CYBERSECURITY FOR TRUCKS AND OTHER HEAVY-DUTY VEHICLES

Mitigating the threat to SAE J1939 CAN bus cybersecurity

GIL LITICHEVER – CTO

Gil.LITICHEVER@nng.com

GILAD BANDEL – VP Product and Marketing

Gilad.Bandel@nng.com

01

SAE J1939 CYBERSECURITY

Why do we need a different approach?

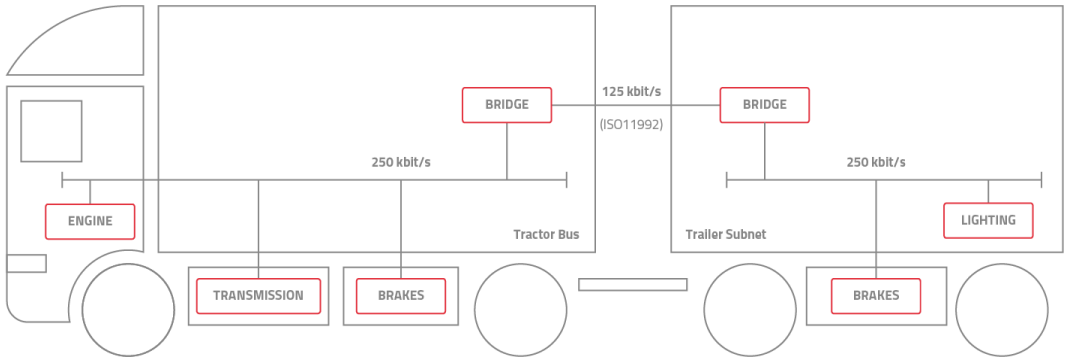
SAE J1939 CYBERSECURITY

Why do we need a different approach?

CUSTOMIZED SOLUTIONS

Tailored solutions are vital to low-bandwidth networks:

- Reduce network overhead
- Limit the need for costly hardware investment
- Threat models and attack vectors vary by protocol



Predicting Future Automotive Cybersecurity – Insight from Other Industries see the series at:
https://ariloutech.com/news/future-automotive-cyber-security-insights-part-1/

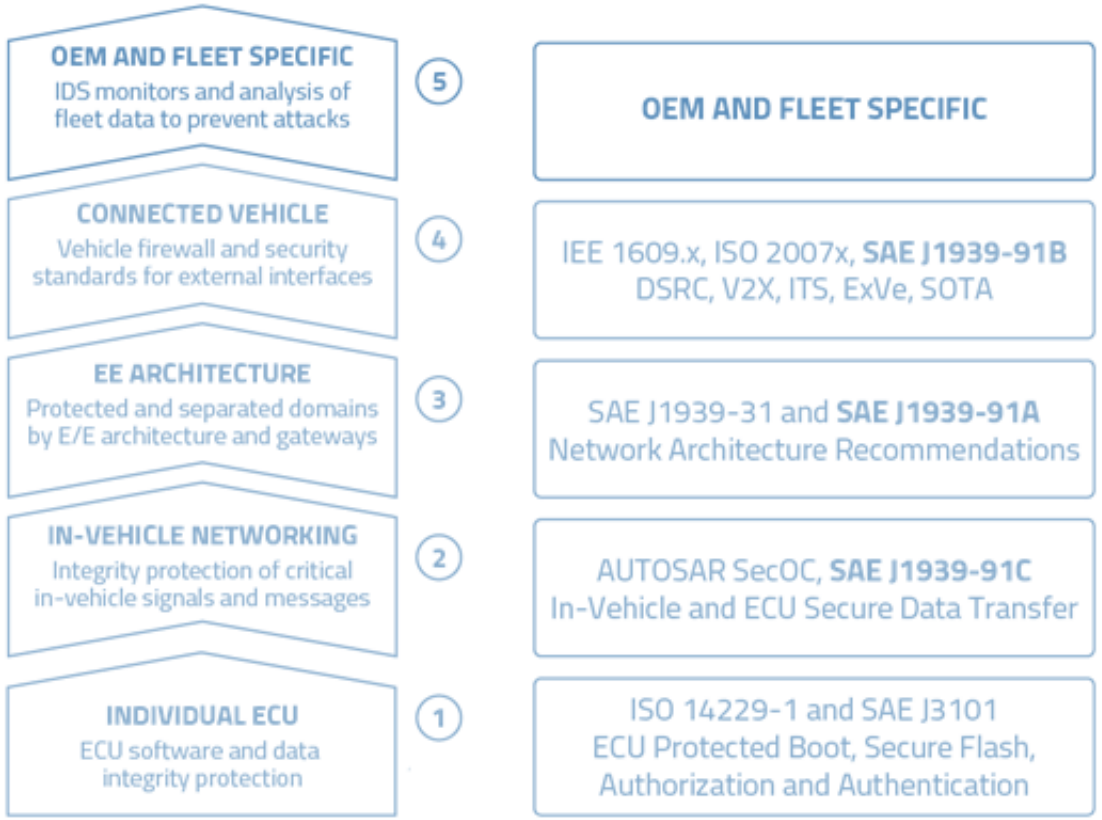
SAE J1939 CYBERSECURITY

Why do we need a different approach?

UNDERSTANDING THE NETWORK LAYERS

Each layer of the network has specific cybersecurity concerns

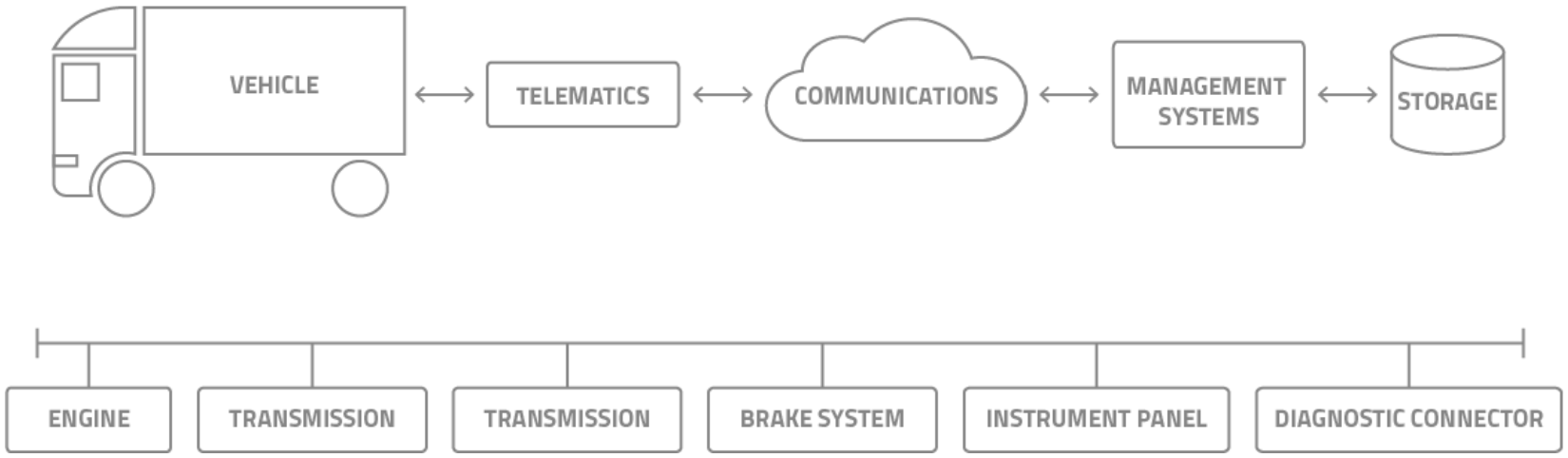
- Individual Electronic Control Unit (ECU)
- **In-Vehicle Network (IVN)**
- Electrical and Electronic (EE) architecture
- Vehicle connectivity
- Fleet connectivity



SAE J1939 CYBERSECURITY

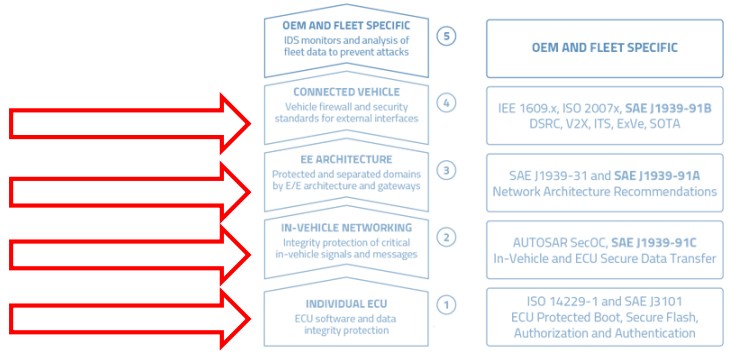
Architecture concept

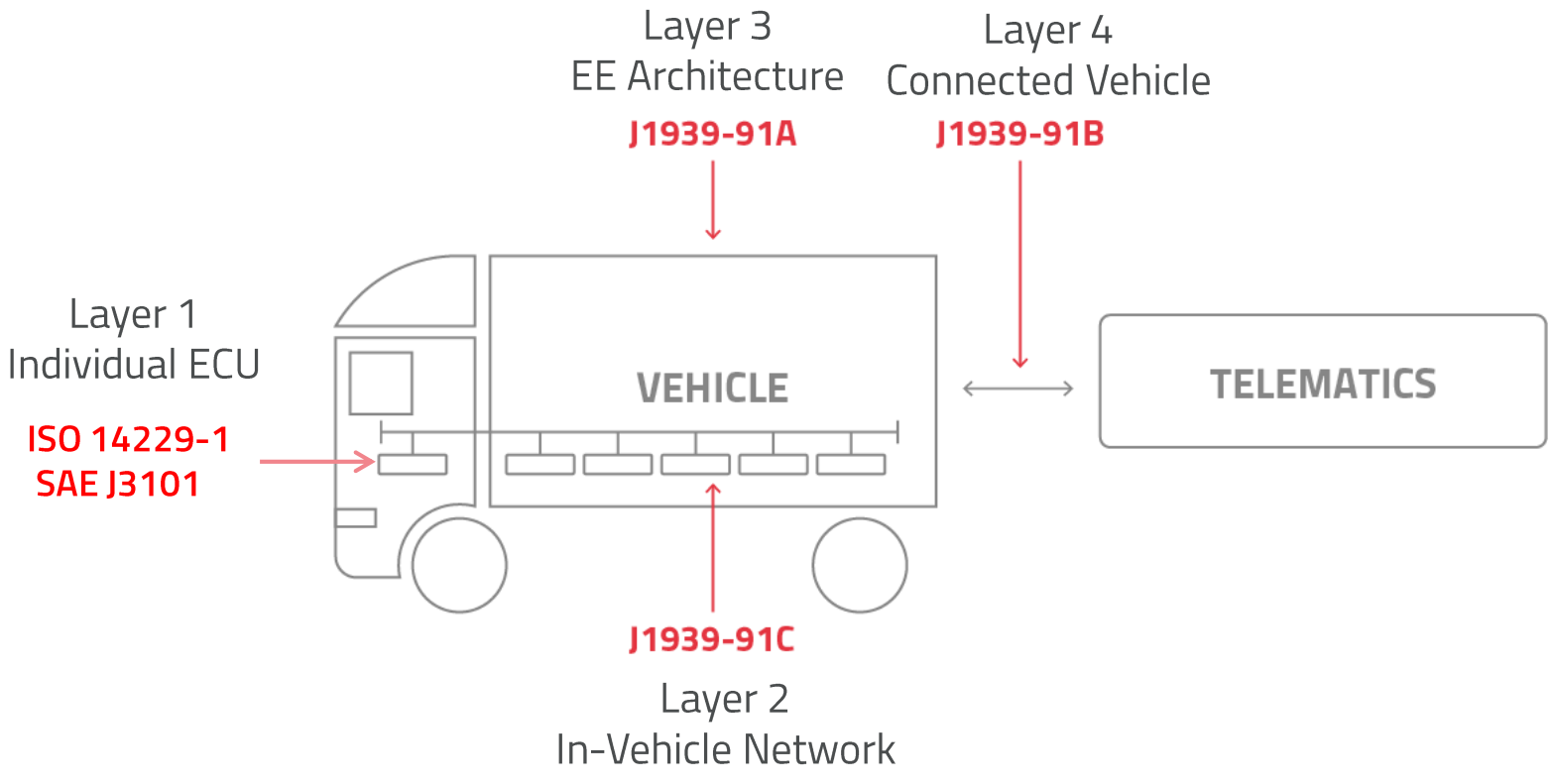
PROVIDE GUIDELINES FOR SECURING COMMUNICATIONS WITH VEHICLES UTILIZING THE SAE J1939 NETWORK



SAE J1939 CYBERSECURITY

Layers scope

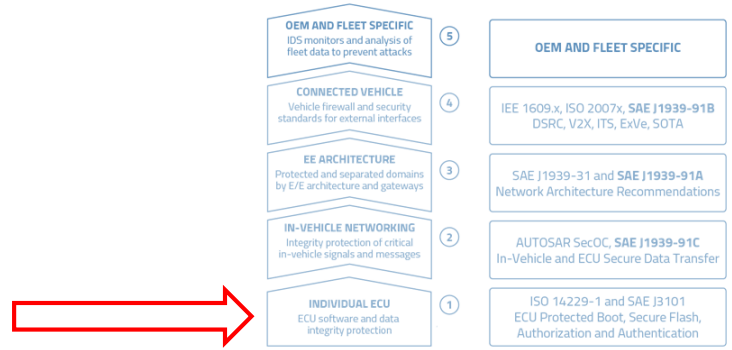




ARILOU
Automotive Cybersecurity
Part of NNG Group

SAE J1939 CYBERSECURITY

Layer 1 security
Individual ECU



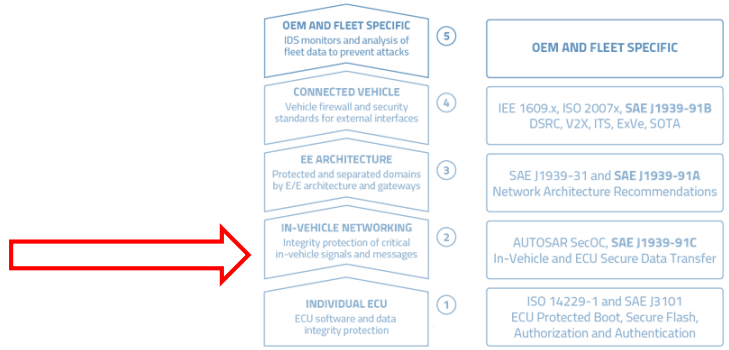
ISO 14229-1 AND SAE J3101

- ECU Protected Boot, Secure Flash
- Authorization and Authentication

For Arilou Secure Boot see:
https://ariloutech.com/solutions/secure-boot-ecu-automotive-cybersecurity/

SAE J1939 CYBERSECURITY

Layer 2 – J1939-91 Part "C"
In-Vehicle network security



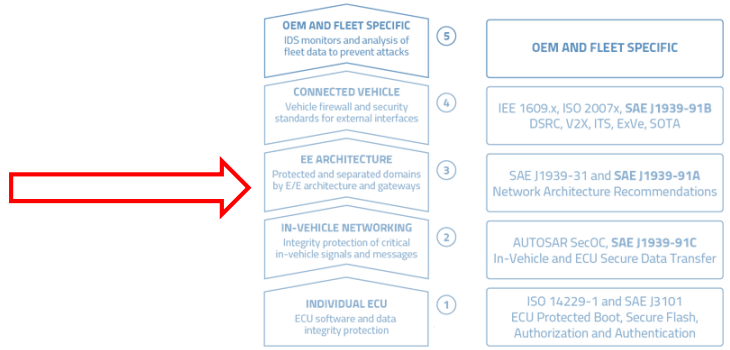
J1939-91C DEFINES RECOMMENDATIONS FOR:

- Secure on-board communications between ECUs
- Update General Vehicle Network Gateway recommendations and network topology reference related to J1939-31

SAE J1939 CYBERSECURITY

Layer 3 – J1939-91 Part "A"

Foundation layer security



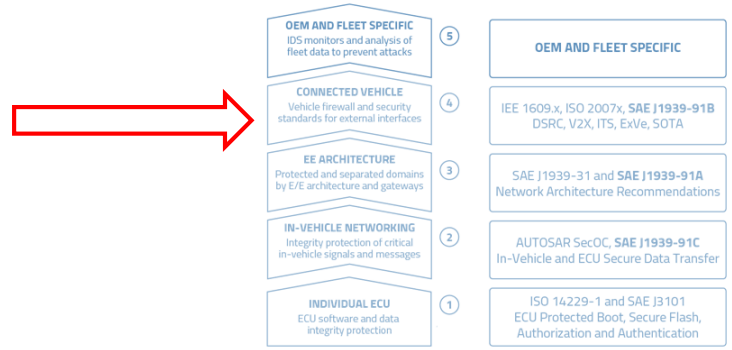
J1939-91A DEFINES THE RECOMMENDATIONS FOR SECURITY OF THE VEHICLE SIDE OF THE J1939-13 CONNECTOR

- Recommendations for vehicle communications functions with a device which is connected to J1939-13 interface - diagnostics interface security. [Similar to SAE J3138 diagnostics link security and SAE J3005-2 "dongle" device security]
- General requirements for "Imposter Reporting" for devices that may spoof J1939 Source Addresses.

SAE J1939 CYBERSECURITY

Layer 4 – SAE J1939-91 Part "B"

Connected vehicle security



SCOPE OF SAE J1939-91B: BI-DIRECTIONAL SECURE OVER THE AIR (OTA) COMMUNICATIONS VIA A TELEMATICS INTERFACE TO THE VEHICLE

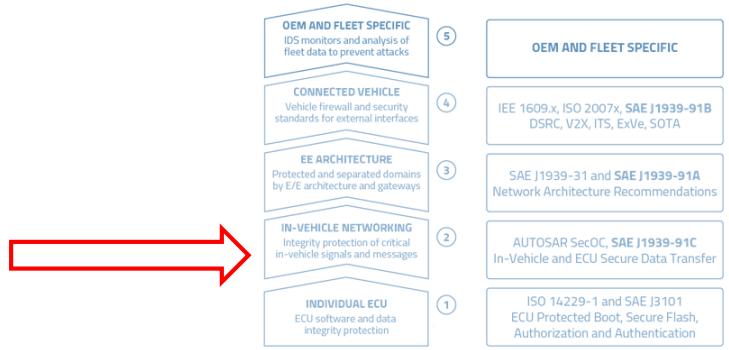
Extended Vehicle (ExVe) Systems and Intelligent Transportation Systems (ITS)

- IEEE 1609.x (DSRC)
- ISO 20077, ISO 20078, ISO 20080, etc.
- **ISO/SAE 21434**
- ISO TC204 work items (ITS)

For TCU protection see:
https://ariloutech.com/news/telematics-control-unit-cybersecurity-battle-two-fronts/

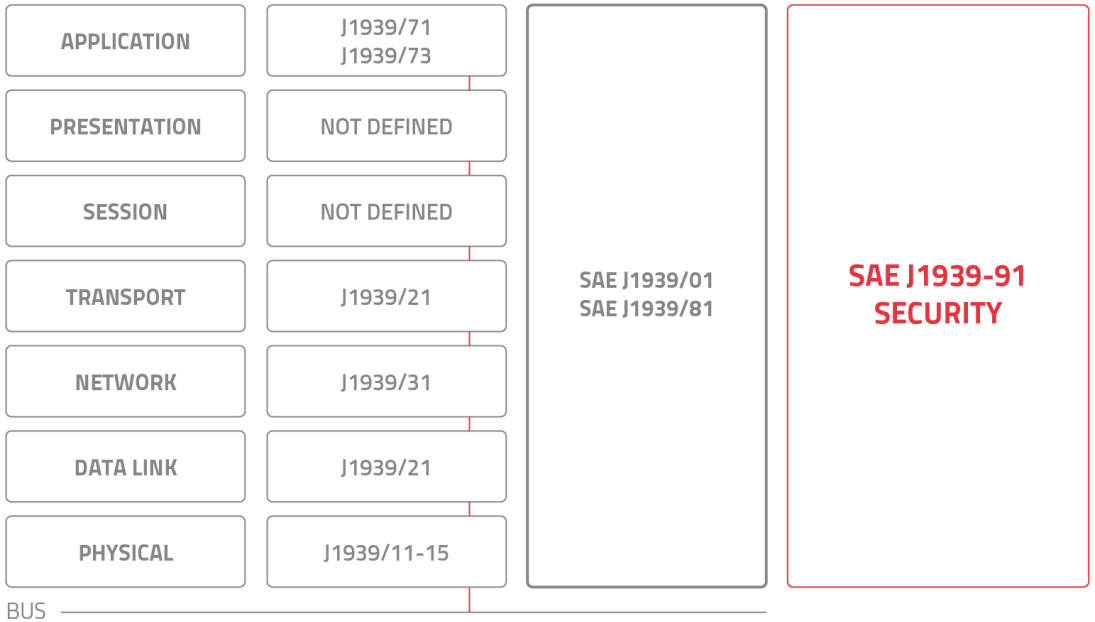
SAE J1939 CYBERSECURITY

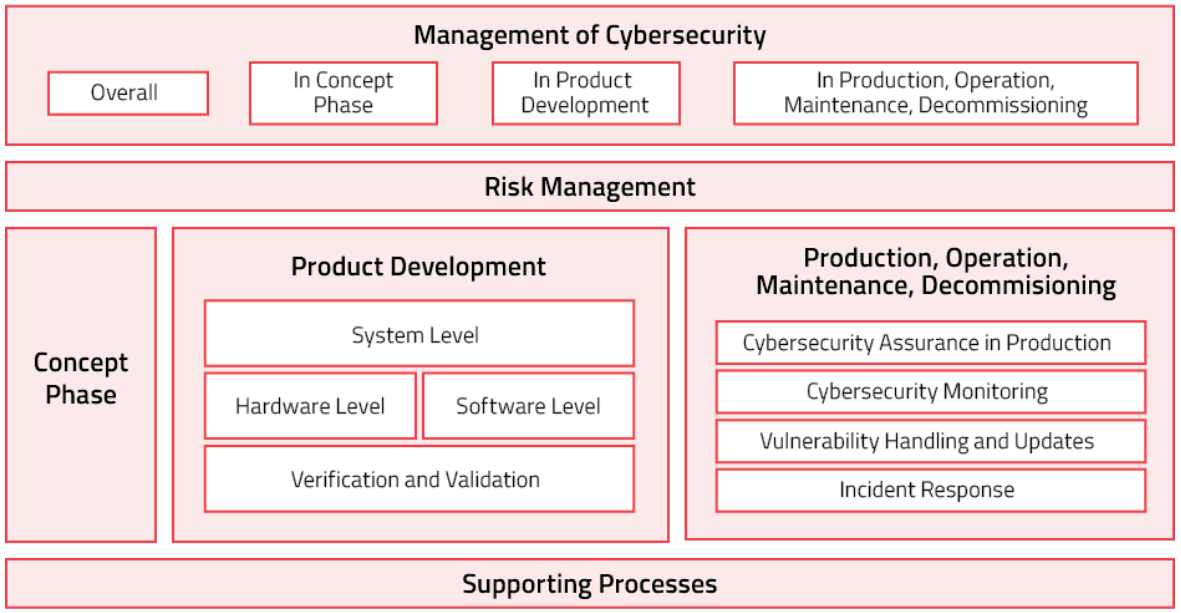
Focus on the IVN layer



In this presentation we will focus on the **IVN layer**, which is due to be address by upcoming standards (WIP – Work In Progress):

- **SAE J1939-91C (IVN security)**
- SAE J1939-91B (Telematics interfaces)





ARILOU
Automotive Cybersecurity
Part of NNG Group

02

SAE J1939 CYBERSECURITY

Who are the threat actors targeting heavy-duty vehicles?

SAE J1939 CYBERSECURITY

Who are the main threat actors targeting heavy-duty vehicles?

THREE MAIN THREAT ACTOR CATEGORIES

- **Criminals** looking for ransom or wishing to inflict physical damage
- **Terrorists**, nation-states, anarchists, activists, or any group/individual with a political/ideological background
- **Owners**/end-users hacking their own vehicles
  - Clone ECU replacements
  - Chip Tuning

03

SAE J1939 CYBERSECURITY

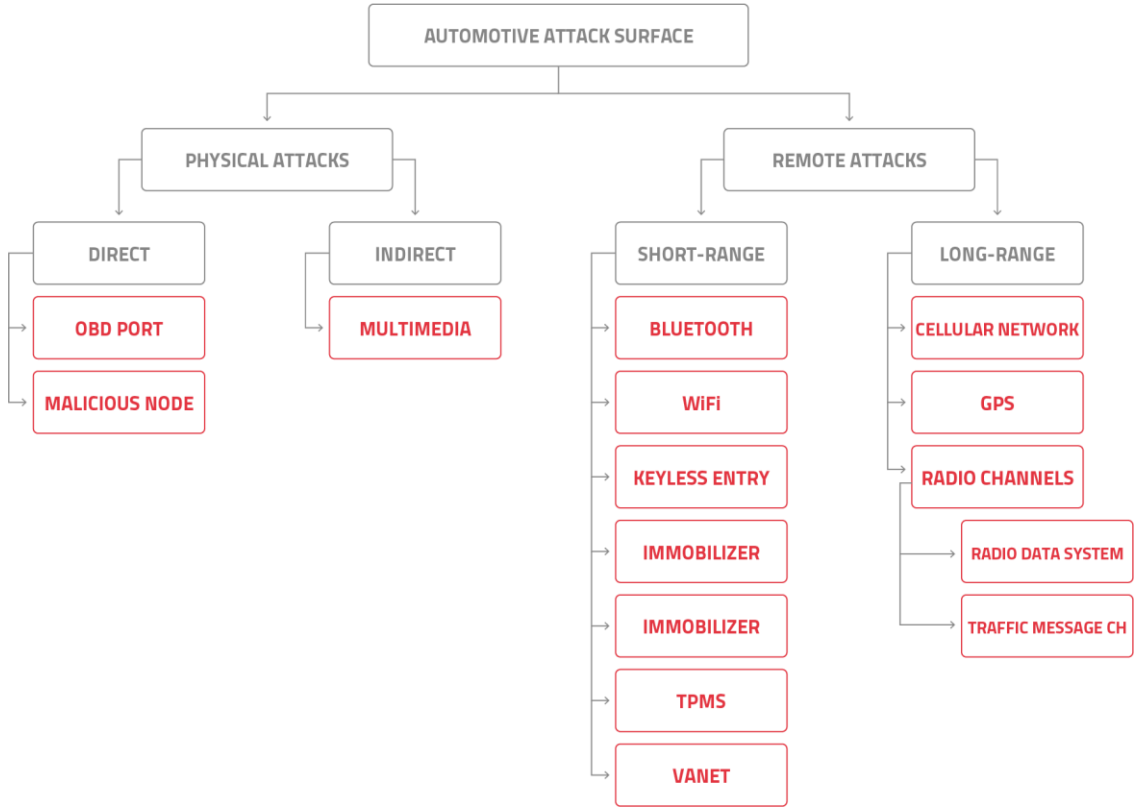
How do attack surfaces and threat models differ to regular CAN?

SAE J1939 CYBERSECURITY

How do attack surfaces and threat models differ to regular CAN?

ATTACK SURFACES AND THREAT MODELS

- Remote attacks as a preferred methodology
- Routine maintenance deters physical attacks, though still a possibility
- Standardized protocol across manufacturers, little to no variation in component design and integration
- Component interoperability leaves multiple OEMs/Tiers open to attack by a single kill-chain



SAE J1939 CYBERSECURITY

How do attack surfaces and threat models differ to regular CAN?

VIRAL EFFECTS OF MODULAR ATTACHMENTS

- Agricultural vehicle **attachments and trailers** can serve as a vector, as easily accessible and compromised
- One trailer/attachment may **serve many vehicles**
- **Compromised vehicles** can, in turn, serve as a vector to attack yet to be compromised attachments and trailers

04

SAE J1939 CYBERSECURITY

Attack vectors and scenarios

SAE J1939 CYBERSECURITY

Attack vectors and scenarios

ADDRESSING

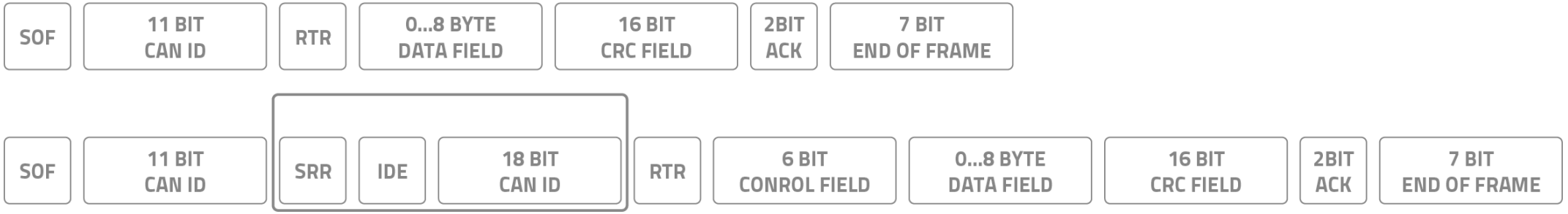
J1939 uses 29-bit, extended CAN addressing, proprietary format. This implies there is no way to truly authenticate the origin of the message.

- Any spoofing or impersonation attack is possible
  - ECUs can send any message ID
  - No authentication
  - Man in The Middle (MiTM) also a possibility

VEHICLE CONFIGURATION

Heavy-duty vehicles have a complex and dynamic life-cycle with many opportunities for rogue actors to integrate compromised components or upload malicious software.

- Interoperability means components can be mixed and matched.
- Attachments and other equipment may be shared by many vehicles.



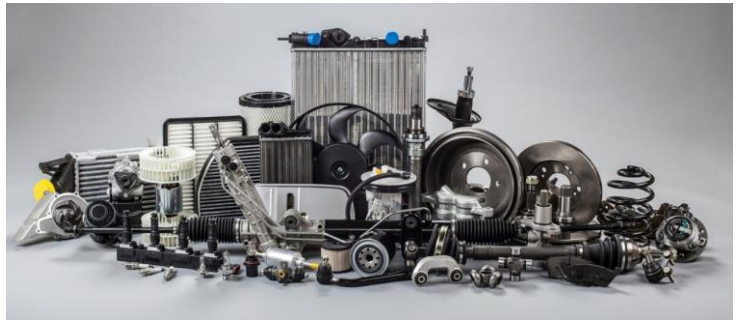
SAE J1939 CYBERSECURITY

Attack vectors and scenarios

AFTERMARKET FLEET MANAGEMENT & EQUIPMENT INSTALLATION

Devices added by fleet owners to monitor and control their fleet. In some cases, regulation requires the installation of driver-hours recording ELDs (Electronic Logging Devices) and other telematics equipment.

- Not part of the OEM cybersecurity control process
- Usually not part of the OEM supply chain
- Cyber-protection cannot be guaranteed



SPECIFIC EMBEDDED SOFTWARE ISSUES

There are several types of vulnerabilities when implementing a protocol or a standard:

- Inherent protocol vulnerabilities
  - Defined in a vulnerable way
- Implementation vulnerabilities
  - Buffer Overflow (BoF)
- Badly defined/complex protocol
  - Or bad code flow exposing the protocol to attack

05

SAE J1939 CYBERSECURITY

General pitfalls in the code

SAE J1939 CYBERSECURITY

Approach and method

INSPECTED CODE

Code used for this presentation was taken out of the public domain and was published for educational purposes.

RESULT

Attacks capabilities:

- Take over communication flow without the knowledge of the parties
- Denial of service
- Buffer overflow and malicious code execution (more than one)!!!

See our article https://ariloutech.com/news/heavy-duty-vehicles-sae-j1939-cybersecurity/

EFFORT

Total – 2 days for de-obfuscation, vulnerability assessment and writing a report

CONCLUSIONS

- As always - security through obscurity does not work
- J1939 is well documented, finding vulnerabilities is fast and easy
- Do not take your code of the internet without checking
  - There is a good reason we call this "general pitfalls"… For obvious reasons we cannot further elaborate in the current presentation.

Sunlight is said to be the best of disinfectants… ~ Louis D. Brandeis

SAE J1939 CYBERSECURITY

Acronyms

BAM – Broadcast Announcement Message

TP – Transport Protocol

CM – Connection Mode

DT – Data Transfer

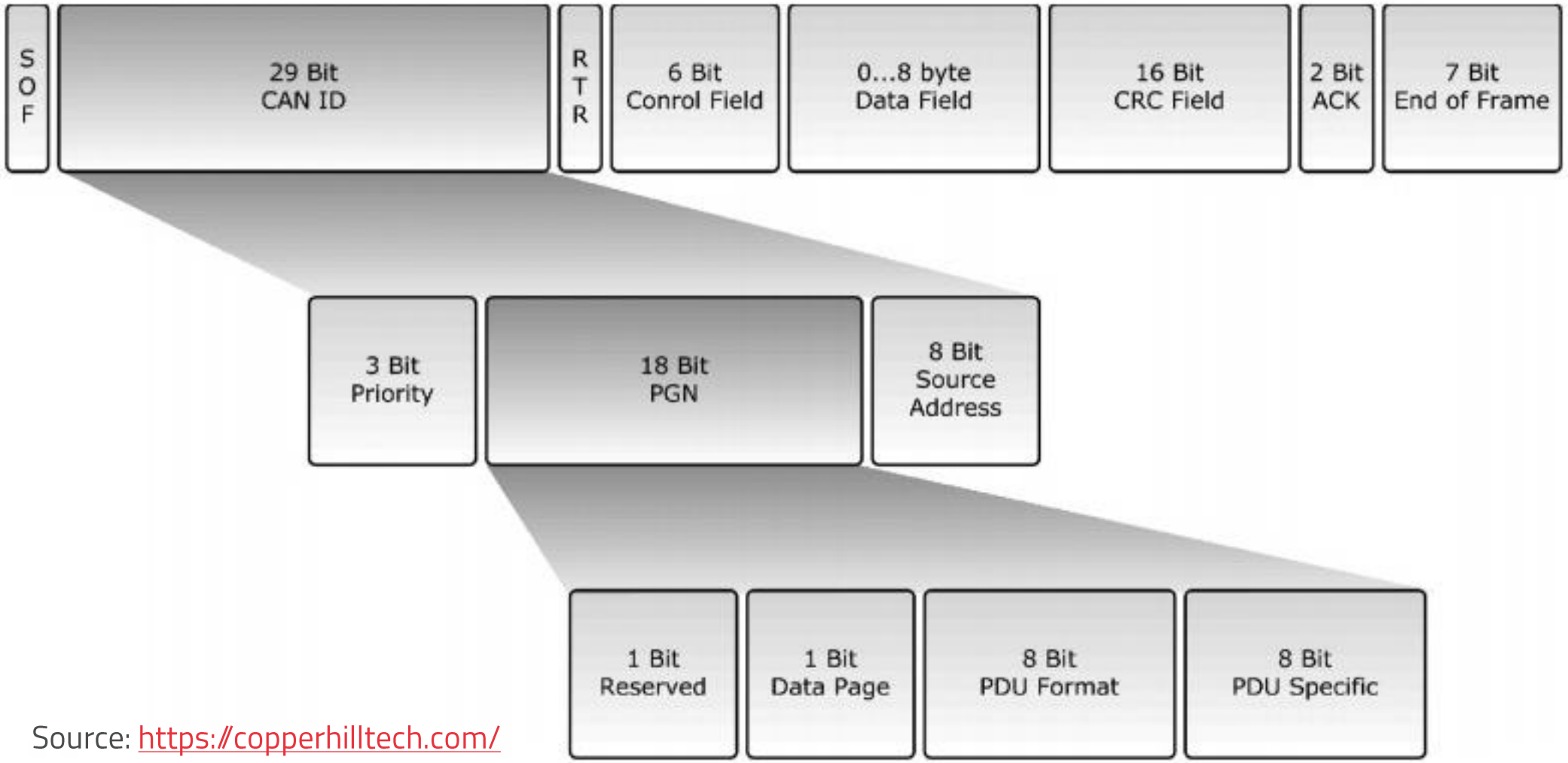
PGN – Parameter Group Number

RTS – Request To Send

CTS - Clear To Send

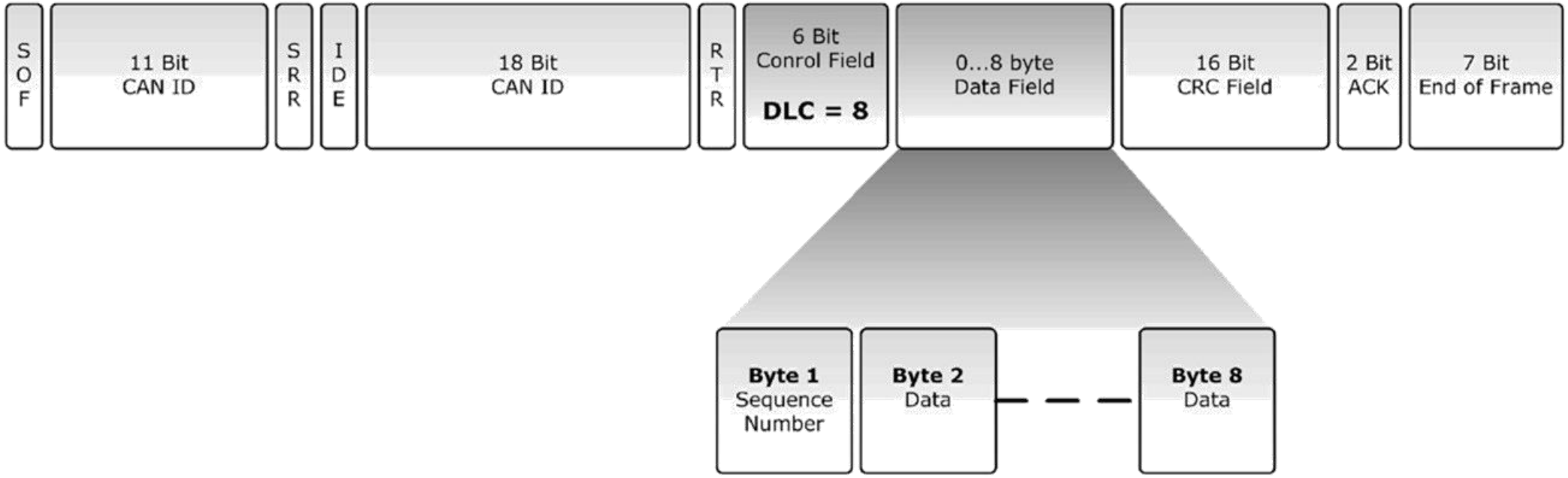
SN – Sequence Number

SAE J1939 - FRAME FORMAT



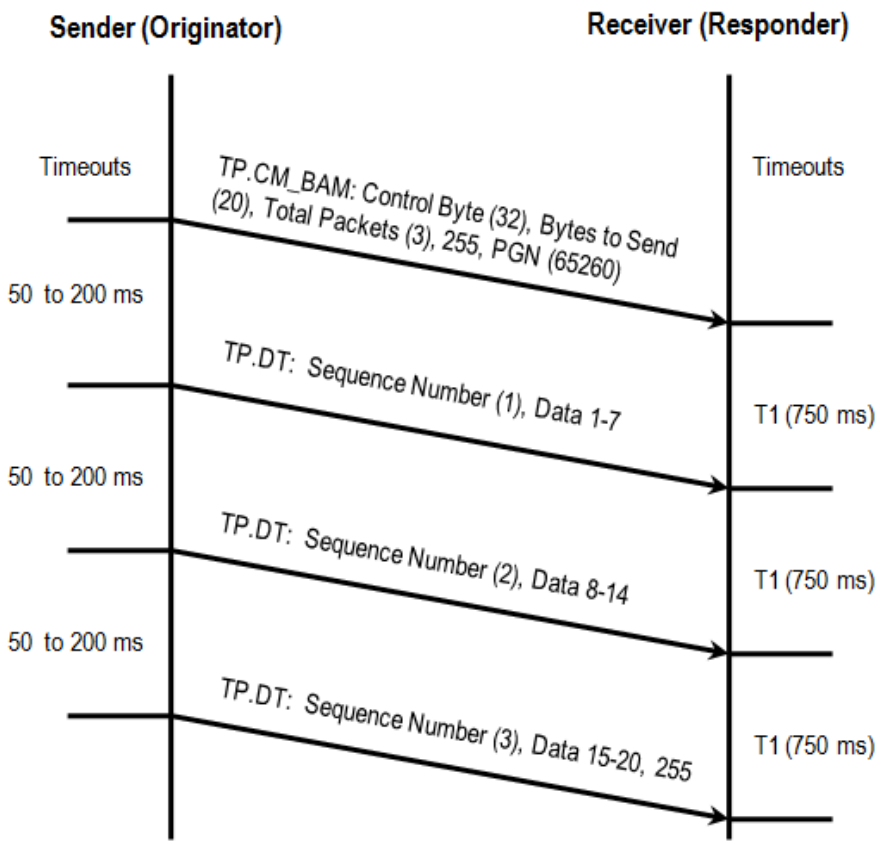
Source: https://copperhilltech.com/

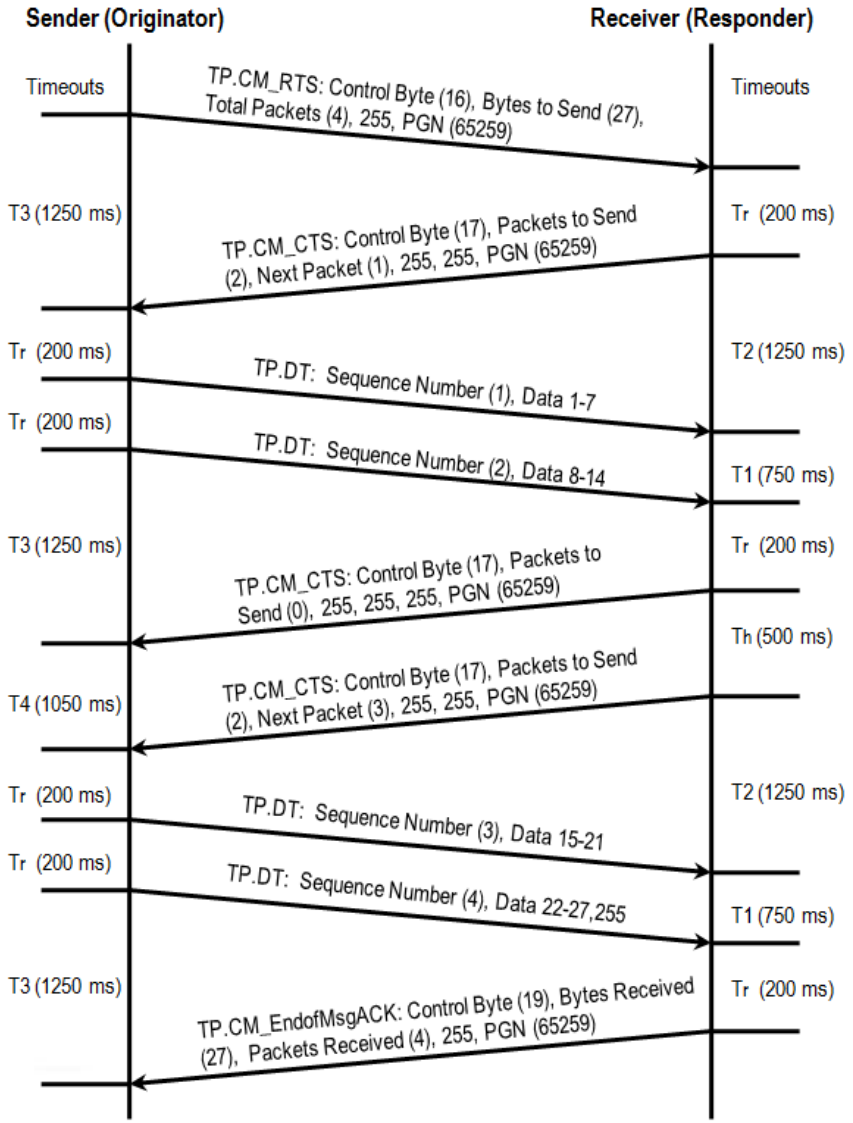
SAE J1939 - FRAME FORMAT



Source: https://copperhilltech.com/

SAE J1939 – TRANSPORT PROTOCOL





Source: https://forums.ni.com/

SAE J1939 CYBERSECURITY

General pitfalls in the code

GENERAL PITFALLS IN THE CODE

A common flaw seen is the use of the J1939 sequence no. (SN) as an index in the message data, without a sanity check (see right -->)

STATE MACHINE TIMEOUTS AND DECISIONS

Here it is vaguer, since every decision may have another effect which in turn, may have a negative effect. In general a "what if" approach should be used to cover as many attack scenarios as possible.

- 0 < SN <= 255 (SN = 0 may easily cause a buffer overflow)
- SN <= number of frames
- SN should go up by one – no reordering in CAN bus

Acceptance of message size and number of frames without doing a sanity check:

- Number of frames = ceil(message_size/7)

When using a message size buffer less than the maximal size of 1785, there is no special care taken to prevent buffer overflow:

- Validate the number of frames and message size to match the buffer size.
- When the buffer size is not a multiple of 7, pay special attention to the last copy instruction.

5.1

SAE J1939 CYBERSECURITY

Machine Override Vulnerabilities

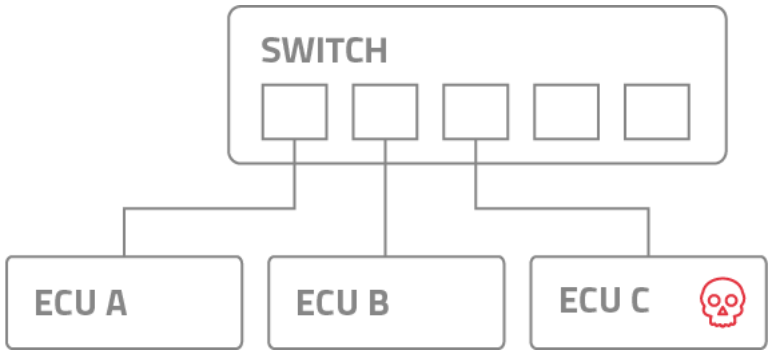
SAE J1939 CYBERSECURITY

General pitfalls in the code

MACHINE OVERRIDE VULNERABILITY

The J1939 transport protocol enables us to completely override someone's messages without the sender or receiver being aware.

- Override message after it has been transmitted
  - Virtual MITM attack



THE ATTACK

Anticipating a legitimate ECU will send a TP.CM BAM message (these are periodic messages).

- Send with double the no. of packets (byte 4)
  - Assuming no. of frames in less than 128
- Send data we want after legit sender sends whole message
  - TP.CM BAM and message data TP.DM messages
- Neither receiver or sender knows message has been modified
  - Attacker can look at original message before sending their own.

SAE J1939 CYBERSECURITY

HOW IT WORKS

If the BAM messages state machine is in an idle state, and we receive a TP.CM message with command BAM(32), we read the BAM message data and move to the next state.

- Further BAM messages will be ignored until message completed or timeout occurs. Second BAM message is ignored
- No sanity check between message length and no. of packets
- Write pointer to frame is deduced from message sequence w/o validation.
- When attacker sends messages with sequence no.'s starting from 1, overrides reassembled message data.
- Double no. of frames means only at end will TP transaction finish and message be received by higher layers.

```
/* int16_t nPointer  - pointer in the reassembled message
pMsg[0] contains the sequence number
BAM_tp_frame.tp_frame_number - number of received TP frames
BAM_tp_frame.number_of_packets - number of total frames expected
BAM_tp_frame.TP_message_state - BAM message handling current state */
  if(BAM_tp_frame.TP_message_state == TP_MSG_STATE_RX &&
    BAM_tp_frame.timeout_enable == true &&
    lPGN == PGN_BAM_TP_DM && nSrcAddr == BAM_tp_frame.src_addr &&
    nDestAddr == BAM_tp_frame.dst_addr)
  {
    nPointer = ((int)pMsg[0] - 1) * 7;
    for(i = 1; i < 8; i++)
      BAM_tp_frame.msg_data[nPointer++] = pMsg[i];
    if(++BAM_tp_frame.tp_frame_number == BAM_tp_frame.number_of_packets)
    {
      init_BAM_tp_transaction(DISABLE_TP_TIMERS);
      BAM_tp_frame.tp_transaction_finished_successfully = true;
    }
  }
```

Fig.1. Code snippet – Message data reassembly

SAE J1939 CYBERSECURITY

MITIGATIONS

Several mitigations could prevent the attack:

- Comparing the number of frames and message length
- Comparing the number of frames/message length with known PGN message length
- Comparing the message sequence no. with a stored value since there is no reordering on CAN bus.

5.2

SAE J1939 CYBERSECURITY

Peer-to-peer sender denial-of-service attacks

(PTP sender DoS)

SAE J1939 CYBERSECURITY

PEER-TO-PEER SENDER DENIAL OF SERVICE (PTP SENDER DOS)

Although DOS (denial-of-service) attacks in J1939 are trivial, we will highlight this one since it could easily have been avoided.

- TP (Transport Protocol) defines a PTP session which requires RTS (Request To Send) messages
- The receiver should send a CTS (Clear To Send) message

THE ATTACK

When receiving RTS requests (even if dedicated to another ECU) the attacker keeps sending CTS replies.

- Prevents the sender transmitting the data
- Continues until the receiver times out and sends and abort message

SAE J1939 CYBERSECURITY

HOW IT WORKS

When receiving a CTS reply, the sender resets the sending, preventing the timeout from occurring.

```
//we can the CTS message multiple times
if(lPGN == PGN_BAM_TP_CM &&
  nDestAddr == PTP_tp_frame.src_addr && pMsg[0] == CM_CTS)
  {
    stop_timer(&PTP_tp_CTS_RX_timer);
    // init the timer again
    PTP_tx_interval_timer.timeout_cnt = PTP_CTS_to_msg_tx_timer_init_value;
    PTP_tx_interval_timer.timeout_enable = true;
    PTP_tp_frame.CTS_received = true;
  }
  //this timer will never expire
  if(PTP_tp_frame.CTS_received == true &&
      PTP_tx_interval_timer.timeout_occured == true)
  {
    nPointer = PTP_tp_frame.tp_frame_number * 7;
    tp_frame_data[0] = ++PTP_tp_frame.tp_frame_number;
```

Fig.2. Code snippet – PTP frame CTS state machine

SAE J1939 CYBERSECURITY

MITIGATION

When receiving repeated CTS messages,
we should never reset the timer.

5.3

SAE J1939 CYBERSECURITY

TP receive buffer overflow (BoF)

SAE J1939 CYBERSECURITY

TP RECEIVE BUFFER OVERFLOW (BOF)

Since memory is statically allocated, we would not expect a buffer overflow into the TP packet data. However, there are two of them.

THE ATTACK

Send a BAM or PTP TP message with a sequence number of 0:

- Copy 7 bytes in bytes 7-0 of the 1785 bytes overriding
  - 3 bytes of the PGN
  - The source address
  - The destination address
  - The number of packets
  - The frame number of the current session

If the pointer was not defined as a signed int (16 bit for Arduino), but rather as an unsigned int, the attack would have copied 7 bytes into bytes 1785-1792 where we have a 1785-byte buffer. This overrides the session length variable, used later for coping data, resulting in a much more dangerous exploitation.

SAE J1939 CYBERSECURITY

HOW IT WORKS

When BAM message data is received, the data is copied according to the message sequence number without validation (See fig.1 again, right).

- The sequence number in the protocol should start from 1
- When placing 0, it means nPointer = -7
- The attacker writes to the 7 bites before the buffer.

```
/* int16_t nPointer  - pointer in the reassembled message
pMsg[0] contains the sequence number
BAM_tp_frame.tp_frame_number - number of received TP frames
BAM_tp_frame.number_of_packets - number of total frames expected
BAM_tp_frame.TP_message_state - BAM message handling current state */
  if(BAM_tp_frame.TP_message_state == TP_MSG_STATE_RX &&
    BAM_tp_frame.timeout_enable == true &&
    lPGN == PGN_BAM_TP_DM && nSrcAddr == BAM_tp_frame.src_addr &&
    nDestAddr == BAM_tp_frame.dst_addr)
  {
    nPointer = ((int)pMsg[0] - 1) * 7;
    for(i = 1; i < 8; i++)
      BAM_tp_frame.msg_data[nPointer++] = pMsg[i];
    if(++BAM_tp_frame.tp_frame_number == BAM_tp_frame.number_of_packets)
    {
      init_BAM_tp_transaction(DISABLE_TP_TIMERS);
      BAM_tp_frame.tp_transaction_finished_successfully = true;
    }
  }
```

Fig.1. Code snippet – Message data reassembly

SAE J1939 CYBERSECURITY

MITIGATION

Validate the sequence number

- SN: 0 < SN < number of frames
- Also validate the number of frames

5.4

SAE J1939 CYBERSECURITY

Small footprint code variant buffer overflow

SAE J1939 CYBERSECURITY

SMALL FOOTPRINT CODE VARIANT BUFFER OVERFLOW

Sometimes to save space, the J1939 stack does not support the maximal frame size of 1785 bytes.

In one of the compilation variations, the maximal frame size was 256 bytes with a 256-byte buffer.

- Relying on the sequence number as part of our pointer, without validation:
  - Can cause buffer overflow
  - Applies to both BAM and PTP sessions

THE ATTACK

Assuming we have a 256-byte buffer. We can:

- Send a message with up to 256-byte message length
  - but with a sequence number >= 36.

This causes a basic buffer overflow of up to 1529 bytes

```
/* int16_t nPointer  - pointer in the reassembled message
pMsg[0] contains the sequence number
BAM_tp_frame.tp_frame_number - number of received TP frames
BAM_tp_frame.number_of_packets - number of total frames expected
BAM_tp_frame.TP_message_state - BAM message handling current state */
  if(BAM_tp_frame.TP_message_state == TP_MSG_STATE_RX &&
    BAM_tp_frame.timeout_enable == true &&
    lPGN == PGN_BAM_TP_DM && nSrcAddr == BAM_tp_frame.src_addr &&
    nDestAddr == BAM_tp_frame.dst_addr)
  {
    nPointer = ((int)pMsg[0] - 1) * 7;
    for(i = 1; i < 8; i++)
      BAM_tp_frame.msg_data[nPointer++] = pMsg[i];
    if(++BAM_tp_frame.tp_frame_number == BAM_tp_frame.number_of_packets)
    {
      init_BAM_tp_transaction(DISABLE_TP_TIMERS);
      BAM_tp_frame.tp_transaction_finished_successfully = true;
    }
  }
```

SAE J1939 CYBERSECURITY

MITIGATION

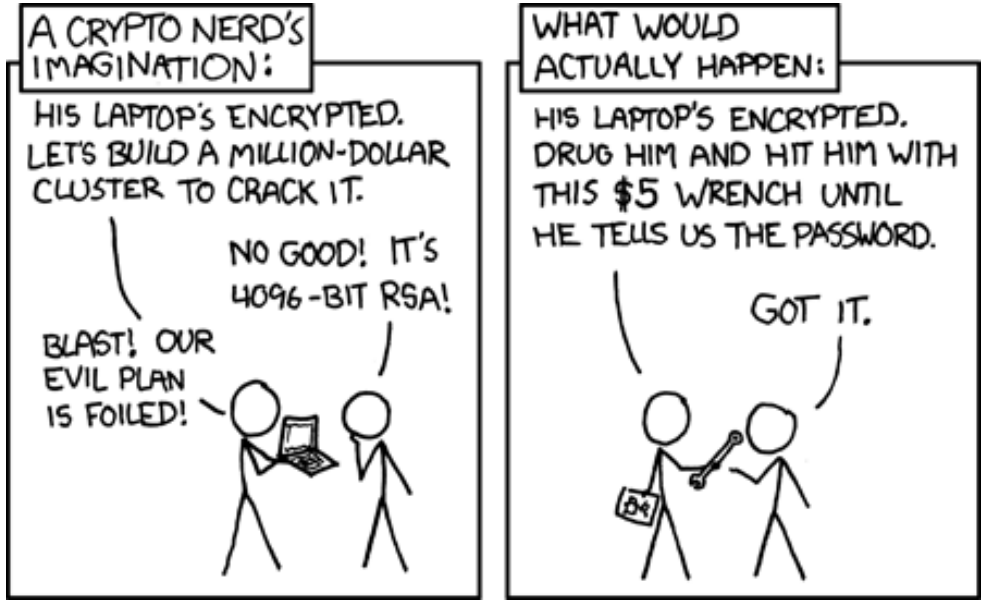
Validate the sequence number;

- SN: 0 < SN < number of frames.
- Validate the number of frames according to buffer size.
- Make sure the last copied frame does not create an overflow
  - (Or increase the buffer size to 7*36 = 259 bytes)

SAE J1939 CYBERSECURITY

Conclusion

- Security through obscurity does not work
- J1939 is well documented, finding vulnerabilities is fast and easy
- Do not take your code of the internet without checking
- You are welcome to contact us: gil.litichever@nng.com



Source: https://xkcd.com/

06

SAE J1939 CYBERSECURITY

Mitigating cyber-attacks on SAE J1939 heavy-duty vehicles

SAE J1939 CYBERSECURITY

Mitigating cyber-attacks on SAE J1939 heavy-duty vehicles

PROACTIVE ACTION IS REQUIRED

Tier-1s and OEMs need to take proactive action to protect the heavy vehicle for many reasons, including:

- Regulations such as the UNECE WP.29
- Growing awareness within professional bodies in the automotive industry
- Top management who wishes to protect their firm's reputation, and prevent loss of life and damage to property, for which they will be liable
- Insurance companies requiring cybersecurity adoption to minimize risk

REDUCING RISK

Reducing risks involves acting in many areas.

- ISO/SAE 21434
- AUTOSAR best practice, and many others

Practicably, this translates to an extensive set of activities:

- Process and procedures
- Cybersecurity management systems
- Secure by design approach of all the systems
- Secured software development lifecycle
- Compliance with standards such as A-SPICE and MISRA
- Dedicated cybersecurity protection mechanisms such as IDS/IPS, end point protection, cryptographic solutions.

SAE J1939 CYBERSECURITY

Mitigating cyber-attacks on SAE J1939 heavy-duty vehicles

INTRUSION DETECTION AND PREVENTION

It is important to note that out of all the above-mentioned solutions, IDS/IPS is the only component that is:

- Dedicated
- Devoted
- Independent

While implementing many security means as part of the overall strategy is imperative, maintaining an IDS/IPS is crucial.

- Only component of a vehicle to have all its resources allocated to the protection of the vehicle.

The IDS/IPS function should reside in the central gateway. Also, can be distributed to the:

- TCU
- IVI
- V2X OBU
- Domain controller
- Any other connectivity or safety critical ECU

Only this way will the best protection be provided to the vehicle.

07

SAE J1939 CYBERSECURITY

Automotive cybersecurity solutions for SAE J1939 heavy-duty vehicles

SAE J1939 CYBERSECURITY

Automotive cybersecurity solutions for SAE J1939 heavy-duty vehicles

ARILOU SENTINEL SERIES IDS/IPS FOR CAN BUS AND AUTOMOTIVE ETHERNET

J1939 CAN bus is heart of the heavy-duty vehicle. Prone to cyber-attack it should be well protected. Call us for additional cases available with us.

The methods to be employed should include a variety of procedural and technological means. **Arilou's IDS/IPS Solution for J1939 heavy-duty vehicles is a customizable and comprehensive protection tool.**

- Sentinel-TRK IDS/IPS for SAE J1939

OTHER RELEVANT SOLUTIONS

- Arilou Sentinel-CAN IDS/IPS for CAN bus
- Arilou Sentinel-ETH IDS/IPS for automotive Ethernet
- CANpress CAN bus traffic compression with optional authentication and encryption
- Professional Services TARA

These, among our many other products, provide holistic protection solutions which answer the challenge of securing vehicle IVNs.

- **See more solutions at https://ariloutech.com/solutions**

ARILOU
Automotive Cybersecurity
Part of NNG Group

THANK YOU FOR YOUR ATTENTION

GILAD BANDEL
VP Product and Marketing

Email: Gilad.Bandel@nng.com
Tel: +972 (54) 246-0006
Website: www.ariloutech.com