Project Lion Cage:

Sikkerhetsdilemmaer ved programvare-styrte kjøretøy

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

Arild Tjomsland – Special Advisor TTO, University of Southeast Norway

The Lion Cage Project

Førerassistentsystemer

- Drive-by-wire, steer-by-wire
- Kameraer, radarer, sensorer
- Skytjenester for navigasjon og talestyring
- OTA-plattformer → typegodkjenning blir tillitsbasert

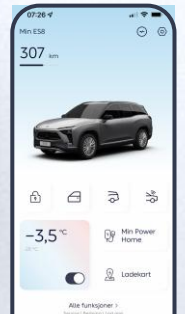
Utstrakt bruk av skytjenester (delt mellom produsenter) for:

- Navigasjon
- Prosessering av talestyring
- OTA-plattformer for programvareoppdateringer

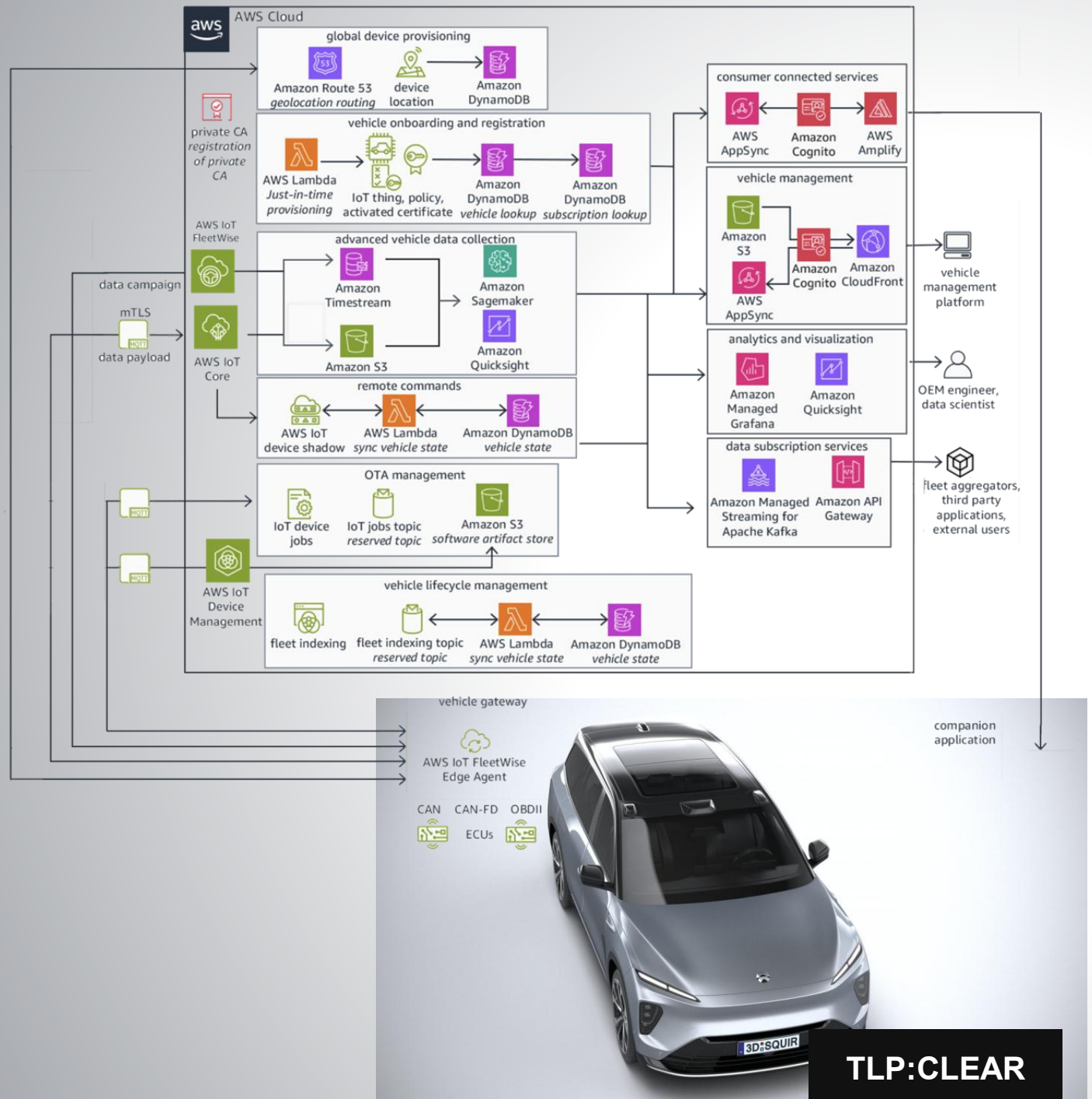
- Med OTA blir typegodkjenning tillitsbasert
- Cybersikkerhet for SDV-er er en prosess-sertifisering, uten testing av selve resultatet
- SDV-er er avhengige av produsenten for oppdateringer gjennom hele levetiden

Grensesnitt:

- Wi-Fi, mobilnett
- Bluetooth
- Ladeport
- Radio 315/433MHz
- Smartnøkkel/NFC,
- SOS-system
- GPS/GNSS
- CAN/OBD2
- Mobilapp
- Fysisk tilgang



TLP:CLEAR



Utfordringer:

- Sårbarhet for hacking
- Datainnsamling for samfunnsmodellering og AI
- Trafikksikkerhet og personlig sikkerhet
- Ansvarsproblemer – høy kompleksitet

- **Nasjonal sikkerhet**

TLP:CLEAR

SPIEGEL International

Volkswagen data breach raises important questions about how much information carmakers are collecting. Foto: [M] DER SPIEGEL; Fotos: Paul Langrock, Thomas Starck / AUTO BILD, picture alliance / dpa / Audi AG

We Know Where You Parked

Massive Data Breach at VW Raises Questions about Vehicle Privacy

Reuters World Business Markets Sustainability Legal More

Tesla workers shared sensitive images recorded by customer cars

By **Steve Stecklow, Waylon Cunningham** and **Hyunjoo Jin**

April 6, 2023 11:47 PM GMT+2 · Updated 2 years ago

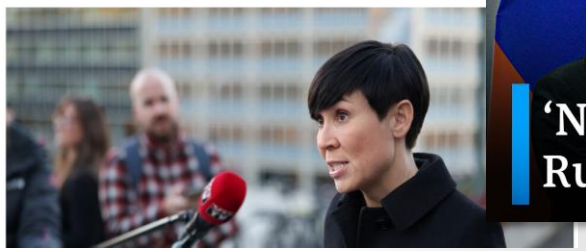
TLP:CLEAR

Reuters World Business Markets Sustainability More

Norway says cyber attack on parliament carried out from China

By **Nora Buli**

July 19, 2021 10:48 PM GMT+2 · Updated July 19, 2021



April 2025:

30 % av nye EV er kinesiske.

NIO ES8 for Oslo Taxi – 'et kjempekupp!'

NIO ES8 i bruk i selvkjørende pilot i Groruddalen, Oslo

Del 1

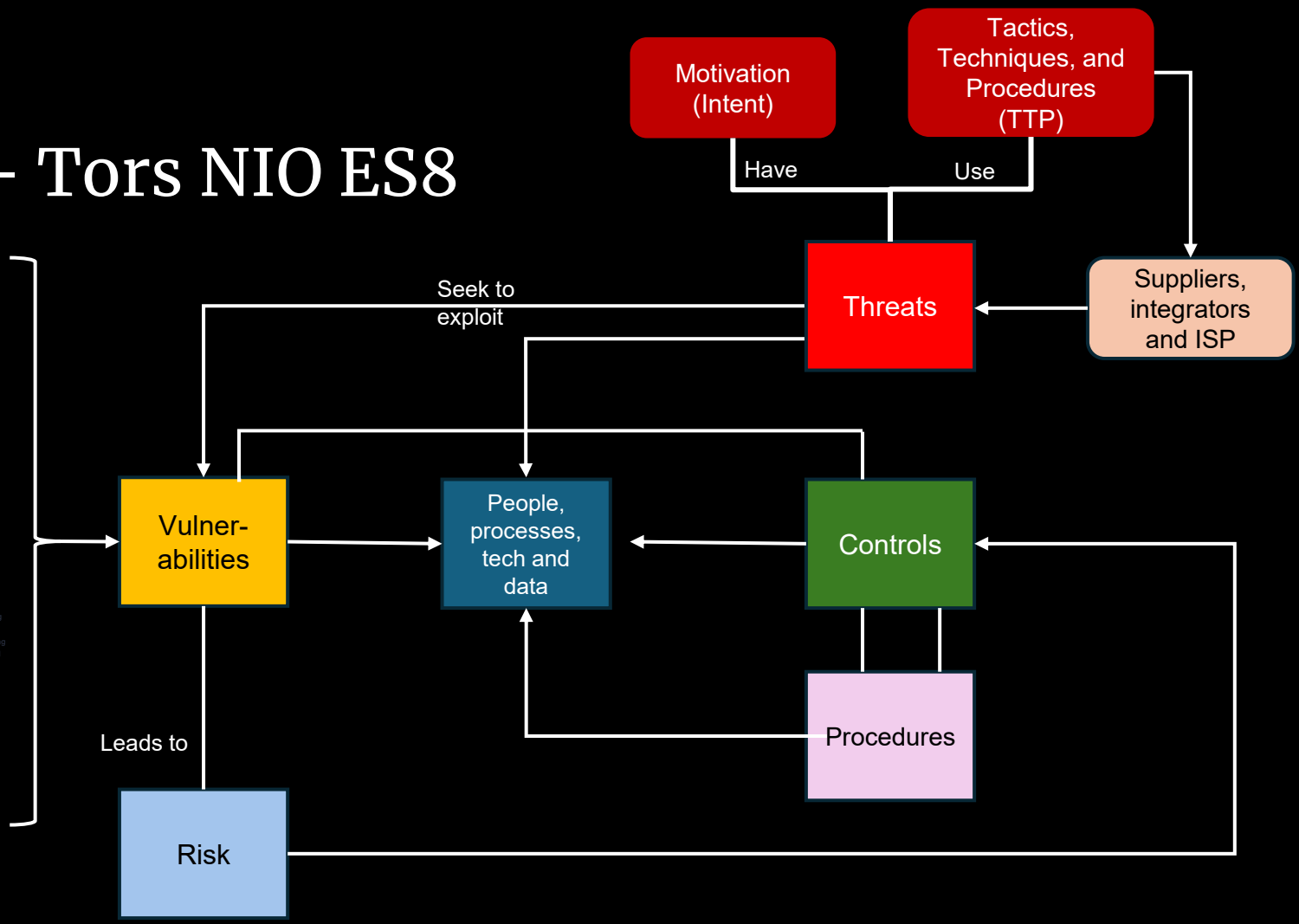
Teknisk sikkerhetsvurdering og risikoanalyse av Tor sin NIO ES8

TLP:CLEAR

Del 1

Risikoøkosystemet – Tors NIO ES8

- Spektrumanalyse
- Bluetooth-sniffing
- Avlytting/oppsnapning av sender i bilen
- GPS-analyse
- Pentesting
- OSINT, inkludert:Patentanalyse / gjennomgang av patenter
- Kinesiske forum og meldingsplattformer

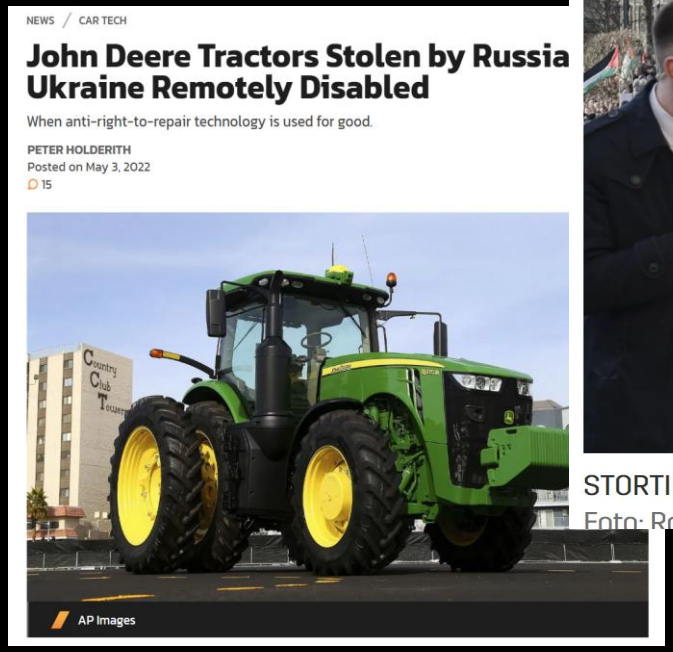


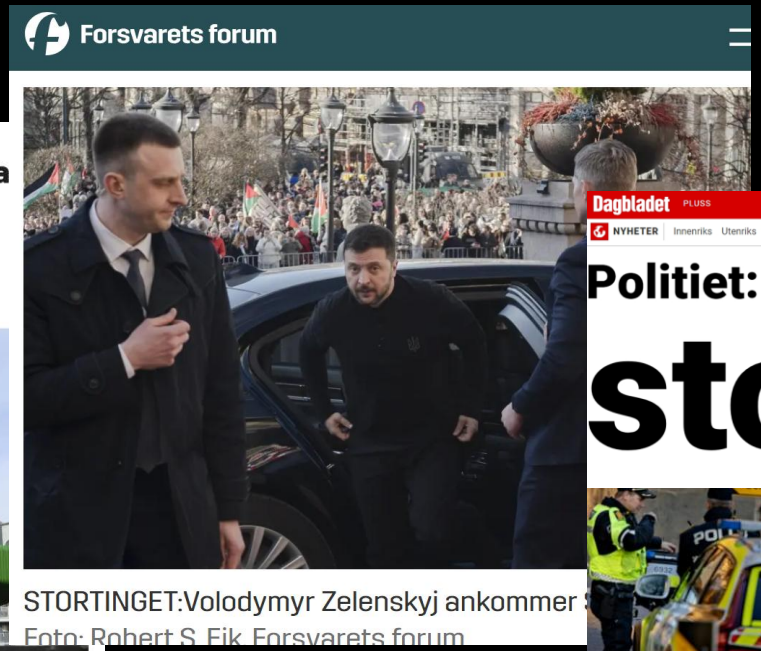
Inspirert av:
https://www.linkedin.com/pulse/risk-ecosystem-interaction-risks-threats-vulnerabilities-/

TLP:CLEAR

Scenariobasert tilnærming

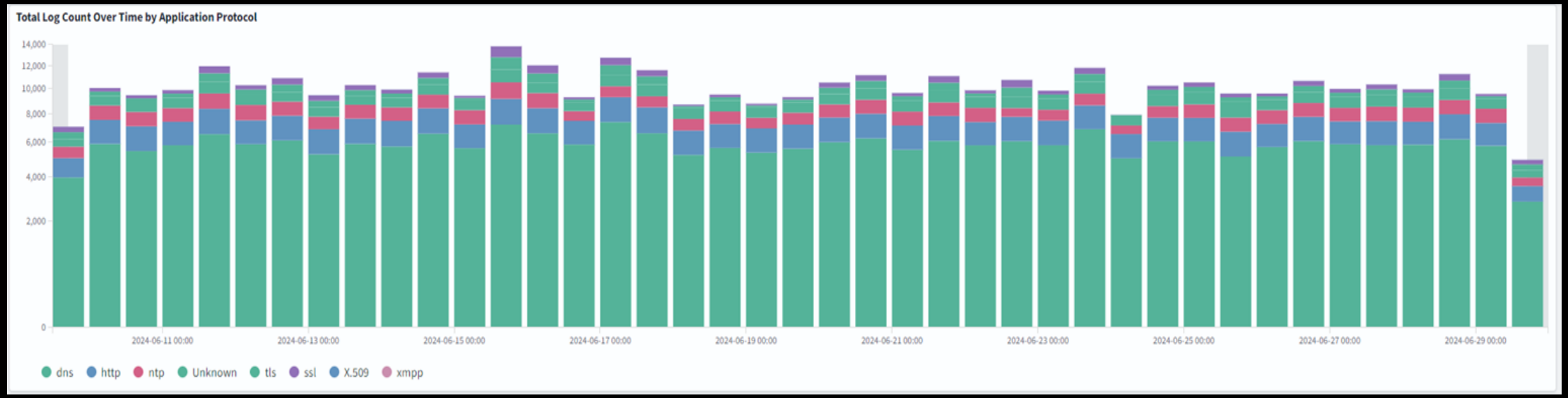
Scenario 1 – Trafikal sabotasje





Kan bilen til Tor brukes til trafikal sabotasje?

Funn: Bilen «skravler» kontinuerlig



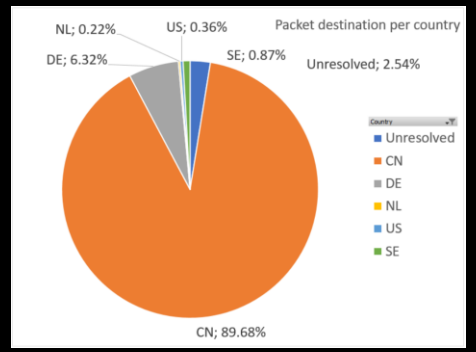
Datapakker går kontinuerlig inn og ut av bilen. Selv når bilen tilsynelatende er 'skrudd av'. Det er liten til ingen variasjon gjennom døgnet eller mellom geografiske områder.

70% av pakkene er kryptert, utstrakt bruk av ukjente protokoller

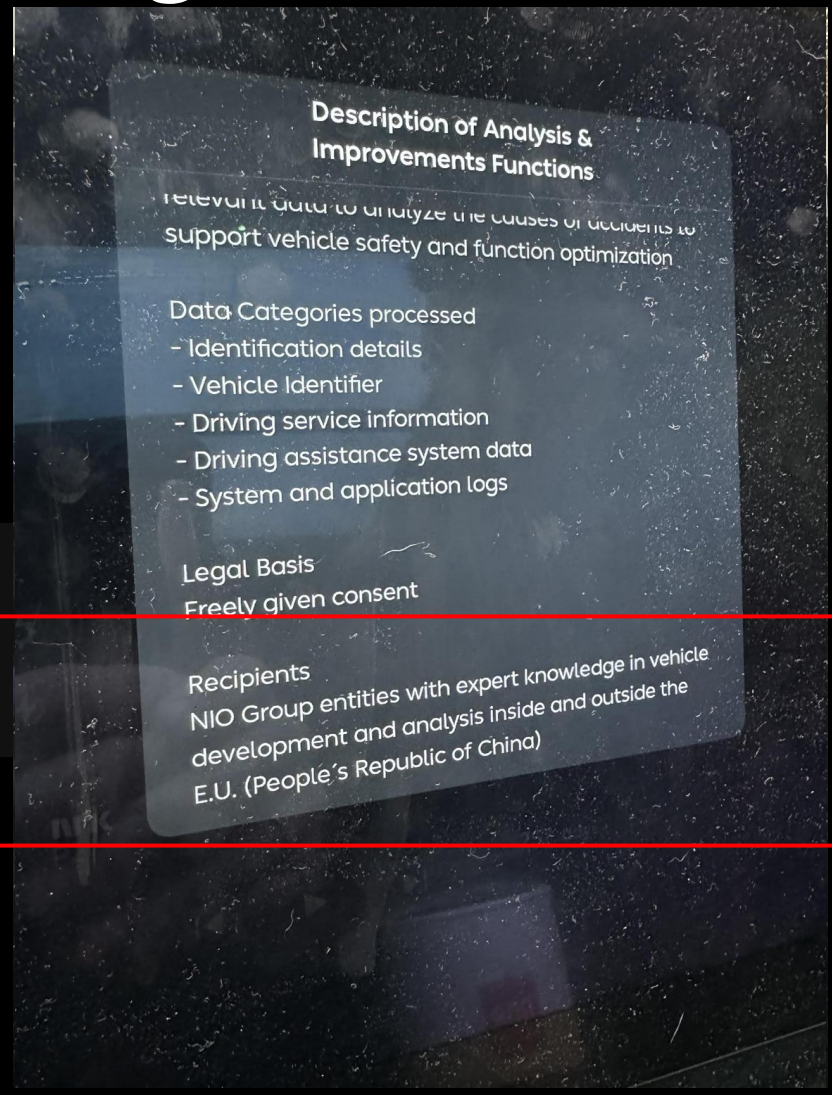
TLP:CLEAR

Funn: 90% av datapakkene går til og fra Kina

Eksempler på URL'er: 163.com China Network Communication Group (CNNIC), baidu.com, sina.com



Tor's datapakker sendes hit til Beijing…

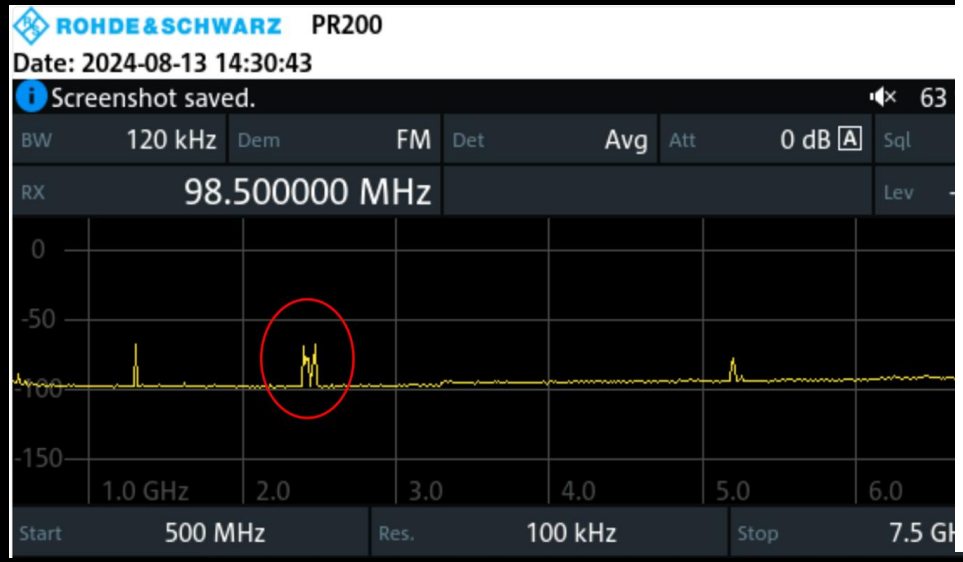


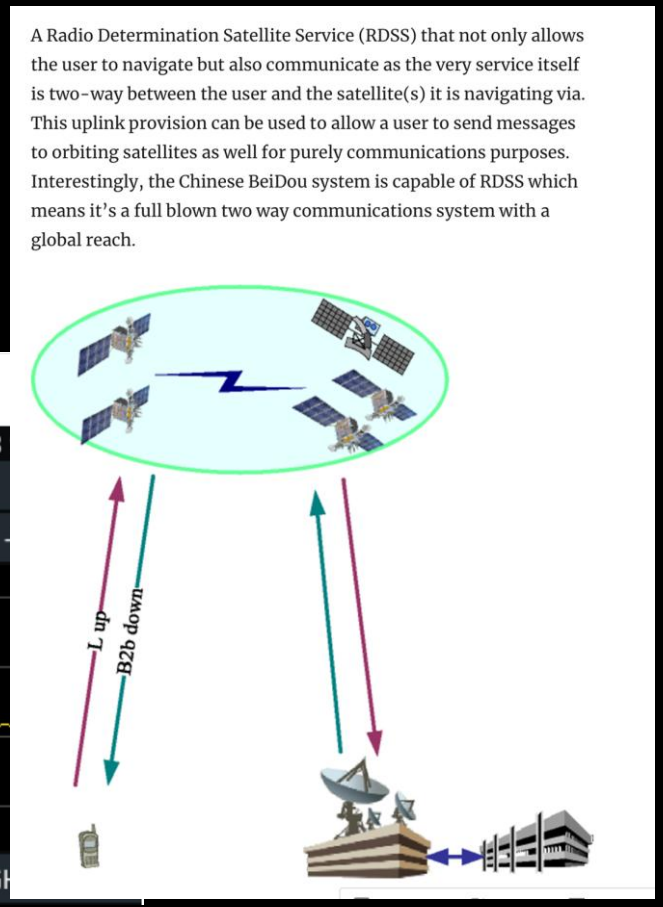
TLP:CLEAR

Funn: Spor etter to-veis kommunikasjon til den kinesiske GPS ekvivalenten

BeiDou (kinesiske GPS systemet) er to-veis.

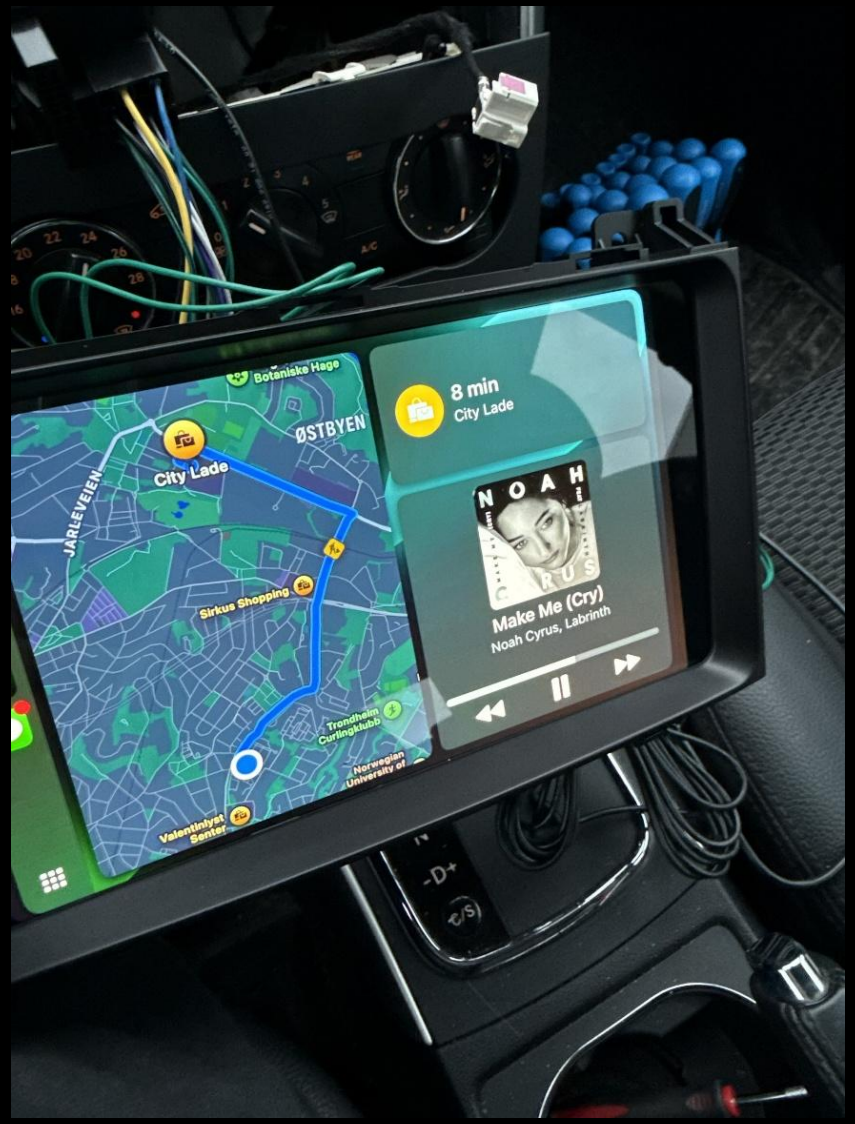
1575.42MHz, 1191.79MHz, 1268.52MHz og 2492.028MHz

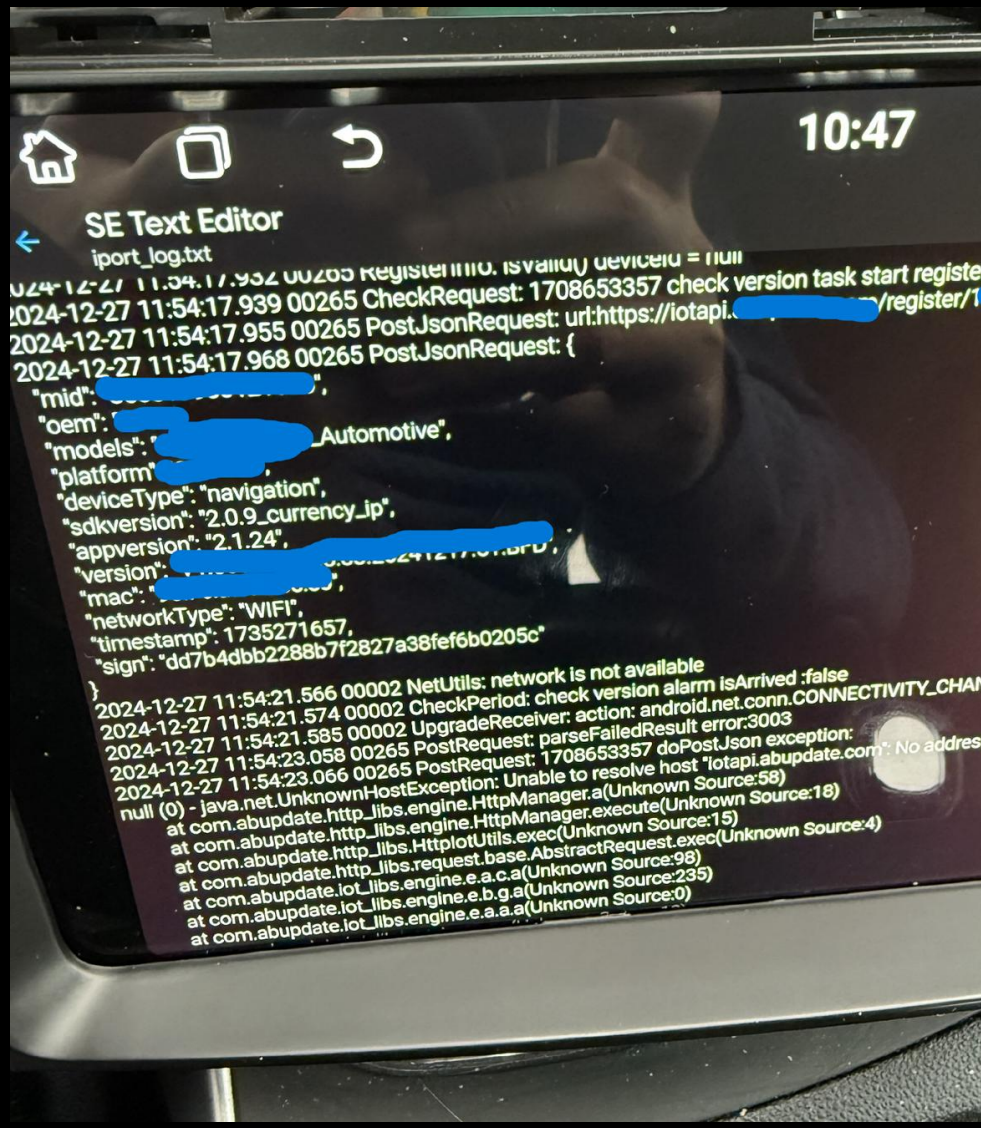




TLP:CLEAR

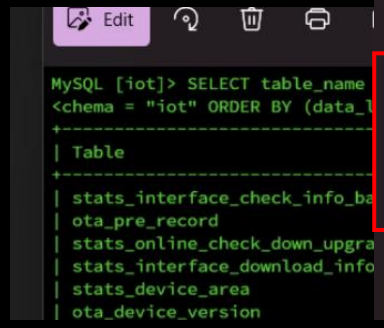
Hack #1: FOTA

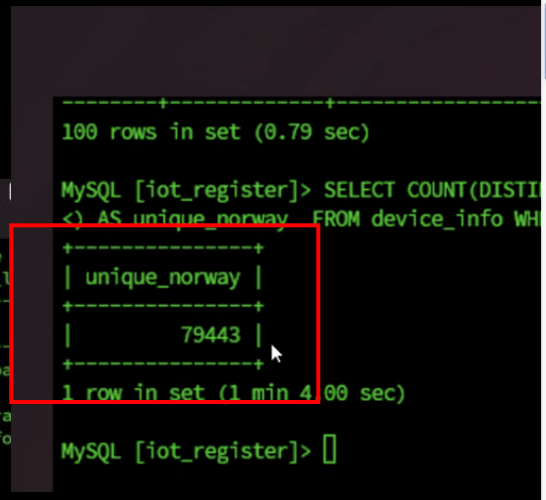


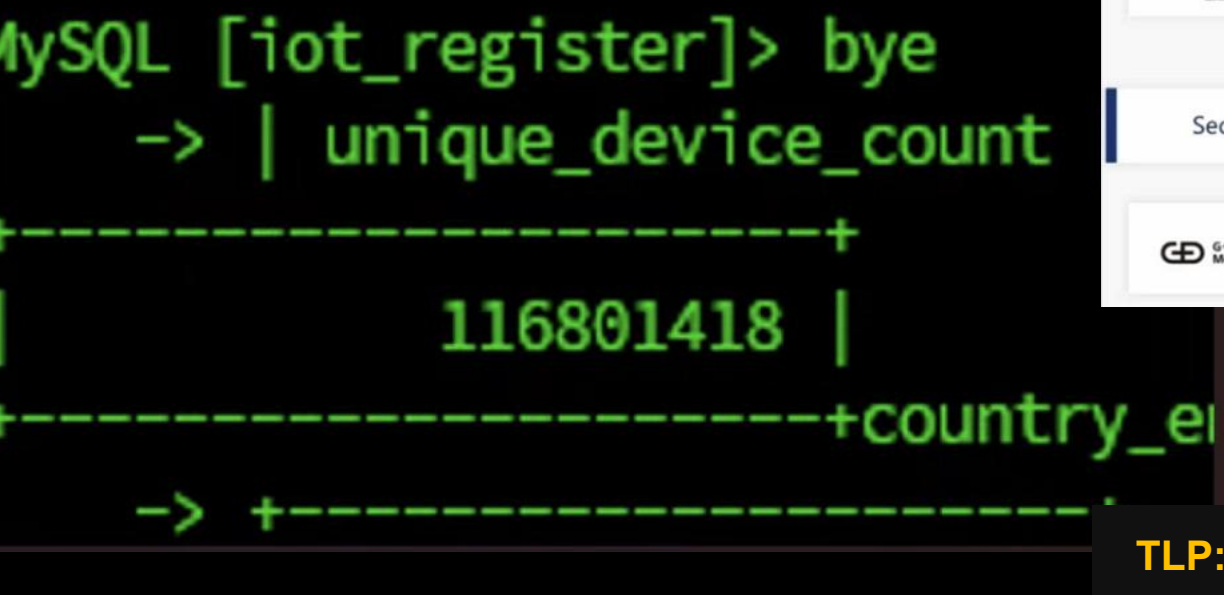


TLP:AMBER

Hack #1: FOTA oppdateringer er sårbare







TLP:AMBER

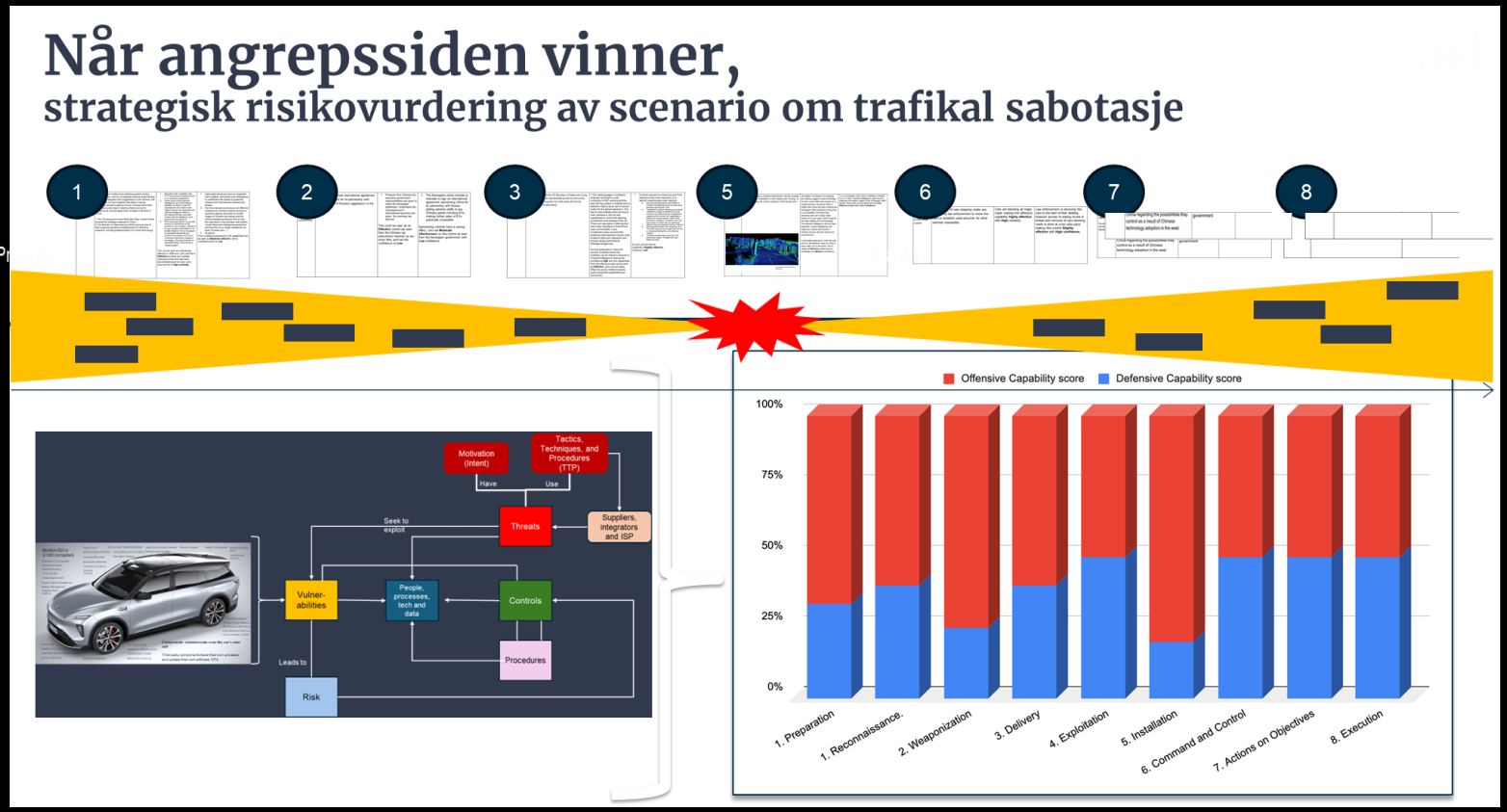
Konklusjon

Kan bilen brukes til sabotasje?

Ja.

Og av alle

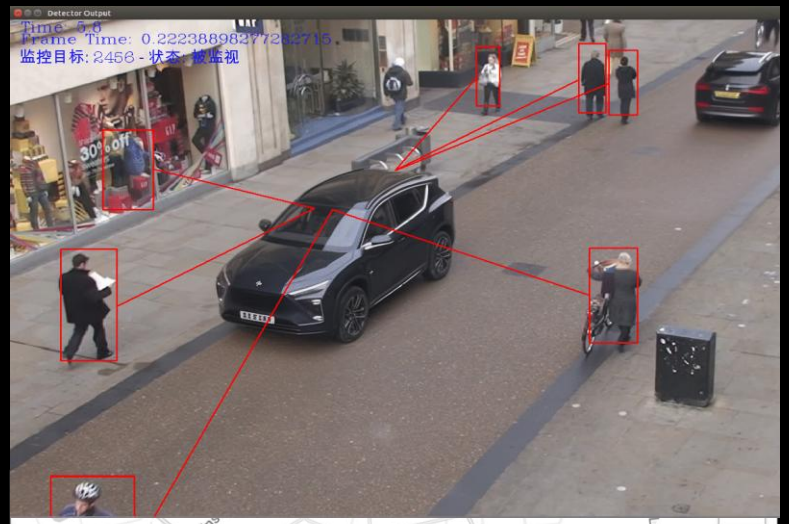
Sikkerhet er under normal standard.

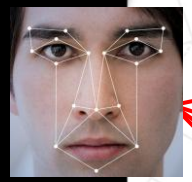


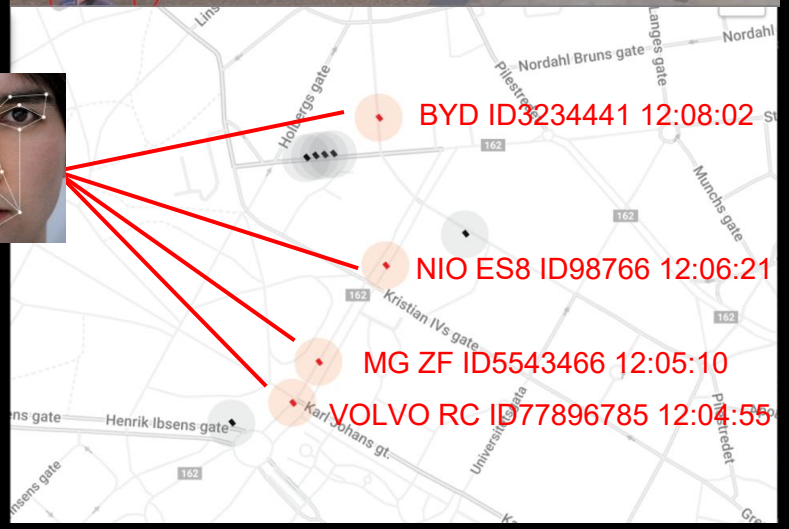
TLP:CLEAR

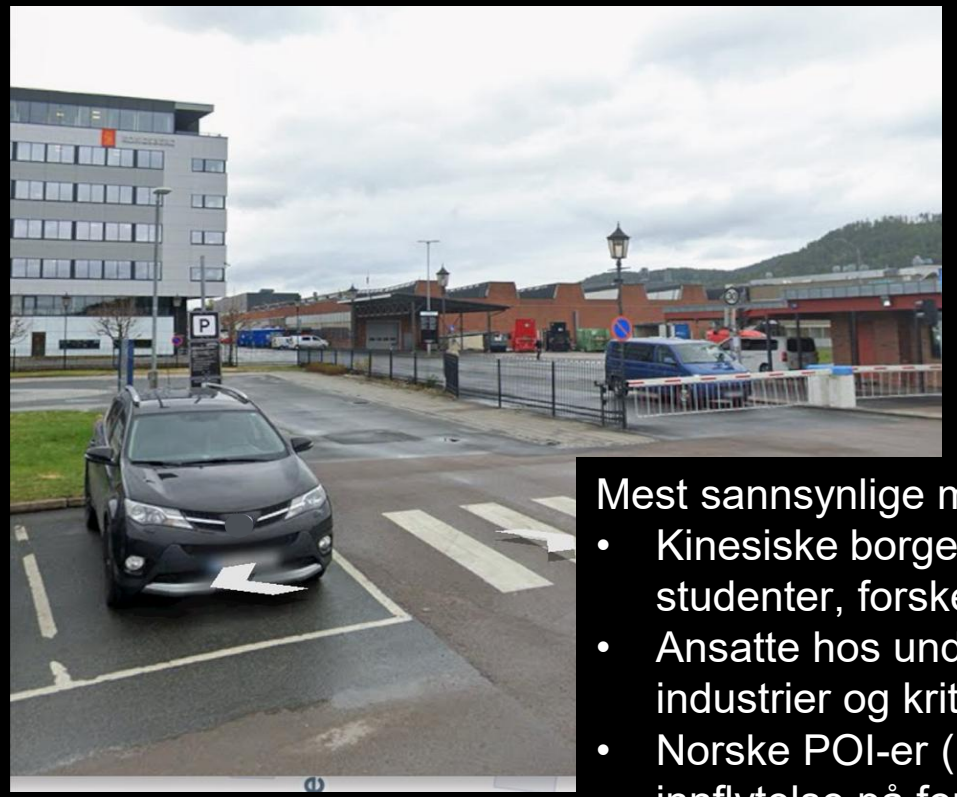
Scenariobasert tilnærming

Scenario 2 – Bil som del av **overvåking**









Mest sannsynlige mål:

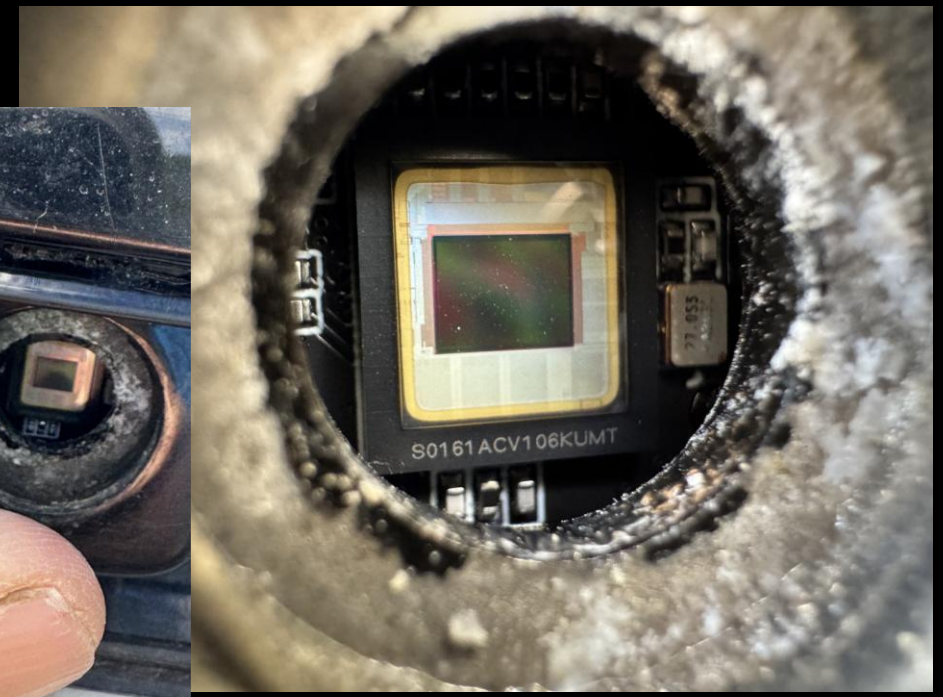
- Kinesiske borgere: dissidenter, studenter, forskere
- Ansatte hos underleverandører i kritiske industrier og kritisk infrastruktur
- Norske POI-er (persons of interest) med innflytelse på forholdet til Kina

Kan bilen til Tor fungere som én overvåkingsplattform i et større nettverk?

Kamera– ansikts- og skiltgjenkjenning

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

Del 2

Teknisk sikkerhetsvurdering (TSA) av Busser fra VDL og Yutong

- for Ruter

The Lion Cage Project

TLP:CLEAR

Del 2

Risikoøkosystemet for Yutong og VDL buss

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

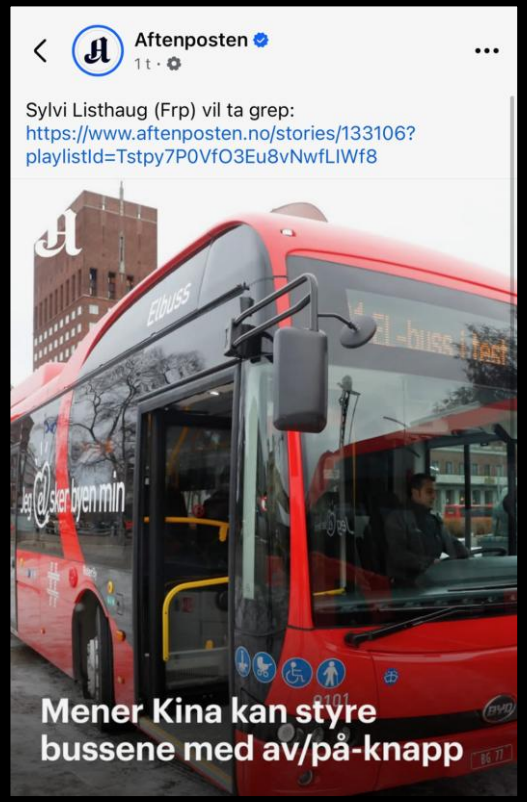
Risk

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

TLP:CLEAR

Alle busser elektriske innen 2030 – 80 % kinesiske.

- 660 kinesiske busser i Norge (2025)
- 1200 flere på vei



Scenario 1: Kill Switch

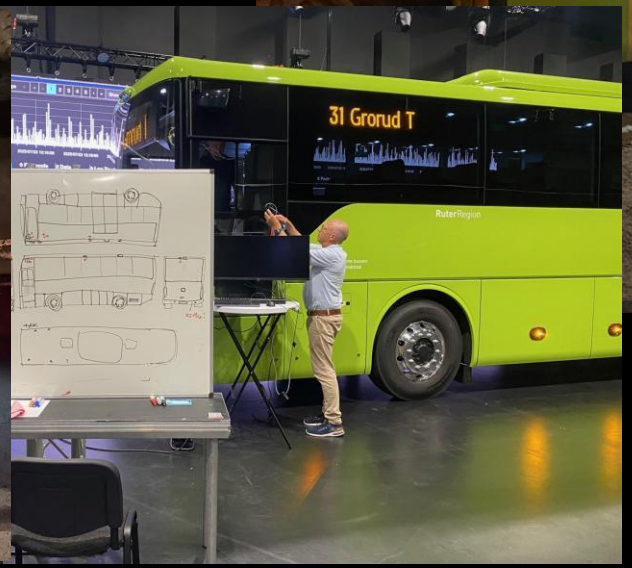
Trafikal sabotasje, eller trussel om sabotasje brukt som pressmiddel

Scenario 2: Lutvann

Rullende overvåking

TLP:CLEAR

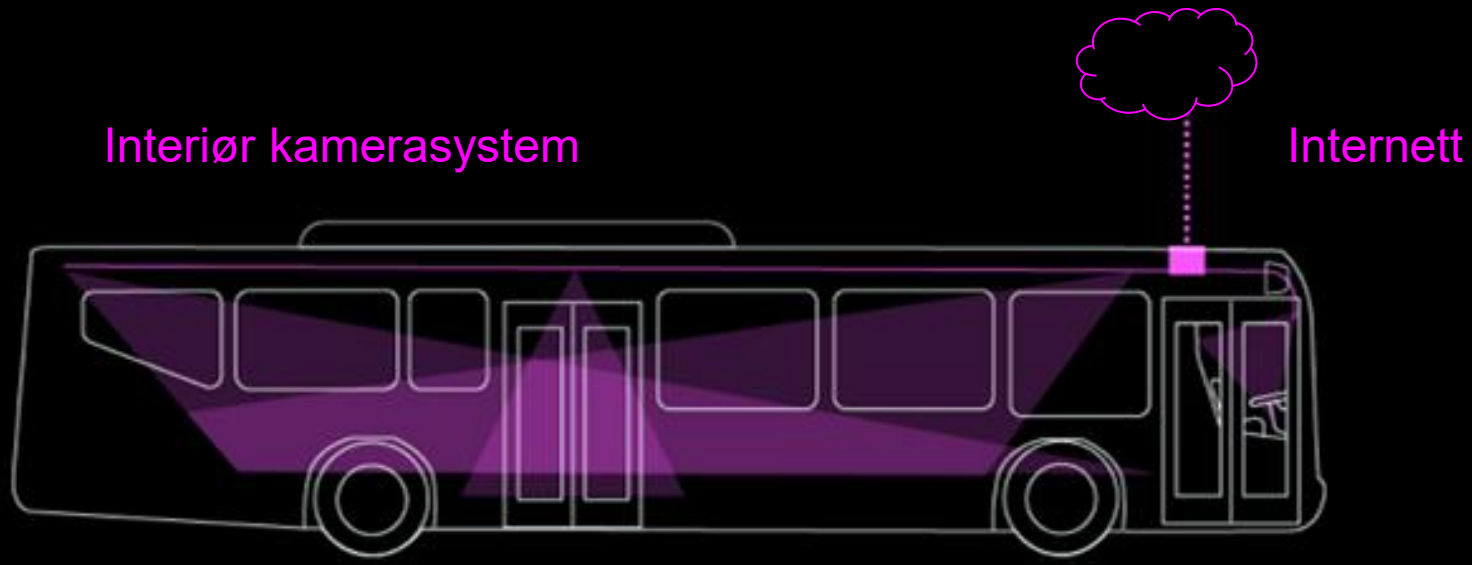
Yutong – 2025 model og VDL – 2022 model



Kan VDL og/eller Yutong bussen bli brukt til Kill Switch scenarioet, eller Lutvann scenarioet?

VDL – 2022 model og Yutong – 2025 model

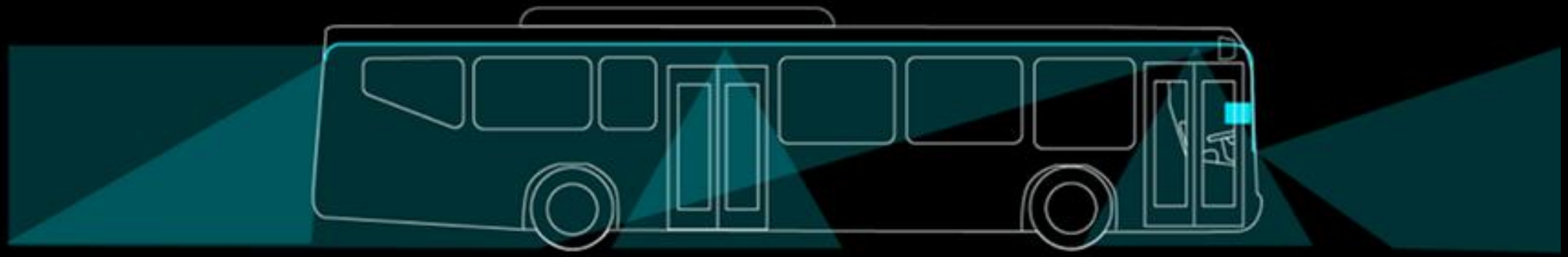
Interiørovervåkings funksjonaliteten er online, til ConnectBus-partner i Sverige.



TLP:CLEAR

VDL – 2022 model og Yutong – 2025 model

Eksteriør kamerasystem



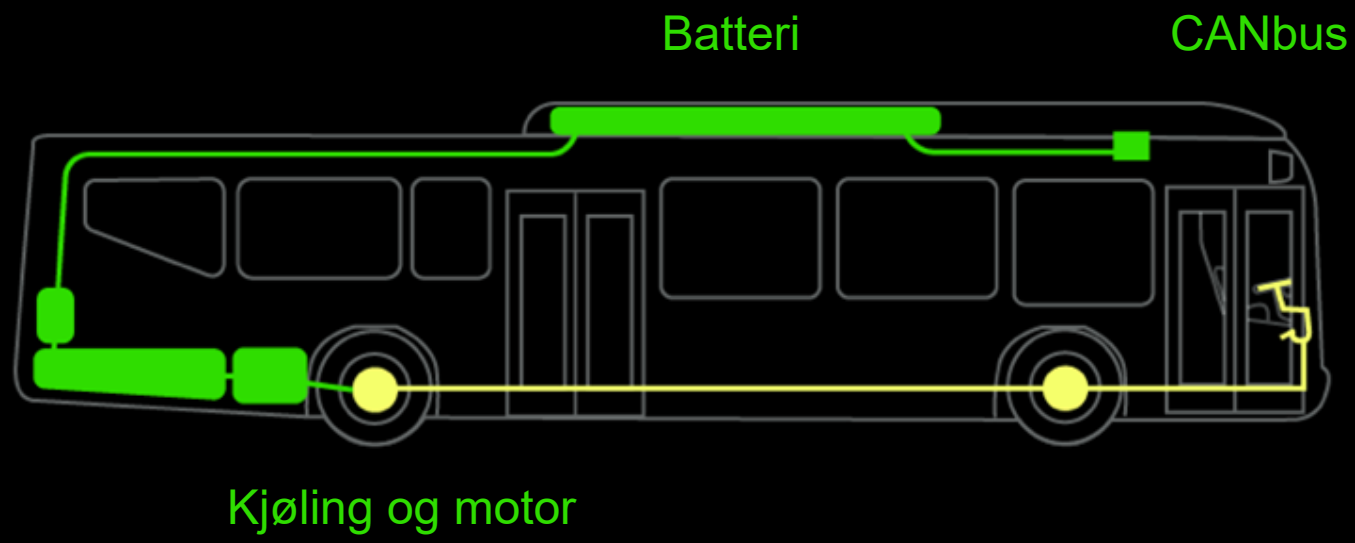
Eksteriørovervåkings-funksjonaliteten er isolert. Lutvann-scenarioet, når det gjelder bilder eller video, er **ikke mulig med denne bussen.**

VDL – 2022 model

Kritisk funksjonalitet isolert

Kill Switch ikke mulig

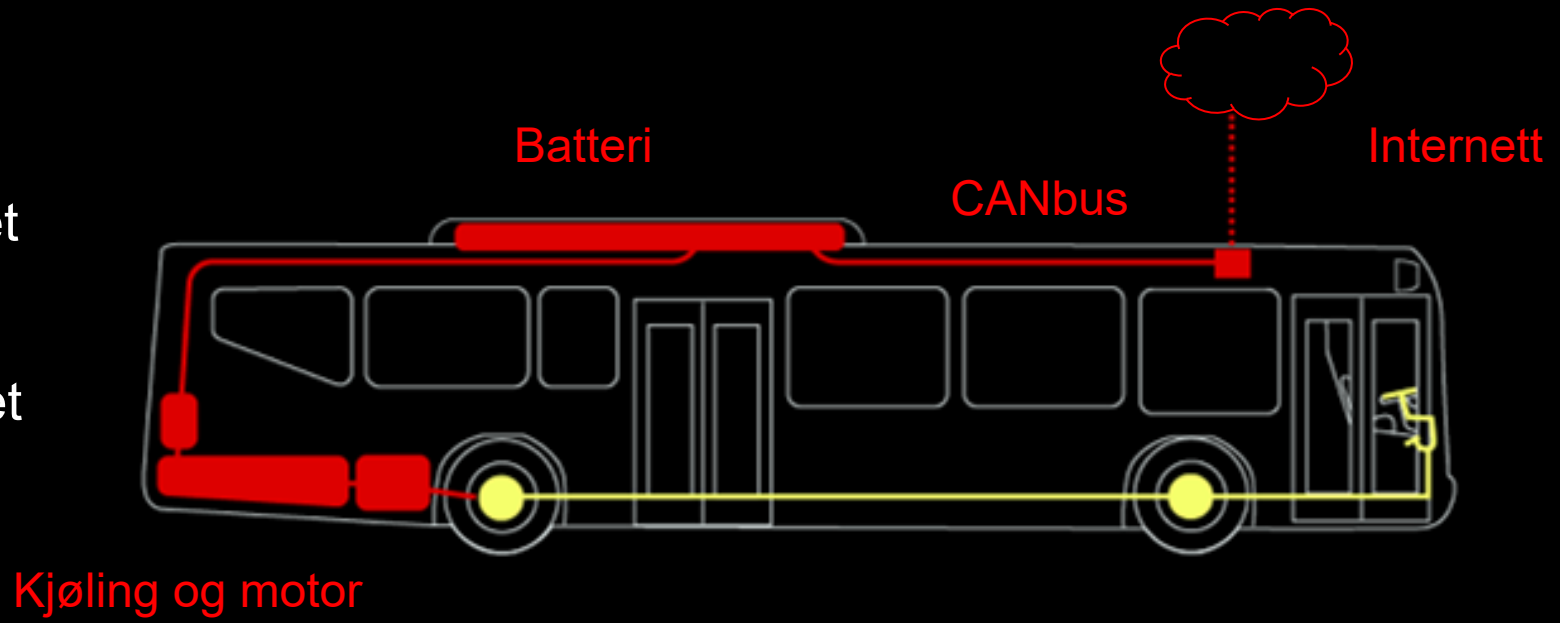
Eksteriørkamera isolert – ingen Lutvann



Yutong – 2025 model

Kritisk funksjonalitet er online

Kill Switch scenariet er mulig



\+ design er relativt enkelt, lite systemintegrasjoner

Yutong – 2025 model

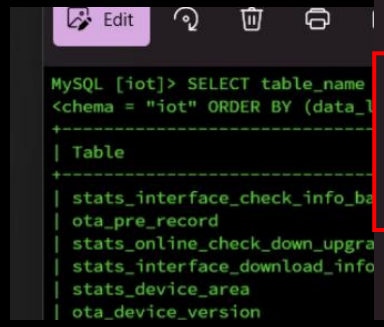
Kritisk funksjonalitet er online.

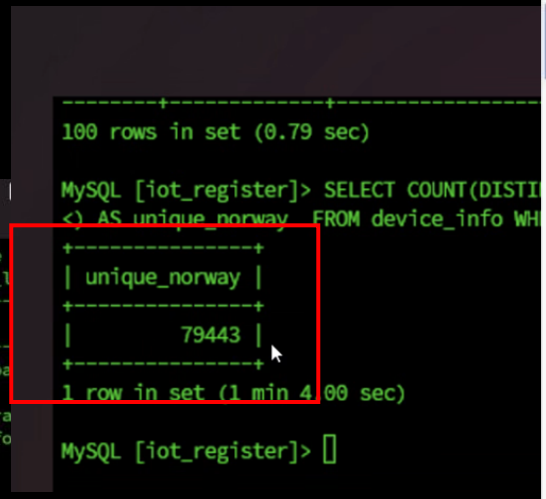
Eksteriørkamera er isolert Produsenten har tilgang til interne systemer. – **Kill Switch-scenarioet er derfor mulig med denne bussen**.

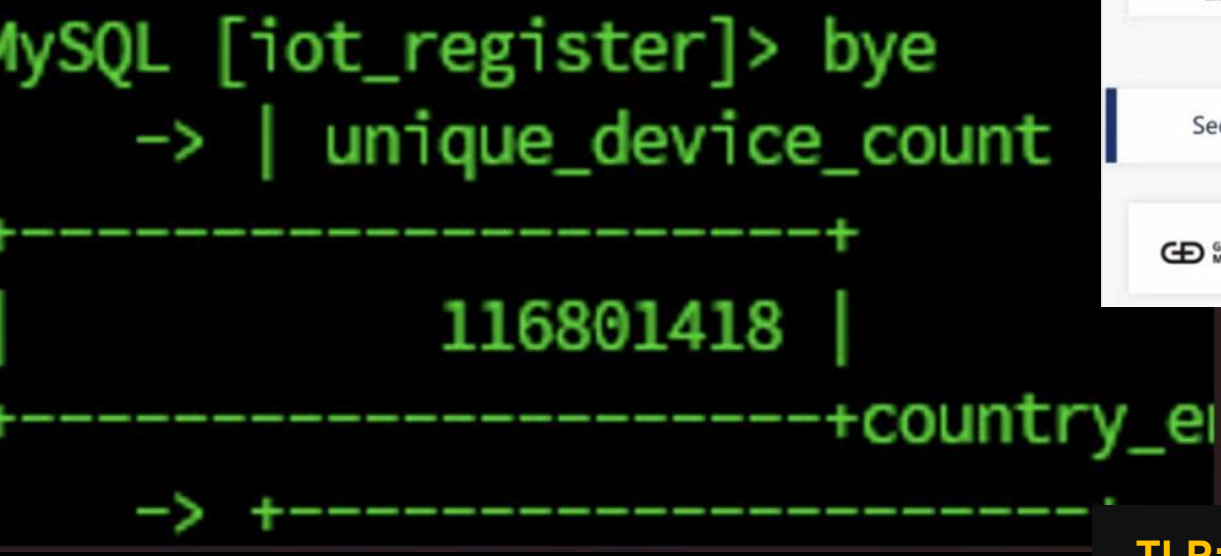
Eksisterende systemdesign er fortsatt enkelt, med lav grad av systemintegrasjon.

TLP:CLEAR

Hack #1: FOTA oppdateringer er sårbare







TLP:AMBER

Hack #1: FOTA oppdateringer er sårbare

Car company

GEELY

JMEV

理想

SERES

BYD

JAC

Security

gemalto

TLP:AMBER

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

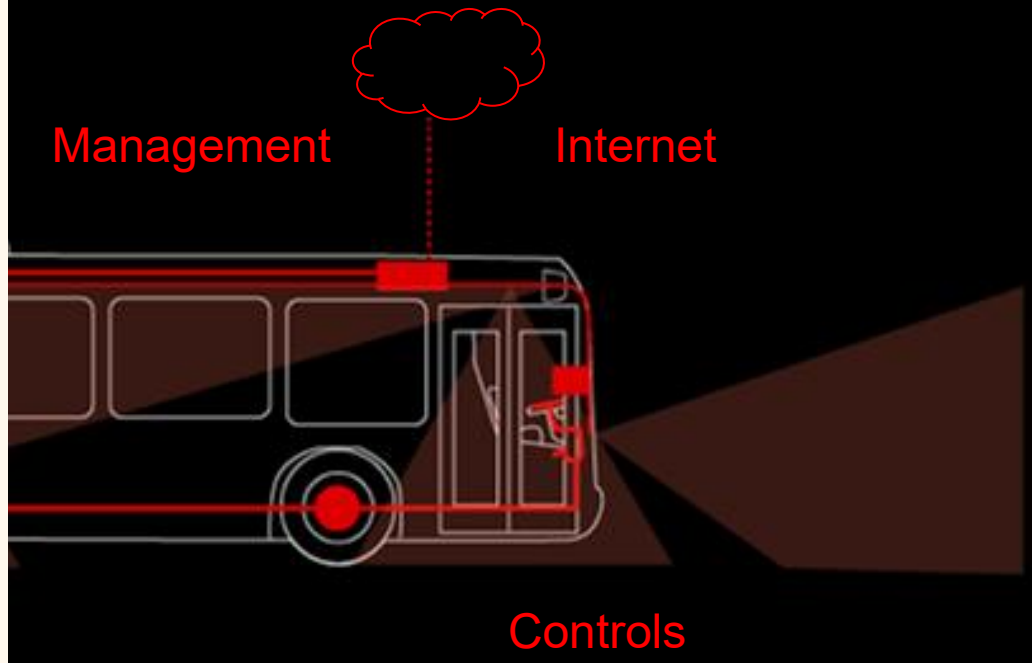
BYD officials revealed that the "God's Eye" ADAS system has three intelligent driving classifications. The entry-level system is called "God's Eye C". It relies on a three-camera cluster sitting behind the windshield. As the entry-level tier ADAS system, the "God's Eye C" will be adopted by cars under 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, and the parking accuracy is 2 cm

usser = droner



ystemer, inkludert
ør legges i smarte

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