The Lion Cage Project

Lion Cage: the Societal Risks of Software Defined Vehicles

Tor Indstøy – VP of Risk Management and Threat Intelligence at Telenor Group

Arild Tjomsland – Special Advisor TTO at the University of Southeast Norway

All technical details at Lion Cage on LinkedIn

The Lion Cage Project

Lion Cage project team of ~10 experts
2,5 years of data harvesting from Tor's NIO ES8

- Spectrum analysis
- Bluetooth sniffing
- Interception of transmitter in car
- GPS analysis
- Pentesting

+ OSINT including
- Patent review
- Chinese message boards

TLP:CLEAR


Modern SDVs:
2-300 computers
Electronic Toll Collection
Instrument Cluster
Head-Up Display
Wiper Control
Airbag Deployment
Electric Motor Management
Battery Management
Adaptive Front Lighting
Night Vision
Driver Alertness Monitor
Accident Recorder
Event Data Recorder
Auto Dimming Mirror
Parental Controls
Active Cabin Noise Suppression
Voice/Data Communications
Navigation System
Cabin Environment Controls
Entertainment System
Security System
Digital Turn Signals
Remote Keyless Entry
Self-Parking System
Modern EVs are Software-Defined Vehicles (SDV)
Active Suspension
Electric Power Steering
Tire Pressure Monitoring
Lane Departure Warning
Active Vibration Control
Active Yaw
Adaptive Cruise Control
Automatic Braking (Brake-by-Wire)
Anti Lock Braking
Blind Spot Detection
Hill-Hold Control
Electronic Stability Control
Seat Position Control
TLP:CLEAR
Components communicate over the car's own wifi
Third party components have their own processor and update their own software OTA

Driver assistance (towards autonomy)

- Drive-by-wire
- Steer-by-wire
- Cameras
- Radars
- Sensors

Extensive use of cloud services (shared among producers)

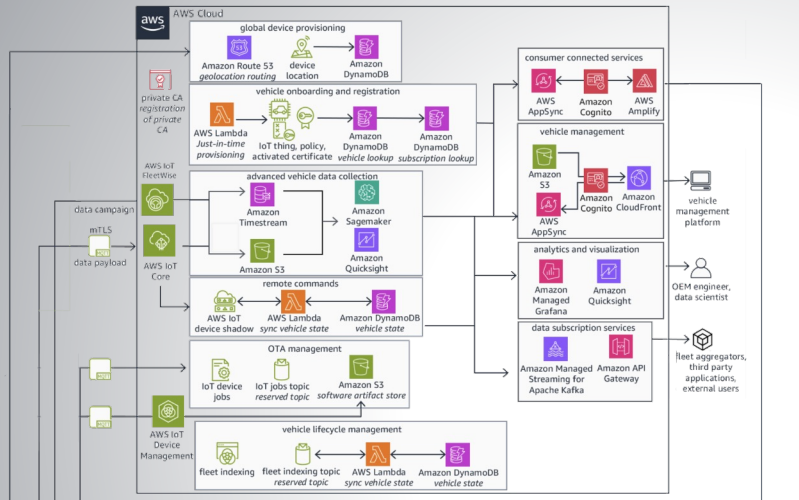
- Navigation
- Voice control processing
- OTA software update platforms

- With OTA type approval becomes trust-based
- Cybersecurity for SDVs is a process certification, without testing of the result
- SDVs are dependant on their producer for updates throughout their lifetime

Interfaces

- Wi-Fi Mobile network, possible from 2G to 4G (LTE-M / NB-IoT bands, most likely not 5G)
- Bluetooth
- Charging port
- Radio receiver on 315MHz and 433MHz
- Smart key (key fob) / NFC card to open doors and start the car
- Emergency call system, which sends the car's position when pressing the SOS button
- GPS / GNSS (GLONASS)
- CAN bus interface (OBD2)
- Physical access, doors, windows
- Interior microphone
- Mobile phone app

TLP:CLEAR



Issues:

- Vulnerability to hacking
- Data collection for modeling society
- Data collection for AI race
- Individual and traffic safety
- Personal security
- Liability issues – complexity is too high for authorities, forensics

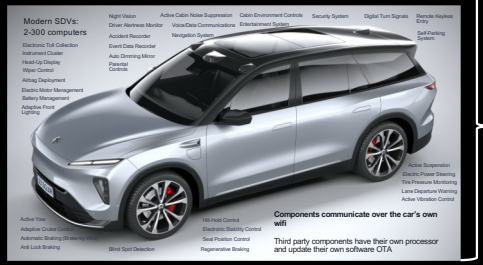
- **National security**

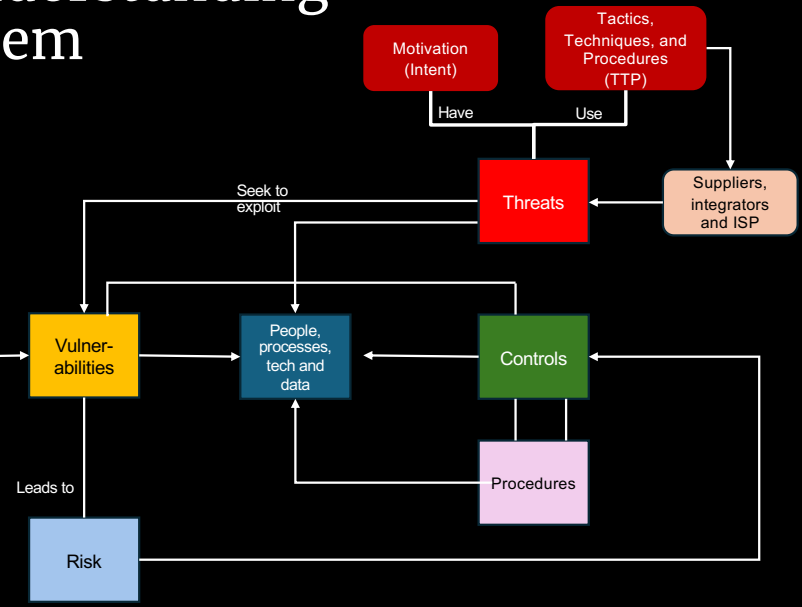
April 2025:

30 % of new cars sold in Norway are Chinese EVs.

TLP:CLEAR

Scenario-based understanding of the Risk Ecosystem





Inspired by:
https://www.linkedin.com/pulse/risk-ecosystem-interaction-risks-threats-vulnerabilities-/

TLP:CLEAR

Scenario 1: Traffic sabotage

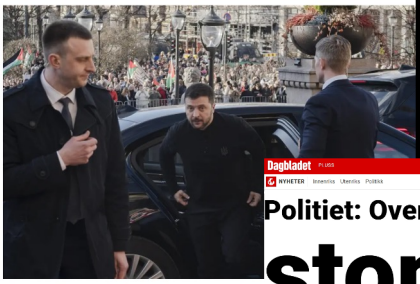
NEWS / CAR TECH

John Deere Tractors Stolen by Russia in Ukraine Remotely Disabled

When anti-right-to-repair technology is used for good.

PETER HOLDERITH
Posted on May 3, 2022
15

Forsvarets forum



STORTINGET:Volodymyr Zelenskyj ank
Foto: Robert S. Eik, Forsvarets forum

China's Nobel anger as Liu Xiaobo awarded peace prize

8 October 2010

Dagbladet PLUSS

NYHETER Innenriks Utenriks Politikk

Politiet: Over hundre biler stoppet

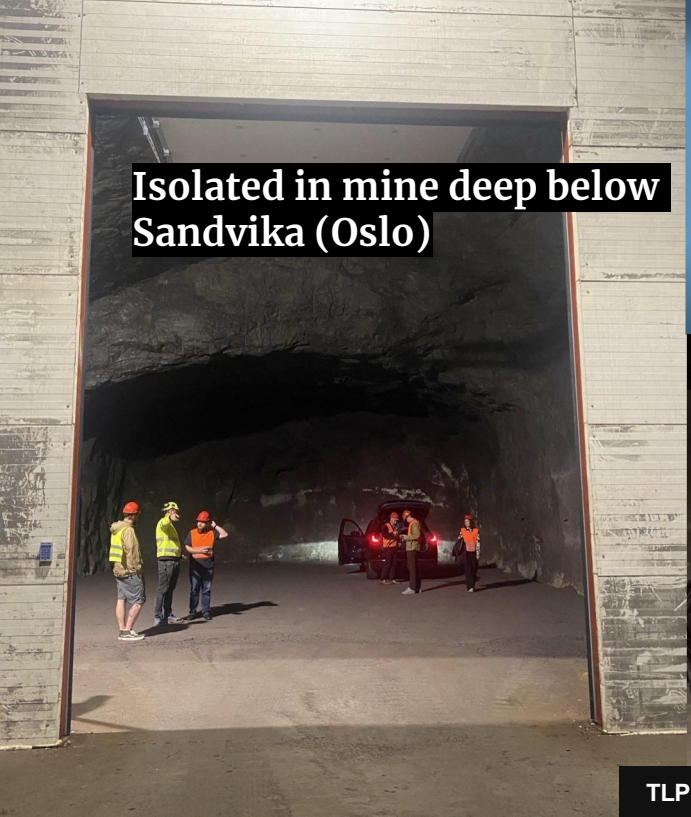
Nyhetssaker

Kjedekollisjon på E6 ved Lillestrøm skaper trafikale problemer

48 ord | annet | 1 måned siden

TLP:CLEAR

Isolated in mine deep below Sandvika (Oslo)

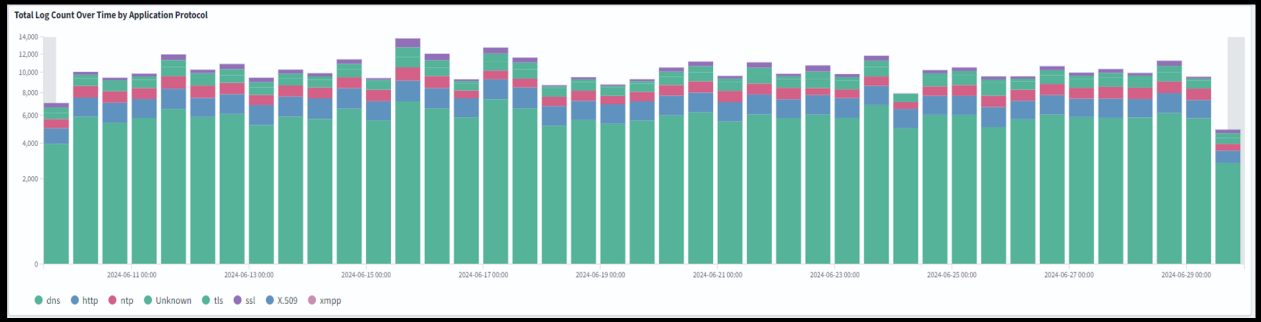


TLP:CLEAR

Findings

Can Tor’s NIO be used for traffic sabotage?

Findings: the car is constantly chatting

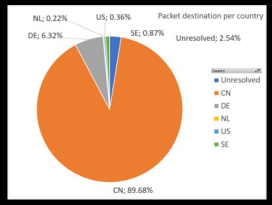


Data packets are moving in and out of the car at all times. Even when the car appears to be «turned off». Little to no variation throughout 24 hours, or geographic factors.

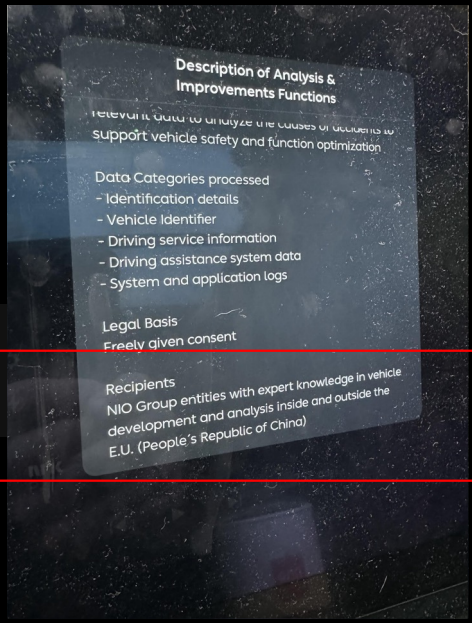
70% of data packets are heavily encrypted, unknown protocol

Findings: 90% of the data packages are routed to China

Among the recieveing URLs: 163.com China Network Communication Group (CNNIC), baidu.com, sina.com



Tor's data packets are being sendt here, in Beijing...



TLP:CLEAR

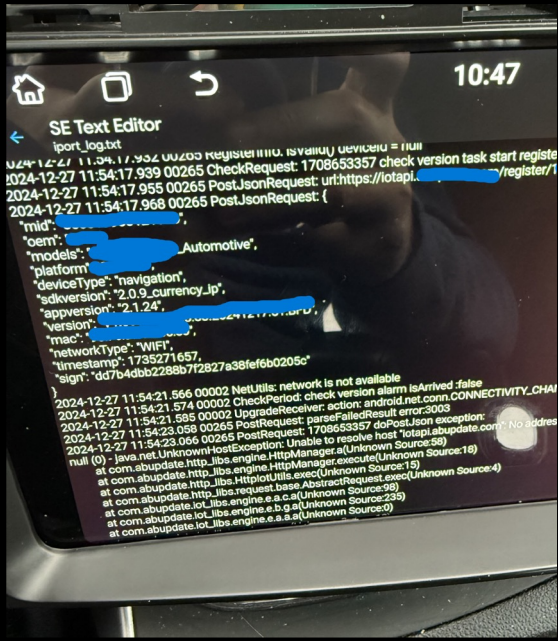
Daniel (20) hacket Telenor – så kom tilbudet om fast jobb

Fra gutterommet angrep han nettsidene. Uken etter fikk 20-åringen tilbud fast jobb fra selskapet – uten utdanning.

ETISK HACKER: Daniel Christensen fikk tilbud om fast jobb i Telenor.
FOTO: BENT LINDSETMO / NRK

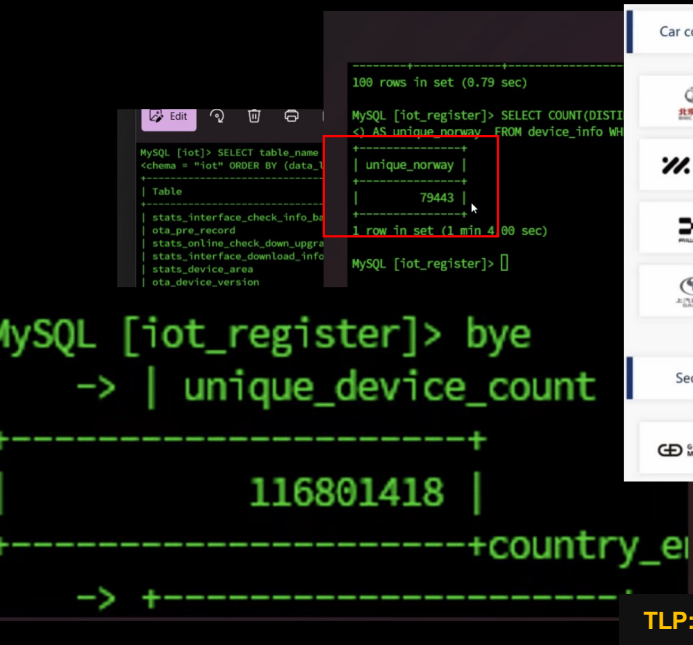
– Jeg elsker dette og brenner skikkelig for datasikkerhet.

Daniel's hack #1



TLP:AMBER

Hack #1: OTA update platforms are a weak link



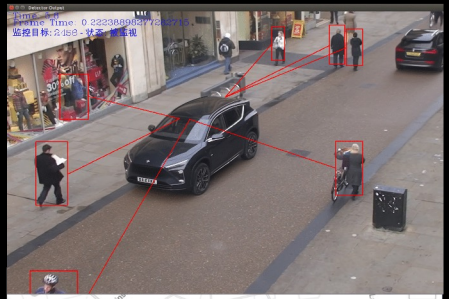
TLP:AMBER

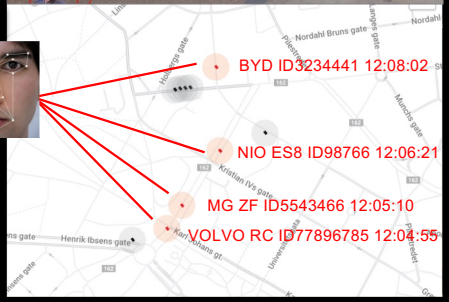
Conclusion

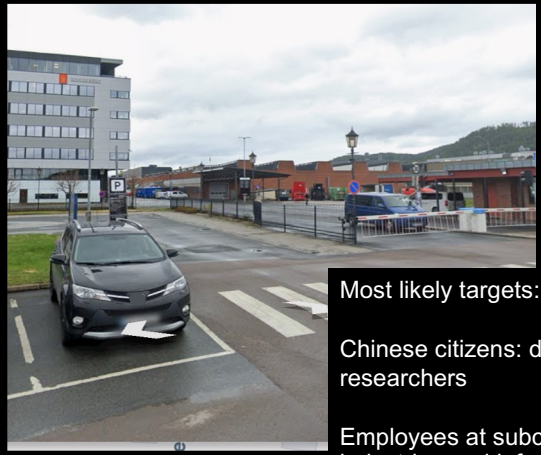
Can Tor’s NIO be used for traffic sabotage?

Yes. And by anyone. Cybersecurity is below standard.

Scenario 2: The car as part of a rolling surveillance network







Most likely targets:

Chinese citizens: dissidents, tudents, researchers

Employees at subcontractors at critical industries and infrastructure

Norwegian POIs with influence on the relationship with China

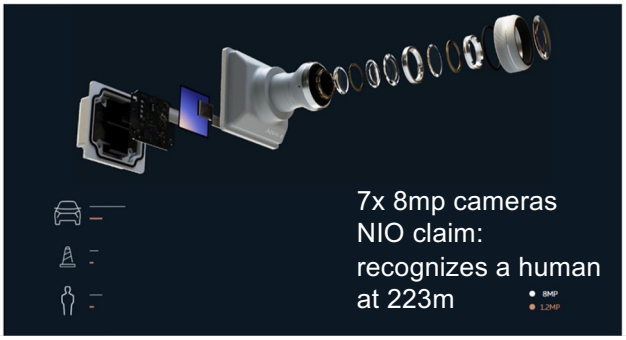
TLP:CLEAR

Findings

Can Tor’s NIO be used as a data collection platform?

Camera capable of facial & license plate recognition + aggregated from multiple sources

ucts Innovation Power & Service

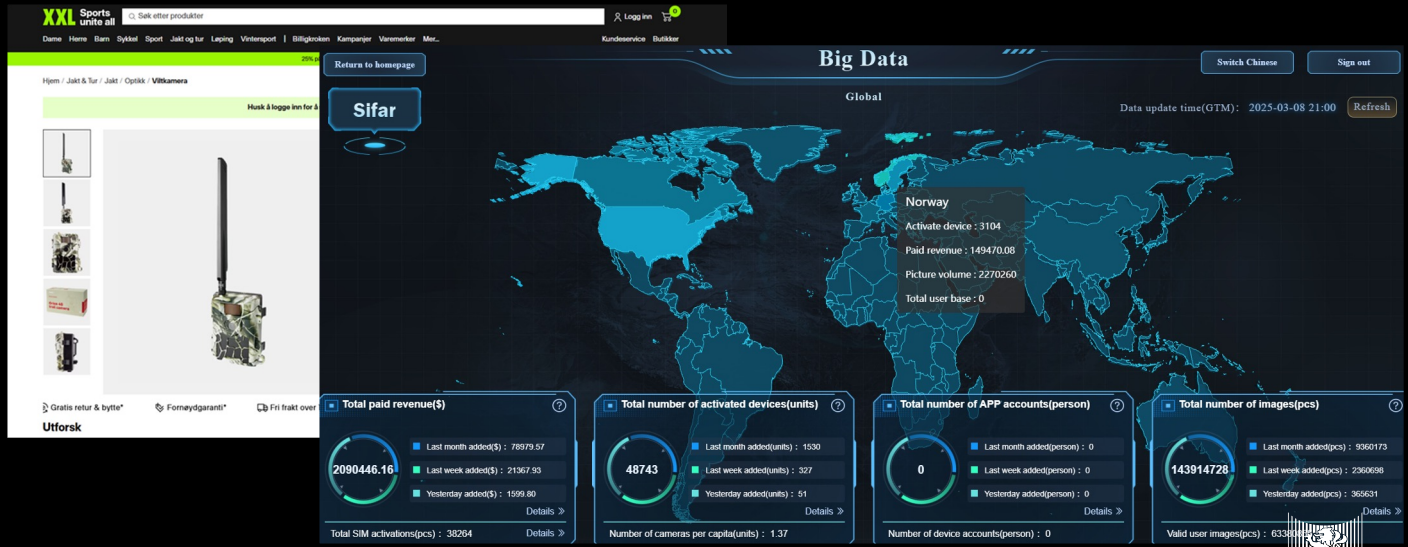


Camera Guidelines for Face Recognition

Match Confidence	Camera Resolution	Minimum Pixels on Face	Pixels per Meter	Pixels per Foot
High	All resolutions	80	457	137
Medium	6 MP or lower	50	286	86
	8 MP	60	343	103

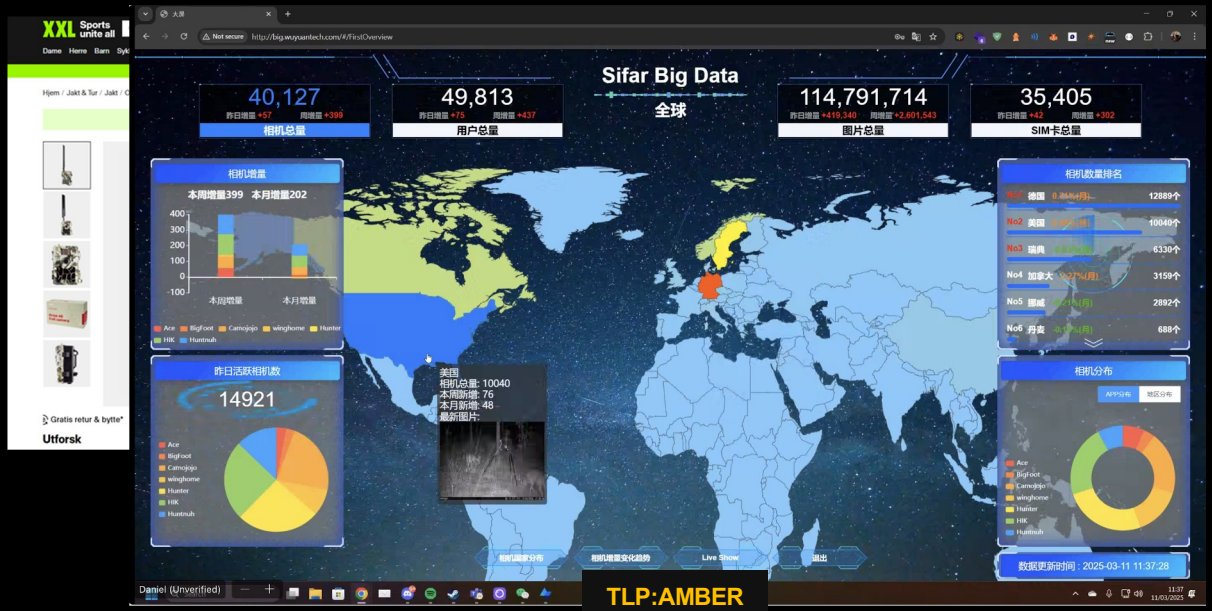
TLP:CLEAR

Hack #2: Third party component (camera) aggregates images to component producer.



TLP:AMBER

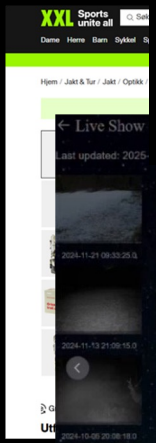
Hack #2: Third party component (camera) aggregates images to component producer.

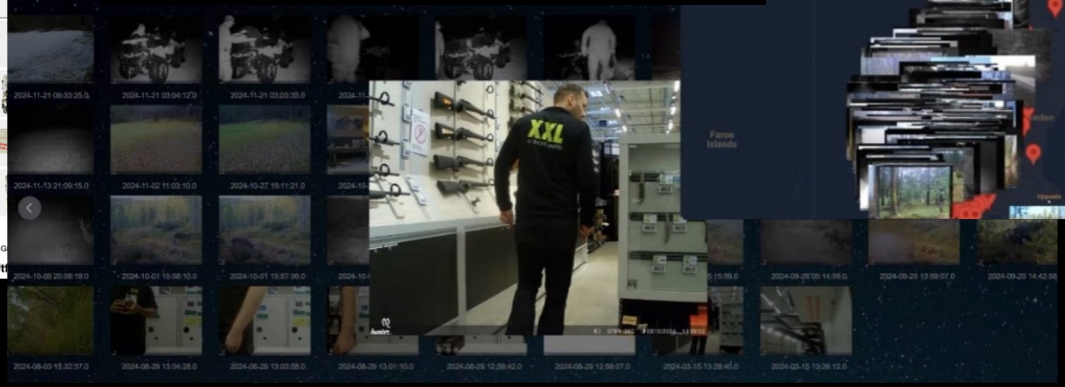


Hack #2: Third party component (camera) aggregates images to component producer.

Hack #2: Third party component (camera) aggregates images to component producer.

The Sifar Big Data system streams directly from products that use their camera component to their own map-based admin interface. An "embedded reserved interface".





Conclusion

Can Tor’s NIO be used as a data collection platform?

Yes.

Part 2

Technical Security Assessment of Buses from VDL and Yutong

- for Ruter AS

The Lion Cage Project

TLP:CLEAR

All buses in Norway will be electric by 2030, 80% will be Chinese.

Norway has 660 electric Chinese buses as of June 2025, an additional 1200 are on the way.

Scenario-based understanding of the Risk Ecosystem

Motivation (Intent)

Tactics, Techniques, and Procedures (TTP)

Have

Use

Threats

Suppliers, integrators and ISP

Seek to exploit

Vulner-abilities

People, processes, tech and data

Controls

Procedures

Leads to

Risk

Inspired by:
https://www.linkedin.com/pulse/risk-ecosystem-interaction-risks-threats-vulnerabilities-/

TLP:CLEAR

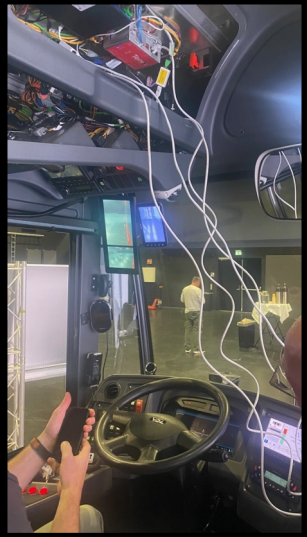
Scenario 1: «Kill Switch»

Traffic sabotage, or threat of sabotage used as leverage

Scenario 2: «Lutvann»

The bus as part of a rolling surveillance network

TLP:CLEAR



TLP:CLEAR

TLP:CLEAR


Ikke i trafikk
Ikke i trafikk
RuterBy


Ikke i trafikk
RuterRegion

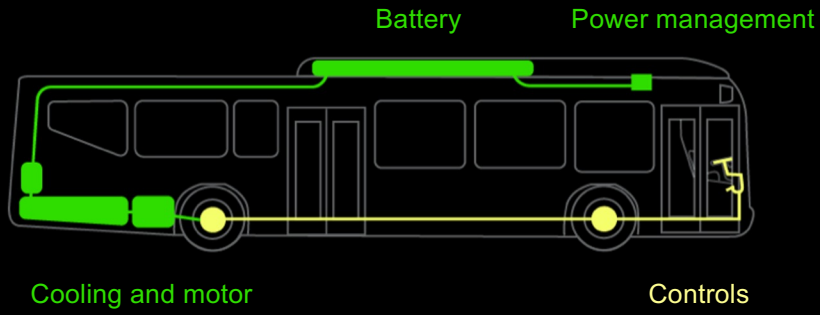
Findings

Can the VDL and/or the Yutong be used for either the Kill Switch scenario, or the Lutvann scenario?

VDL – 2022 model

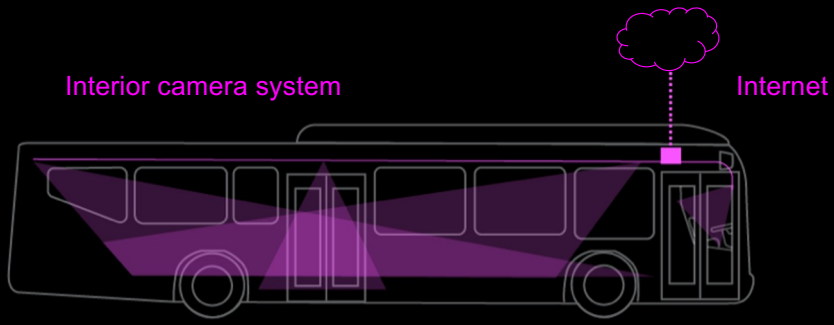
Critical functionality is effectively isolated.

The Kill Switch scenario is not possible with this bus.



VDL – 2022 model

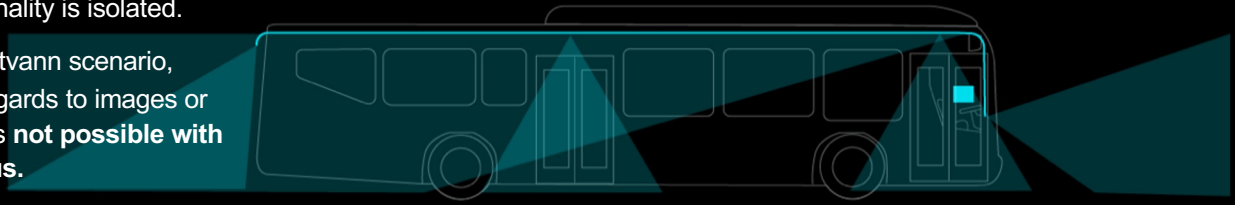
Interior surveillance functionality is online, to ConnectBus partner in Sweden.



VDL – 2022 model

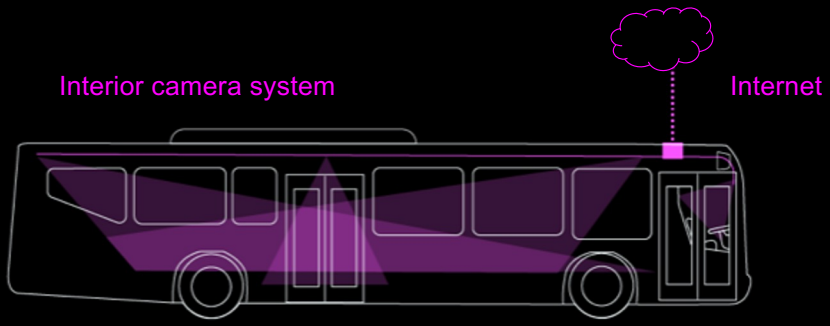
Exterior surveillance functionality is isolated.

The Lutvann scenario, with regards to images or video is **not possible with this bus.**



Yutong – 2025 model

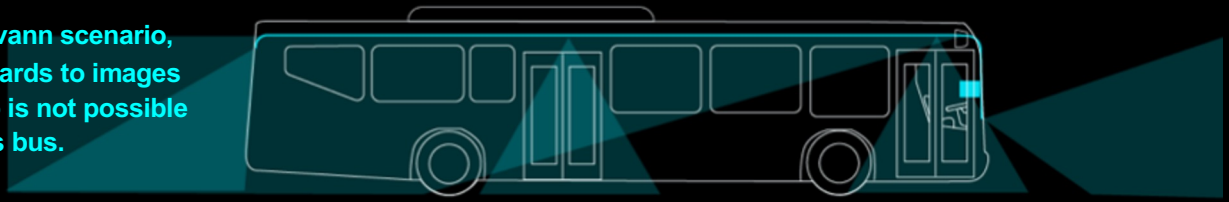
Interior surveillance functionality is online, to ConnectBus partner in Sweden.



Yutong – 2025 model

Exterior surveillance functionality is isolated.

The Lutvann scenario, with regards to images or video is not possible with this bus.

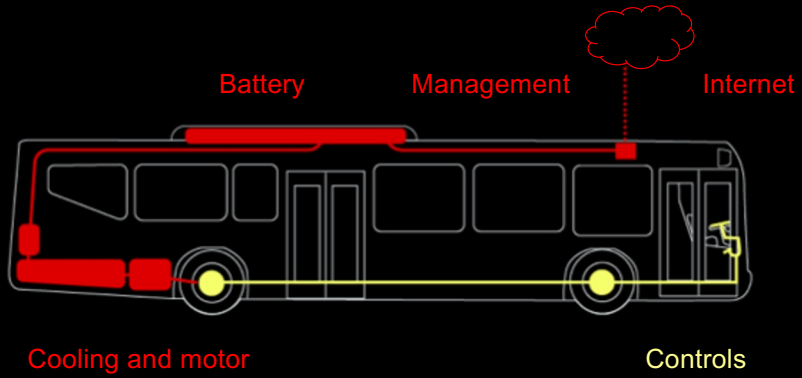


Yutong – 2025 model

Critical functionality is online, direct digital access for OTA updates and diagnostics.

- Manufacturer has the capability to remotely disable or destroy software, **the Kill Switch scenario is possible with this bus.**

+ current system design is still simple, low degree of system intergration



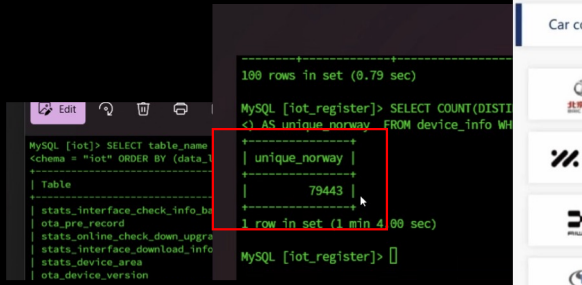
Yutong – 2025 model

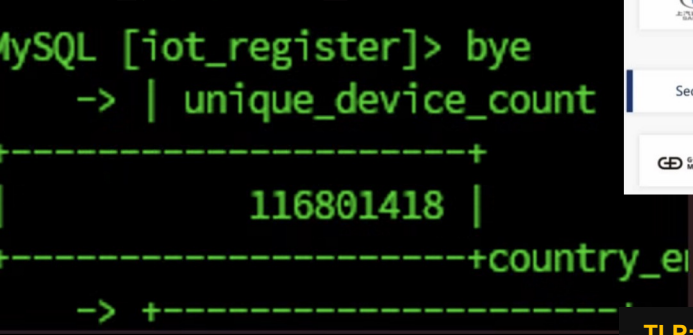
Critical functionality is online, direct digital access for OTA updates and diagnostics.

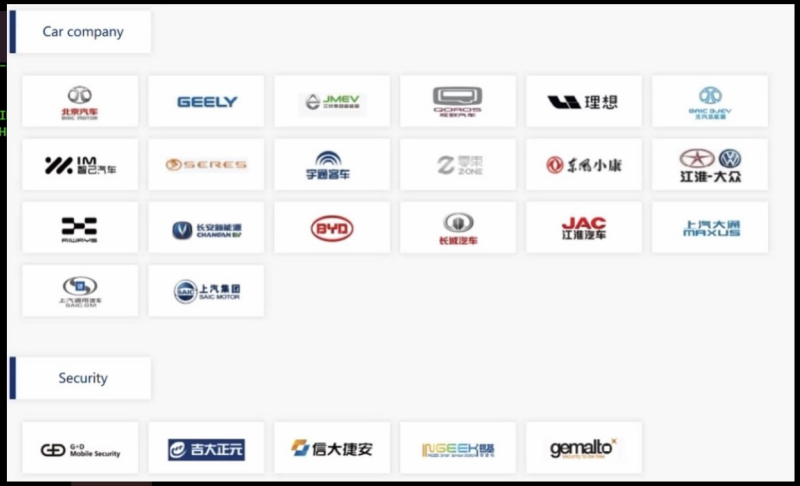
- Manufacturer has the capability to remotely change, disable or destroy software, **the Kill Switch scenario is possible with this bus.**

+ Current system design is still simple, low degree of system intergration

Hack #1: OTA update platforms are a weak link

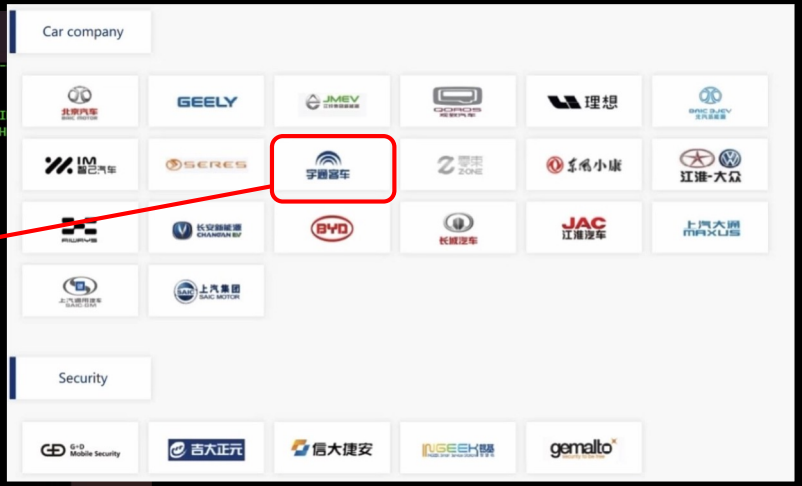






TLP:AMBER

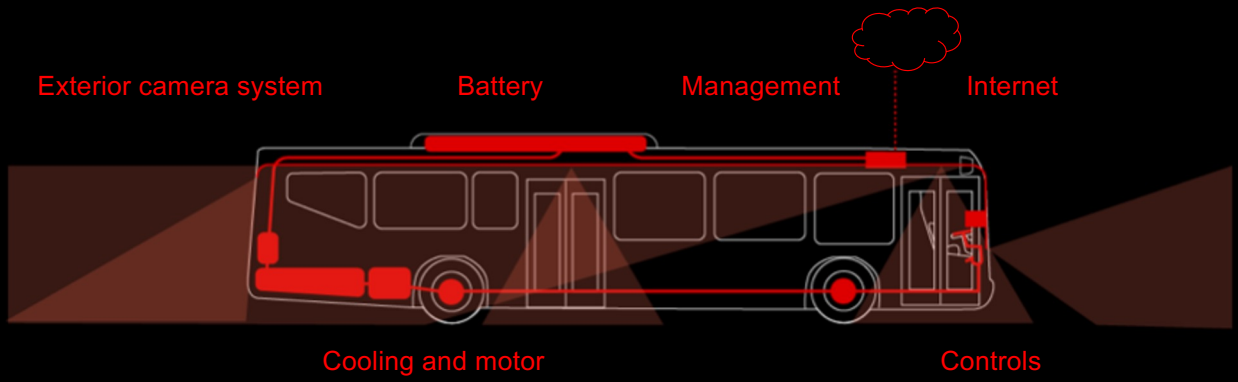
Hack #1: OTA update platforms are a weak link



Can the 2022 VDL be used for the Kill Switch scenario? **NO**
Can the 2022 VDL be used for the Lutvann scenario? **NO**

Can the 2025 Yutong be used for the Kill Switch scenario? **YES**
Can the 2025 Yutong be used for the Lutvann scenario? **NO**

The Future: An Autonomous Bus is a Drone



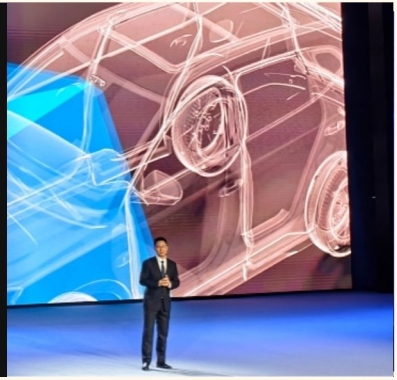
With increased levels of driver assistance and autonomy systems including cameras, will become more integrated and thus impossible to isolate.

More about the BYD's "God's Eye" driving assistance system

BYD officials revealed that the "God's Eye" ADAS system has three intelligent driving classifications. The entry-level system is called "God's Eye C". It relies on a three-camera cluster sitting behind the windshield. As the entry-level tier ADAS system, the "God's Eye C" will be adopted by cars under the BYD brand. This perception system will be powered by the DiPilot 100 system with a peak computing power of 100 TOPS.

BYD next gen:

12 cameras
3 front-view
5 panorama
4 surround view
5 mm wave radar
12 ultrasonic radar



Other hardware elements of the "God's Eye C" include 12 cameras, 5 mm-wave radars, and 12 ultrasonic radars. Those 12 cameras consist of 3 front-view cameras, 5 panoramic cameras, and 4 surround-view cameras. Five mm-wave radars provide 360-degree non-dead angle perception, the front radar has a detection distance of 300 meters. The accuracy of the 12 ultrasonic radar sensors is 1 cm [illegible] accuracy is 2 cm

TLP:CLEAR

DeepSeek Is Already Making Its Way Into Chinese EVs

Two Chinese automakers—including Geely—have announced support for China's AI disruptor.

Photo by: Voyah

Tor Indstøy – VP of Risk Management and Threat Intelligence at Telenor Group
tor.indstoy@telenor.com

Arild Tjomsland – Special Advisor TTO at the University of Southeast Norway
arild.tjomsland@usn.no

All technical details at Lion Cage on LinkedIn