

Automotive ECU

Secure CAN Communication

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644080."



SAFURE

SAFety and secURity by

dEsign for interconnected mixed-critical cyber-physical systems

Magneti Marelli PWT

HiPEAC

22th January 2017

Manchester (UK)

Automotive Demonstrator

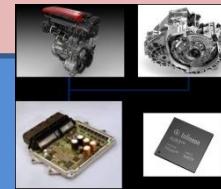
SAFURE FRAMEWORK

Modelling &
integrity
algorithms



Run-time
Systems

Automotive
multi-core
Dem
Powertrain multicore ECU
with **hard real-time**,
safety, and **security**
requirements. Function
consolidation to reduce
costs, complexity, and
time-to-market



SAFETY

SECURITY



Powertrain Multicore ECU – technical features

- **Support mixed-critical ECU to reduce cost**
 - Engine Ctrl – Automated Manual Transmission Ctrl
- **Data Protection**
 - Compliancy with ISO-26262
- **OS extensions**
 - Timing and memory protection for *Infineon Aurix SW/FW multicore Architecture and ERIKA OS*
- **Data Integrity on Inter-ECU communications**
 - Prevent attacks through ECU communication channels
- **Timing analysis**
 - Performance and CPU load calculation
 - WCET estimation



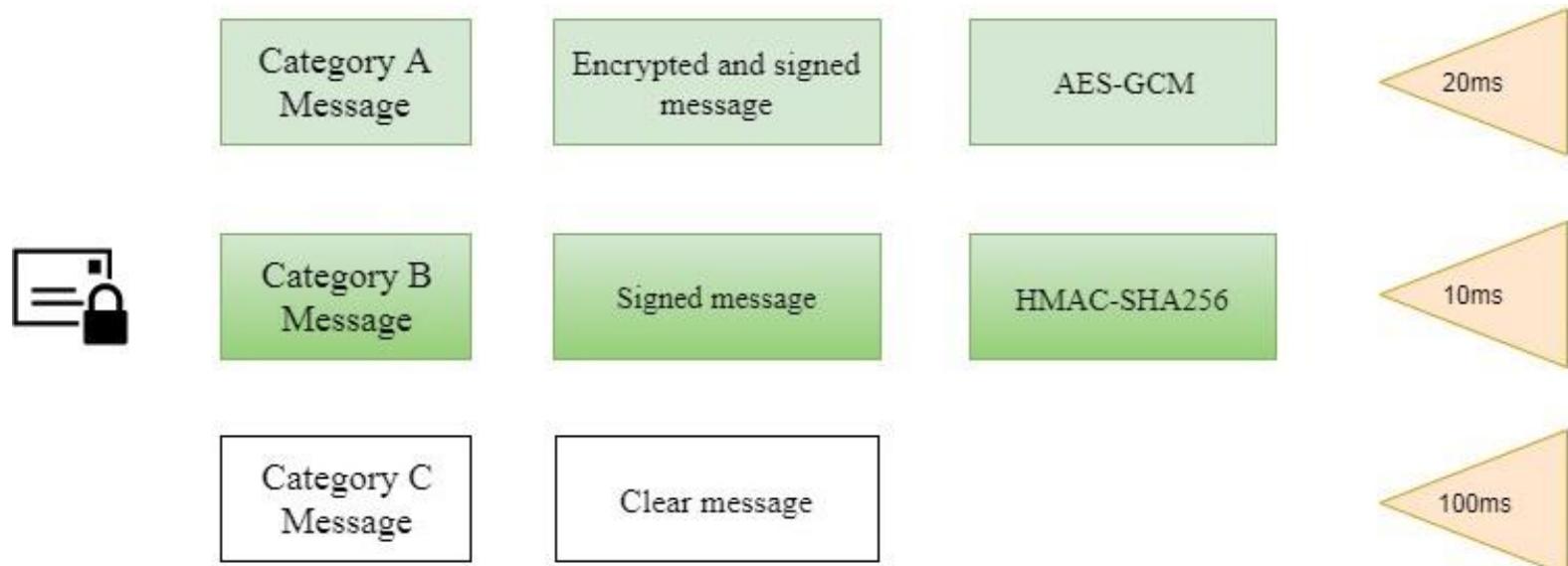
Automotive Multicore ECU – main goals

- **SAFE - Freedom of interferences:** timing protection and memory protection at firmware level – alternative to OS implementation: lower costs
- **SECURE - communication on CAN:** guarantee security requirements
- **Mixed – Criticalities** - Exploitation of Multicore to **reduce the number of control units:** reduction of complexity, costs and time-to-market

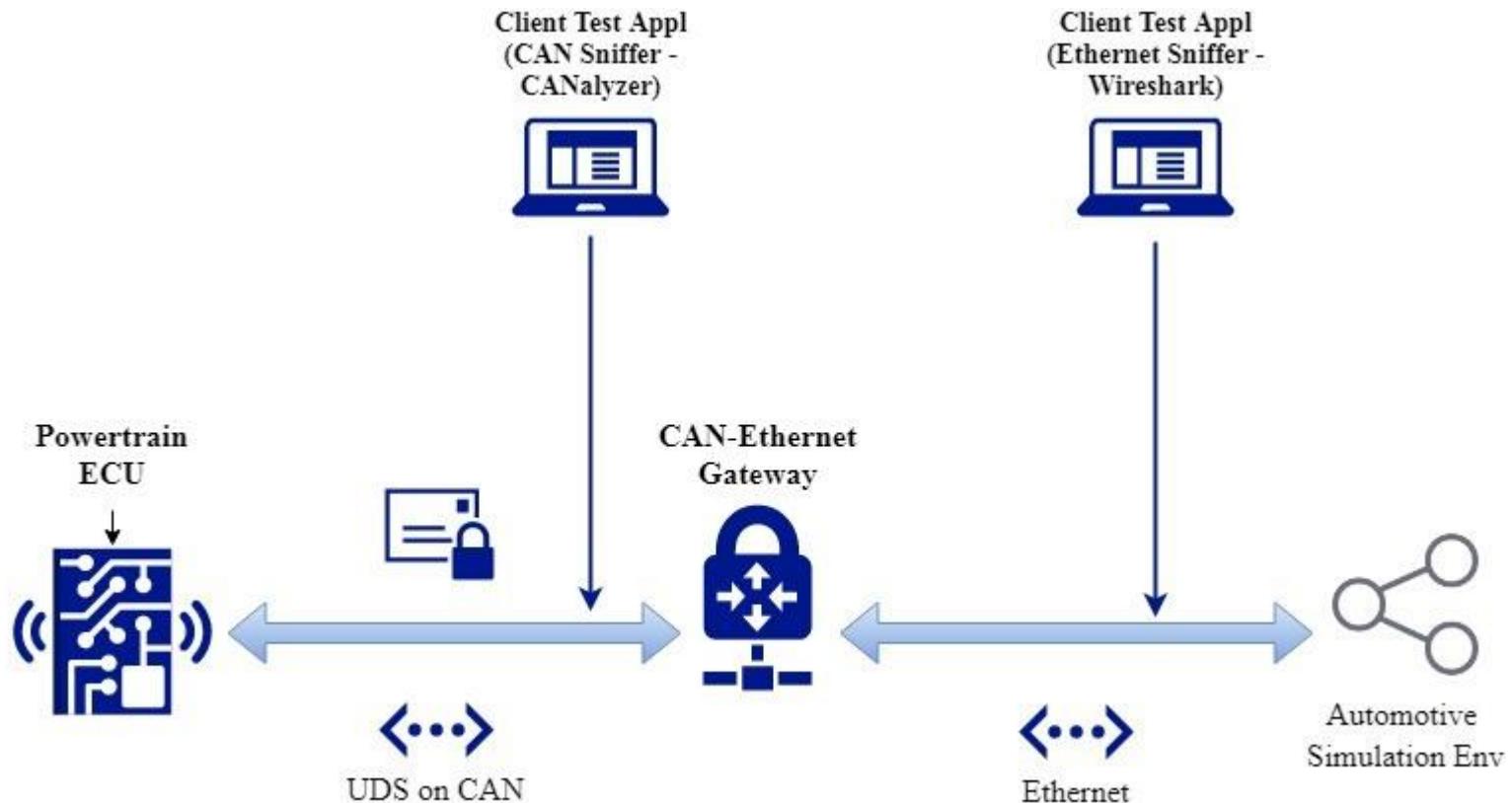
Secure communication details – ECU side

- **Functional classification of messages supported**
- **Cyclic activation (period of 10-20-100 ms)**
- **Error handling implementing**
 - Detection of corrupted messages -> logging and diagnosis activation

Message categories



Communication scenario



Category B Massages TESTS

TEST succeeded

- Emulator view: 4 completed messages transmitted and this is last message



```
B::Var.Watch (on ibol1u18)
Watch View ×

Safure_Motor_11_Buffer = (0x6, 0x0, 0x0, 0x3, 0x4D, 0x41, 0x47, 0xC1, 0x47, 0x9E, 0xFE, 0x96, 0xFD, 0x85, 0xF1, 0x22, 0xEB, 0x4, 0xC1, 0x47, 0x9E, 0xFE, 0x96, 0xFD, 0x85, 0xF1, 0x22, 0xEB, 0x4, 0x48, 0x16, 0x8E, 0x86, 0x64)
Safure_Sign_Buffer = (0xC1, 0x47, 0x9E, 0xFE, 0x96, 0xFD, 0x85, 0xF1, 0x22, 0xEB, 0x4, 0x48, 0x16, 0x8E, 0x86, 0x64)
Safure_MsgCatB_Status = 1 ≈ 1
Safure_MsgCatB_Rx = (0x4, 0x25, 0xE4, 0x55, 0x55, 0x55, 0x55, 0x55)
Safure_MsgCatB_Ready = 1
Safure_MsgCatB_ErrCnt = 0
Safure_MsgCatB_Err = 0 ≈ 0
Safure_MsgCatB_Cnt = 0
Safure_MsgCatB = (0x6, 0x0, 0x0, 0x2, 0x4D, 0x41, 0x47, 0xB0, 0x28, 0x71, 0x52, 0x46, 0x9, 0xAE, 0x7E, 0xE3, 0x10, 0x67, 0x2, 0x1
Safure_Motor_11_FrameCnt = 0
Safure_CntMsg11 = 4
```

Message content on CAN

- ECU (Message ID - A7 -- RX)
- CANalyzer view (Message ID - A7 -- TX)

0.009337	CAN 1 A7	CAN Frame	Rx	8	01 06 00 00 FF 4D 41 47
0.000733	CAN 1 B2	CAN Frame	Tx	8	01 06 00 00 FF 4D 41 47
0.009260	CAN 1 A7	CAN Frame	Rx	8	02 F2 09 16 19 9B 1F B4
0.000678	CAN 1 B2	CAN Frame	Tx	8	02 F2 09 16 19 9B 1F B4
0.009327	CAN 1 A7	CAN Frame	Rx	8	03 6F 4A 79 80 B3 59 58
0.000709	CAN 1 B2	CAN Frame	Tx	8	03 6F 4A 79 80 B3 59 58
0.009295	CAN 1 A7	CAN Frame	Rx	8	04 36 94 55 55 55 55 55
0.000644	CAN 1 B2	CAN Frame	Tx	8	04 36 94 55 55 55 55 55
0.009381	CAN 1 A7	CAN Frame	Rx	8	01 06 00 00 00 4D 41 47
0.000735	CAN 1 B2	CAN Frame	Tx	8	01 06 00 00 00 4D 41 47
0.009258	CAN 1 A7	CAN Frame	Rx	8	02 6D 42 9A F3 EE C5 D6
0.000646	CAN 1 B2	CAN Frame	Tx	8	02 6D 42 9A F3 EE C5 D6
0.009363	CAN 1 A7	CAN Frame	Rx	8	03 DE 11 02 E2 2C 69 BA
0.000719	CAN 1 B2	CAN Frame	Tx	8	03 DE 11 02 E2 2C 69 BA
0.009282	CAN 1 A7	CAN Frame	Rx	8	04 E8 8F 55 55 55 55 55
0.000719	CAN 1 B2	CAN Frame	Tx	8	04 E8 8F 55 55 55 55 55
0.009303	CAN 1 A7	CAN Frame	Rx	8	01 06 00 00 01 4D 41 47
0.000731	CAN 1 B2	CAN Frame	Tx	8	01 06 00 00 01 4D 41 47
0.009262	CAN 1 A7	CAN Frame	Rx	8	02 BD AA D4 F1 2F BD 9D
0.000622	CAN 1 B2	CAN Frame	Tx	8	02 BD AA D4 F1 2F BD 9D
0.009387	CAN 1 A7	CAN Frame	Rx	8	03 9A 86 19 4D B1 1D FE
0.000721	CAN 1 B2	CAN Frame	Tx	8	03 9A 86 19 4D B1 1D FE
0.009284	CAN 1 A7	CAN Frame	Rx	8	04 A3 33 55 55 55 55 55
0.000606	CAN 1 B2	CAN Frame	Tx	8	04 A3 33 55 55 55 55 55
0.009414	CAN 1 A7	CAN Frame	Rx	8	01 06 00 00 02 4D 41 47
0.000721	CAN 1 B2	CAN Frame	Tx	8	01 06 00 00 02 4D 41 47
0.009275	CAN 1 A7	CAN Frame	Rx	8	02 B0 28 71 52 46 09 AB
0.000576	CAN 1 B2	CAN Frame	Tx	8	02 B0 28 71 52 46 09 AB
0.009429	CAN 1 A7	CAN Frame	Rx	8	03 7E E3 1C 67 02 1E 07
0.000723	CAN 1 B2	CAN Frame	Tx	8	03 7E E3 1C 67 02 1E 07
0.009280	CAN 1 A7	CAN Frame	Rx	8	04 25 E4 55 55 55 55 55
0.000584	CAN 1 B2	CAN Frame	Tx	8	04 25 E4 55 55 55 55 55

Message content on Ethernet

- Wireshark view

The screenshot shows a Wireshark capture of network traffic on interface 0. The list of frames shows several ECHO Request and ECHO Response messages between two hosts, 192.168.40.11 and 192.168.40.10. The message content pane highlights the details of Frame 28, which is an ECHO Request from the source host. The packet bytes are shown in hex and ASCII format, with the ASCII output showing the echo data: 000000a70000000802eb4b0e830fc09f.

Frame	Time	Source IP	Destination IP	Protocol	Content
27	0.195177	192.168.40.11	192.168.40.10	ECHO	60 Request
28	0.205197	192.168.40.11	192.168.40.10	ECHO	60 Request
29	0.210167	192.168.40.11	192.168.40.10	ECHO	60 Request
30	0.215180	192.168.40.11	192.168.40.10	ECHO	60 Request
31	0.225194	192.168.40.11	192.168.40.10	ECHO	60 Request
32	0.230161	192.168.40.11	192.168.40.10	ECHO	60 Request
33	0.235148	192.168.40.11	192.168.40.10	ECHO	60 Request
34	0.245084	192.168.40.11	192.168.40.10	ECHO	60 Request
35	0.250036	192.168.40.11	192.168.40.10	ECHO	60 Request
36	0.255065	192.168.40.11	192.168.40.10	ECHO	60 Request
37	0.265052	192.168.40.11	192.168.40.10	ECHO	60 Request

Frame 28: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: TttechCo_00:53:cc (88:23:fe:00:53:cc), Dst: MS-NLB-PhysServer-02_02:02:00:31 (02:02:02:02:00:31)
Internet Protocol Version 4, Src: 192.168.40.11 (192.168.40.11), Dst: 192.168.40.10 (192.168.40.10)
User Datagram Protocol, Src Port: commplex-main (5000), Dst Port: echo (7)
Echo
Echo data: 000000a70000000802eb4b0e830fc09f

0000 02 02 02 02 00 31 88 23 fe 00 53 cc 08 00 45 001.# ..S...E.
0010 00 2c ea 93 40 00 40 11 7e c7 c0 a8 28 0b c0 a8 ..,.@.~....
0020 28 0a 13 88 00 07 00 18 00 00 00 00 a7 00 00 (.....).....
0030 00 08 01 06 00 00 d7 4d 41 47 00 00M AG..

Can side (traces)

- ECU (Message ID - A7 -- RX)
- CANalyzer (Message ID - B2 -- TX)

✉ 0.009407	CA... A7	CAN Frame	Rx	8	8	01 06 00 00 A4 4D 41 47
✉ 0.000731	CA... B2	CAN Frame	Tx	8	8	01 06 00 00 A4 4D 41 47
✉ 0.009258	CA... A7	CAN Frame	Rx	8	8	02 5B 62 57 12 81 1F C5
✉ 0.000598	CA... B2	CAN Frame	Tx	8	8	02 5B 62 57 12 81 1F C5
✉ 0.009405	CA... A7	CAN Frame	Rx	8	8	03 B9 EE 2E 97 DE 23 5C
✉ 0.000721	CA... B2	CAN Frame	Tx	8	8	03 B9 EE 2E 97 DE 23 5C
✉ 0.009314	CA... A7	CAN Frame	Rx	8	8	04 07 93 55 55 55 55 55
✉ 0.000721	CA... B2	CAN Frame	Tx	8	8	04 07 93 55 55 55 55 55
✉ 0.009291	CA... A7	CAN Frame	Rx	8	8	01 06 00 00 A5 4D 41 47
✉ 0.000731	CA... B2	CAN Frame	Tx	8	8	01 06 00 00 A5 4D 41 47
✉ 0.009266	CA... A7	CAN Frame	Rx	8	8	02 66 7C 6E A5 C9 89 6E
✉ 0.000550	CA... B2	CAN Frame	Tx	8	8	02 66 7C 6E A5 C9 A5 6E
✉ 0.009457	CA... A7	CAN Frame	Rx	8	8	03 B9 EF 77 60 6C 17 9A
✉ 0.000721	CA... B2	CAN Frame	Tx	8	8	03 B9 EF 77 60 6C 17 9A
✉ 0.009286	CA... A7	CAN Frame	Rx	8	8	04 6F FD 55 55 55 55 55
✉ 0.000514	CA... B2	CAN Frame	Tx	8	8	04 6F FD 55 55 55 55 55

Man in the middle attack

- **Corrupted signature**
- **Wrong «Error counter»** -----→



B::Var.Watch (on ibol1u18)

```
Safeure_Motor_11_Buffer = (0x6, 0x0, 0x0, 0xA6, 0x4D, 0x41, 0x47, 0x3D, 0xC5, 0x98, 0x25, 0xD6, 0x74, 0x7C, 0x89, 0xAD, 0x
Safeure_Sign_Buffer = (0x66, 0x7C, 0x6E, 0xA5, 0xC9, 0xB9, 0x6E, 0x89, 0xEF, 0x77, 0x60, 0x6C, 0x17, 0x9A, 0x6F, 0xFD)
Safeure_MsgCatB_Status = 1 ≈ 1 .
Safeure_MsgCatB_Rx = (0x4, 0x6F, 0xFD, 0x55, 0x55, 0x55, 0x55, 0x55)
Safeure_MsgCatB_Ready = 0
Safeure_MsgCatB_ErrCnt = 104
Safeure_MsgCatB_Err = 0 = 0 .
Safeure_MsgCatB_Cnt = 0
Safeure_MsgCatB = (0x6, 0x0, 0x0, 0xA5, 0x4D, 0x41, 0x47, 0x66, 0x70, 0x6E, 0xA5, 0xC9, 0xA5, 0x6E, 0xB9, 0xEF, 0x77, 0x60
Safeure_Motor_11_FrameCnt = 0
Safeure_CntMsg11 = 167
```

Category A Massages TESTS

Man in the middle attack

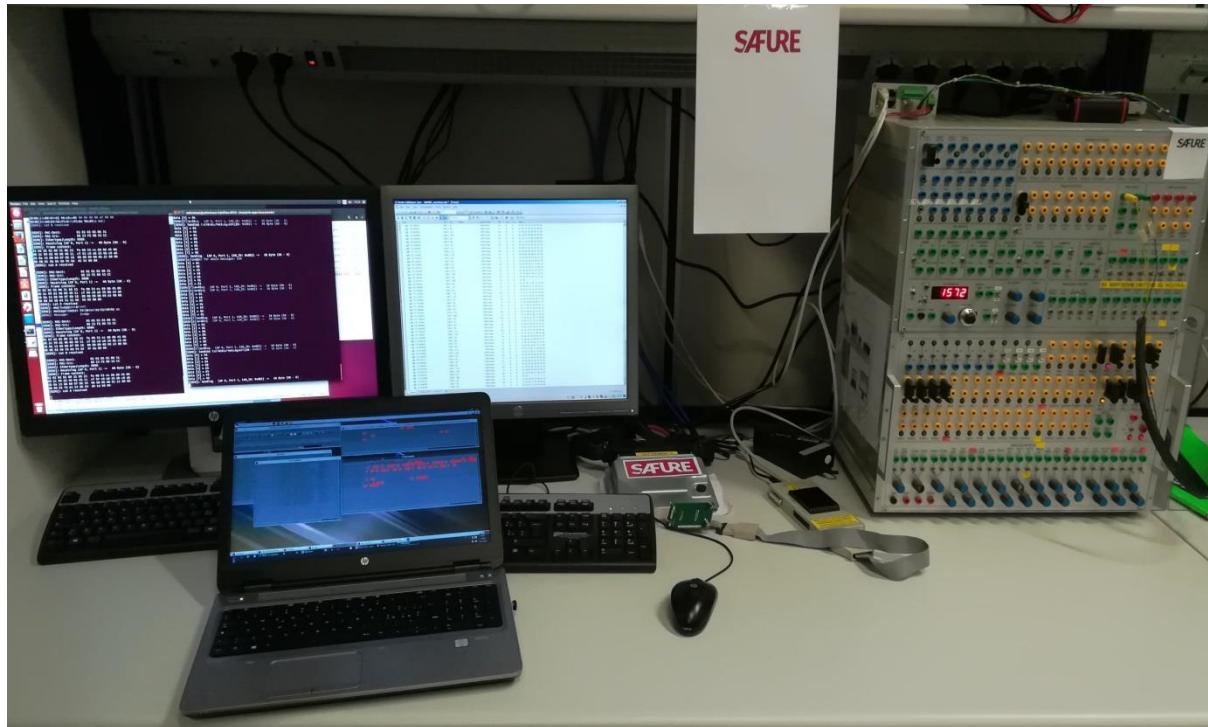
- **6 corrupted messages sent**
- **Error counter increased!** -----→



B::Var.Watch

Safure_MsgCatA_Status = 1 \triangleq 1
Safure_MsgCatA_Rx = (1, 250, 225, 226, 144, 4, 212, 90)
Safure_MsgCatA_Ready = 0
Safure_MsgCatA_ErrCnt = 6
Safure_MsgCatA_Eep = 0 \triangleq 0
Safure_MsgCatA_Cnt = 1
Safure_MsgCatA_Eep = 0/255, 225, 226, 144, 4, 212, 90, 220, 75 \triangleq 75 boolean, 220 \triangleq 220 boolean, 118 \triangleq 118 boolean, 100 \triangleq 100 boolean, 68 \triangleq 68 boolean

Full Equipment



SAFURE Grant Agreement No. 644080

"This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 644080."

"This work was supported by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0025. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government."

If you need further information, please contact the coordinator:

TECHNIKON Forschungs- und Planungsgesellschaft mbH

Burgplatz 3a, 9500 Villach, AUSTRIA

Tel: +43 4242 233 55 Fax: +43 4242 233 55 77

E-Mail: coordination@safure.eu

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.