

CAN Secure

Alejandro Cervantes

Automotive FAE

October 2019 | Session #AMF-AUT-T3873



SECURE CONNECTIONS
FOR A SMARTER WORLD

Agenda

- What is Security
- Connectivity Mega Trends
- CAN Bus Threads
- Technologies and Standards
- Implementations and Solutions



What is Security?

First Things First



Secure System Definition

Functional Security Design Goals Definition

Trustworthy System definition:

A Trustworthy system is a system which does what its stakeholders expect it to do, resisting attackers with both remote and physical access, else it fails safe.

Security Enabled SoCs will provide OEM controlled silicon features which simplify the development of trustworthy systems.

- Security features are an opt in scheme

- OEM controlled trade-offs in cryptographic strength

- Debug visibility


- Sensitivity of tamper detection

- Anti-cloning mitigation

What is Security?

- Security is a **quality aspect**...
 - Attackers should not be able to bring down the proper operation of a system
- ...in an **uncontrolled** and **evolving environment**
 - Attackers do not obey to “the rules”
 - Attack(er)s only get better over time
- Security must be an **integral part of the system design**
 - Security is as strong as the weakest link → point solutions usually don't work
 - Secure by design vs. security as an afterthought
- System security solutions are (usually) **custom-made**
 - Different use cases & architectures may (will) require different security solutions
 - But they often use **generic building blocks**
- **100% secure** (or safe) **does not exist** in the real world
 - The challenge is to find the right balance between risk and protection (cost)

**Security is a
quality aspect.**

A photograph of a terminal screen displaying an error message. The screen is black with white text. The text reads: "WE REGRET THAT THIS TERMINAL IS TEMPORARILY OUT OF SERVICE". The terminal has a keypad below the screen and several indicator lights on the sides.

WE REGRET THAT THIS
TERMINAL IS TEMPORARILY
OUT OF SERVICE

**Attackers should
not be able to
bring down the
proper operation
of a system.**

An aerial photograph of a road with a large pothole. A car is driving through the pothole, and the road surface is heavily damaged and uneven. The text 'Security is as strong as its weakest Link.' is overlaid on the top part of the image.

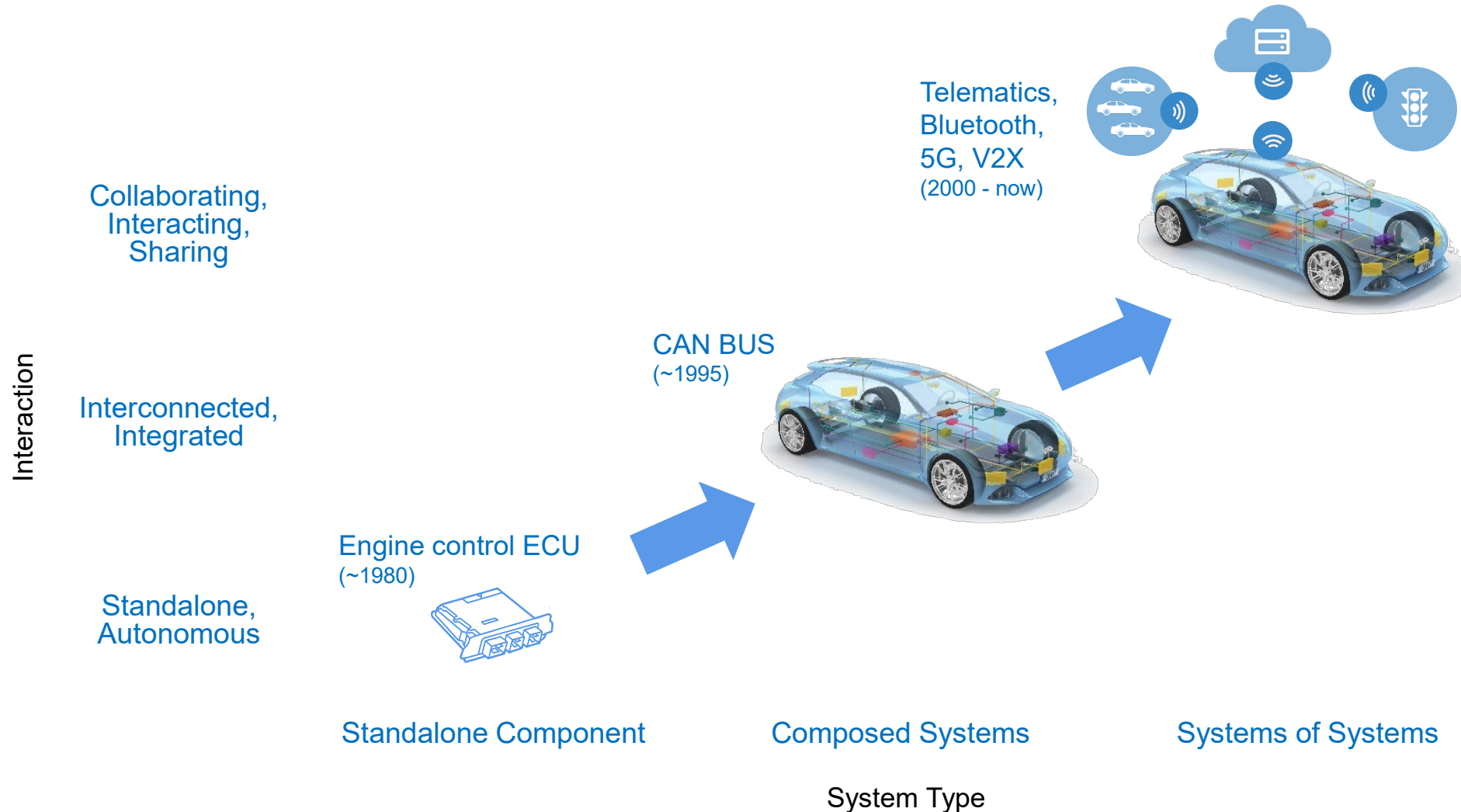
**Security is as
strong as its
weakest Link.**

**...it must be an
integral part of
system design.**

Why Now?



History: Vehicle Electronics & Connectivity



Cybersecurity Threats in Automotive



Local Attacks

Tampering the odometer



<https://www.nhtsa.gov/equipment/odometer-fraud>

Engine tuning



Workshop around the corner, or in your garage

Vehicle theft by relay attack



<https://www.youtube.com/watch?v=8pfcngJJq0>

Ransom for a drive

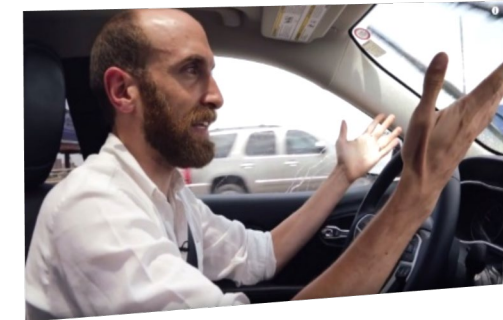


VDI Conference on IT Security for Vehicles (Berlin / July 2017)

Remote Attacks



Remote hack of an unaltered car (July 2015)



<https://www.youtube.com/watch?v=MK0SrxBC1xs>

Mega Trends Force Vehicle Architecture Transformation

Today: Flat



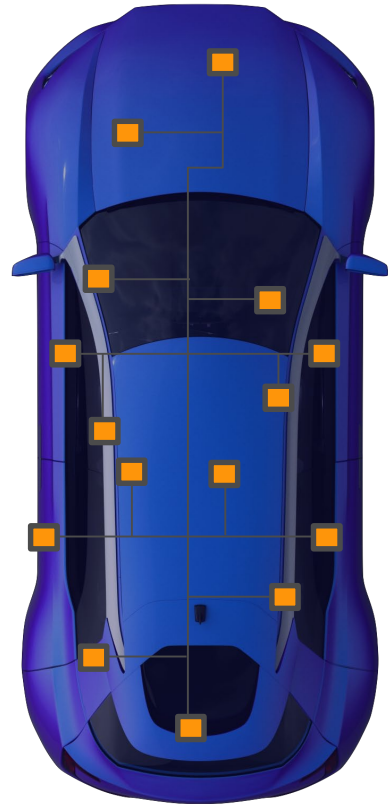
Flat to hierarchical

Tomorrow: Domains



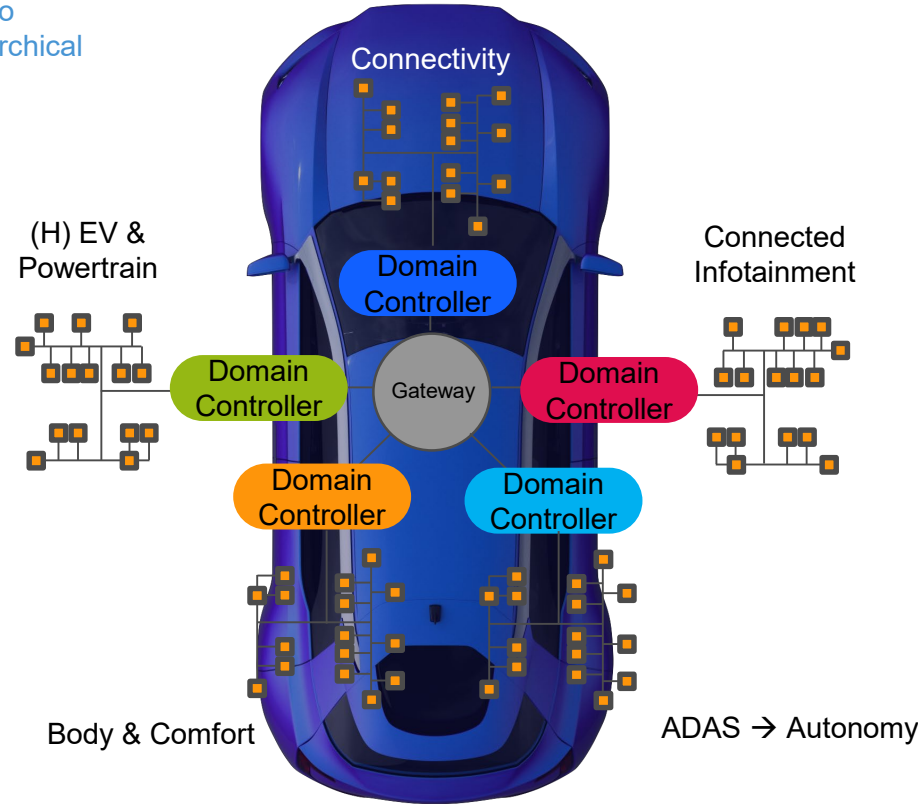
Wires go virtual

After Tomorrow: Zones



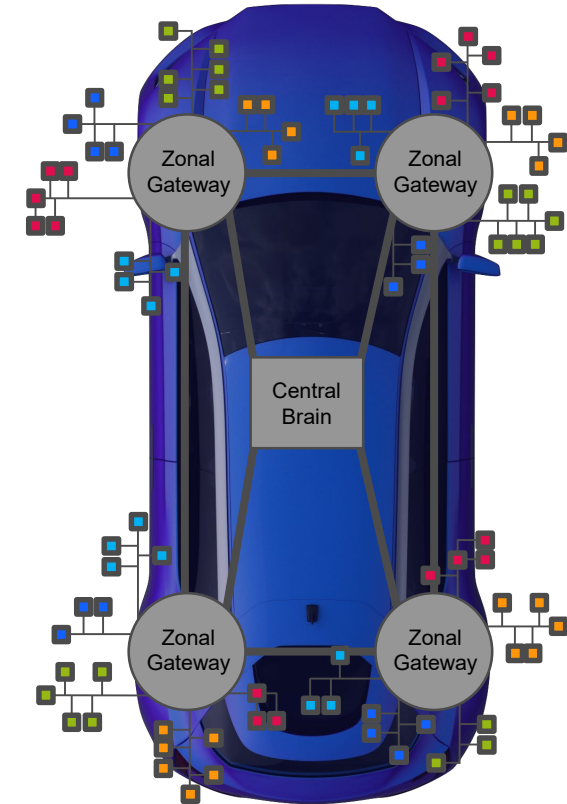
Low bandwidth, flat network
One MCU per application

Unfit for future mobility



High bandwidth network
Gateway key to communication between domains

Step to autonomous car



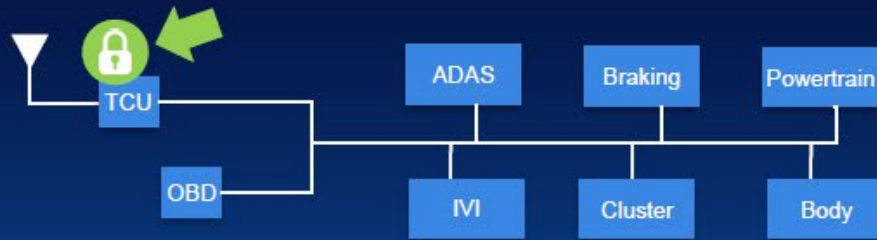
Domains virtualized by SW – enabling high flexibility
Easy enable/disable or update functions

Step to user-defined car

4 Layers to Securing a Car

Layer 1: Secure Interface

Secure M2M authentication, secure key storage



Layer 2: Secure Gateway

Domain isolation, firewall/filter, centralized intrusion detection (IDS)



Layer 3: Secure Network

Message authentication, filtering, distributed intrusion detection (IDS)

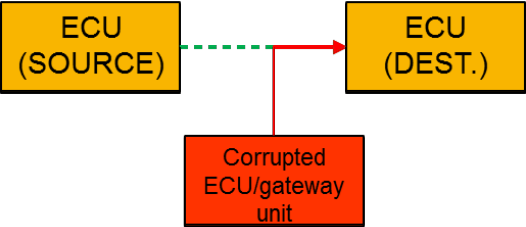
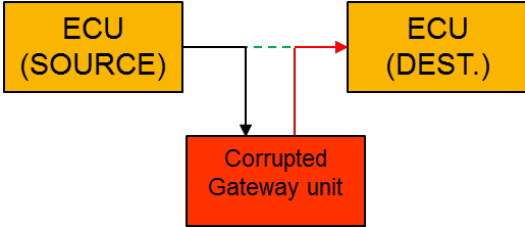
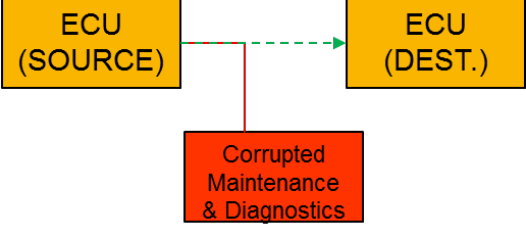
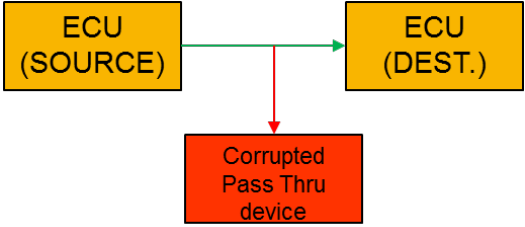
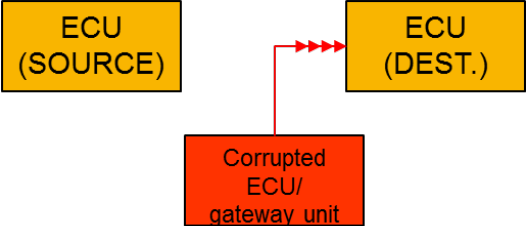
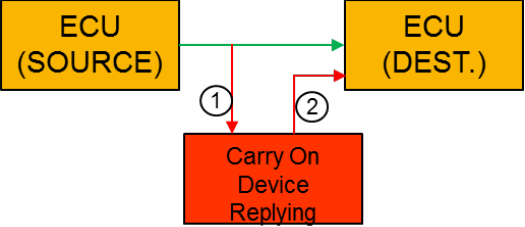


Layer 4: Secure Processing

Secure boot, run time integrity, OTA updates



Expected Types of Threats on the CAN Bus




<p>Spoof (S)</p>  <p>Authentication</p>	<p>Tampering (T)</p>  <p>Data Integrity</p>
<p>Repudiation (R)</p>  <p>Non-repudiation</p>	<p>Information Disclosure (I)</p>  <p>Confidentiality</p>
<p>Denial of Service (D)</p>  <p>Availability</p>	<p>Elevation of Privilege (E)</p>  <p>Authorization</p>

Threat / Security properties

Technologies & Standards



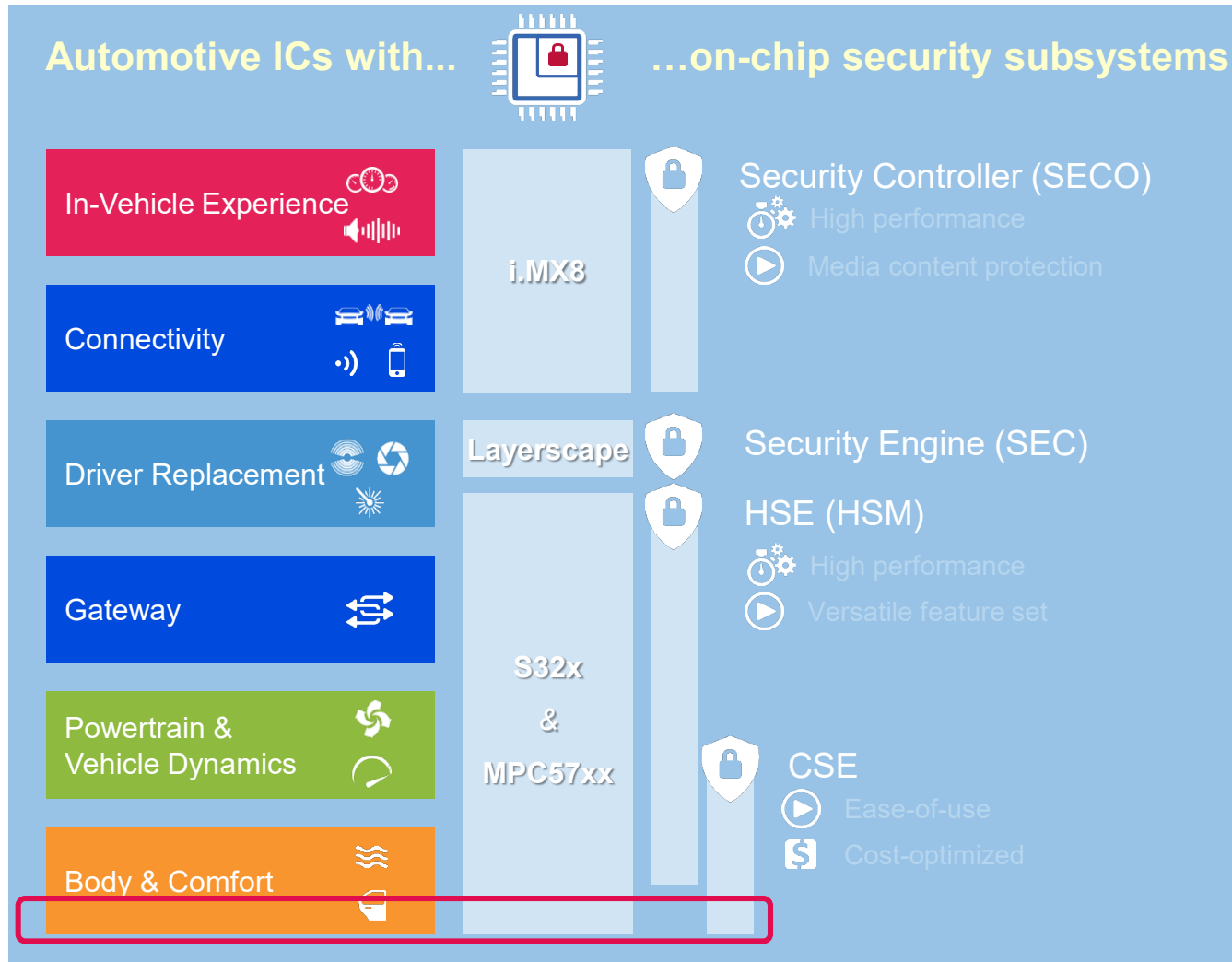
Security Requirements – Today's Landscape

	SHE	EVITA (Light / Medium / Full)	More recent needs
Architecture	<ul style="list-style-type: none"> Configurable, fixed function 	<ul style="list-style-type: none"> Programmable (except EVITA Light) 	<ul style="list-style-type: none"> Acceleration close to the interfaces (CAN and ETH MAC/PHYs) Support for Flash-less technologies
Functionality	<ul style="list-style-type: none"> Secure boot Memory update protocol AES-128 (ECB, CBC) CMAC, AES-MP TRNG, PRNG Key derivation (fixed algorithm) 10+4 keys, key-usage flags 	<p>Same as SHE, plus:</p> <ul style="list-style-type: none"> AES-PRNG monotonic counters (16x, 64bit) <p>Plus, for EVITA Medium and Full:</p> <ul style="list-style-type: none"> WHIRLPOOL, HMAC-SHA1, ECDH and ECDSA (P256) 	<ul style="list-style-type: none"> Further crypto algorithms (e.g. RSA, SHA1-3, Curve25519, ...) Rollback protection Key negotiation protocols Communication protocol offloading (e.g. TLS, IPsec, MACsec, ...) Context separation / multi-application scenarios
Other			<ul style="list-style-type: none"> Increased attack resistance (e.g. SCA, Fault Injection, ...)
Covered by:	<p> CSE family (since 2010)</p> <hr/> <p> HSM family (since 2015)</p> <hr/> <p> HSE family (since 2019)</p>		


Implementations/ Solutions







NXP's Automotive Security Solutions



Security companions

 **Secure Element (SE)**
 Tamper-resistant secure system ideal for M2M authentication (e.g. V2X)

Function-specific secure ICs

-  **Secure CAN Transceiver (TJA115x)**
 - For enhanced IDS & IPS
-  **Secure Ethernet Switch (SJA1110)**
 - Network frame analysis (L2/L3/L4)
-  **Secure Car Access ICs**
 - For advanced RKE / PKE solutions
-  **V2X DSRC Baseband (SAF5x00)**
 - Ultra-fast ECDSA verifications

S32K144 Block Diagram

High performance

- ARM Cortex M4F up to 112MHz w FPU
- eDMA from 57xxx family

Software Friendly Architecture

- High RAM to Flash ratio
- Independent CPU and peripheral clocking
- 48MHz 1% IRC – no PLL init required in LP
- Registers maintained in all modes
- Programmable triggers for ADC no SW delay counters or extra interrupts

Functional safety

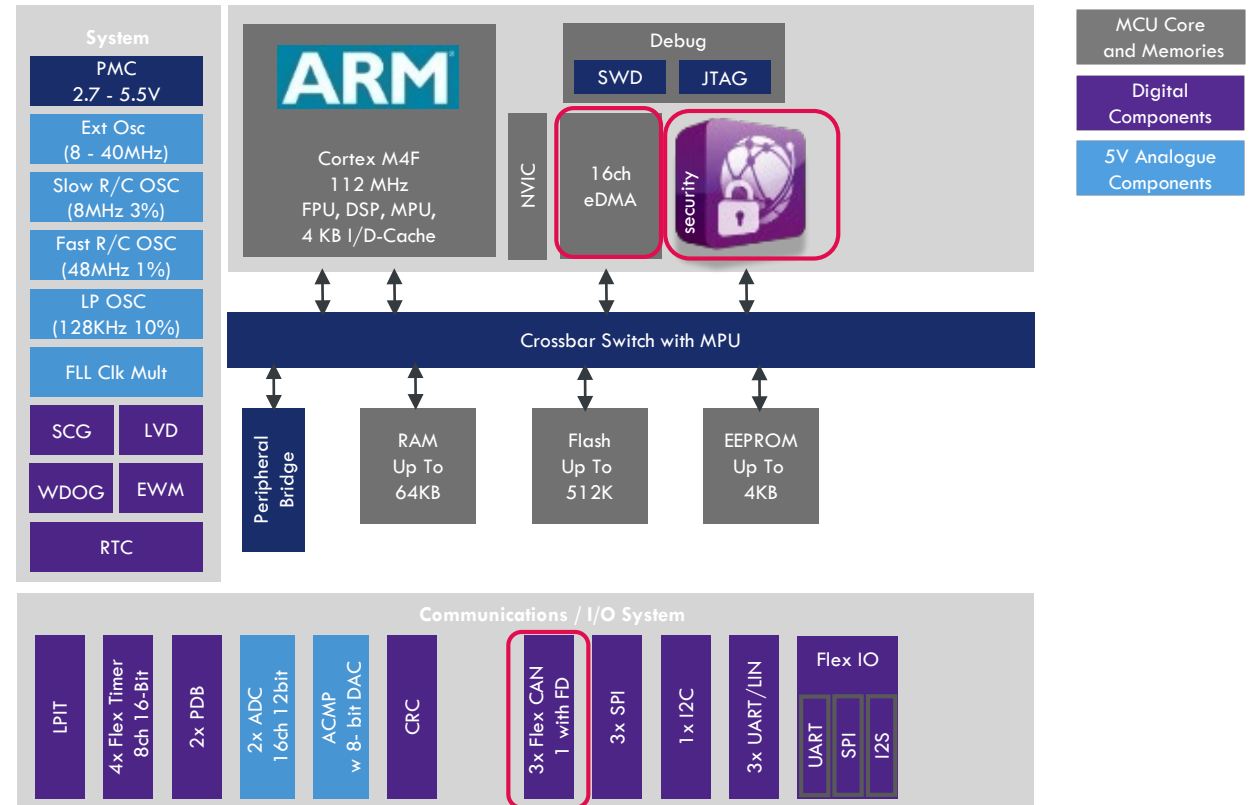
- ISO26262 support for ASIL B or higher
- Memory Protection Unit, ECC on Flash/Dataflash and RAM
- Independent internal OSC for Watchdog
- Diversity between ADC and ACMP, SPI/SCI and FlexIO
- Core self test libraries
- Scalable LVD protection, CRC

Low power

- Low leakage technology
- Multiple VLP modes and IRC combos
- Wake-up on analog thresholds

Security

- CSEc (SHE-spec)



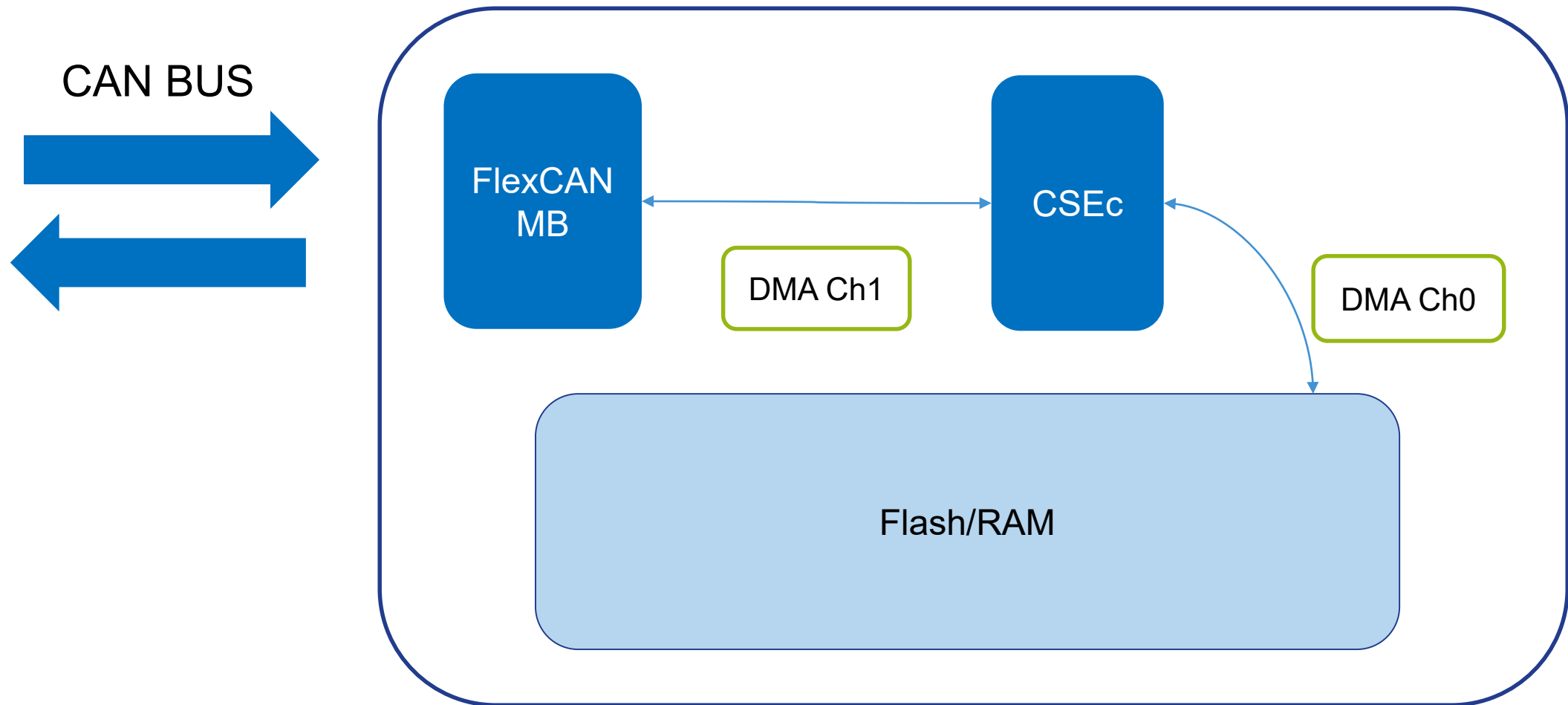
Operating Characteristics

- Voltage range: 2.7V to 5.5V
- Temperature (ambient): -40°C to +125°C

Packages & IO

- Open-drain for 3.3 V and hi-drive pins
- Powered ESD protection
- Packages: 100 BGA, 64 LQFP, 100 LQFP

Secure CAN (FlexCAN + DMA+ CSEc)

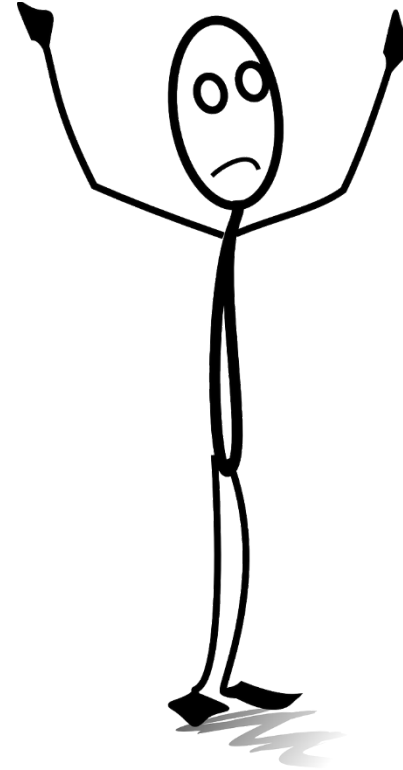


S32K Security Module (CSEc) – PRAM

- 128 bit (16 bytes) SRAM with 8 x128 bit (16 bytes) pages.
- Command header must be las data written
- Write to the command header locks PRAM.

Bits	[127:0]															
Bits	31:2 4	23:1 7	15:8	7:0	31:2 4	23:1 7	15:8	7:0	31:2 4	23:1 7	15:8	7:0	31:2 4	23:1 7	15:8	7:0
WD	Word 0				Word 1				Word 2				Word 3			
	Byte															
Page	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	FUN ID	CM D FOR MAT	CALL SEQ	KEY ID	ERROR BITS	COMMAND SPECIFIC I.E. PAGE LENGHT										
1	DATA INPUT OR OUTPUT FROM CSEc															
2																
3																
4																
5																
6																
7																

Encryption or Authentication?

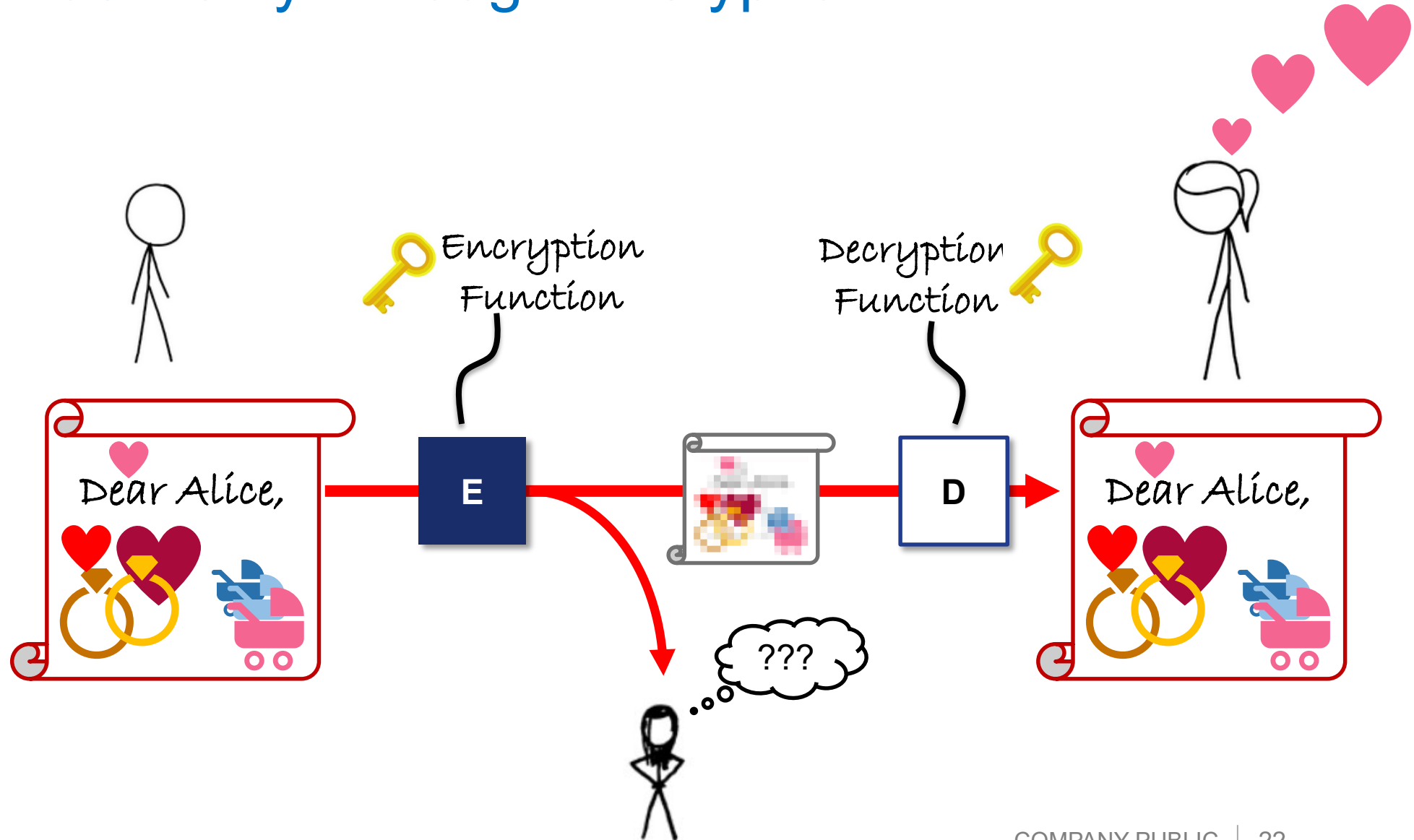


Communication Example

Objective: Bob wants to transmit a message to Alice, without Eve reading it...



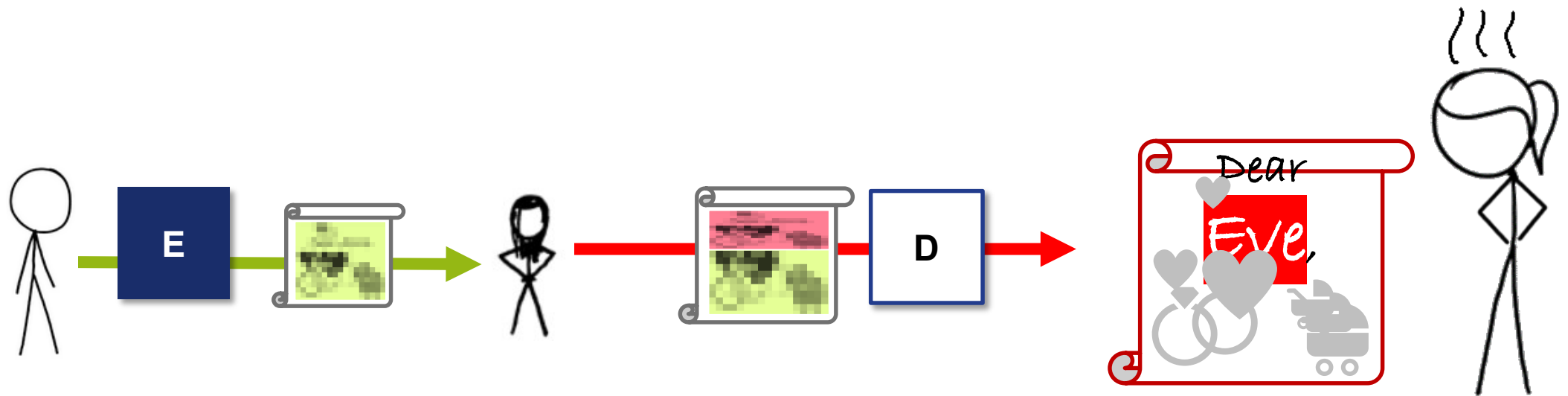
Confidentiality Through Encryption



Eve Just Got Smarter...

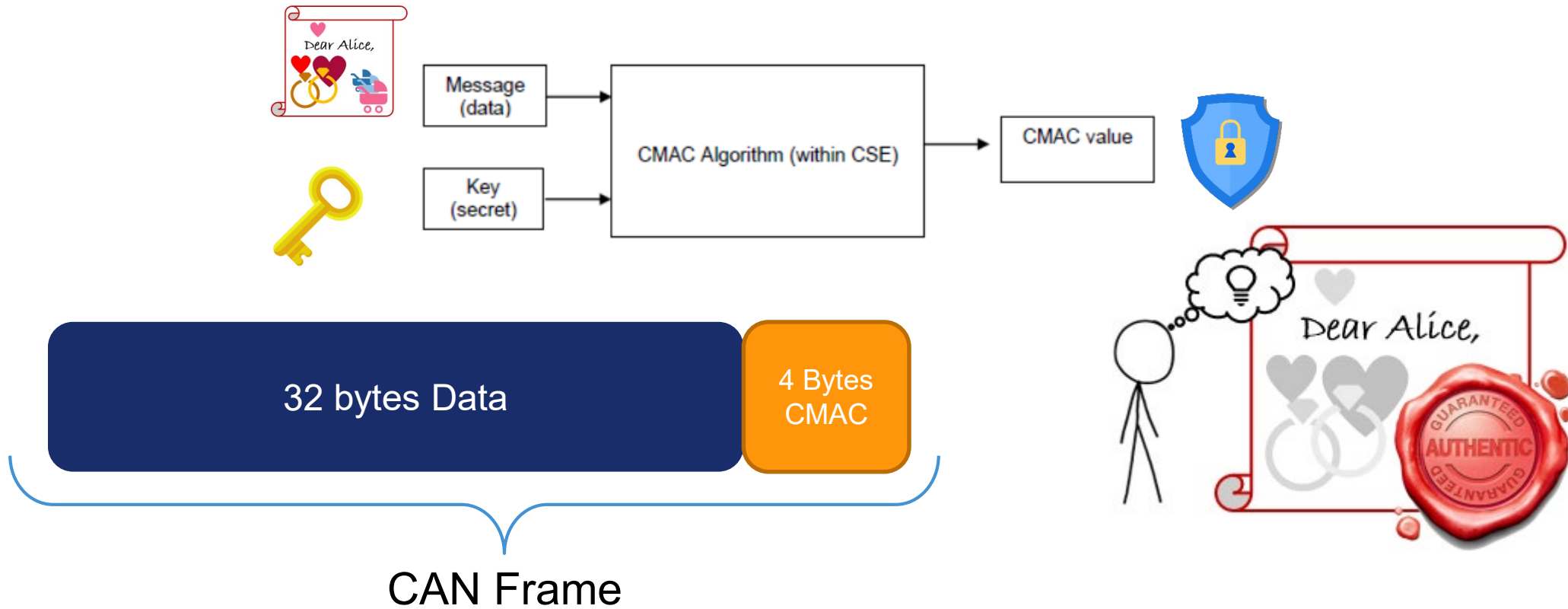
Eve observed several messages exchanged between Alice & Bob and noticed certain recurring **patterns** in the ciphertext...

What if Eve could alter the ciphertext to her advantage?

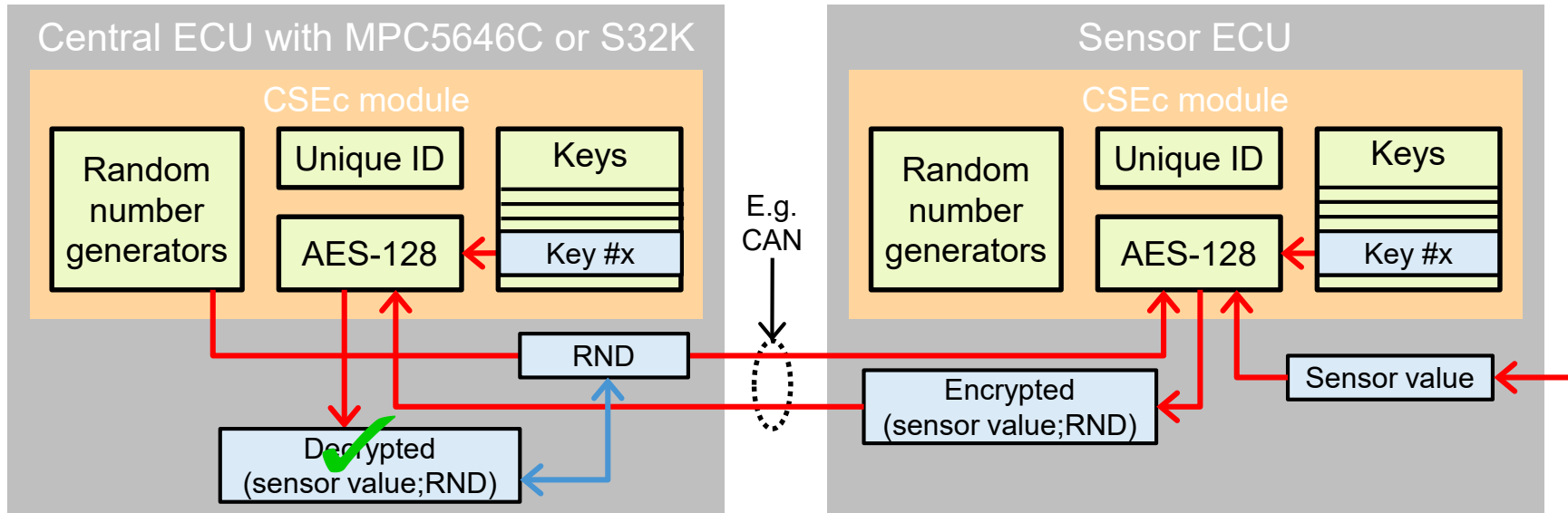


CMAC Generation

MAC = message authentication code
MACs are used for data authentication
Cipher key is the “identifier”, only the secret owner can produce the right CMAC for a given message



Secure Communication

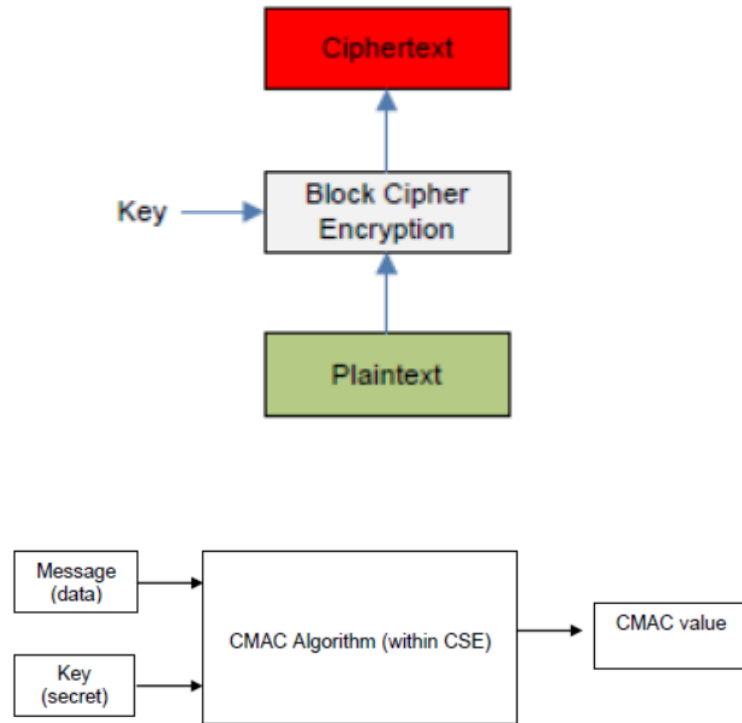


- Step 1: Central ECU obtains random number and sends it to sensors ECU (e.g., after power-on of car)
- Step 2: Sensor ECU reads sensor value and asks CSE module to encrypt it and the received random number (using key #x)
- Step 3: Sensor ECU sends encrypted message to central ECU.
- Step 4: Central ECU asks CSE module to decrypt received message (using key #x).
- Step 5: Central ECU checks sent random number vs. received/decrypted random number.

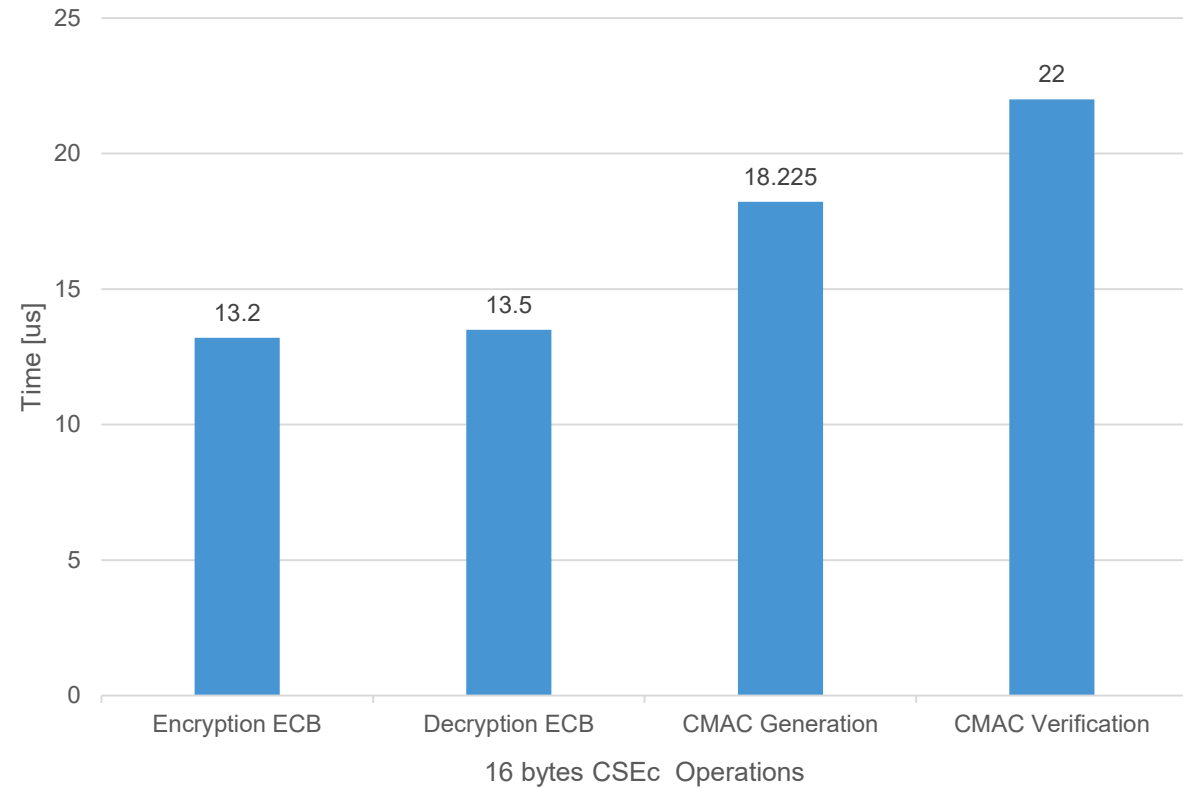
- Random number: protects against replay attacks.
- Encryption: protects against eavesdropping.
- Random number and encryption: ensures data integrity and authenticity.



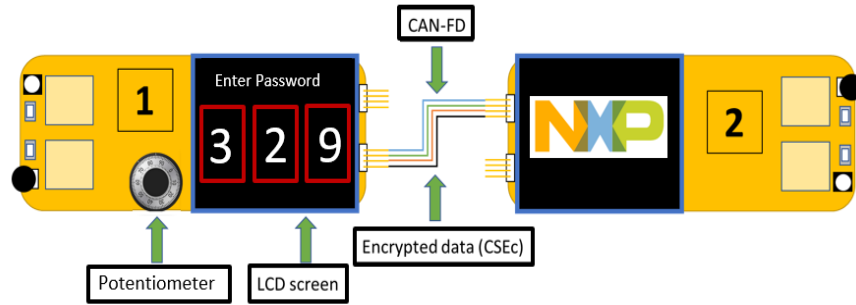
CSEc Performance



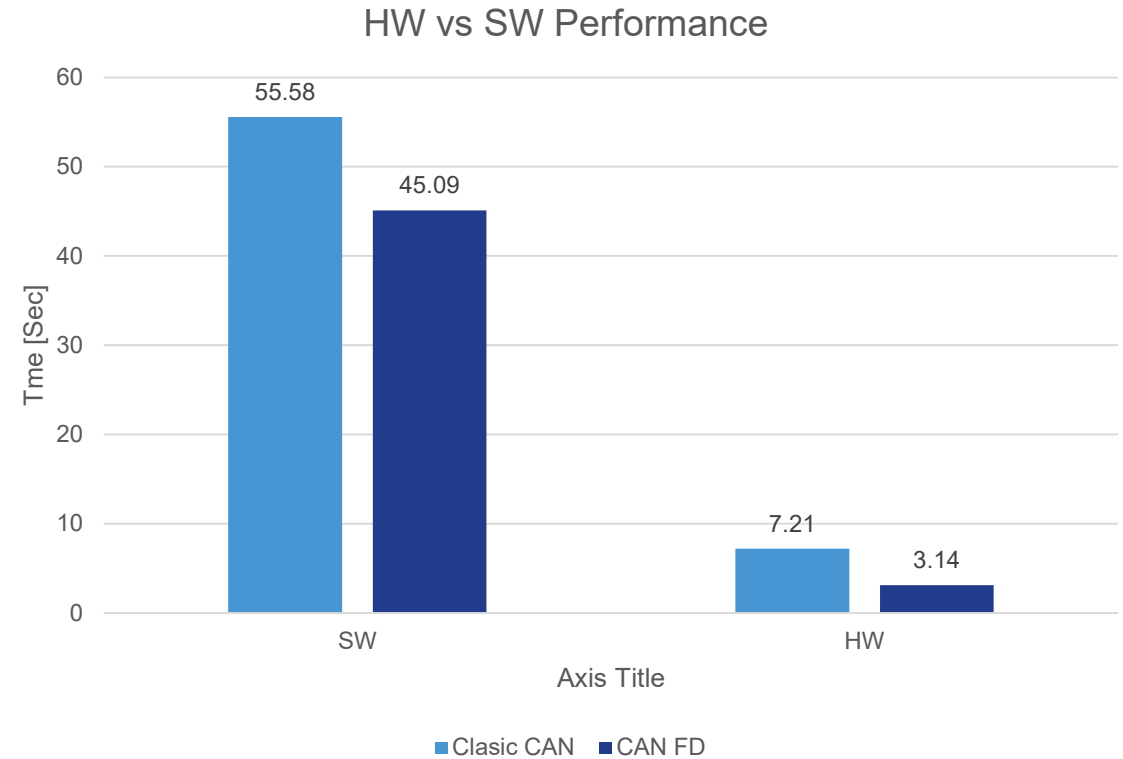
CSEc Timing



HW(CSEc) vs. SW Performance



- Board 1 sends a 73KBytes encrypted image, which is decrypted by board 2
- Decryption by HW improves ~1500% with CAN-FD





**SECURE CONNECTIONS
FOR A SMARTER WORLD**