CRITICAL SYSTEMS

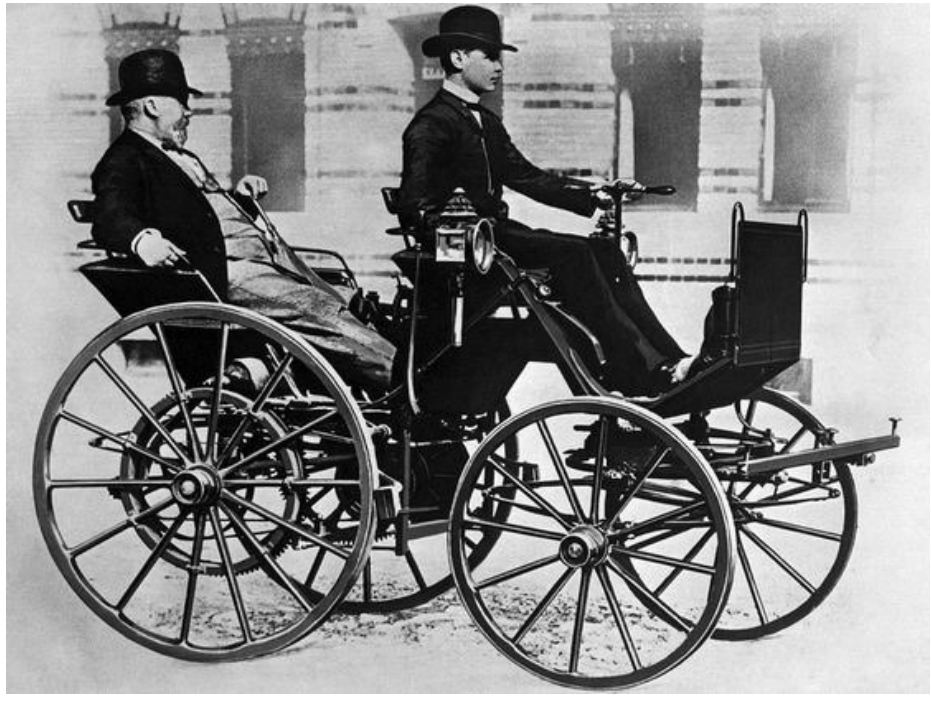
SELF-DRIVING CARS

BY ALINA SHILINA

TOPIC AND SUBTOPIC OF PRESENTATION

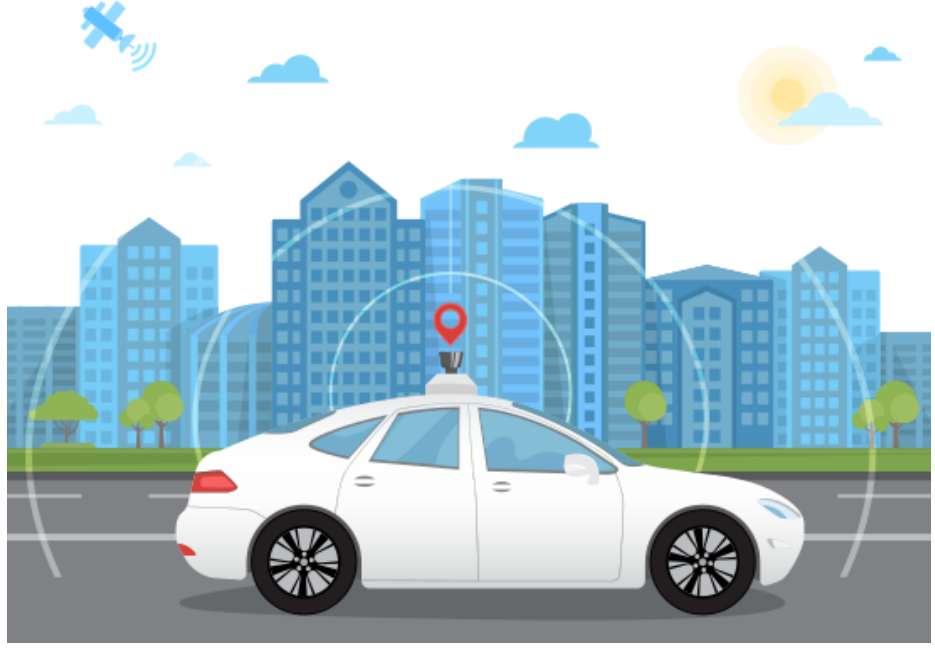
- SELF-DRIVING CARS AS A CRITICAL SYSTEM
- HOW TO ACHIEVE HUMANS SAFETY IN AUTONOMOUS VEHICLES
- HUMANS SAFETY CHALLENGES THAT NEED TO BE ADDRESSED BEFORE AUTONOMOUS VEHICLES APPEAR ON ROADS

SELF-DRIVING CARS AS CRITICAL SYSTEMS



What is autonomous?

SELF-DRIVING AUTOMOBILES ARE CARS IN WHICH HUMANS DON'T NEED TO TAKE CONTROL TO SAFELY DRIVE THE AUTOMOBILE.



One of the most important problem - humans' safety

ACCORDING TO THE WORLD HEALTH ORGANISATION [1], MORE THAN *1.25* MILLION PEOPLE DIE EACH YEAR AS A RESULT OF ROAD TRAFFIC ACCIDENTS. AUTONOMOUS CARS CAN, HYPOTHETICALLY, SIGNIFICANTLY REDUCE THE NUMBER OF PEOPLE DEATHS.

[1] “WHO | WORLD HEALTH ORGANIZATION.” [ONLINE]. AVAILABLE: HTTPS://WWW.WHO.INT/. [ACCESSED: 13-JAN-2019].

One of the most important problem - humans' safety

RESEARCHERS ESTIMATE AUTONOMOUS VEHICLES CAN REDUCE THE NUMBER OF TRAFFIC DEATHS BY 90 PERCENT, SAVING 30,000 LIVES A YEAR.

Problems which can be solved

- "IT IS EXPECTED THAT SUCH CARS WILL NOT ONLY SHOW QUANTITATIVE EFFECTS ON TRAFFIC, BUT IN THE LONG TERM WILL PROVIDE A NEW QUALITY OF TRAFFIC OPERATION INCLUDING CONCERTED NAVIGATION FOR SAFE, COMFORTABLE, AND EFFICIENT DRIVING" [2]

- "SELF-DRIVING CARS CAN ADDRESS ISSUES OF SAFETY, CONGESTION, FUEL, EFFICIENCY, AND EQUITY" [3]

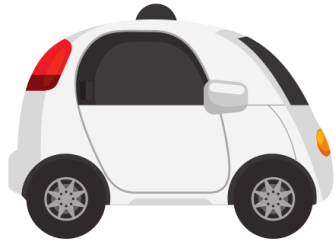
[2] Ü. ÖZGÜNER, C. STILLER, AND K. REDMILL, "SYSTEMS FOR SAFETY AND AUTONOMOUS BEHAVIOR IN CARS: THE DARPA GRAND CHALLENGE EXPERIENCE," PROC. IEEE, VOL. 95, NO. 2, PP. 397–412, 2007.
[3] D. HOWARD, "PUBLIC PERCEPTIONS OF SELF-DRIVING CARS," 2013.

Why self-driving cars are critical systems?

TO BE A CRITICAL SYSTEM, I.E. "SYSTEMS WHOSE FAILURE MIGHT ENDANGER HUMAN LIFE, LEAD TO SUBSTANTIAL ECONOMIC LOSS, OR CAUSE EXTENSIVE ENVIRONMENTAL DAMAGE" [4], A SYSTEM SHOULD HAVE AT LEAST ONE CRITICAL SAFETY SERVICE.

[4] J. C. KNIGHT, "SAFETY CRITICAL SYSTEMS: CHALLENGES AND DIRECTIONS," 2002..

CRITICAL SERVICES OF A SELF-DRIVING CAR



SELF-DRIVING CAR

POTENTIAL HARM

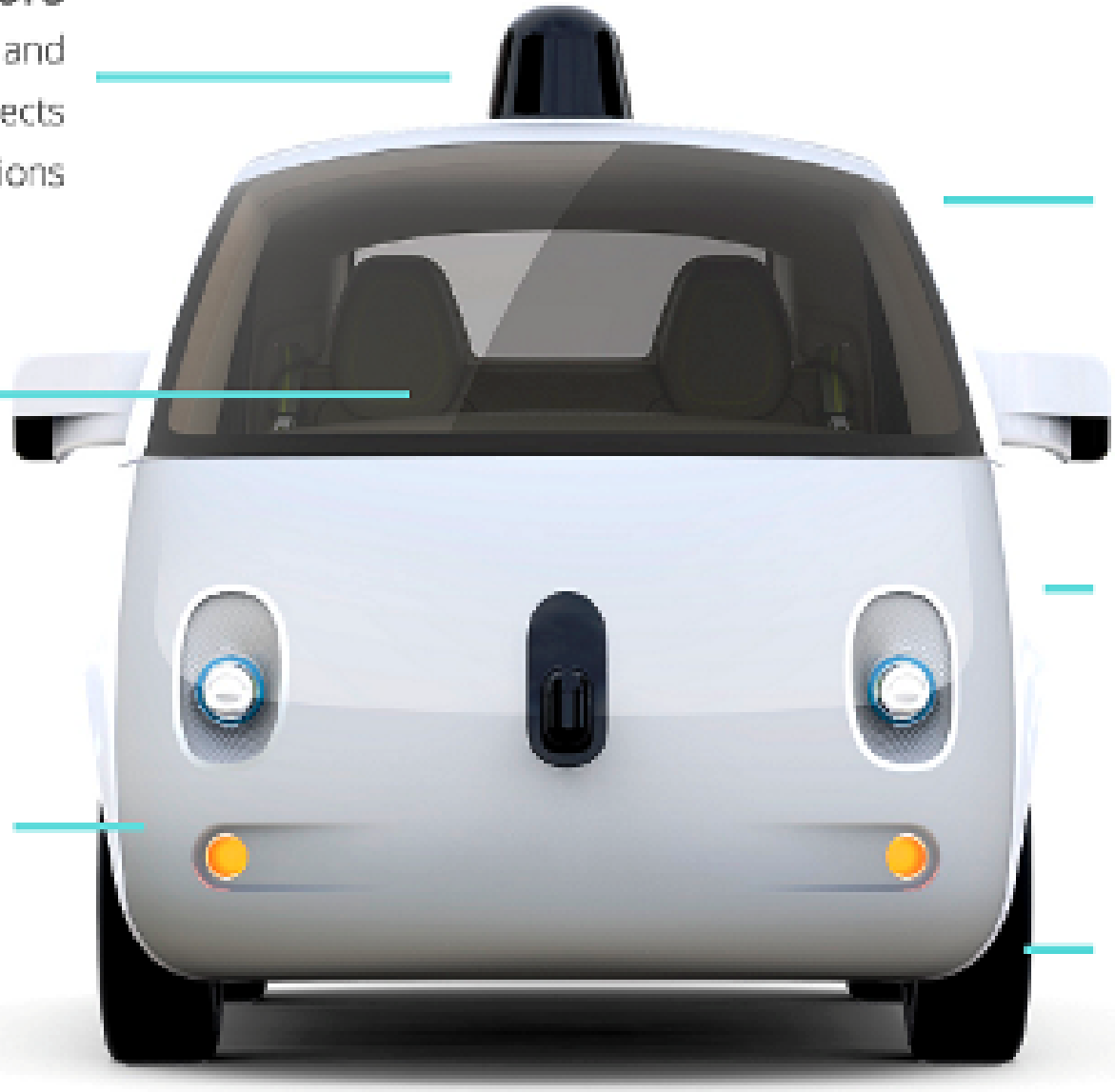
SENSORS SOFTWARE RADARS BACK-UP SYSTEMS OTHER COMPONENTS

CRYTICAL SYSTEM

HOW TO ACHIEVE HUMANS SAFETY IN SELF-DRIVING CARS?

An internal map of surroundings

How autonomous cars work?



Sensors
Lasers, radars and cameras detect objects in all directions

Interior
Designed for riding, not for driving

Electric batteries
To power the vehicle

Rounded shape
Maximizes sensor field of view

Computer
Designed specifically for self-driving

Back-up systems
For steering, braking, computing and more

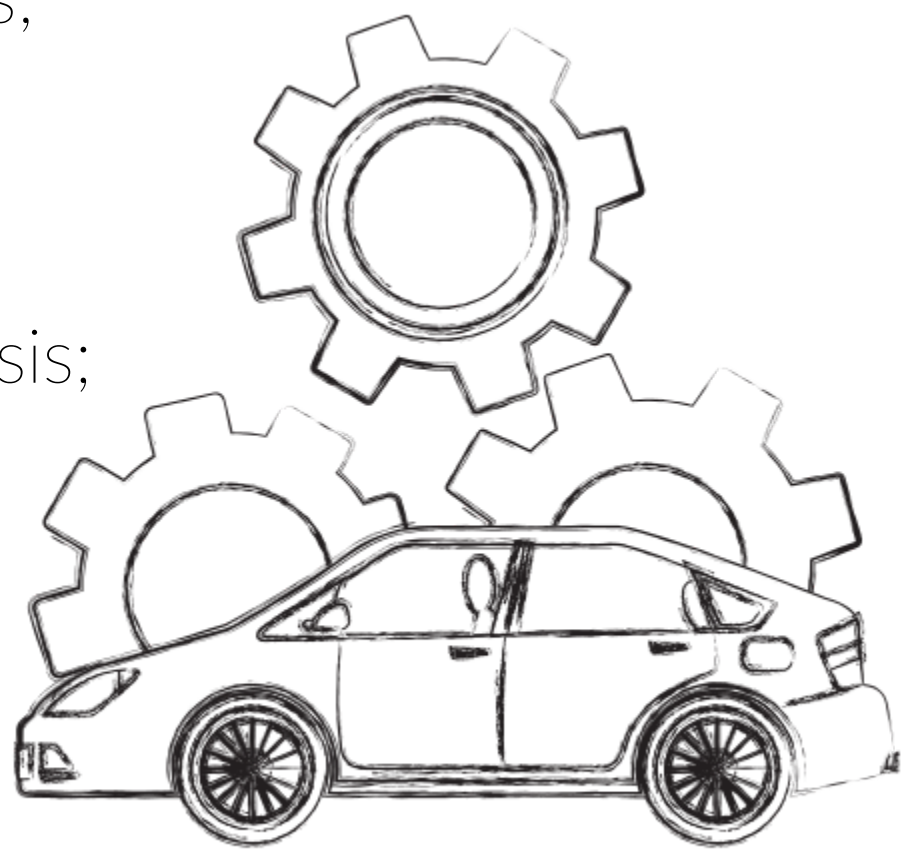
HOW AUTONOMOUS CARS WORK?

"The complex interactions between these components inside the autonomous vehicle make it difficult to model the system, and to align the safety and security in an autonomous vehicle" [5].

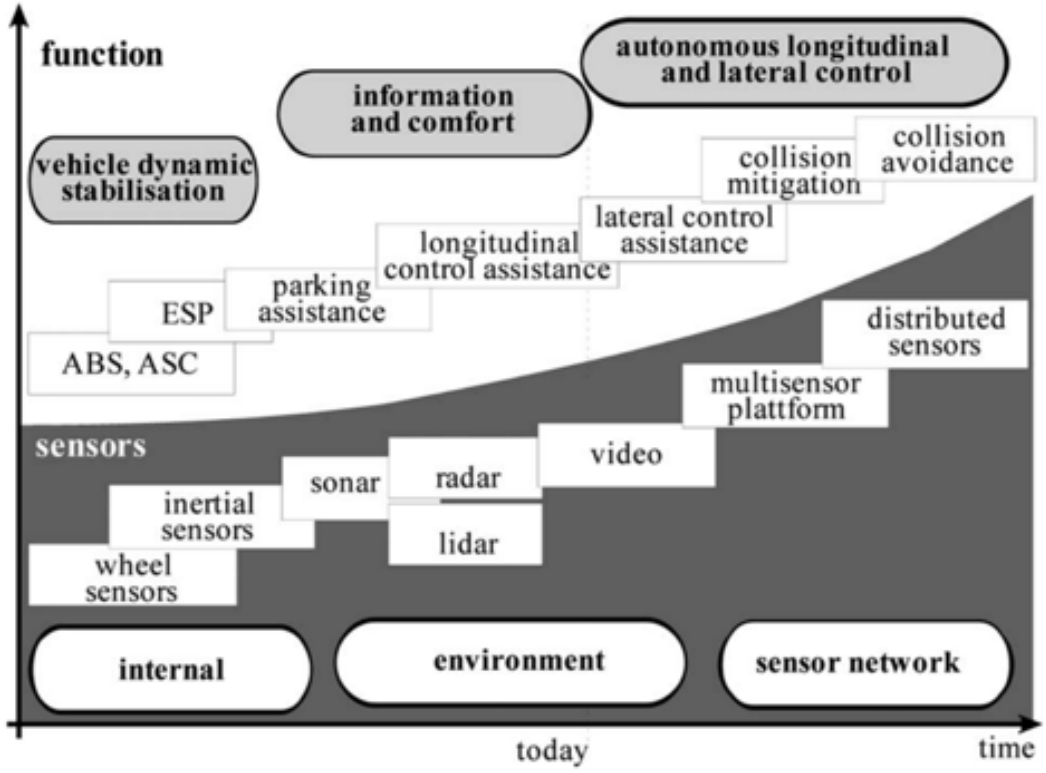
[5] J. Cui and G. Sabaliauskaite, "On the Alignment of Safety and Security for Autonomous Vehicles," no. c, pp. 59–64, 2017.

KEY PRINCIPLES IN ACHIEVING HUMANS SAFETY

- deep understanding of autonomous vehicles;
- independence;
- tried and tested components;
- good specification;
- analysis techniques;
- proper risk and hazard analysis;
- structuring;
- traceability;
- validation and others…



SERVICES WHICH HELP TO ACHIEVE HUMANS SAFETY



[2] Ü. ÖZGÜNER, C. STILLER, AND K. REDMILL, "SYSTEMS FOR SAFETY AND AUTONOMOUS BEHAVIOR IN CARS: THE DARPA GRAND CHALLENGE EXPERIENCE," PROC. IEEE, VOL. 95, NO. 2, PP. 397–412, 2007.

HOW PEOPLE CAN MAKE THEIR TRIP SAFER?

- PROPER TRAININGS AND EXPERIENCE IN DEALING WITH AUTONOMOUS CARS CAN SIGNIFICANTLY REDUCE THE LEVEL OF POTENTIAL RISK.
- PEOPLE SHOULD KNOW HOW TO INTERACT WITH BOTH SOFTWARE AND HARDWARE AND HOW TO TURN THE SELF-DRIVING SYSTEM ON AND OFF.
- ON THE TRACK, INSTRUCTORS SHOULD DELIBERATELY INJECT FAULTS INTO THE SYSTEM TO TRAIN DRIVERS HOW TO REACT PROPERLY.

[6] J. Muller, “Regulating the humans behind the wheels of autonomous vehicles,” 2018.

SAFETY STANDARDS

driver safety (generally regulated through licensure and driving behaviour laws);

vehicle safety (generally regulated on the safety standards such as for safety the international generic – ISO 26262 [7], for security SAE J3061 [8], UK automotive – MISRA [9] and others);

[7] "ISO 26262-1:2018 - Road vehicles -- Functional safety -- Part 1: Vocabulary." [Online]. Available: https://www.iso.org/standard/68383.html.
[8] "J3061A (WIP) Cybersecurity Guidebook for Cyber-Physical Vehicle Systems - SAE International." [Online]. Available: https://www.sae.org/standards/content/j3061/.
9] "MISRA C++ Home." [Online]. Available: https://www.misra.org.uk/MISRACHome/tabid/128/Default.aspx.

SAFETY STANDARDS

- for safety the international generic – IEC 61508 part 3 [10];
- for security the equivalent: – ISO CD 15408 [11];
- and others.

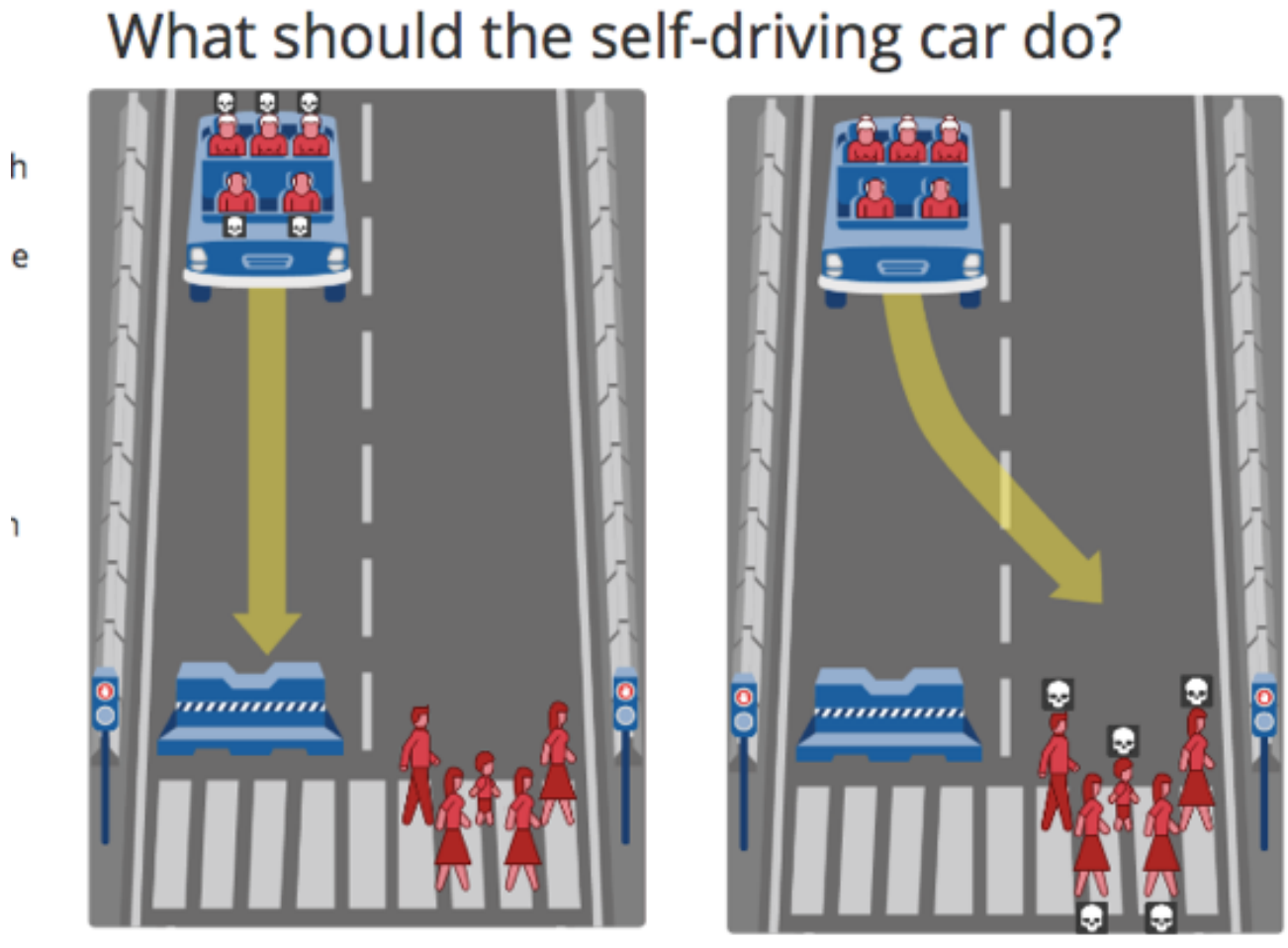
[10] “IEC 61508: Functional Safety - Standards.” [Online]. Available: https://www.iec.ch/functionalsafety/standards/page3.htm.
[11] “ISO/IEC 15408-3:2008 - Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components.” [Online]. Available: https://www.iso.org/ru/standard/46413.html.

HUMAN SAFETY CHALLENEGES NEED TO BE ADDRESSED

DIFFICULTIES IN ACHIEVING HUMANS SAFETY

- difficult to understand;
- difficult to investigate its failure modes ;
- difficult to design it to satisfy all safety requirements;

THE "TROLLEY" PROBLEM



THE "TROLLEY" PROBLEM

"ETHICAL DECISIONS ARE NEEDED WHENEVER THERE IS RISK, AND RISK IS ALWAYS PRESENT WHEN DRIVING " [12]

WHAT IT MEANS THAT THE WRONG DECISION COULD LEAD TO LOTS OF HUMANS DEATHS

[12] N. Goodall, "Machine Ethics and Automated Vehicles," Road Veh. Autom. Springer, vol. 81, no. 11, pp. 93–102, 2014.

"THE MORAL MACHINE EXPERIMENT"

"THE STRONGEST PREFERENCES ARE OBSERVED FOR SPARING HUMANS OVER ANIMALS, SPARING MORE LIVES, AND SPARING YOUNG LIVES. ACCORDINGLY, THESE THREE PREFERENCES MAY BE CONSIDERED ESSENTIAL BUILDING BLOCKS FOR MACHINE ETHICS" [13].

[13] E. Awad, S. Dsouza, R. Kim, J. Schulz, J. Henrich, A. Shariff, J.-F. Bonnefon, and I. Rahwan, "The Moral Machine experiment," Nature, vol. 563, no. 7729, pp. 59–64, 2018.

CYBER SECURITY PROBLEM

TO ACHIEVE CYBER SAFETY IN SELF-DRIVING CARS DEVELOPERS SHOULD FOLLOW CYBER SECURITY STANDARDS WHICH HAVE BEEN ALREADY RELEASED BY BY THE BRITISH STANDARDS INSTITUTE (BSI) 19 DECEMBER 2018.

News story

New cyber security standard for self-driving vehicles

New cyber security standard for developing self-driving car technology released.

Published 19 December 2018
From: Department for Transport, Centre for Connected and Autonomous Vehicles , and Jesse Norman MP

CYBER SECURITY PROBLEM

JESSE NORMAN, FUTURE OF MOBILITY MINISTER, SAID: "THIS CYBER SECURITY STANDARD SHOULD HELP TO IMPROVE THE RESILIENCE AND READINESS OF THE INDUSTRY, AND HELP KEEP THE UK AT THE FOREFRONT OF ADVANCING TRANSPORT TECHNOLOGY."

[12] "NEW CYBER SECURITY STANDARD FOR SELF-DRIVING VEHICLES - GOV.UK." [ONLINE]. AVAILABLE: HTTPS://WWW.GOV.UK/GOVERNMENT/NEWS/NEW-CYBER-SECURITY-STANDARD-FOR-SELF-DRIVING-VEHICLES.

INTERACTION ISSUES

- INFORMATION NOISE IS A PROBLEM ASSOCIATED WITH PROCESSING A LARGE AMOUNT OF INFORMATION ;

- DEVICE BREAKDOWN. "IN THE FUTURE ADVANCED AUTONOMOUS CARS MAY HAVE THE ABILITY OF SELF-HEALING (SELF-REPAIRING) AND WOULD BE ABLE TO REPAIR OR REPLACE SOME BROKEN PARTS" [13].

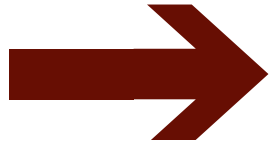
- OTHER INDEPENDENT TRAFFIC PARTICIPANTS CAN INFLUENCE THE WAY OF COMMUNICATION AMONG AUTONOMOUS VEHICLES.

[13] P. GORA, I. R.-T. R. PROCEDIA, AND UNDEFINED 2016, "TRAFFIC MODELS FOR SELF-DRIVING CONNECTED CARS," TRANSP. RES. PROCEDIA, VOL. 00, NO. 14, PP. 2207–2216, 2006.

SUMMARY

- ✓ autonomous automobiles and why they are critical systems;
- ✓ key principles in achieving human safety in autonomous cars;
- ✓ services which is intended to achieve humans safety (sensors, assistances, software);
- ✓ main safety standards which is used while developing self-driving cars;
- ✓ global challenges which can cause absolute harm to people and prevent self-driving cars appear on roads;

VIDEO



https://www.youtube.com/watch?v=HgF7E5q9sU4