Tactical Safety Reasoning. A case for autonomous vehicles

CA2V 2018

Alexandru C. Serban[1,2]
Erik Poll[1]
Joost Visser[2]

[1]Radboud University, Nijmegen

[2]Software Improvement Group, Amsterdam

The Netherlands

03.06.2018

Traffic safety in a nuthshell

Safety concerns are divided between:

- Car manufacturers - *functional* safety - ISO 26262
- Drivers - [tactical?] safety

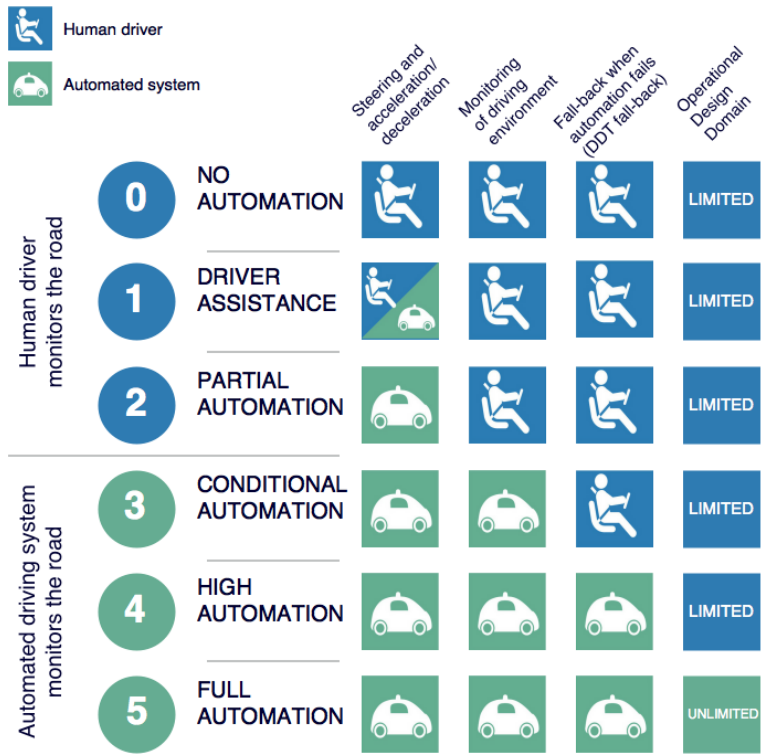
Functional safety - risk management

ISO 26262 sees safety as a *functional property* of a system and enforces safe operation in response to *inputs*, *hardware failures* or *environmental changes*.

$$Risk_{component} = Severity \times (Exposure \times Controllability)$$

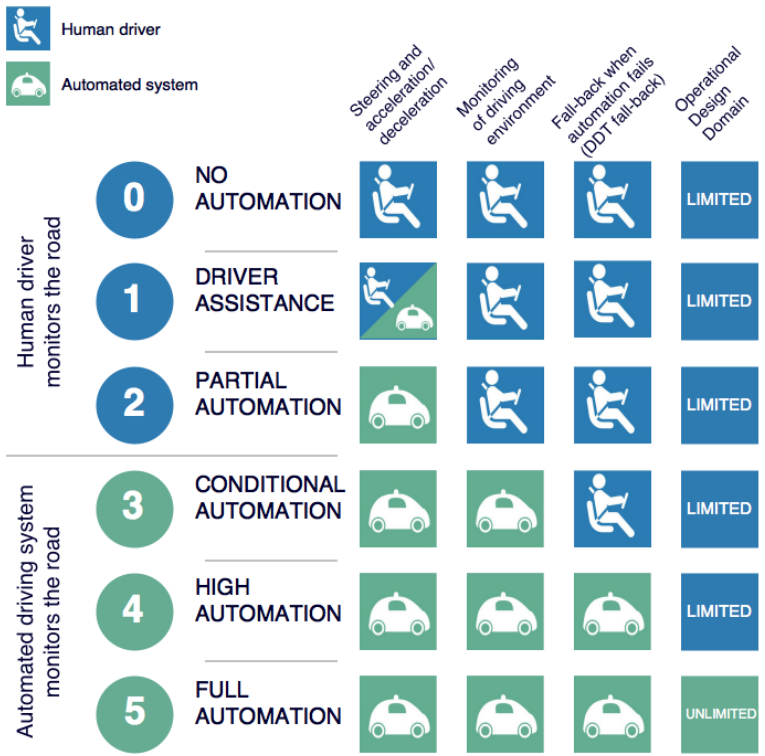
Driver/Tactical safety?

Progressively removing the driver



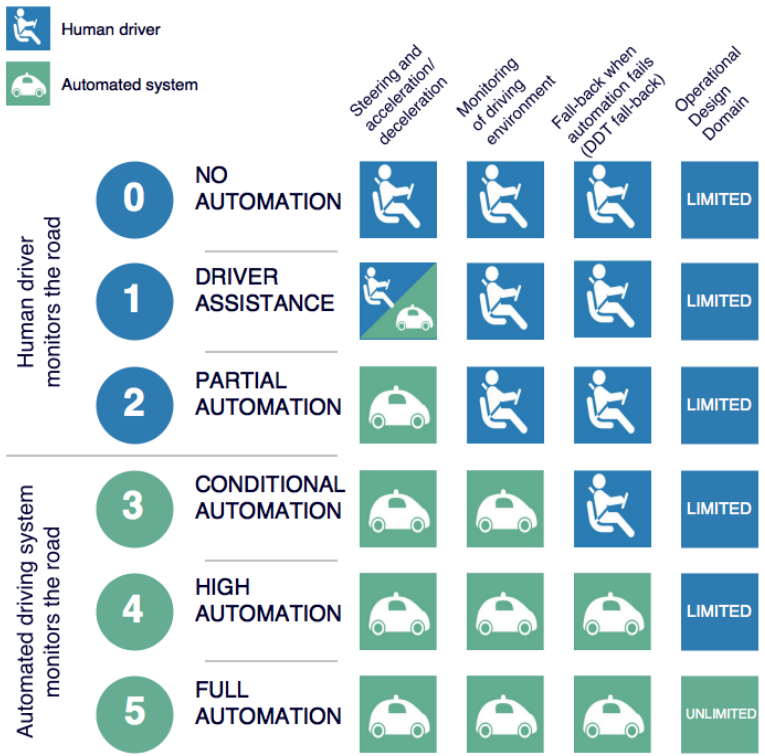
Progressively removing the driver

- Step 1 - The vehicle monitors the environment.



Progressively removing the driver

- Step 1 - The vehicle monitors the environment.
- Step 2 - The vehicle is responsible for all safety fall-back mechanisms.



Tactical safety[1]

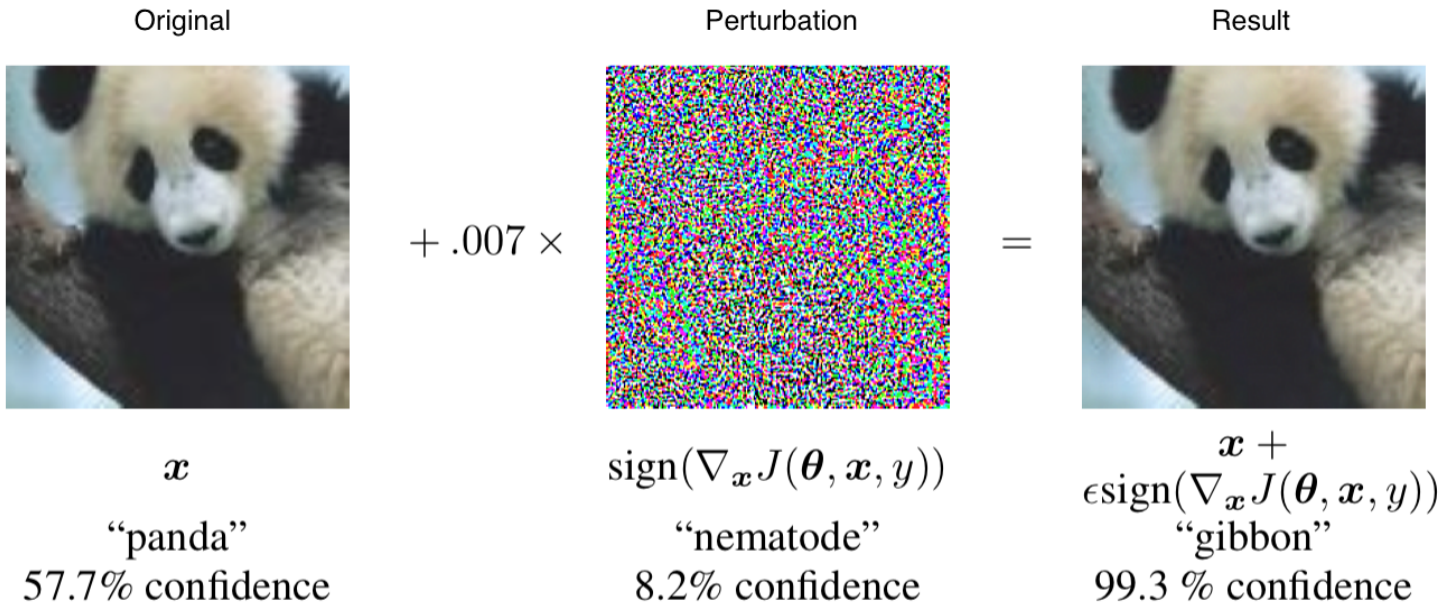
Definition

Safe planning and execution of driving manoeuvres, response to traffic events and dynamic driving task fall-back.

[1] Tactical safety is meant to complement functional safety and not replace it

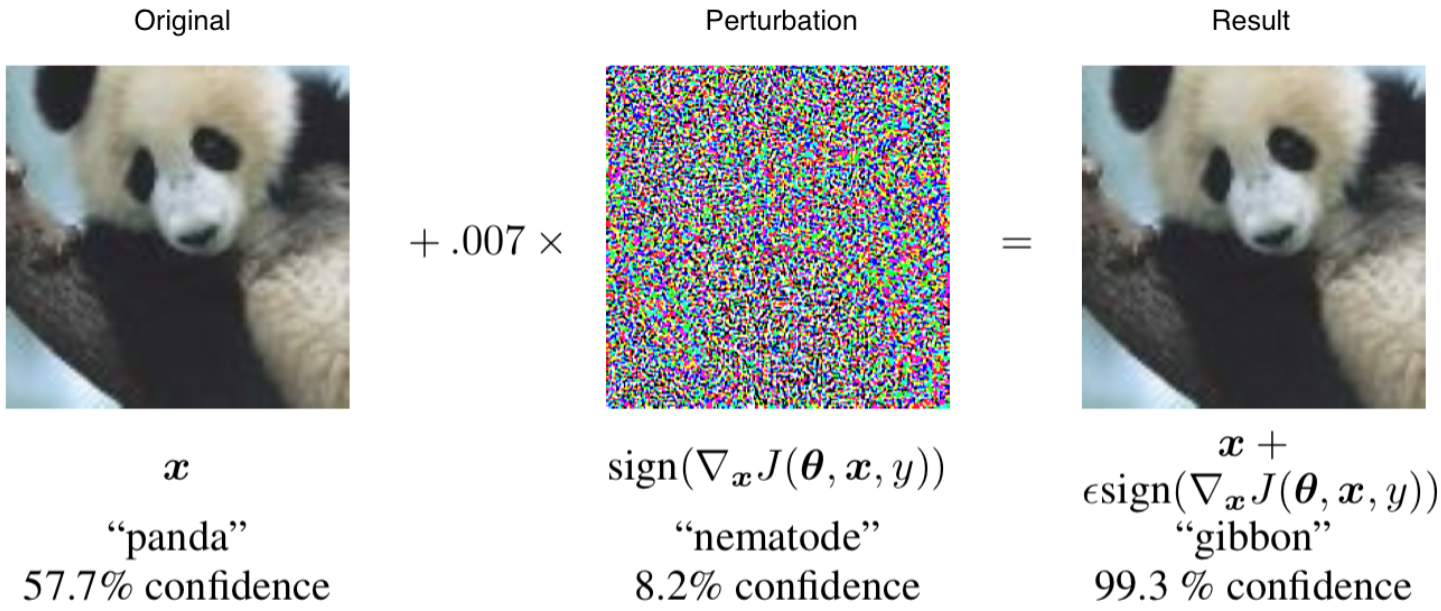
Tactical safety requirements

Sensors threat to safety



Small perturbations of inputs for computer vision algorithms cause miss-classification with high confidence intervals [1].

Sensors threat to safety



Small perturbations of inputs for computer vision algorithms cause miss-classification with high confidence intervals [1].
Source of perturbations: sensor wear, malicious attacks, algorithms non-determinism, etc.

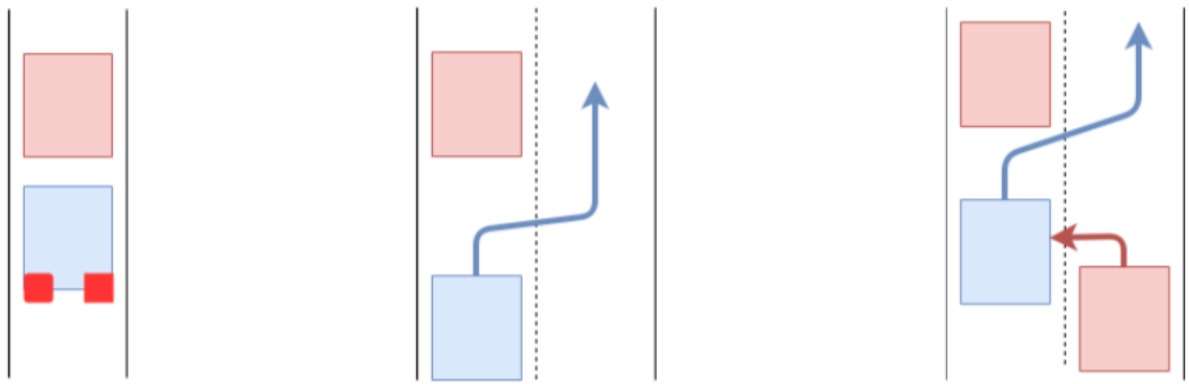
Safety objectives?

We can not specify all traffic situations. So a car will have to *reason* about a new situation.

Safety objectives?

We can not specify all traffic situations. So a car will have to *reason* about a new situation.

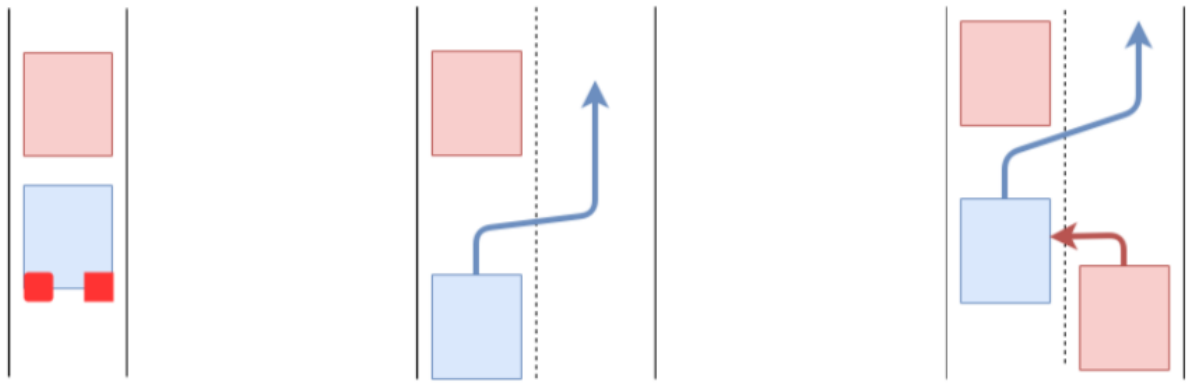
What happens when an accident can not be avoided?



Safety objectives?

We can not specify all traffic situations. So a car will have to *reason* about a new situation.

What happens when an accident can not be avoided?



How about *standard* safety objectives?

Safety fall-back means?

"Does your car have any idea why my car pulled it over?"

Tactical safety requirements

SAE Level	Functional Requirements	Tactical requirements
3	Runtime hazard identification & mitigation	Error resilient algorithms for environmental monitoring; Standard safety objectives; Methods to prove correct safety reasoning in limited ODDs; Decision to transfer control; Standard & provable transfer time;
4	Runtime hazard identification & mitigation	DDT fall-back reasoning; Standard DDT fall-back objectives; Methods to prove correct DDT fall-back reasoning;
5	Runtime hazard identification & mitigation	Enhanced context awareness; Advanced methods to prove correct safety reasoning in all contexts;

Conclusions

- How this tech will work *safely* is still ambiguous

Conclusions

- How this tech will work *safely* is still ambiguous
- It's clear that new regulations and standards are needed

Conclusions

- How this tech will work *safely* is still ambiguous
- It's clear that new regulations and standards are needed

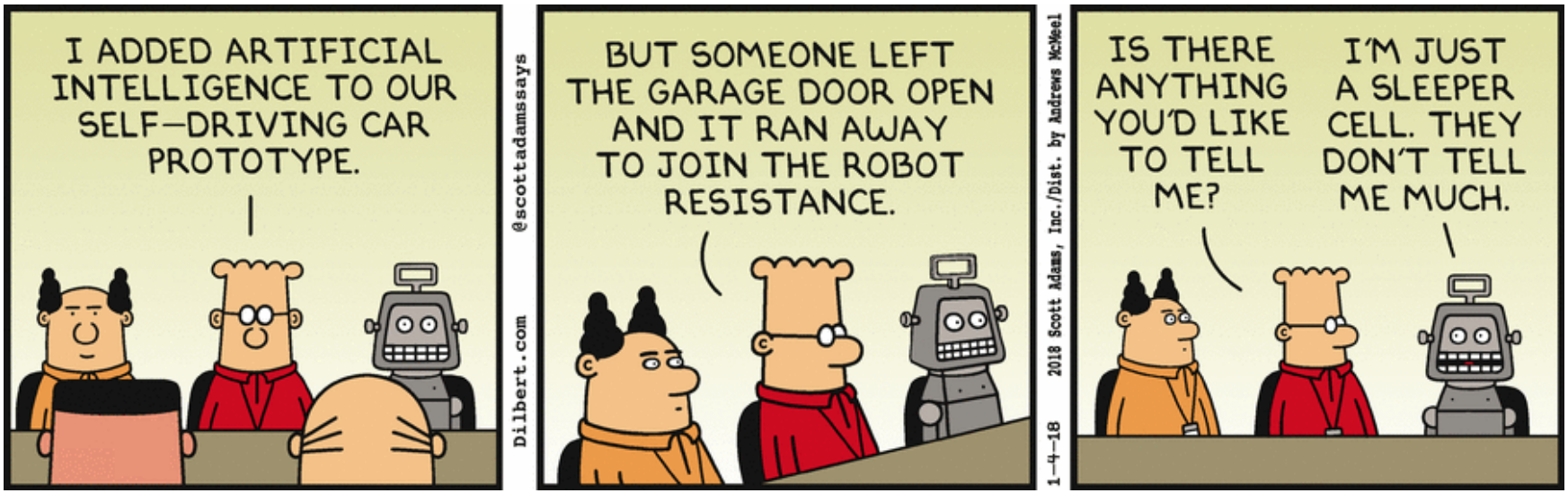
- We outline an *initial* definition and basic requirements for *tactical* safety

Conclusions

- How this tech will work *safely* is still ambiguous
- It's clear that new regulations and standards are needed

- We outline an *initial* definition and basic requirements for *tactical* safety
- And provide insights into new research directions

Thank you for your attention. Questions?



References I

 Christian Szegedy et al. “Intriguing properties of neural networks”. In: *arXiv preprint arXiv:1312.6199* (2013).