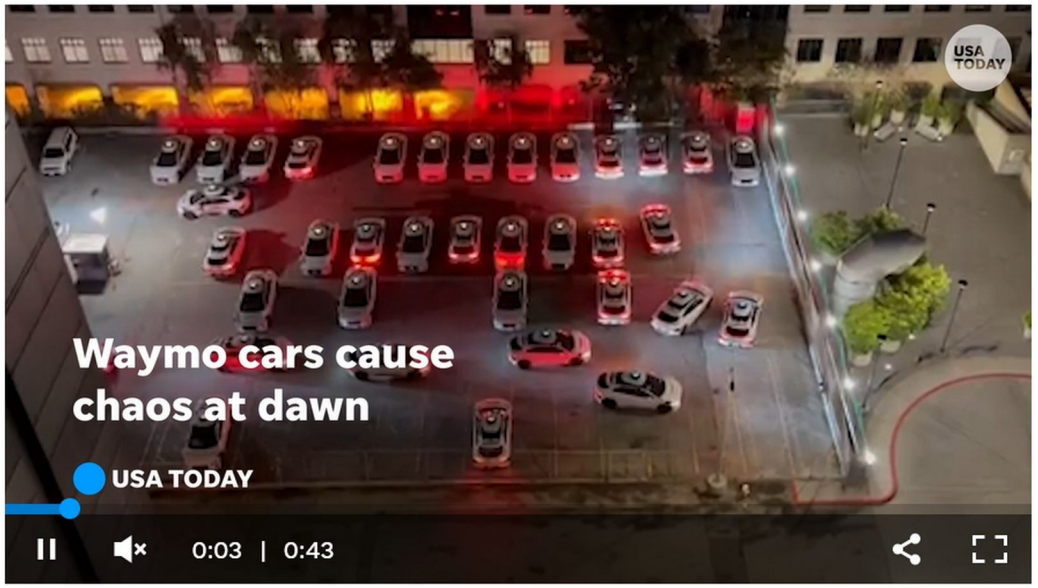
Panel Moderator Position

Venice
Oct. 2024

Cyber Security Now - Dealing with Autonomous Systems

Are AI-based autonomous systems ready for the market?

(Automated parking activates collision alarms)



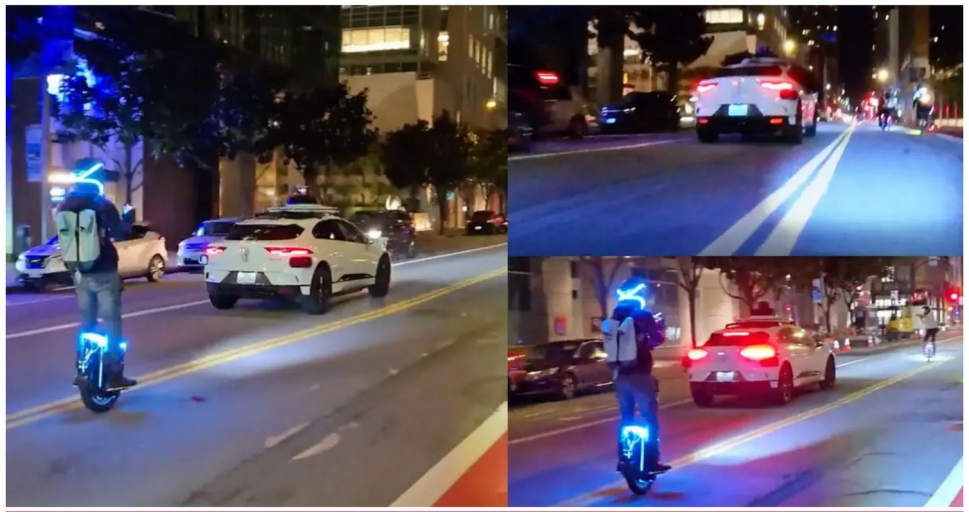
Driverless Waymo taxis caught on video honking at each other at 4 A.M.

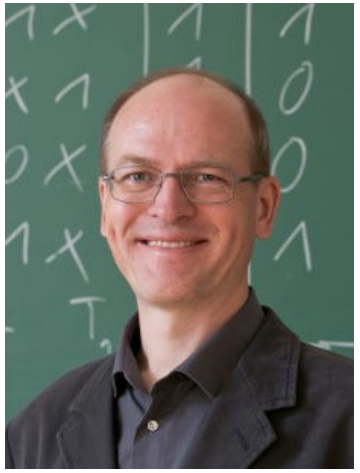
A cluster of Waymo cars were caught on video honking at one another outside a housing complex.

(Driverless car on the wrong side of a street)

"I think we can all agree that the decision making of the Waymo was not good."

/ Advanced Transport / Cruise / Robotaxis / Waymo





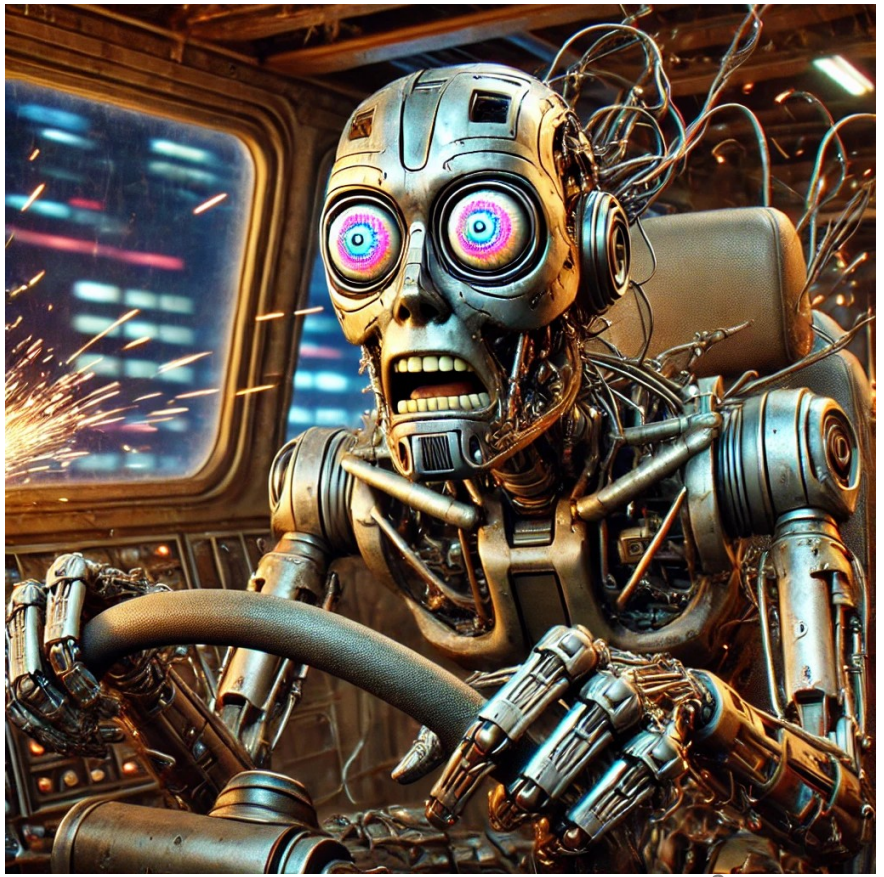
Erik Buchmann
Center for Scalable Data Analytics and Artificial Intelligence Dresden/Leipzig, Germany

Panel Moderator Position

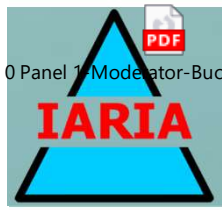
Venice
Oct. 2024

Are AI-based autonomous systems ready for the market?

- **Semantic Gap**
  - A throughout specification does not exist / cannot exist
    e.g., due to complexity of the environment
  - *Example*: Cleaning robot should "clean all accessible floors"
    Counter-example: Automatic subways on special tracks
- **Responsibility Gap**
  - Undecidable whether an accident was caused by system or human
  - *Example*: Driver expect the brake assist to stop, but it does not
    Counter-example: Automated warehouse where humans are banned
- **Liability Gap**
  - Responsibility for compensating for an accident
  - *Example*: An autonomous drone crashes into a pedestrians area
    Counter-example: A lawn mover in a fenced area hurts an intruder



Atakishiyev, Shahin, et al. "Explainable artificial intelligence for autonomous driving: A comprehensive overview and field guide for future research directions." IEEE Access (2024).



0 Panel 1 Moderator-Buchmann.pdf

SoftNet 2024 & NexTech 2024

Theme

Cyber Security Now - Dealing with Autonomous Systems

CONTRIBUTORS

PORTO
July 2024

Moderator

Prof. Dr. Erik Buchmann, Leipzig University, Germany

Panelists

Prof. Dr. Marko Jäntti, University of Eastern Finland, Finland

Prof. Dr. Lasse Berntzen, University of South-Eastern Norway (USN), Norway

Dr. Tiago Gasiba, Siemens AG, Munich, Bavaria, Germany

Prof. Dr. Joshua Sipper, Air University, Air Command and Staff College, USA

Panelist Position

Dr. Tiago Gasiba
Siemens AG

- Cybersecurity plays and will keep playing a critical role in the safety and reliability of autonomous systems
- Increased interconnection between systems posses a severe risk
- Autonomous systems are like critical infrastructure “on the go”
  - Hacking such systems can lead to loss of human life
  - Privacy plays a significant role
- Recent usage of AI in autonomous systems causes potential issues:
  - Ethical and moral dilemmas, e.g. injure pedestrian vs injure passengers
  - Lack of explainability can lead to problems with certification
  - Performance under adverse weather conditions?
- Cybersecurity as a continuous process ↦ we must make sure that security never has a negative impact on safety

Panelist Position

Venice
FALL 2024

Cyber Security Now - Dealing with Autonomous Systems

Josh Sipper
ACSC

- **Lethal Autonomous Weapons Systems (LAWS)**
  - Militaries testing numerous systems across the globe
  - These will likely be the norm on mobile and fixed platforms in coming years
  - Systems need very refined locational, parametric, and systems data to prevent harming civilians/fratricide
  - These parameters are used to enhance algorithms for autonomous systems like Israel's Iron Dome
- **Autonomy in IDS/IPS**
  - Autonomy in IDS to identify and mitigate intrusions after they happen (reactive)
  - Autonomy in IPS to identify or predict intrusions before they happen (proactive/predictive)
- **Cybersecurity in ICS/SCADA (Information Warfare effects)**
  - Many systems are air-gapped, but still vulnerable through the EMS
  - Adversary intelligence gathering puts systems and information at risk
  - Psychological effects persist even after mitigations and hardening
  - Autonomous systems for ICS/SCADA must cover a wider landscape than only cyber

Panelist Position

Venice
ICSEA 2024

- **Can autonomous vehicles be killing machines?**
- **Heavy machinery vehicles become increasingly smarter**
  - Forest machines
  - Excavators
  - Trucks & buses
- **A cyber attack on an autonomous vehicle can**
  - Crash a vehicle
  - Cause life-threatening risks to passengers or people near the vehicle
  - Cause environmental damage
  - Reveal confidential data etc
- **Take a holistic approach on cybersecurity and information security**

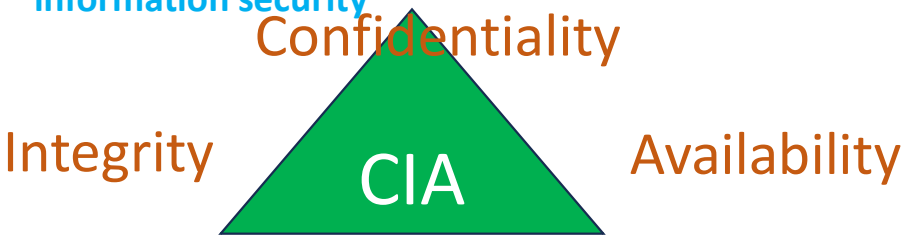


Figure: Kuopio bus accident in 2018. The behavior of the driver was the root cause of the accident, not a cybercrime. 17 injured, 4 dead. Source: Iltasanomat. Photographer: Pertti Hänninen

Marko Jäntti, UEF

UNIVERSITY OF
EASTERN FINLAND

Panelist Position

Venice
ICSEA 2024

How to prevent cybersecurity attacks to autonomous vehicles?

Investigate cyber-security controls/measures related to specific functionality of an autonomous vehicle and related risks:

- GPS spoofing to affect navigation of the autonomous vehicle
- Hacking a vehicle camera
- Hacking electric windows and doors
- Hacking vehicle breaks
- Man in the middle attack to access confidential information
- Installing malware or harmful components to a vehicle
- Unauthorized access to the control system of a cargo ship with explosives

UNIVERSITY OF
EASTERN FINLAND

Panelist Position

- Everything is connected to the Internet
- All devices connected to the Internet has a risk of being hacked
- Autonomous systems are supposed to work on their own without human interventions
- Therefore, the impact of autonomous systems being hacked is high
- Cybersecurity is critical
- Failsafe mechanisms to handle incidents

- **Most accidents are caused by human failures, not by technology**
- **Autonomous systems may contribute to a safer society**
- **Need to address possible vulnerabilities in autonomous systems**

Lasse Berntzen
University of South-Eastern Norway

Background

- USN has participated in several projects on autonomous systems, primarly in the maritime sector, but also with autonomus vehicles

Training programs

- Cybersecurity for the aviation sector
- Cybersecurity for the maritime sector (with NormaCyber)

Research

- Current project on ransomware

Autonomous ships