Introduction to CiA 620 Ethernet on CAN (“Ethernetification”)

How MACsec secured Ethernet frames are transported over a small-frame link layer

November 2026

Dr. Ken Tindell

Motivation for supporting Ethernet over CAN

1. Re-use proven, robust and low-cost physical layer of CAN
2. Support **all legal Ethernet MAC frames**
3. Respect Ethernet's existing priority scheme (i.e. PCP priorities)
    - 8 FIFO transmit queues
    - 8 priority levels on the multi-drop bus

No existing tunnelling schemes were appropriate (none respect Ethernet priorities) and so a new scheme was developed by CAN-in-Automation (CiA).

CiA 620 Ethernet on CAN: Concept

Ethernet frames are broken into small ‘fragments’ of up to 64 bytes, which are then transmitted as a set of CAN FD frames.

A compression scheme is used to replace Ethernet MAC field values with bit flags when common field values are seen:

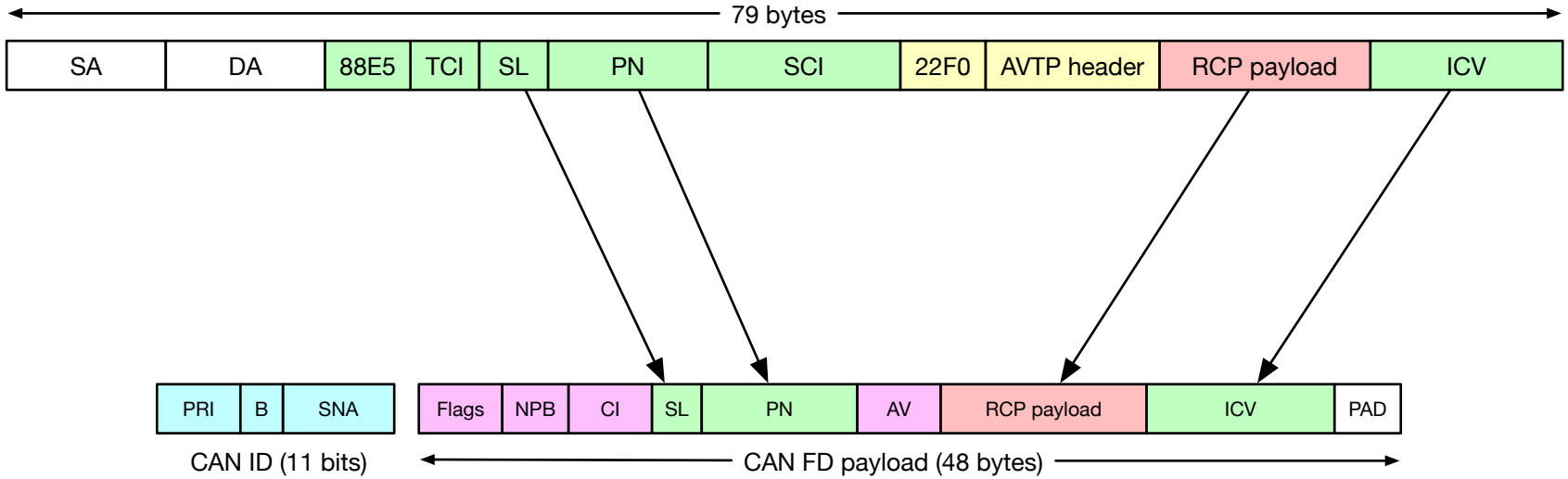
- SA and DA (become short codes in a table)
- EtherType
- **MACsec SecTAG**
- IEEE 1722
- VLAN tags (outer and inner)

Many fields are predictable. E.g. SecTAG SCI is typically 6 bytes SA, followed by 0000_H

SA short code (“SNA”) is a 6-bit lookup code in a node’s configuration table.

Compressing MACsec: example

Flags for when (e.g.) SCI is predictable (typically 6 bytes SA, followed by 0000_H)



Most urgent real-time control frames compress to a **singleton**: a single CAN FD frame

Lessons for MACsec data security in embedded systems

Pure Ethernet MAC frame MACsec can be encoded for embedded networking protocols

- CiA 620 today supports CAN FD
- Other protocols could by supported with the same concept

MACsec can be used as an end-to-end security transport layer over diverse networks

- CiA 620 encoded CAN FD frames decode back to the original Ethernet MAC frame
- Nodes do not need to be aware of the underlying communications protocol
- Multi-drop MACsec issues are inherent to multi-drop (e.g. apply to 10BASE-T1S)

MACsec can be used as a security transport layer with non-Ethernet networks

- CiA 620 is equally applicable to pure CAN FD networks
- MACsec can secure application payloads directly
- MACsec can secure encapsulated protocols (e.g. via IEEE 1722)