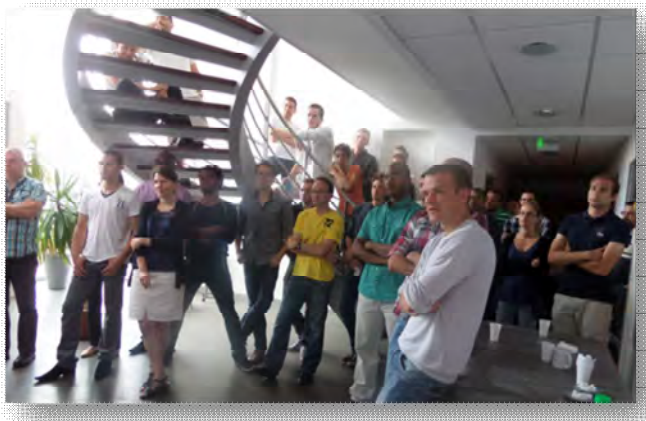
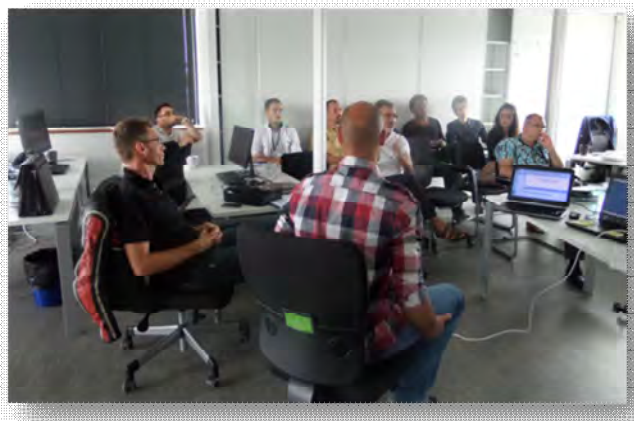
Cyber security in the field

Our job activity

Test Engineering and Software Quality Laboratory





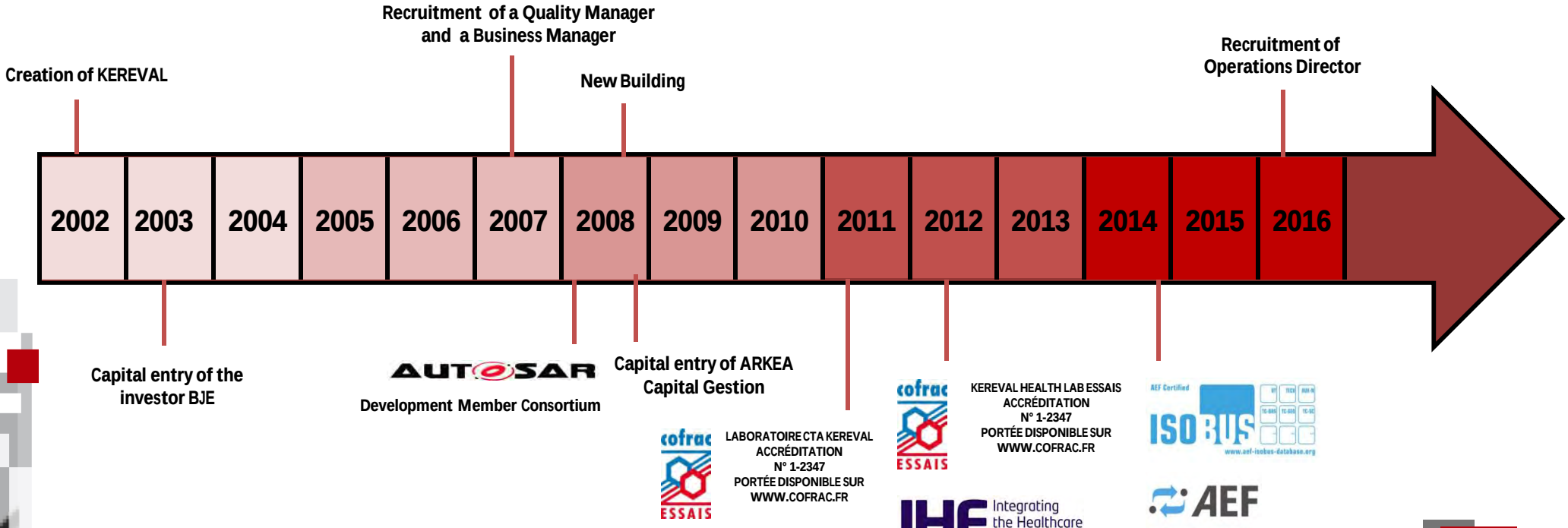
Our values

Independence

Impartiality

Excellency

Our history: 15 years of experience, A unique job



Our accreditations

LABORATOIRE CTA
KEREVAL
ACCRÉDITATION
N° 1-2347
PORTÉE DISPONIBLE SUR
WWW.COFRAC.FR

PASSI Accreditation in progress

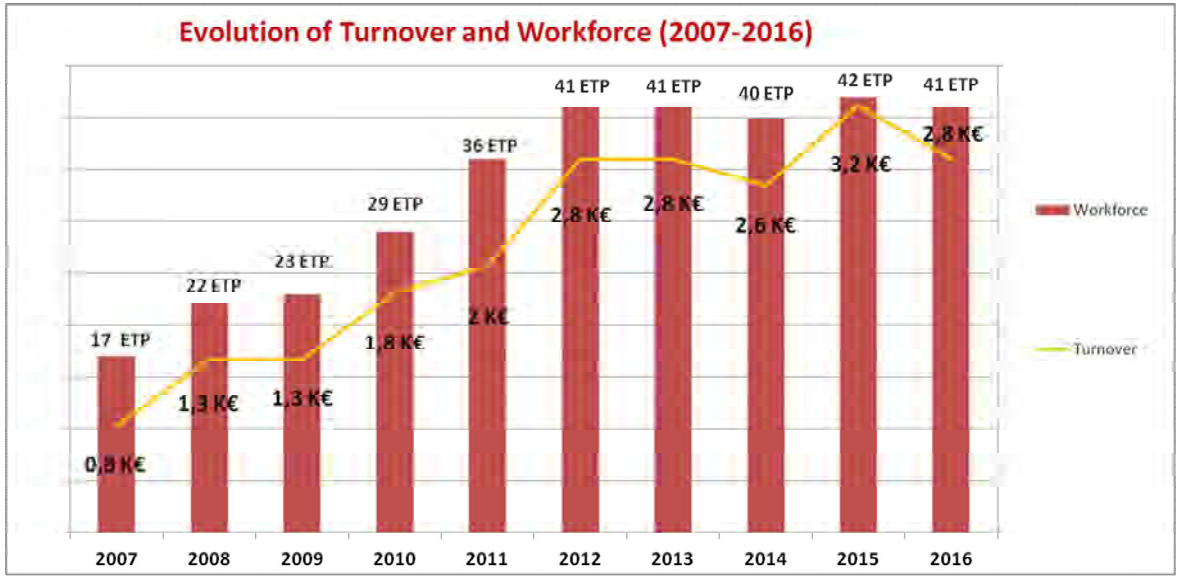
Our Expertise

Our key figures

2,8 millions Turnover

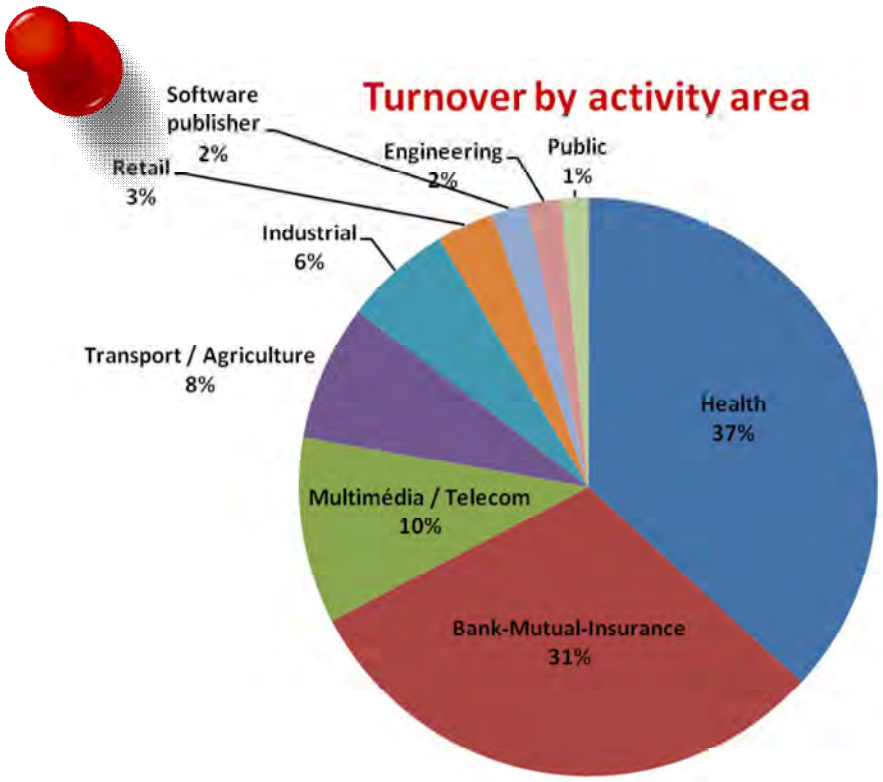
42 employees

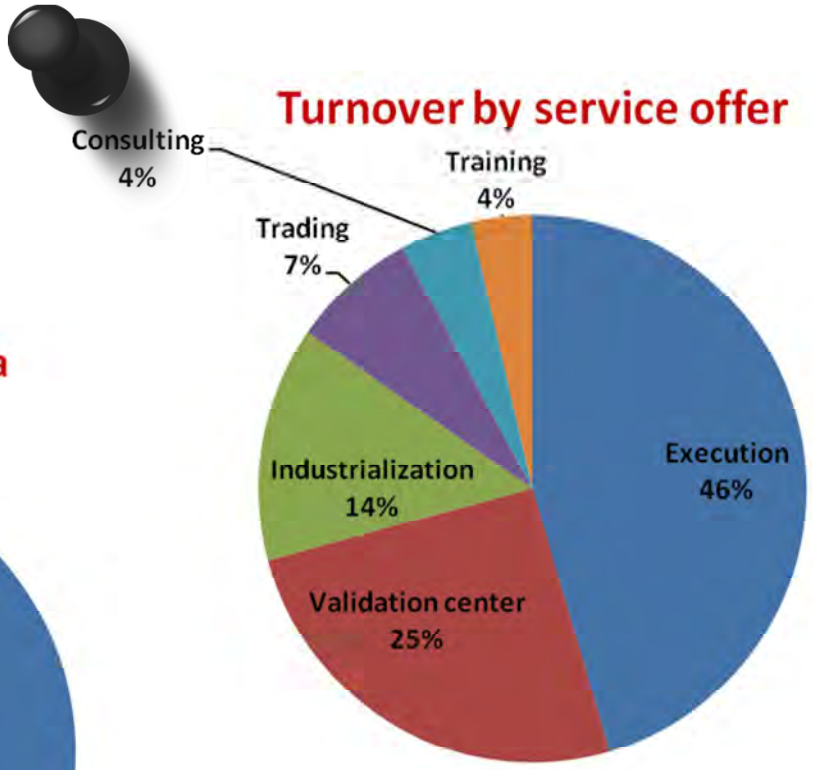
160 customers



Service offer and activity area

15% of turnover devoted to R & D





Among our clients

BANK / INSURANCE / PREVOYANCE / HEALTH

Harmonie mutuelle
SOCIETE GENERALE
MUTEX
Crédit Mutuel ARKEA

INDUSTRIAL

THALES
Sofrel LACROIX
dalkia GROUPE EDF
DCNS

RETAIL

YVES ROCHER
Mr.Bricolage
GROUPE BEAUMANOIR
les Mousquetaires

HEALTH

IHE Integrating the Healthcare Enterprise
BIOMÉRIEUX
asipsanté AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ
sesam-vitale

MULTIMEDIA-TELECOM

orange Business Services
EUROSPORT
ouest france
PagesJaunes

PUBLIC

CNED
MINISTÈRE DE L'ÉDUCATION NATIONALE, DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE
MGDIS
DGA

AGRICULTURAL

SULKY
AGRO TRONIX
CLAAS
AGCO Your Agriculture Company

COLLECTIVITY

Nantes Métropole COMMUNAUTÉ URBAINE
semitan
Région BRETAGNE

TRANSPORT

PSA GROUPE
SNCF
avancial
Valeo

SERVICE

ORSYS formation
BUREAU VERITAS

Focus on Cybersecurity

Our activity :

- ✓ Audit of architecture and configuration of systems
- ✓ Risk analysis
- ✓ Intrusion testing
- ✓ Consulting and Training
- ✓ R&D in the field of intrusion detection

ANSSI | Agence nationale de la sécurité des systèmes d'information

PASSI Accreditation
in progress

Our expertise fields :

Health

Transport

Défence / Air traffic control

Among our customers

Atos · Bodet · DGA · Sofrel LACROIX · Mutualité Française · MUTEX

Focus on Communication Bus

Our activity :

- ✓ Certification
- ✓ Trainings
- ✓ Technical Support

AEF Certified ISOBUS www.aef-isobus-database.org

AEF AGRICULTURAL INDUSTRY ELECTRONICS FOUNDATION

Our expertise fields :

Automotive

Agricultural

Among our customers :

Valeo BERTHOUD CLAAS HARDI EVRARD JOHN DEERE SULKY

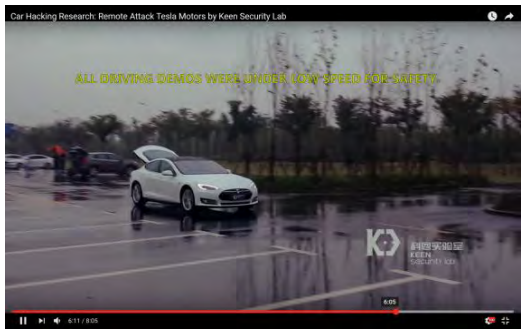
Example of cyber Attack

Jeep Cherokee (2015)

- Increase the volume of the radio

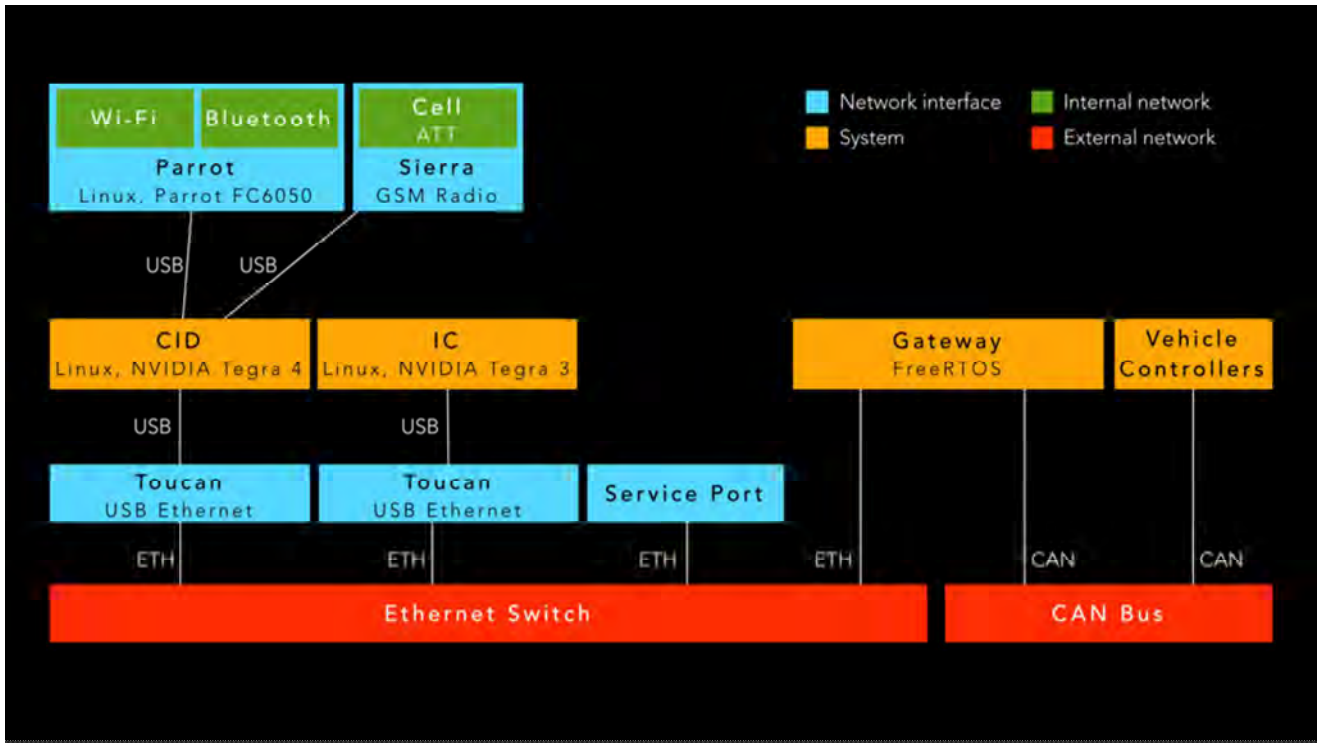
- Start the horn

Tesla Model S (2016)



Tesla Model S

- The hacking was done by the infotainment system connected to internet by a sim's card or by user's phone

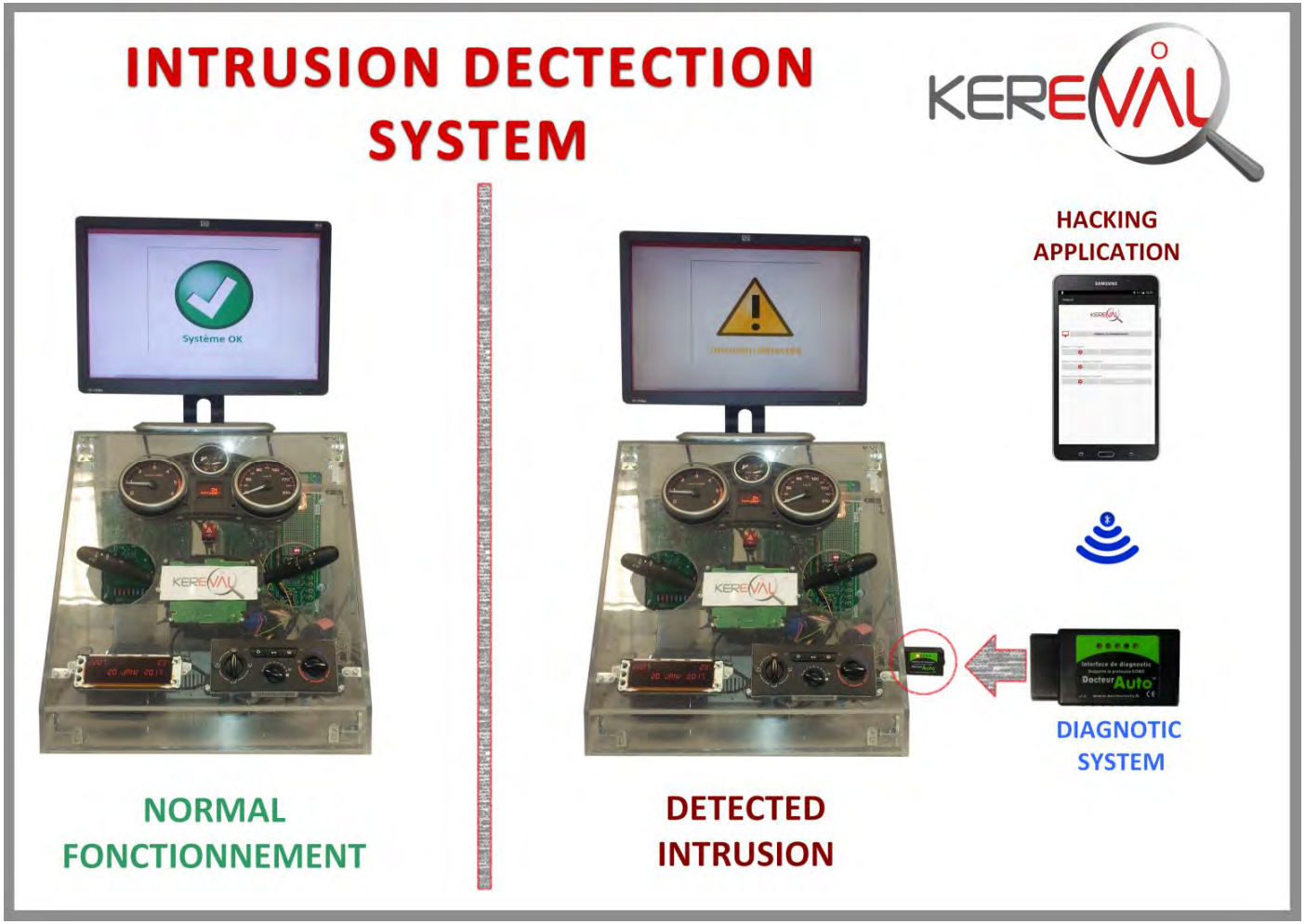


Tesla Model S

- Why the Tesla Model S has been hacked?
  - Weak passwords stored in the system
  - Accounts with weak passwords and with high privileges
    - Access to administration functionalities
  - Some passwords are stored in clear (not ciphered) in the system
  - Weakness in the network gateway
  - And … access to internet from the infotainment system
    - Increase of the attack surface

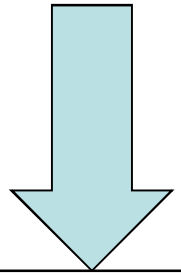
OBDII connector

- Diagnostic connector present inside all car since 1996 (USA)



Automotive <-> Agricultural

- More and more telematic's system inside the tractor
- Possibility to connect Phone or pad by Wifi /Bluetooth
- Diagnostic connector inside the cabin of the tractor



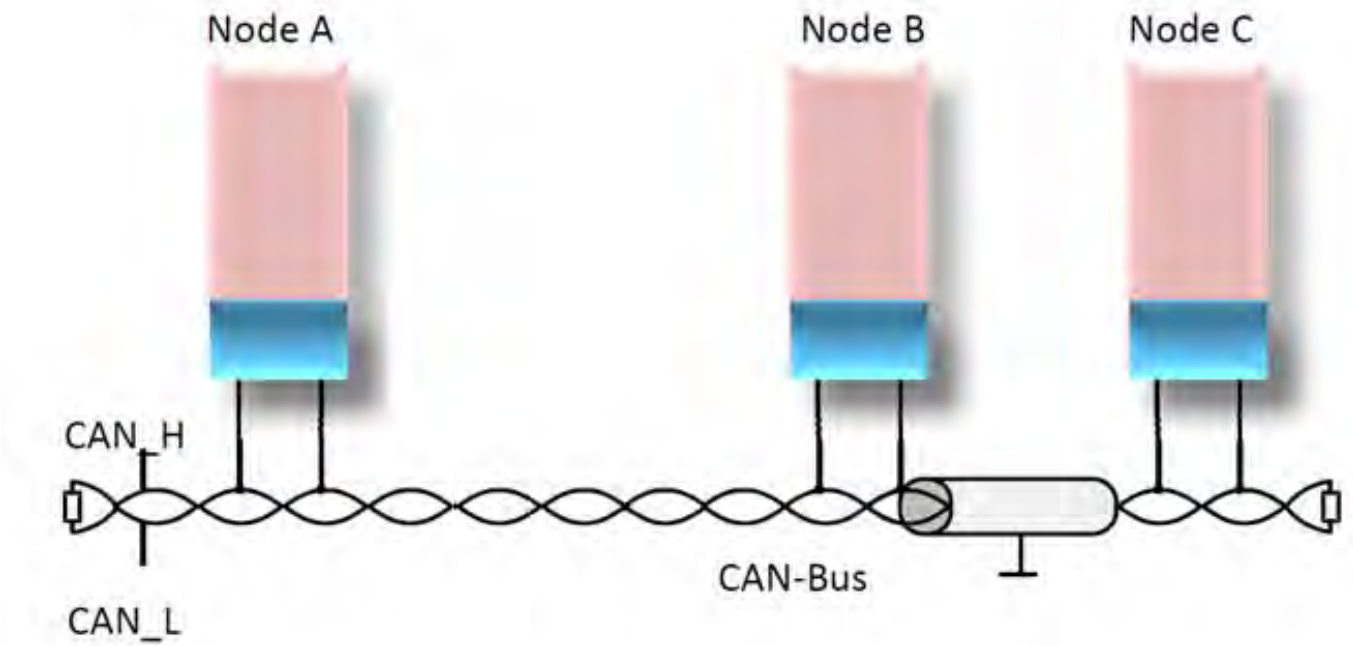
Possibility to access to the CAN bus or ISOBUS to modify the functioning of the vehicle / tractor / tools

Possibility to take some personal information stored in several module, like licenses

CAN / ISOBUS

CAN bus

- The CAN bus is not safety



CAN frame

Standard frame

- Start of frame
- Identifier: 11 bits (Standard Frame) / 29 bits (ISOBUS Frame)
- Control field
- Payload : from 0 to 8 octets
- Cyclic redundancy check : only on the contents of the frame
- Acknowledge
- End of frame

CAN frame

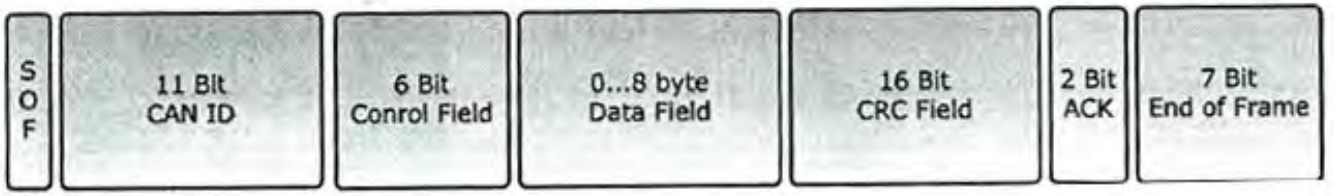
Standard frame

- The identifier indicates which data are in the frame
  - Standard frame (11 bits) : no information about the transmitter and receiver node
  - ISOBUS Frame (29 bits) : information about the transmitter and in some cases the receiver

If a hacking system uses an existing identifier, a module without algorithm of detection of intrusion can't detect the bad message.

CAN frame

Arbitration



- CAN bus is multi-master and there's an arbitration realized on the identifier.
- The smaller identifier wins the access of the bus

If a hacking system sends a frame with an identifier equals to 0 with a periodicity very fast, the CAN bus would be overloaded and the functionalities on the bus would be lost.

ISOBUS

- The fact that ISOBUS is a standard, all messages are defined and known easily by anybody.

- It’s easy to connect a hacking system to the diagnostics connector, or to the Isobus cabin connector, to access to the ISOBUS bus.

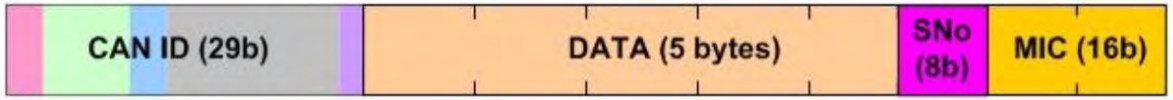
Example of Hacking protection

Firewall

- Could be implemented inside gateway (diagnostic connector)
- Permits to eliminate (drop) not authorized messages
- Useful only if the hacking system is connected to the firewall.
- In the case that the hacking system is connected directly to Can bus, the use of firewall inside all gateways, could decrease the impact of the attack

Algorithm of detection of intrusion

- Check the periodicity of the frame reception and delete it, if the periodicity is not respected
- Add a new CRC with a secondary CRC (MIC) to check the data in the frame (like ARINC 825)



- Add a counter inside the transmitter and receiver which would be increased at each sending (like signal tan for the fileserver).

Conclusion

Conclusion

- The hacking of agricultural system is possible like in automotive.
- The target of the hacking could be to steal some personal information or to block / modify the functioning of a system.
- With all current possibility of wireless connections, the hacking could be hacking remotely.
- The ISOBUS standard doesn’t implement some cyber-protections