SDK definition for safety functions for UART, CAN and TCP/IP communications

Leonardo Valdivia
CEIT and Tecnun (University of Navarra)

NETS4TRAINS 2016
Donostia – San Sebastián
6-7 **June 2016**

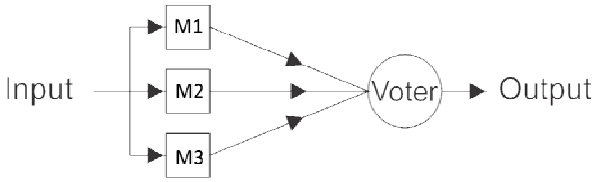
Outline

- Introduction
  - Voters and saboteurs
  - SDK
- Features of the SDK
- Voter
  - Synchronization process
- Saboteur
- Sniffer
- Railway application
- Conclusions

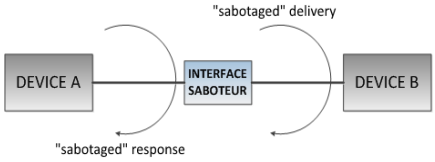
Introduction

- Safety critical applications
  - Railway
  - Automotive
  - Avionics

Dependability → Redundancy → Voter

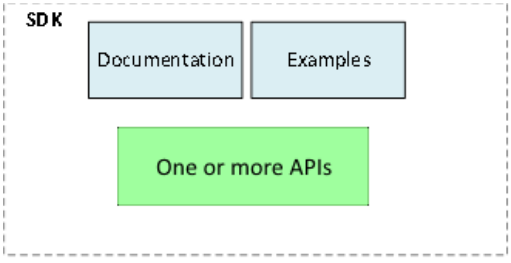


- If a fault occurs?
  The system must be fault tolerant



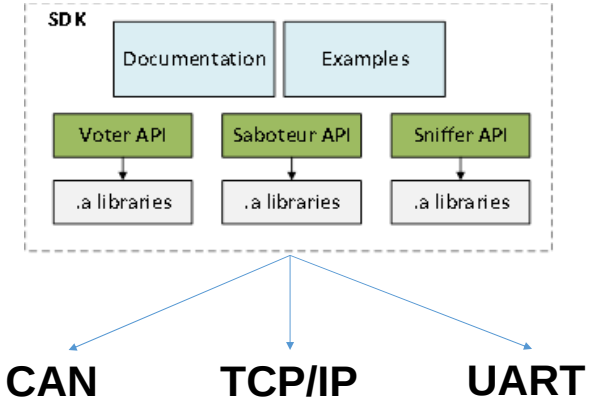
Introduction

- Software Development Kit (SDK)



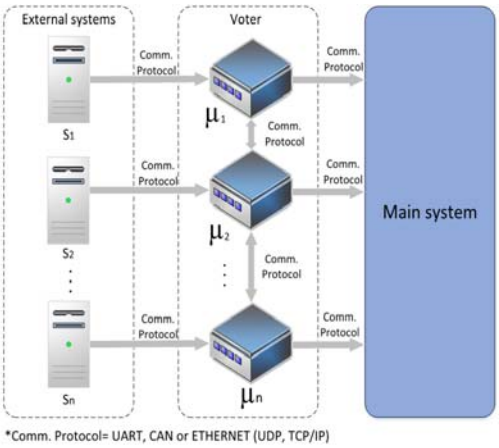
- Example of SDK: Android SDK (to develop applications).
- Examples of APIs: Google maps, Facebook.

SDK



Voter

- Features
  - The voter can have “n” number of inputs (2 out of 3 is the most common).
  - It can use CAN, TCP/IP or UART as communication protocol.
  - Single or multiple output.
  - Voting type can be literal or numeric.
  - The messages between the microcontrollers contains safety layer.

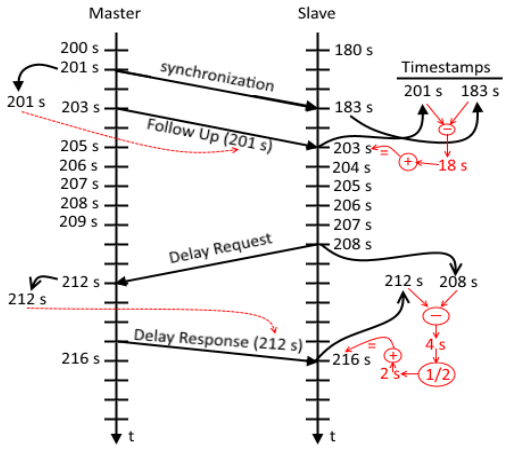


Safety Layer

Seq. number	Timing	Link data	CRC16

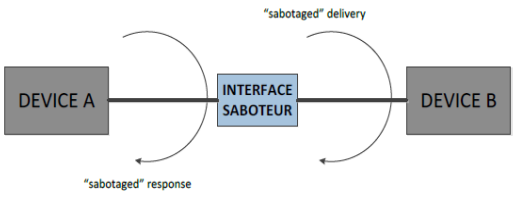
Voter Synchronization

- Precision Time protocol (PTP)
  - Synchronization.
  - Follow up.
  - Delay request.
  - Delay response



Saboteur

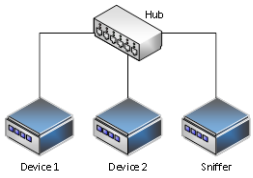
- Interface saboteur
  - Alters the information in wired communication: CAN, TCP/IP or UART.
  - Acts as a bridge when the sabotage is not performed.
  - Fault can be: delete message, flip message, message creation and corrupt message.



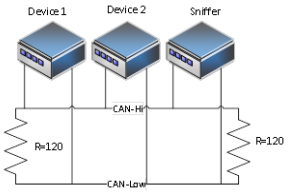
Sniffer

- Prints information that passes through a network.
- Can be configured for CAN, UART or TCP/IP.
- Two ways to display the information: console or via communication port (CAN, UART or TCP/IP).

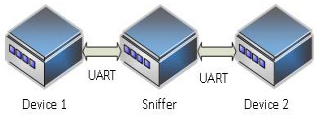
TCP/IP



CAN

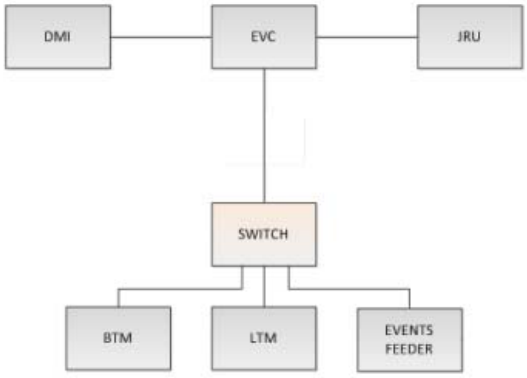


UART



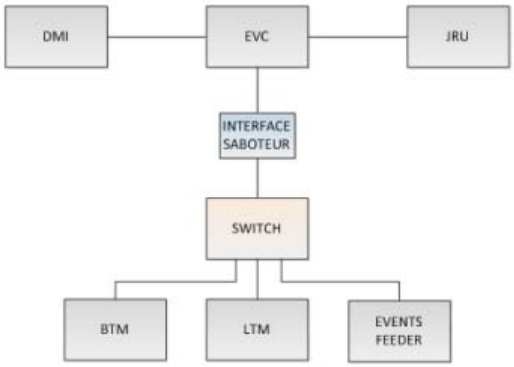
Railway Application

- Applied in a virtual lab.
  - The Virtual lab simulates the on-board equipment during a trip.
- The trips are XML files with the information of all the messages sent in a real train (BTM, LTM, ODO, etc.).
- Communication via Ethernet (TCP/IP).



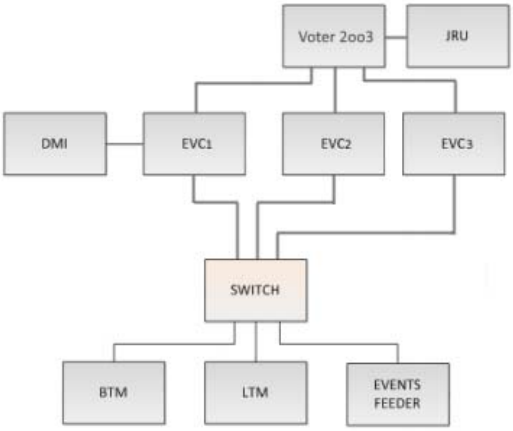
Saboteur in the virtual lab

- The SDK is applied in a commercial Linux (Debian) board.
- The saboteur is configured to handle TCP/IP protocol.
- The saboteurs alters the information sent by the on-board modules.
- Fault tolerance can be analyzed.



Voter in the virtual lab

- The most common configuration is with three EVCs.
- The voter receives the outputs of the EVCs.
- Literal voting.
- The voter sends the result to the JRU module.



Conclusion

- The SDK allows to test redundancy systems.
  - The voter can perform different type of voting (literal and numerical).
  - Can be configured “m out of n”
- It is possible to test fault tolerance.
  - The saboteurs can inject four type of fault to the communication network.
  - The saboteur is non-invasive.

All the modules can be configured by the user, allowing customize and use the SDK in different kind of applications, this flexibility can be translated into saving of time, effort and money.

SDK definition for safety functions for UART, CAN and TCP/IP communications

Leonardo Valdivia
CEIT and Tecnun (University of Navarra)

NETS4TRAINS 2016
Donostia – San Sebastián
6-7 **June 2016**