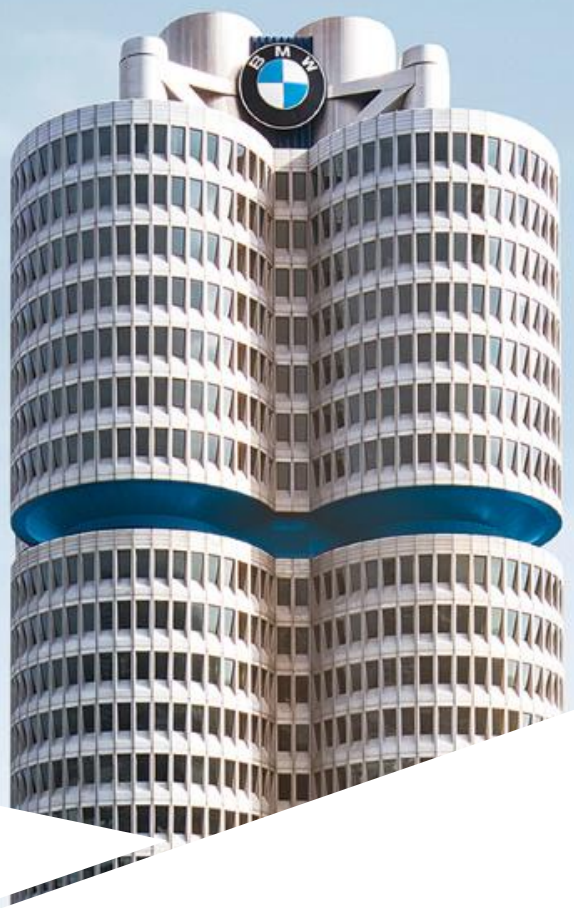
COMPARING AUTOMOTIVE NETWORK SECURITY FOR DIFFERENT COMMUNICATION TECHNOLOGIES.

AUTOMOTIVE ETHERNET CONGRESS 2018.



Dr. Lars Völker.
2018-01-31.

BMW GROUP THE NEXT 100 YEARS

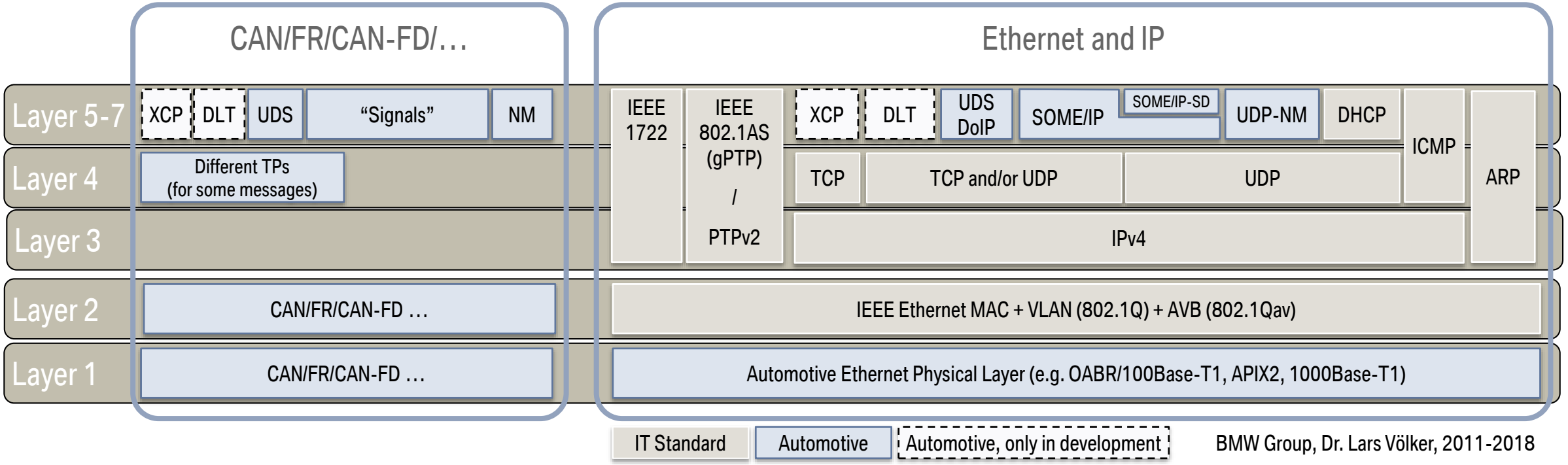
MOTIVATION.

IS THERE A DIFFERENCE IN THE LEVEL OF SECURITY THAT DIFFERENT COMMUNICATION TECHNOLOGIES CAN ACHIEVE?

Disclaimer: I will focus on protecting in-vehicle communication.

INTRODUCTION.

CLASSIC BUS SYSTEMS VS ETHERNET AND IP-BASED SYSTEMS.



Selected additional differences:

- Ethernet is a network and therefore scales over different speeds, which can be mixed and matched.
- Ethernet allows with line speed multiport bridges (Switches) with various features (e.g. frame filtering).
- Ethernet allows line speed virtualization via IEEE 802.1Q VLANs.
- IP allows global connectivity and routing.
- Ethernet and IP are used everywhere and have an extremely well supported eco system.

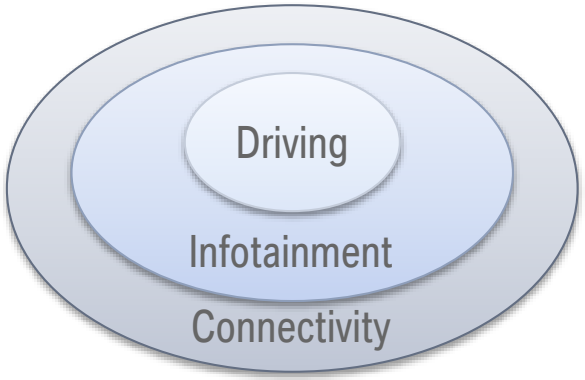
PROBLEMS, PROPERTIES, AND CRITERIA.

- Separation and Isolation.
- Bandwidth, Message size, and Overhead.
- Key Exchange and Startup.
- Multicast and Broadcast Communication.
- Placement of Security within the Stack.

SLICING THE ELEPHANT.
NETWORK ARCHITECTURE FOR SEPARATION OF DOMAINS.

- In-vehicle communications, different domains meet: Backend Connectivity, Infotainment, Autonomous Driving, …
  - In security design you try to separate different parts to reduce attack surfaces, e.g. by separating vehicle domains.

- Separation on CAN/FR/CAN-FD:
  - Increasing the number of busses (e.g. 10 CANs, 2 CAN-FDs, 1 FR) + use gateways.
  - The theoretical optimum: Multiple gateways + minimum number of devices per bus (2).
    - This basically means you emulate a point-to-point system.
    - This allows to filter on gateways.

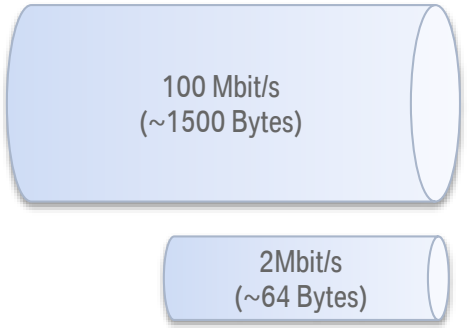


- Ethernet:
  - The network topology and the placement of Ethernet Switches is critical.
  - VLANs and line-speed filtering helps a lot.

- Authentication of traffic can somewhat achieve the separation as well.

BANDWIDTH, MESSAGE SIZE, AND OVERHEAD. DO THEY MATTER FOR MESSAGE AUTHENTICATION?

- Standardized state-of-the-art security solutions protect communications by adding to the messages:
  - 12-16 Bytes for the Integrity Check Value (ICV).
  - 6 Bytes for the Initialization Vector (IV)/Freshness.



- Ethernet:
  - Easy, you have 1500 Byte packets. If you are smart, you leave room for security by using a less than 1500 bytes.

- CAN-FD:
  - Shortening of ICV reduces security – you want to avoid this. Too short and brute force attacks are feasible. ☹
  - Shortening of Freshness to 1-2 Bytes? Basically possible since CAN-FD is rather slow.
  - Overhead of 16 Bytes would mean 25% of a 64 Bytes CAN-FD payload is already used!

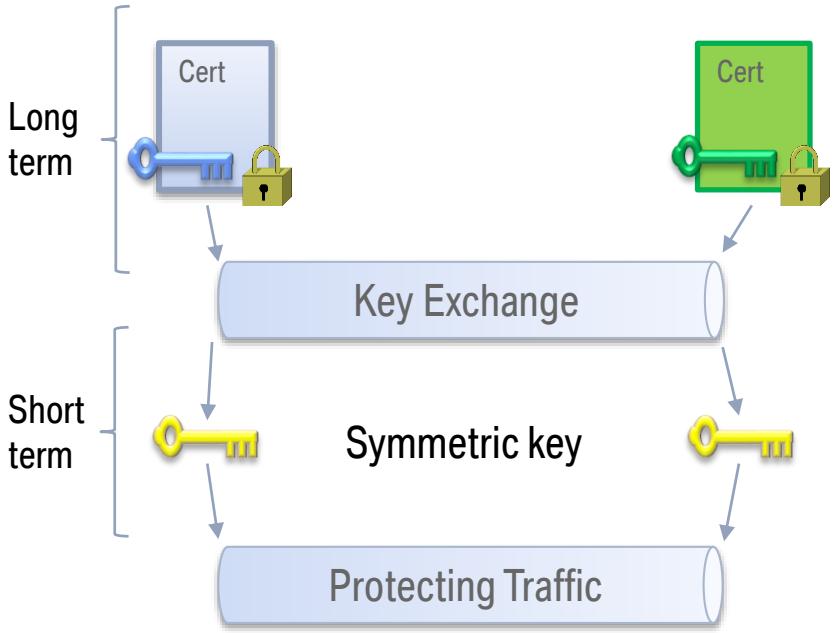
- Classical CAN:
  - Need to shorten the ICV (reduced security) or using TP (possibly reducing robustness).

KEY EXCHANGE.
STARTING UP IS DIFFICULT.

- For high security, you want to protect the traffic with short term symmetric keys.
  - Those are exchanged via long-term asymmetric keys.

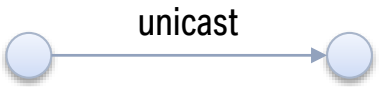
- Challenges:
  - Additionally messages at startup needed – the slower your bus, the longer it takes.
  - The more ECUs you talk to, the more to exchange.
  - Key Exchange is challenging (see SSL/TLS bugs). A well understood solution is best.

- What does that mean?
  - For CAN, FR, CAN-FD: use static keys or build something yourself.
  - For Ethernet and IP-based: state-of-the-art solutions exist.

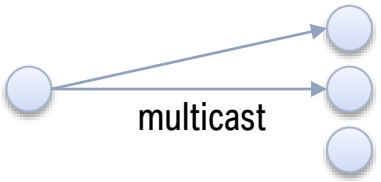


PROTECTING MULTICAST COMMUNICATION AND GROUP KEYS.

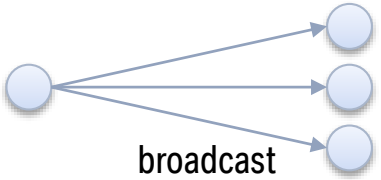
- How to protect the Multicast traffic on Ethernet and CAN? Broadcast?



- For performance reasons symmetric algorithms are used to protect messages (e.g. AES).
- For group communication, we need group keys:
  - Problem 1: Distribution of group keys is not a trivial problem.
  - Problem 2: Trust in group keys is rather difficult (“receiver” can impersonate sender).

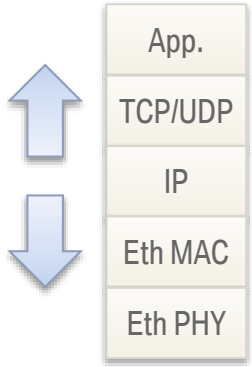


- Solutions:
  - Avoid Problem 1+2 by protecting link-based (MACsec).
  - Use static symmetric keys to avoid Problem 1 (generic, e.g. SecOC).
  - Use key master to distribute keys on startup (reduced security and performance!)
  - Use special crypto hardware to reduce Problem 2.
  - Use a lot of keys (and more hardware) to reduce Problem 2.



ON WHICH LAYER DO YOU PROTECT YOUR COMMUNICATION?

- Network Security can be implemented on different layers:
  - Application-based solutions can supply very specific security. E.g. different key for different SOME/IP message.
    - The higher, the more differentiated the solution can process packets.
    - Better against internal attackers, when used for separation/isolation.
  - Security solutions on lower layers can protect more messages with less associations and cover “helper” protocols like ICMP.
    - The lower, the more traffic is covered.
    - Better against external attackers.



- For maximum Network Security combine:
  - Network Security on low layer to make it hard for external attacker.
  - Solution to increase strong separation for needed use cases to make it hardware for internal attacks.

- For CAN/FR/CAN-FD the number of options is very limited due to the simple communications stack.

COMPARISON AND CONCLUSION

COMPARISON

		Auth? Enc?	Multicast Broadcast	100% protected?	# of keys?	Dyn. Keys?	Minimum Overhead	Selector	Implementation	Config Complexity
Ethernet	MACsec	Yes/Yes	Yes	Yes	Lowest	Yes	~2%	L1/L2	State-of-the-art **Hardware** + Software	Low
	IPsec	Yes/Yes	No	No	Low	Yes	~2%	L3 + L4	State-of-the-art Software	Low-Medium
	(D)TLS	Yes/Yes	No	No	Medium	Yes	~2%	L4 only	State-of-the-art Software	Low-Medium
	SecOC Eth	Yes/*1	somewhat possible	No	High	*2	~2%	Depends	New Software + *4	High
CAN …	SecOC CAN	Yes/*1	somewhat possible	somewhat possible	High	*2	**~100%** *3 *5	ID	New Software + *4	High
	SecOC CAN-FD FR	Yes/*1	somewhat possible	somewhat possible	High	*2	~25% (CAN-FD)	ID	New Software + *4	High

*1 Possible to integrate in standard
*2 No standardized solution exists.
*3 Only reduced security.
*4 Additional new Hardware might be needed to reduce group key trust limitations.
*5 Avoiding TP due to Safety reasons.

CONCLUSION

Communication Technologies:

– Ethernet supports a wide-range of security solutions, most of them designed for the Internet.
– For Ethernet MACsec allows to protect all packets.
– Classic CAN is very limited on Network Security due to low bandwidth and message size.
– CAN-FD as migration technology allows to increase the Network Security somewhat. Achieving a similar level of Security as Ethernet will be expensive and very hard to achieve.

Use Cases:

– New use cases and applications requiring higher Security.

For use cases and applications with higher security needs, Ethernet is the better alternative:

→Lets look into rolling out MACsec as the best Ethernet Security solution!

→Lets create a competitively priced Ethernet solution to replace classical busses!

THANK YOU FOR YOUR ATTENTION.

Bayerische
Motoren Werke
Aktiengesellschaft

BMW GROUP

Dr. Lars Völker
Diplom-Informatiker

Electronics
Security Architecture, Security Management

Postal Address
BMW AG
80788 Munich
Street Address
Max-Diamant-Str. 25

Phone +49-89-382-31429
Mobile +49-151-601-31429
E-Mail Lars.Voelker@bmw.de

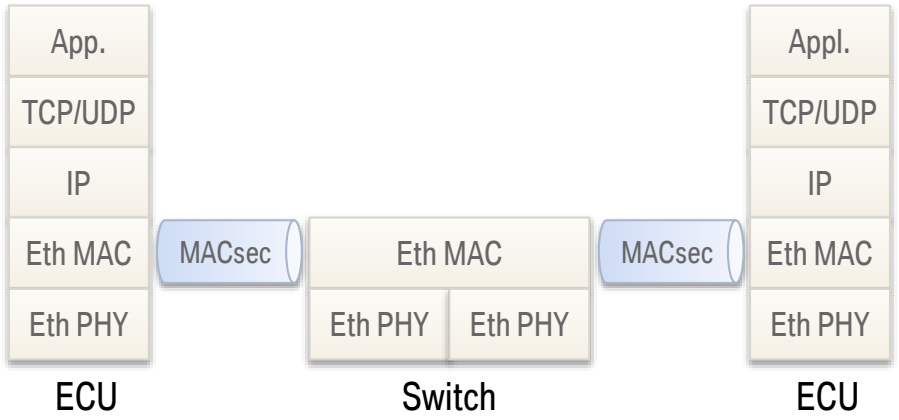
BACKUP: NETWORK SECURITY SOLUTIONS

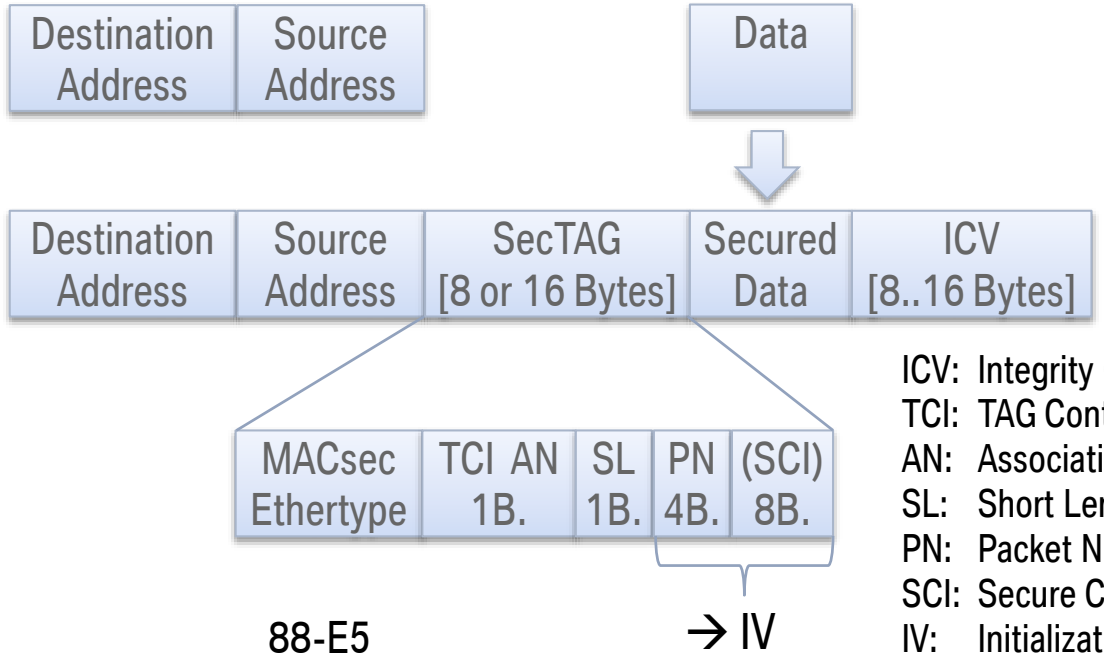
SECURITY ON LAYER 2
IEEE 802.1AE MACSEC

- MACsec protects on layer 2.
  - Encryption and Authentication: supported.
  - Authentication only: supported.

- Pros:
  - Protects all traffic.
  - Configuration: easy.
  - Minimum number of keys.

- Cons:
  - Difficult if some messages are not to be protected (e.g. for setup and configuration).
  - Requires hardware support



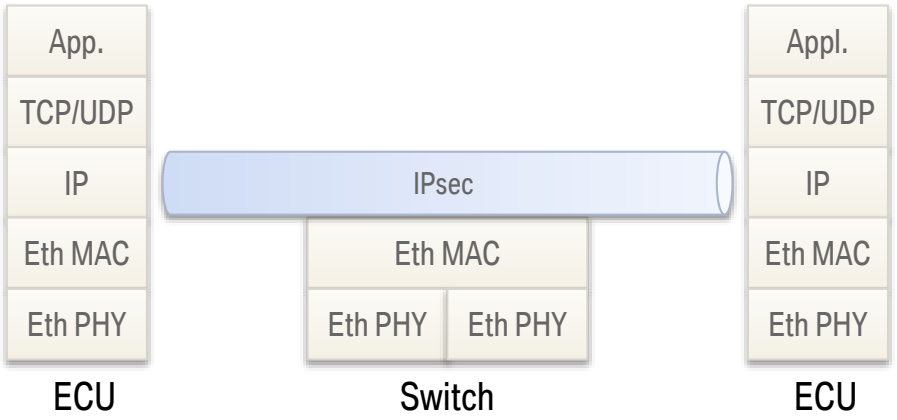


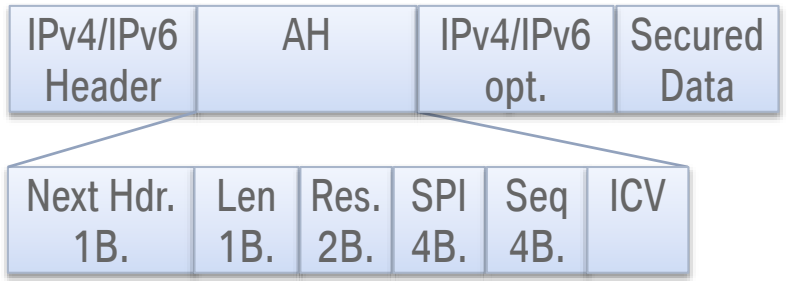
ICV: Integrity Check Value
TCI: TAG Control Information
AN: Association Number [2 bit]
SL: Short Length [6 bit]
PN: Packet Number
SCI: Secure Channel Identifier
IV: Initialization Value

SECURITY ON LAYER 3
IETF IPSEC (RFC 4301, …)

- IPsec protects on layer 3.
  - Encapsulating Security Payload (ESP).
    - Encryption and/or Authentication.
  - Authentication Header.
    - (Transparent) Authentication.

- Pros:
  - Can protect based on IPs and Port numbers.
  - Configuration: easy-medium.
  - Sym. keys per peer.
  - Easy to use hardware crypto.
- Cons:
  - No multicast, no broadcast.





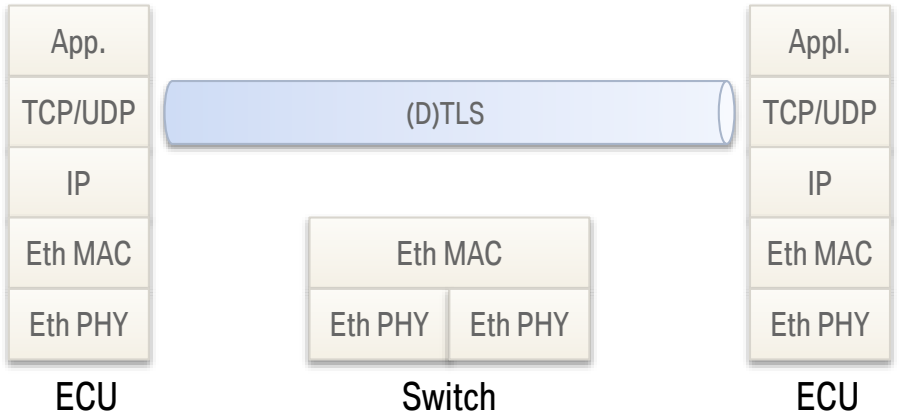
SPI: Secure Parameter Index
Seq: Sequence Number (~IV)
Pad: Padding
Pad.Len.: Length of Padding
ICV: Integrity Check Value
Len: Length
Res: Reserved (0x00)

SECURITY ON LAYER 4
IETF TLS / IETF DTLS

- TLS runs on TCP and protects the TCP connections data.
- DTLS runs on UDP and protects data over UDP association.

- Pros:
  - Well-known and used everywhere (TLS).
  - Configuration: easy-medium (because per connection).
  - Sym. keys per connection.
  - Application specific security possible.

- Cons:
  - Security of implementations still somewhat limited.
  - Overhead due to many connections.
  - Somewhat complicated to use hardware crypto.



SECURITY ON LAYER 7 OR CAN SECURE ON-BOARD COMMUNICATION

- SecOC is an application specific solution.

- Pros:
  - Very flexible for new applications/messages.
  - Can support classic busses.

- Cons:
  - New standard.
  - Can be very hard to retrofit.
  - No Open Source implementations.
  - Key Exchange not standardized.
  - Massive numbers of keys.