurisdiction of location(situational awareness) and to adjust its algorithms of control to be in accordance with local laws. A considerable problem may occur if the car is operating in a disputed area.

2. An autonomous car would be challenged with the problem of developing or acquiring new control algorithms pertaining to unforeseeable enacted legislation.
At times of war V2X infrastructure in a disputed area may broadcast false signals, leading to allegations of treachery as a result of harm to non-combatant occupants of an autonomous car.

With the already existing concept of the “Internet-of-Things” V2X communications protocols shall most likely end-up as standards determined and approved by the Internet Engineering Task Force. Autonomous control devices on cars shall be assigned unique identifiers probably of the IPv6(Internet Protocol version 6) addresses, and some utilizing IPv4 via Internet proxy technology.

The same old “big boy” car manufacturers shall continue to prosecute the usual market share wars. The implication of such competition shall be:

1. Market saturation (many cars with limited demand)
2. Market shortage in some parts of the world (too few cars to adequately service demand, due to perceived low financial power of residents).
3. Markets with weak regulations shall not remain open, they shall be cornered by specific manufacturers or autonomous car fleet service providers, who are endowed with more dynamic market networks and greater advertising budgets,
reaching out to clients, and offering advanced booking over computing devices.

4. Competing swarms of autonomous cars utilizing sensors, sentiment analysis and data fusion shall monitor emerging/available opportunities and re-position “themselves” to exploit emerging market opportunities on a real-time basis (dynamic swarming).

In the business domain there shall also be the same old and dirty business tricks, e.g.:

1. Regulatory/State Capture
2. Sabotage, e.g. hacking, jamming and deceptions
3. Incompatible V2X technologies and infrastructure
4. Restrictive trade practices and protectionism

A number of these problems could be solved by autonomous cars without V2X communications capabilities or essential active sensing capabilities. Litman 2015 probably wrongly assumes that walking and cycling shall become much more safer. It is overwhelmingly probable that this shall not be the case. Cars are likely to make and prioritize “kill” decisions, something that could result in deaths and injuries.
Many of the deaths and injuries shall be caused by autonomous cars particularly when their software controls have erroneous or repugnant Lethal Autonomy algorithms. It is clearly demonstrated at the onset of this research paper that use of V2X communications signals shall lead to the development of Driverless Lethal Autonomy algorithms.

But Litman 2015 is probably one of the most insightful papers to date, in that in his conclusion he foresees that autonomous car technologies may harm people who do not use it – this harm is implicit in his paper. This researcher goes a step further and projects that good, fault-free, high quality and fully autonomous cars may from time to time “habour” bad “intentions”. The underlying algorithms that are only dependent upon the ethics and morals of the specific players in the Automotive Industry cannot be given a clean bill of health.

Unlike Litman who foresees the autonomous civilian car being charged with making tricky and deadly decisions, Eno 2013 has the perspective that autonomous car technology would work to avert deadly crashes. It is a whole different ball game in Eno, “I-KILL-YOU-NOT” (sic “I-kid-you-not…”). But given past experiences with
over-hyped technologies, disappointment is likely to be patiently lurking around the “corner”, waiting to “pounce” on the unsuspecting public!

With the vast array of sensors on civilian autonomous cars (already in the market) and the huge amount of data-streams generated by the same for autonomous control. It would be nothing less than wishful thinking, to imagine that those real-time data-streams shall not be deployed in Lethal Autonomy decision execution.

These life, harm and death decisions by civilian autonomous cars, “re-introduce” the factor of death/harm by driverless “driver” error. Eno correctly acknowledges that there are complex questions to be solved, and lists security as one of those complexities. However it does not specify whether the security issues pertain to the car occupants or human beings external in the environment (including in other cars) or by the “good-car-gone-bad”.

Yet another security concern would be that if autonomous cars do indeed respond to road signs, they would be required to possess a statutory location list of the same. This would prevent saboteurs from misleading a car with phony road signs. But
more complex issues would arise from such simplicity, ie. Several impromptu hazard road signs placed by a saboteur or driver in distress. How would the intelligent car read the situation? What about the use of optical flow navigation as a parallel system to protect an autonomous car from GPS(global position system) jamming and spoofing?

Conclusion

What are the ethical positions of potential buyers, manufacturers and service providers? Would a buyer ignore the ethical twists of autonomous car control systems, in a world in which equity investments with tobacco or slave labour content are shunned by some? What would be the main ethical purchase/hire decision points?

With the Value Stream concept as studied by Womack and Jones 2003, even the Inevitable Collision State is not a bad thing when it occurs. A car shall make measurements and report to insurance, law enforcement and other authorities. Other value streams shall instantly sprout from thereon, those of the insurance, judiciary/litigation, law enforcement, medivac, news reporting(mass media), etc. The car then autonomously drives away from the scene of accident, if it is possible.
There is no haggling at the scene of accident with autonomous cars, as they may carry unaccompanied minors who can be exposed to more harm e.g. a furious lynch mob – a point worth considering? Yes the car can flee a lynch mob, with an injured victim(pedestrian) impaled on the bonnet and the stunned children watching in shock from inside the car. These are some of the puzzling scenarios in the world of Informatics, that if tackled shall make it all possible to safely use driverless cars.

References


Nyagudi Musandu Nyagudi, Independent Researcher and Security Analyst, Nairobi, KENYA
ORCID ID : http://orcid.org/0000-0001-5809-2209


Accessed on 8th – 10 – 015 (5:30GMT)


Research Paper Published on 11th-11-015