AI-based cybersecurity for CAN and IP communication in existing vehicle environment

Can your vehicle withstand a Cyberattack?

Sensors

Navigation

Communication

Engine control

Video cameras

broon.

BAE SYSTEMS

clavister®

CONNECT . PROTECT

or

broon.

BAE SYSTEMS

clavister®

CONNECT . PROTECT

or

clavister®

CONNECT . PROTECT

Project Purpose

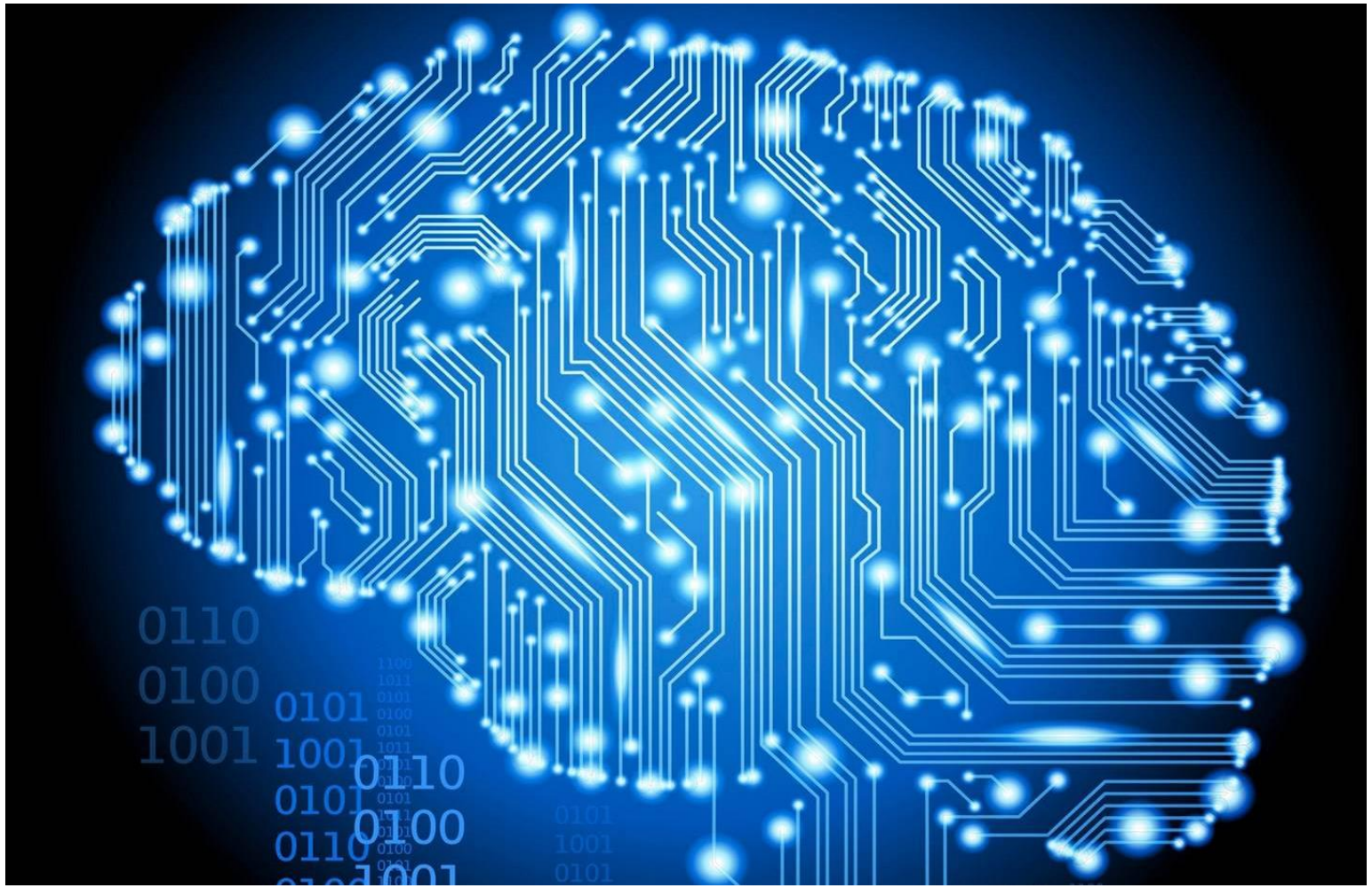
Validate a concept to show that it is possible to equip connected vehicles with efficient systems for detection of cyberattacks, using modern scientific and data driven techniques.

Project Goal

Demonstrate the feasibility of using suggested ways of developing a security system which can analyze CAN bus communication in complex systems, where also other communication protocols such as IP are used, both for vehicle and nonvehicle applications.

Artificial Intelligence

- Realtime analysis of IP and CAN bus data
- Anomaly detection
- Innovative and extremely efficient algorithm
- Ideal for in-vehicle deployment



Exhibition demo / IP - AI Exhibition
Departure Score
Score
Output from AI component
Attack Indicator
Normal
Network Activity
PPS
Total IP frames on network
SSH Connection Activity
PPS
Frames generated from attack
Attack
SSH Connection
Execute

Vehicles and Industry 4.0

- CAN bus very common
- 775 million cars connected by 2023
- 70% of all new trucks can be connected
- EU regulation for Cybersecurity
- Industry 4.0

Contact persons

Jennie Roos

Bron Innovation

jennie.roos@broninnovation.se

Stefan Brodin

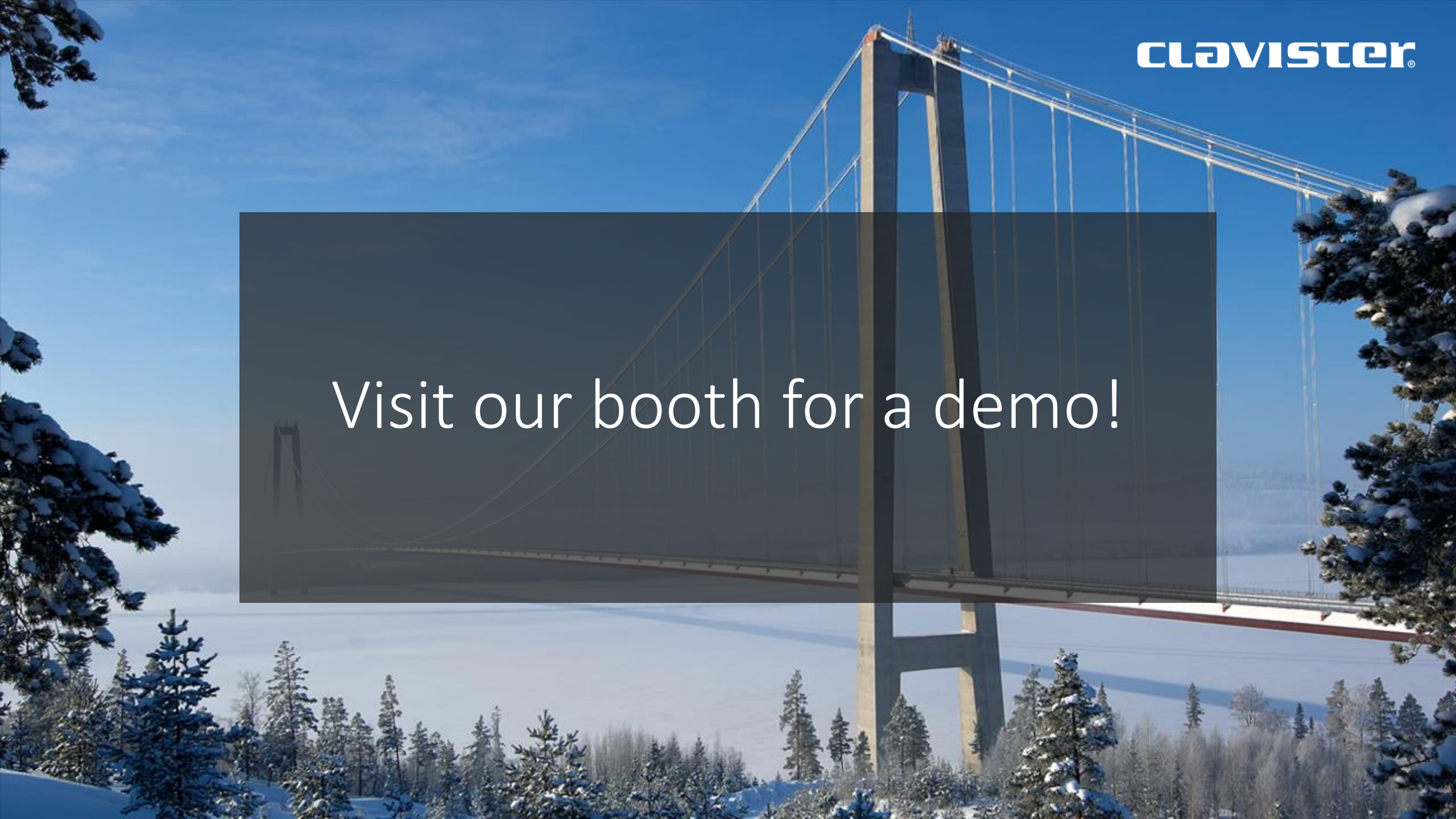
Clavister

stefan.brodin@clavister.com

Måns Eriksson

BAE Systems Hägglunds

mans.eriksson@baesystems.com


Visit our booth for a demo!

Thank you!