ANOMALY DETECTION SYSTEM

By Arun Mane and Nikhil Bogam

WHOAMI…!!!

- ./../Arun

- Founder and director of AmynaSec Labs
- Security (Hardware,Vehicle, ICS,IoT)
- Speaker and Trainer – Defcon,Blackhat, Nullcon,HITB,HIP,Defcon….many
- Reachable on twitter @rootkill3r
- armane@amynasec.io

..

- ./../Nikhil Bogam
- Safety and Security Manager at Lear Corporation
- Reachable on twitter @nikhilbogam
- bogamnikhil@gmail.com

Agenda

- Role of security in CARs
- Briefing of CAN bus
- Attack vectors
- Introduction of Anomaly detection system (ADS)
- Why ADS could be the best solution for CAN network attacks ?
- ADS working principle
- Basic attack demo for ADS

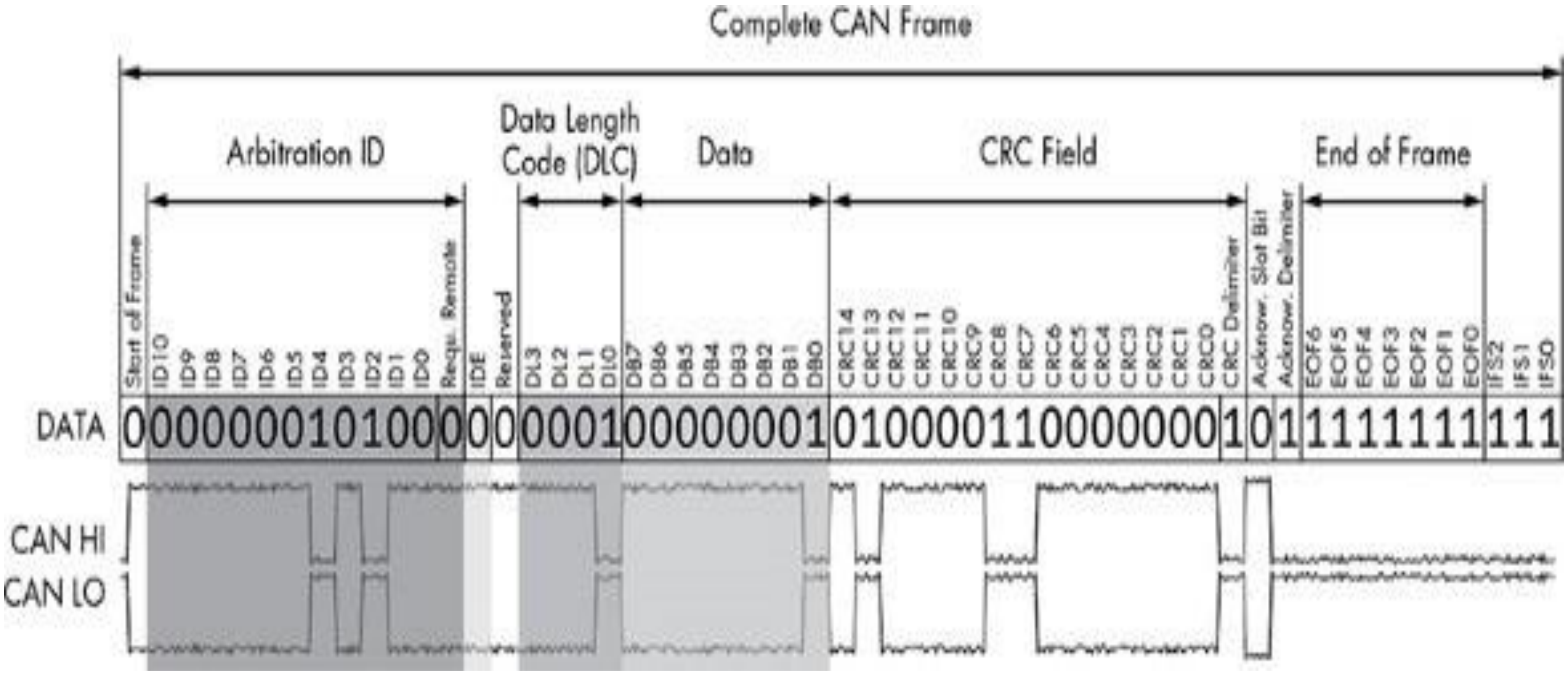
WHY SECURITY NEEDED IN CARS ?

- Now a days car are connected to internet which lead to risk of remote attack
- Safety risk : e.g. Compromise brake ECU
- Privacy risk: e.g. driver information
- Brand image.
- etc

CAN BUS INTRODUCTION

- Controller Area Network
- Modern vehicles are full of little embedded systems and electronic control units (ECUs) that can communicate using the CAN protocol.
- Runs on Two wires
  - CANH
  - CANL
- CAN uses differential signaling
- It supports OBD-2

CAN FRAME

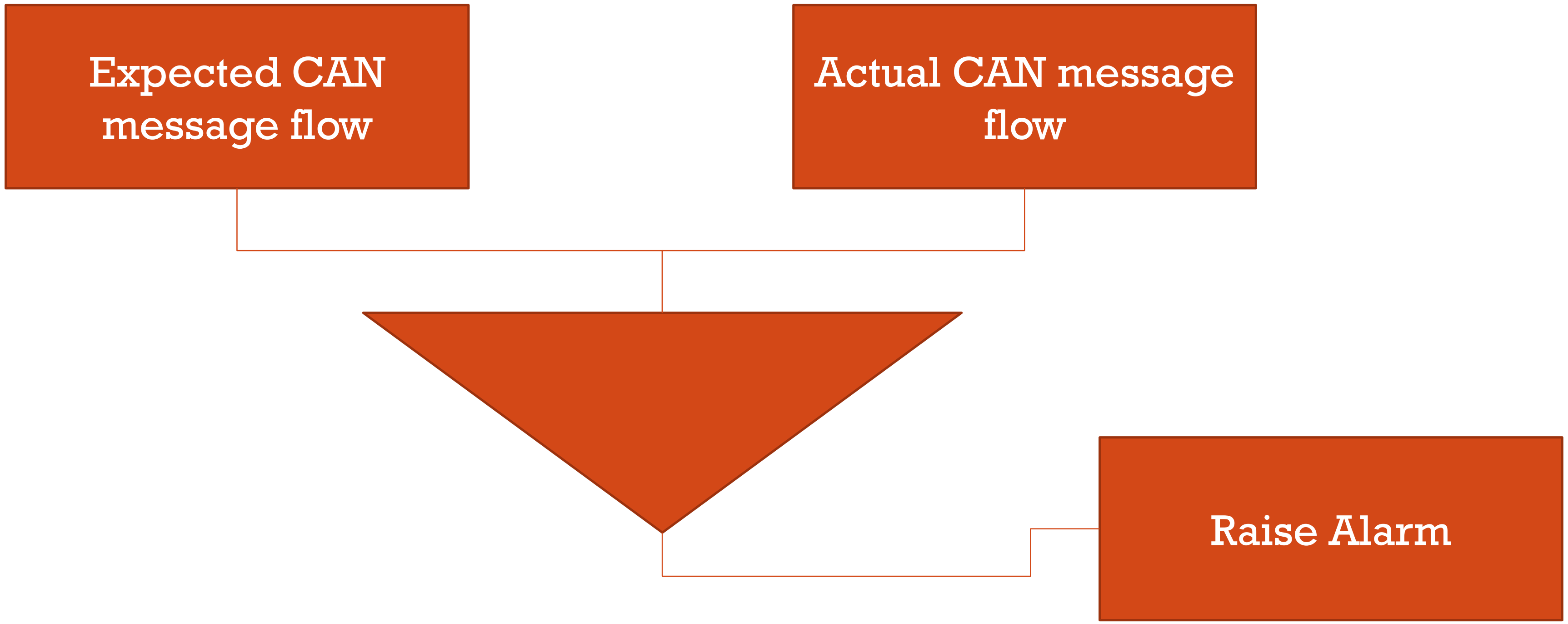

Complete CAN Frame
Arbitration ID
Data Length Code (DLC)
Data
CRC Field
End of Frame
Start of Frame
ID10
ID9
ID8
ID7
ID6
ID5
ID4
ID3
ID2
ID1
ID0
Requ. Remote
IDE
Reserved
DL3
DL2
DL1
DL0
DB7
DB6
DB5
DB4
DB3
DB2
DB1
DB0
CRC14
CRC13
CRC12
CRC11
CRC10
CRC9
CRC8
CRC7
CRC6
CRC5
CRC4
CRC3
CRC2
CRC1
CRC0
CRC Delimiter
Acknow. Slot Bit
Acknow. Delimiter
EOF6
EOF5
EOF4
EOF3
EOF2
EOF1
EOF0
IFS2
IFS1
IFS0
DATA
0 00000010100 0 0 0 0001 00000001 010000110000000 1 0 1 1111111 111
CAN HI
CAN LO

CAN BUS ATTACKS

- DOS
- Firehose
- Packet payload modification
- Packet replay
- Right after / Before attack

ANOMALY DETECTION SYSTEM

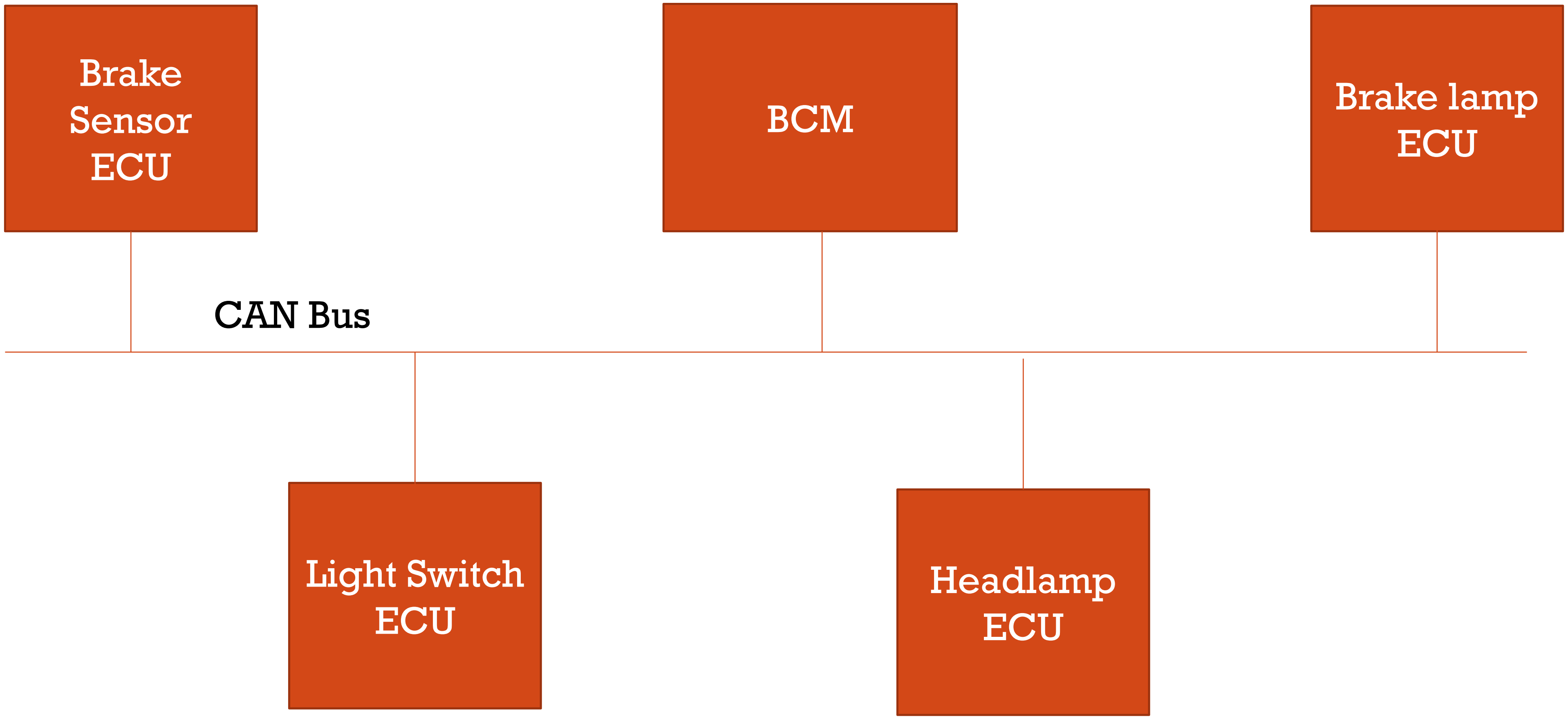
- Anomaly-based IDS observes a real-time system's activities and compare it against a normal behavior that has been recorded into a profile. Whenever the deviation from normal profile behavior reaches a certain threshold, it will raise the alarm



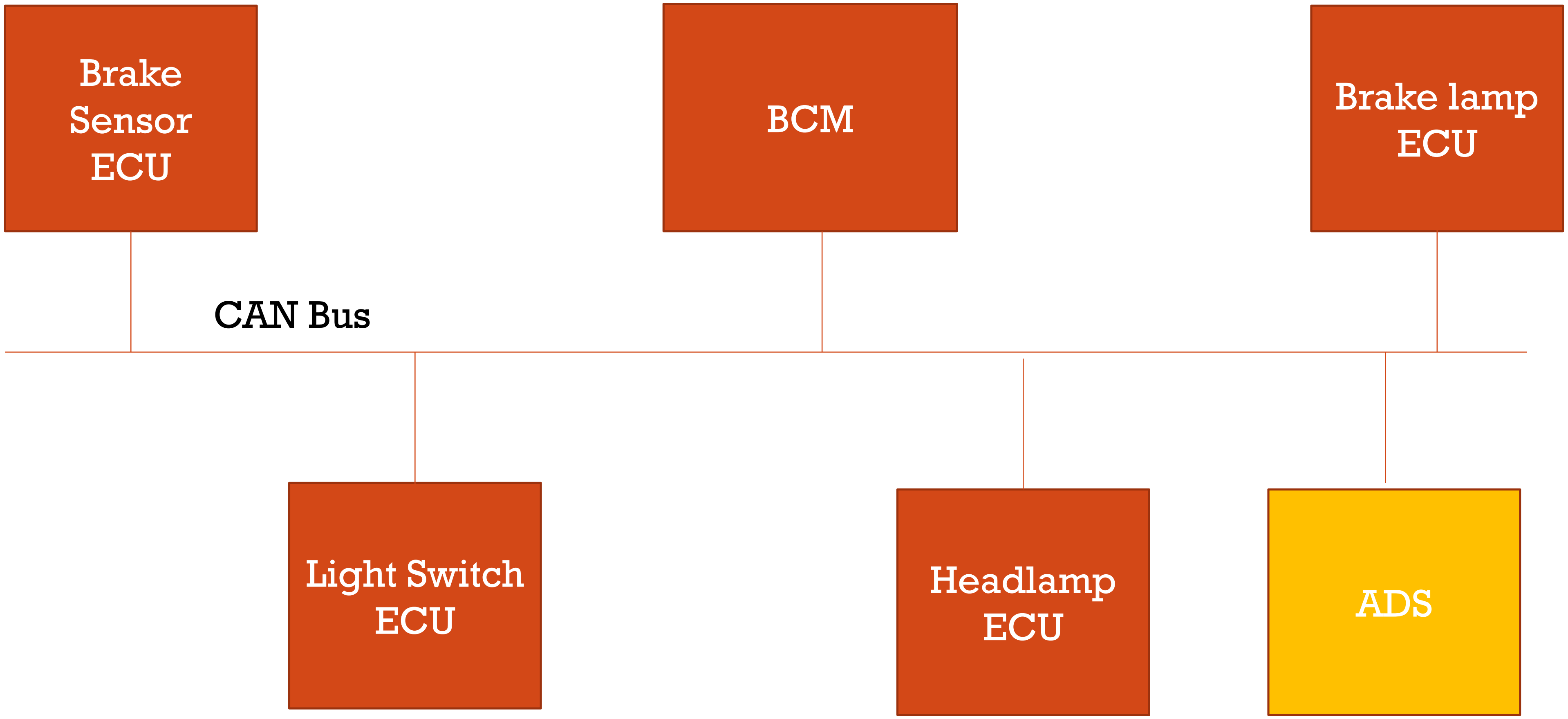
WHY ADS COULD BE THE BEST SOLUTION ?

- Easy to adopt to existing CAN network
- Low cost
- Other solutions need many changes in CAN network, which lead to ECU modification
- Changing ECU system /software is time consuming for automotive sector due to many compliances.

CAN NETWORK:


Brake Sensor ECU
BCM
Brake lamp ECU
CAN Bus
Light Switch ECU
Headlamp ECU

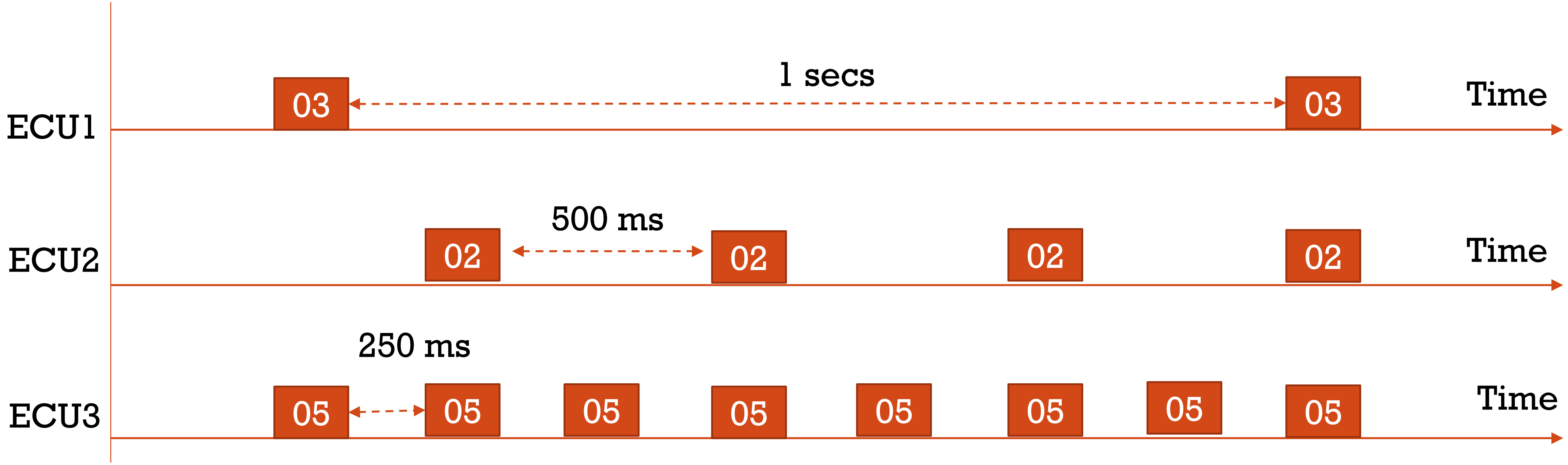
CAN NETWORK WITH ADS:



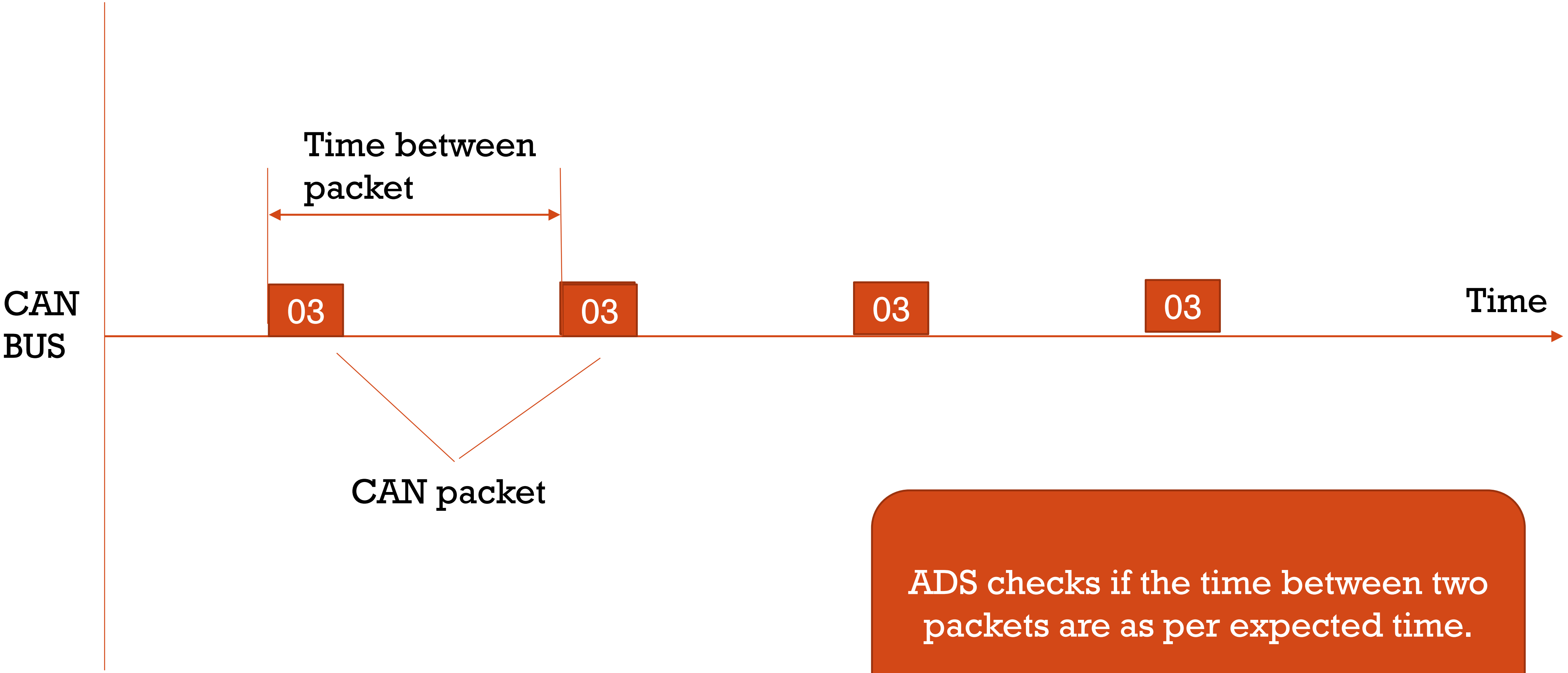
ADS METHODS

- Frequency
- Filtering messages
- Sequence of IDs
- Machine Learning
- etc

CAN TRANSMISSION

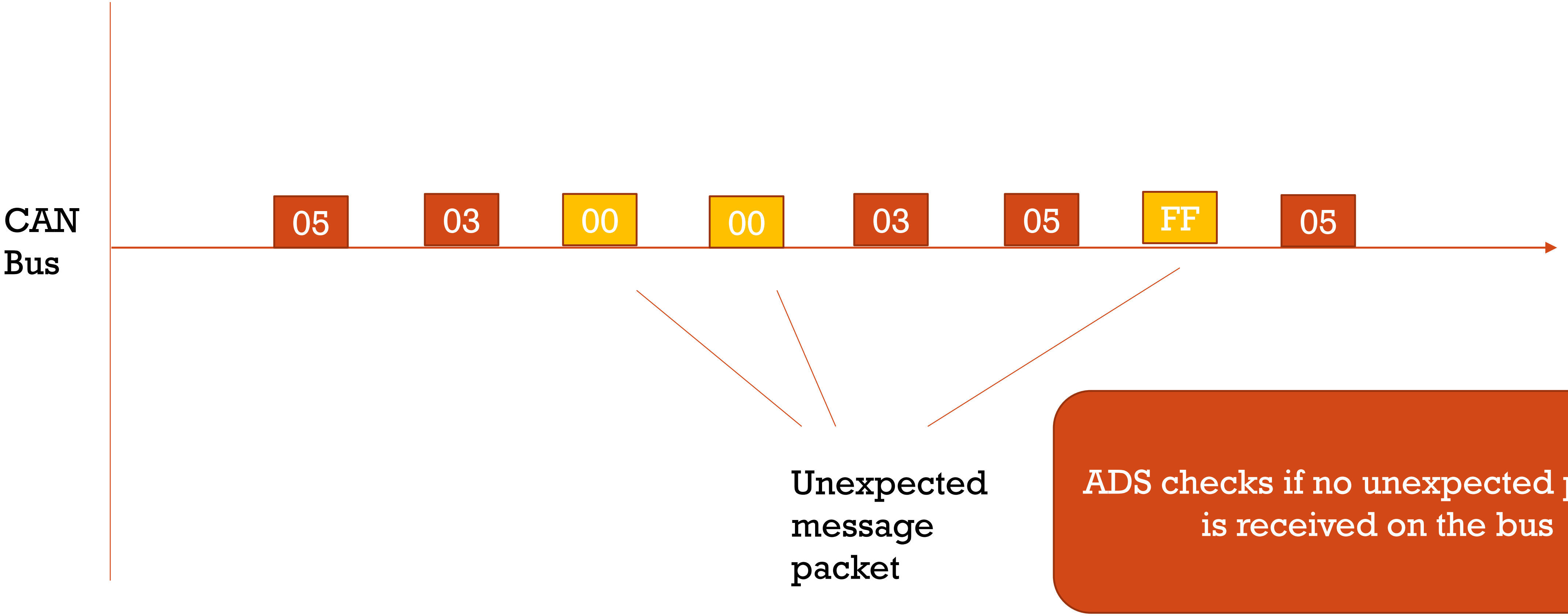


FREQUENCY BASED ADS



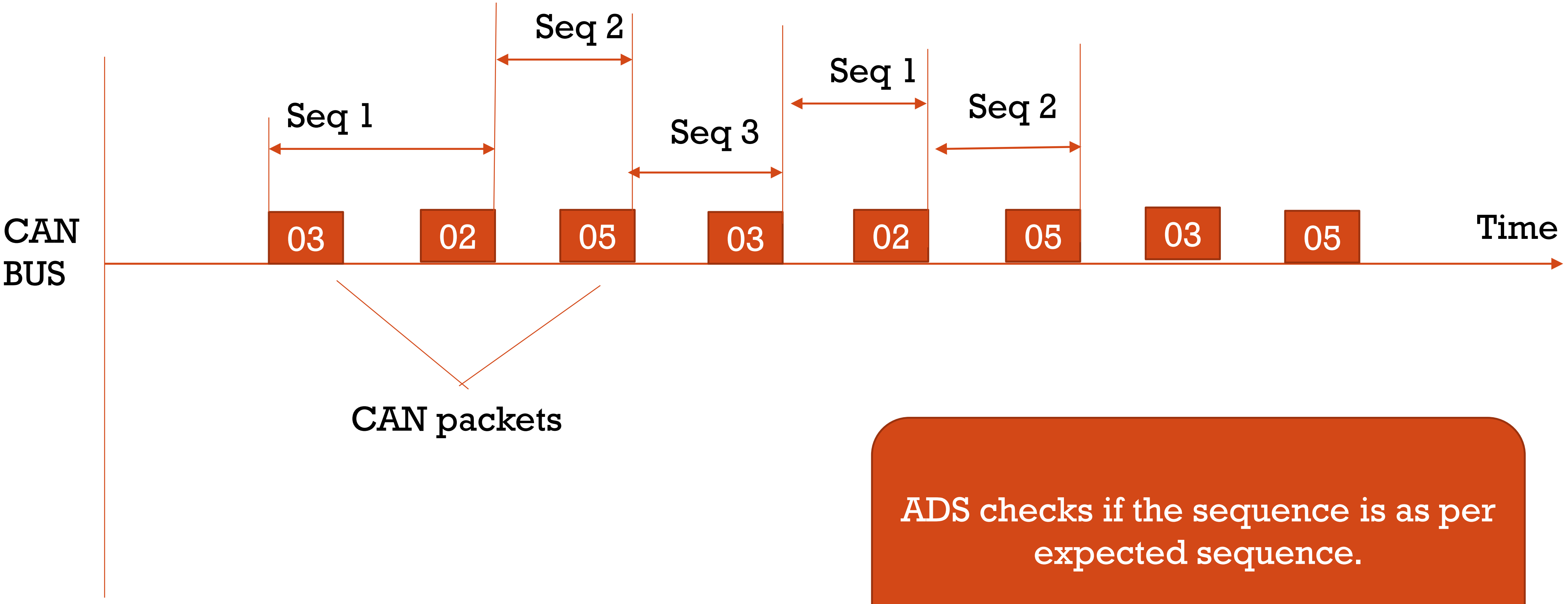
ADS checks if the time between two packets are as per expected time.

FILTER MESSAGES BASED ON IDS



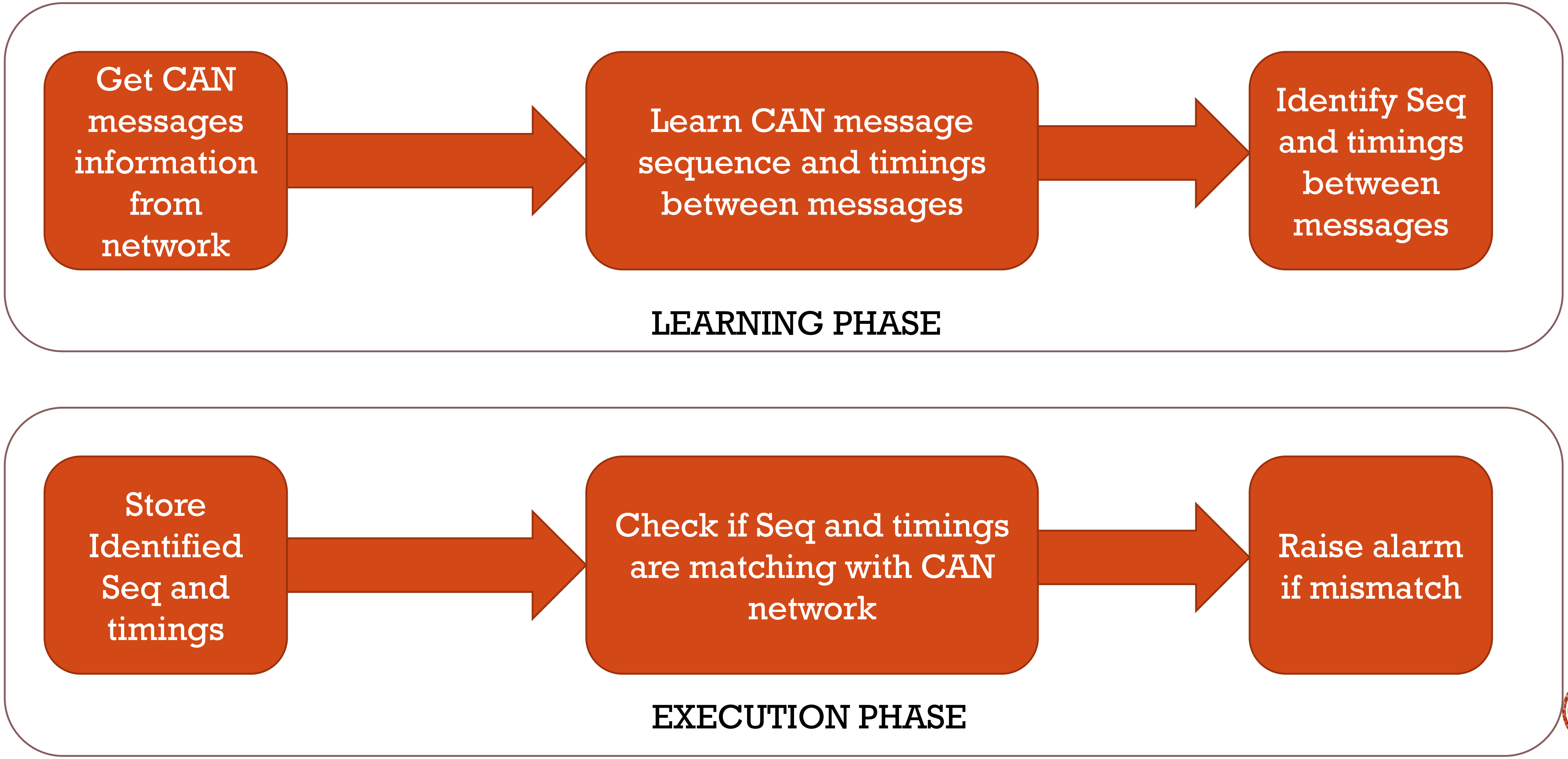
ADS checks if no unexpected packet is received on the bus

SEQUENCE OF ID BASED ADS



ADS checks if the sequence is as per expected sequence.

MACHINE LEARNING BASED ADS



Get CAN messages information from network

Learn CAN message sequence and timings between messages

Identify Seq and timings between messages

LEARNING PHASE

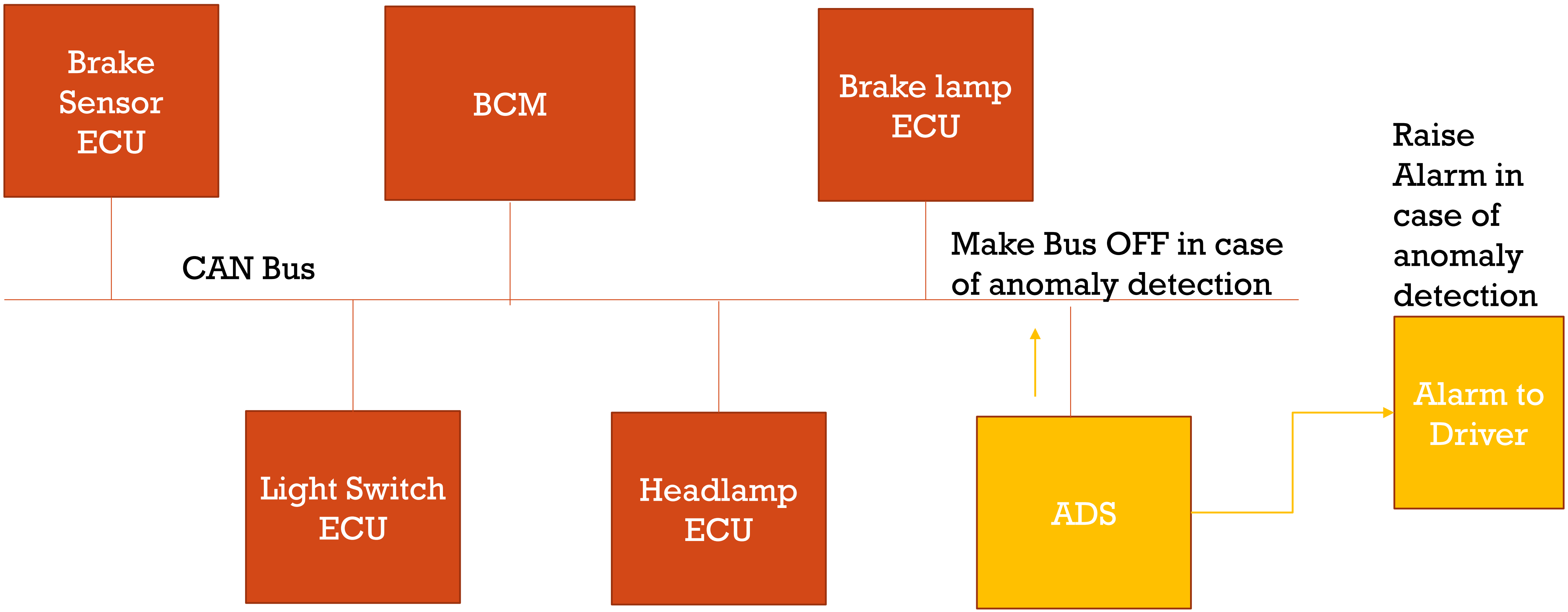
Store Identified Seq and timings

Check if Seq and timings are matching with CAN network

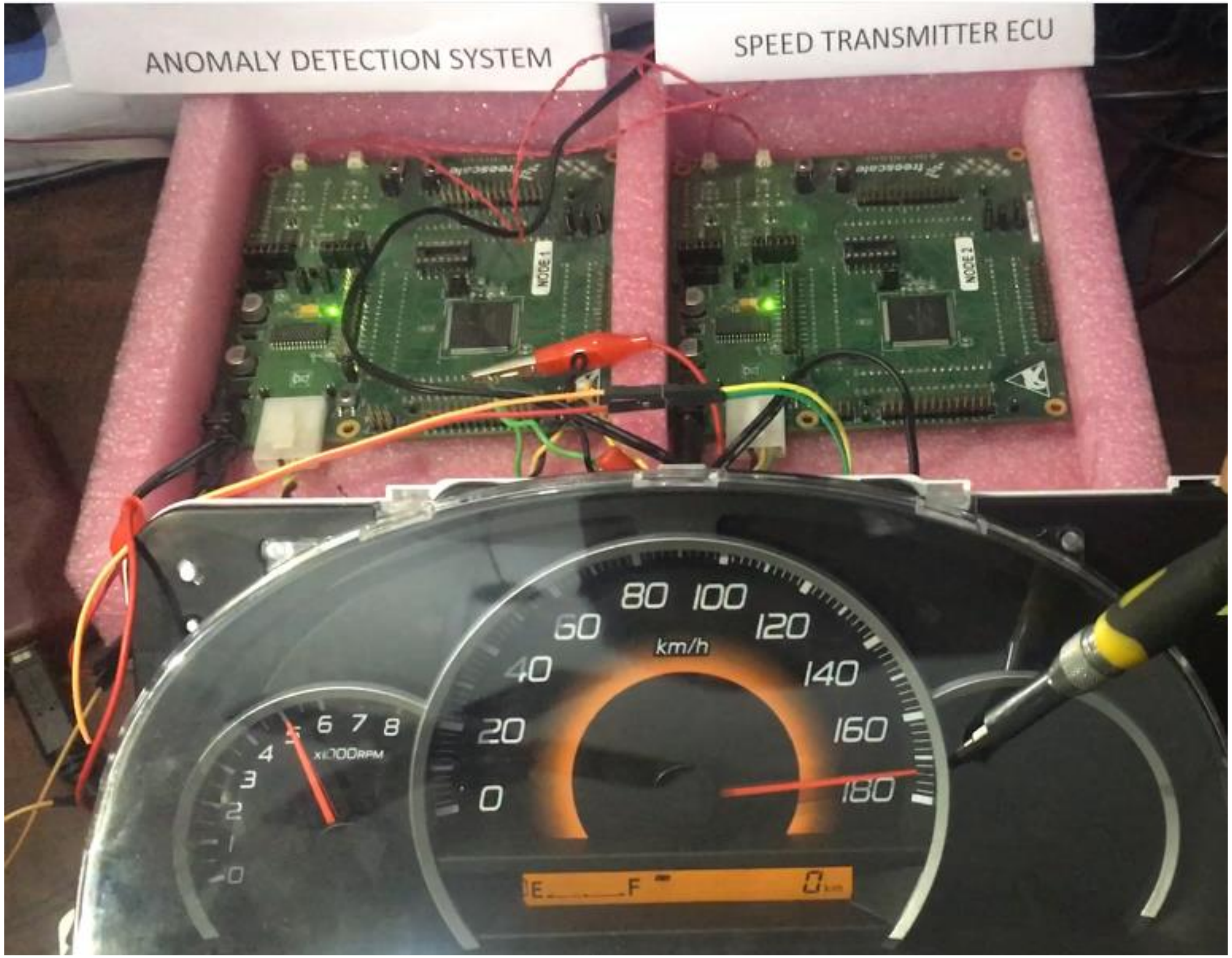
Raise alarm if mismatch

EXECUTION PHASE

CAN NETWORK WITH ADS:



ADS AT OUR LAB



Thank you