The EASIS Security Architecture Approach

Thomas Eymann, Robert Bosch GmbH

1st C2C-CC Security Workshop

Berlin, 16th November 2006

Table of Contents

- Motivation
  - EASIS Project
- Applications
- Attack scenarios
- Security management
- EASIS Telematics Validator
- Summary and future prospects

Motivation

- The European Union set the target to halve the number of mortal accidents until 2010
- Promotion of the EUCAR programme “Integrated Safety” in the 6 FP of the European Union
- The EASIS[1] Project is a part of the EUCAR Programme “Integrated Safety”

Integrated Safety:

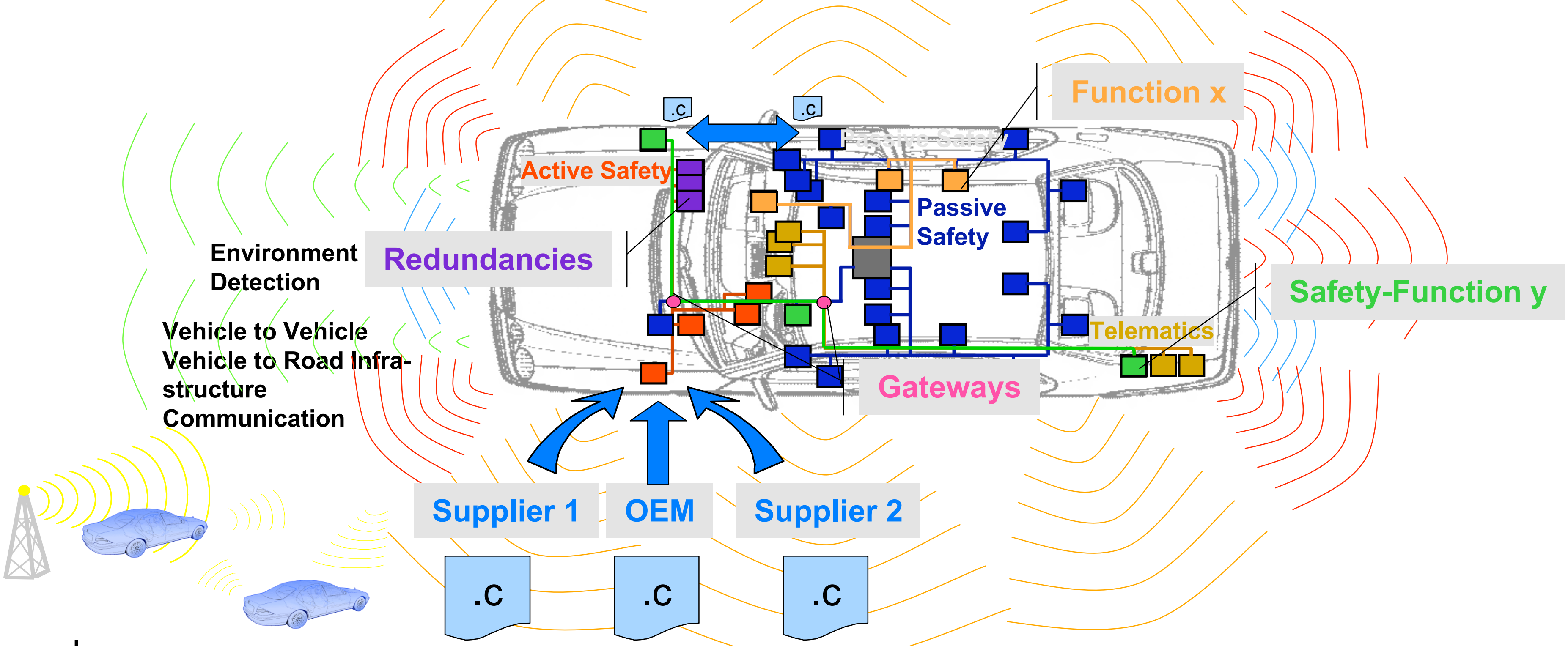
	AIDE	**EASIS**	**PReVENT**	**APROSYS**	**GST: On-line Safety Services**
	Adaptive Integrated Driver-vehicle Interface -Driver Modelling -HMI Design -Evaluation	Electronic Architecture and System Engineering for Integrated Safety Systems	Preventive and Active Safety Applications -Lane Keeping -Collision Warning -Intersection Safety -VRU & Colli. Mitig.	Advanced Protective Systems Enhanced restraint and protection systems. Crashworthiness	Traffic Info. Hazard Warning Rescue Service
OEMs:	BMW, CRF, DC, Ford, Opel, Seat Renault, PSA	CRF, DAF Opel, PSA, Renault, Volvo	BMW, CRF, Ford, Opel, Renault, PSA, VW, Volvo	AUDI, CRF, DC, PSA, Renault, VW	BMW, DC, Opel, …
Co-ordinator:	**Volvo**	**DC**	**DC**	**TNO**	**Ertico**

) [1] Electronic Architecture and System Engineering for Integrated Safety Systems

Project Data

- **Project duration:** 01.2004 – 03.2007
- **Total budget** 9,4 M€ / **Funds** 5 M€
- **Project Partners**
  DaimlerChrysler, DAF Trucks, Centro Ricerche FiatOpel, PSA, Renault, Volvo
  Bosch, ContiTeves, Lear, Motorola, Philips, Valeo, ZF
  DECOMSYS, dSPACE, ETAS, Vector
  Offis, MIRA, University Duisburg/Essen
- **Core Group**
  DaimlerChrysler, Bosch, Centro Ricerche Fiat, Valeo, Volvo and ZF

The EASIS Project



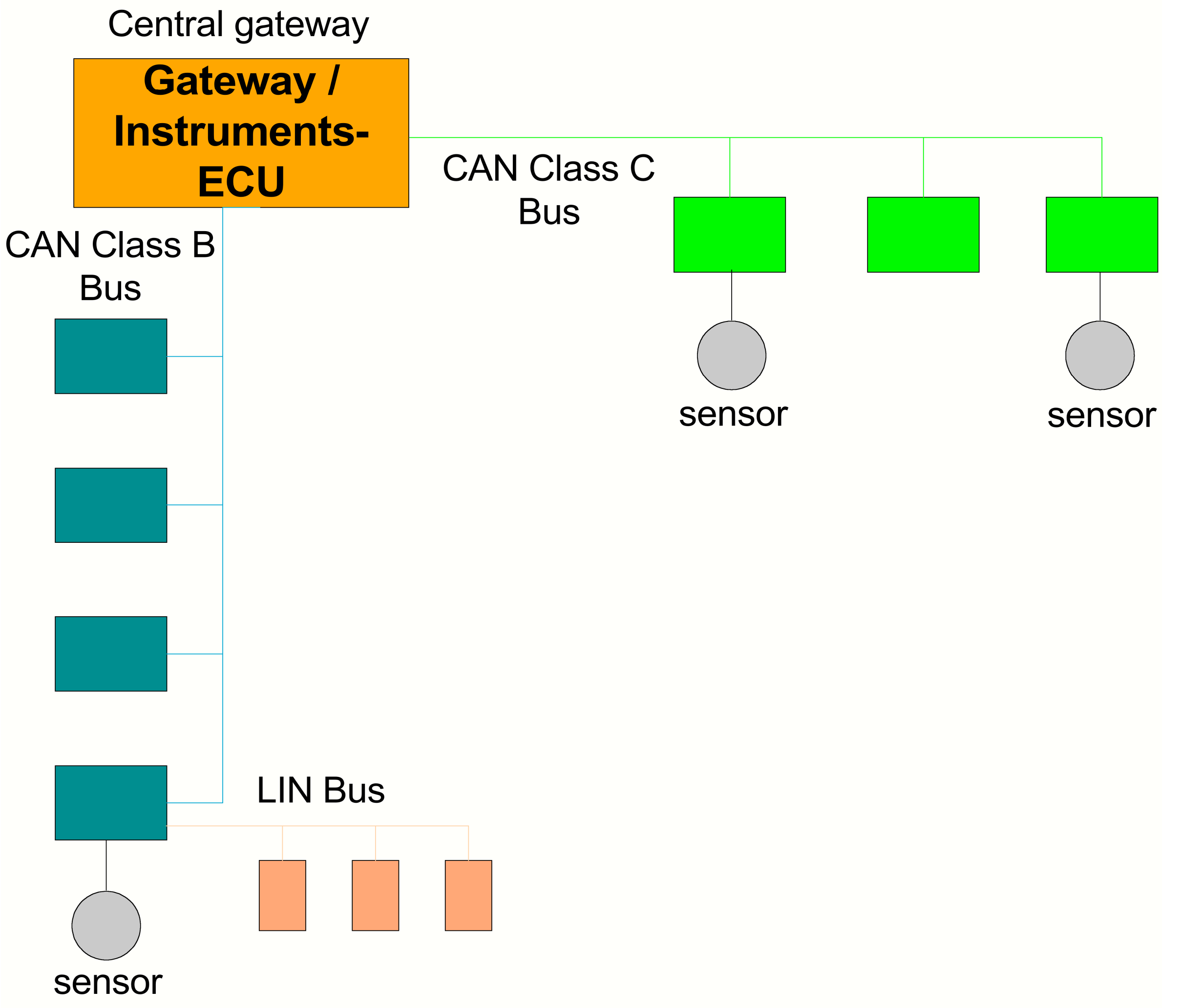
Approach

Develop a standardised in-vehicle electronic architecture and a standardised system engineering approach for integrated safety systems

Provide an enabling technology for the introduction of integrated safety systems

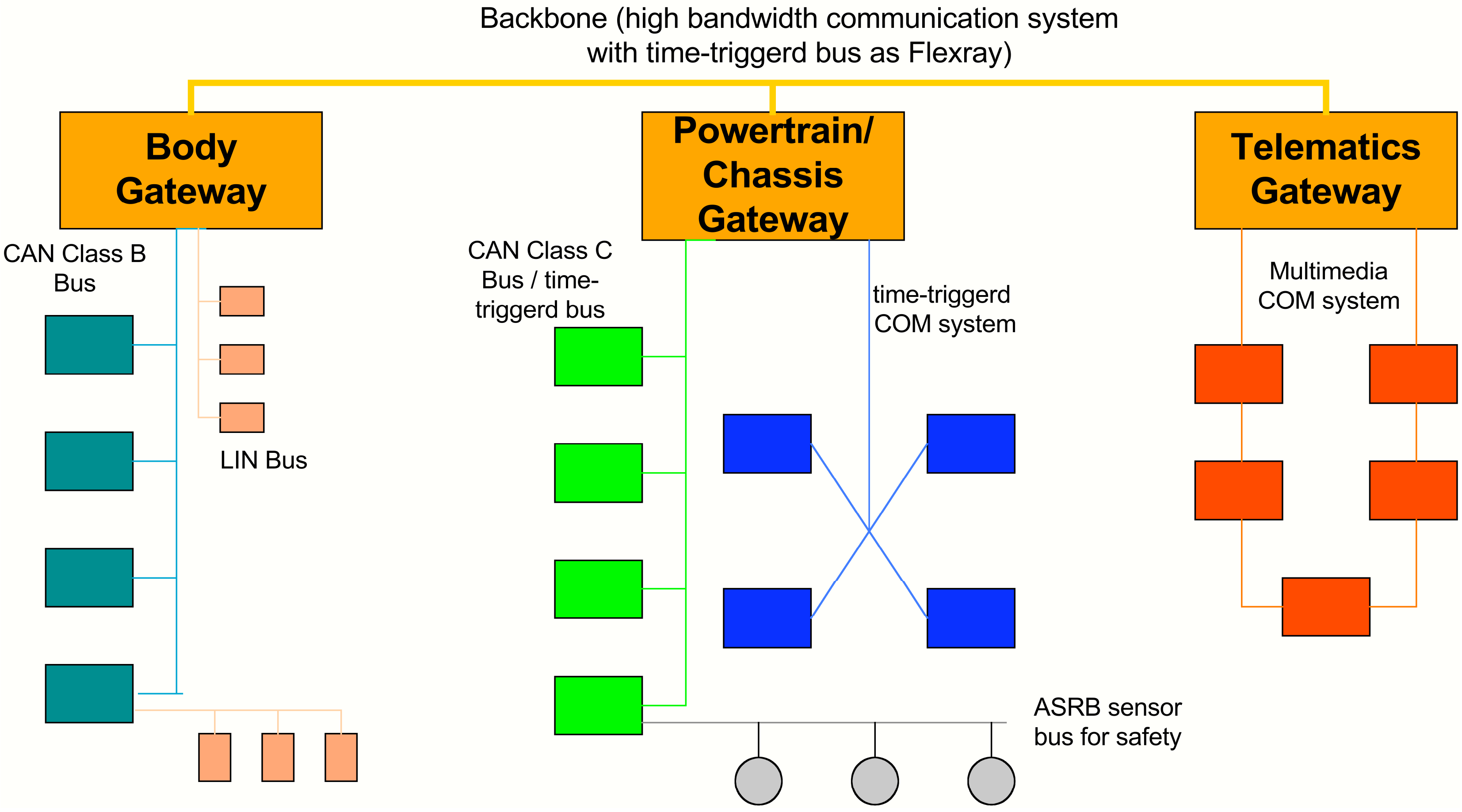
Network Architecture: Low-End Vehicle

- Diagnosis via direct connection at the Gateway-/Instruments-ECU



Network Architecture: High-End Vehicle

- Distributed Diagnosis
- Domain


Backbone (high bandwidth communication system
with time-triggerd bus as Flexray)
Body Gateway
Powertrain/ Chassis Gateway
Telematics Gateway
CAN Class B Bus
LIN Bus
CAN Class C Bus / time-triggerd bus
time-triggerd COM system
Multimedia COM system
ASRB sensor bus for safety

EASIS Communication Possibilities

- **EASIS defines four communication relations between possible communication entities (Integrated safety applications or systems):**
  - **Exchange of information with**
    - **other Vehicle (e.g. Vehicle-to-vehicle)**
    - **the infrastructure (e.g. vehicle-to-road-side-unit, Commercial service providers)**
  - **Inter-domain communication**
    - **protocol conversion (e.g. signal conversion)**
    - **end-to-end (e.g. common transport protocol)**

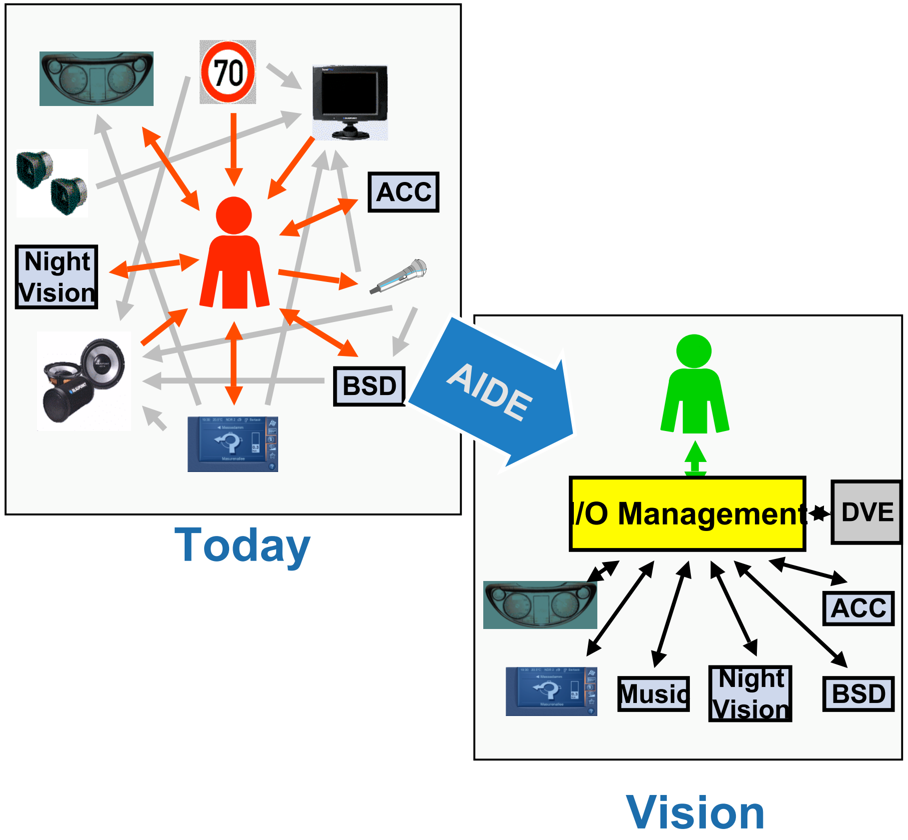
⇨ Safe and reliable communication is needed

⇨ Safe and reliable SW and HW implementation is needed

Application I

- **Adaptive Integrated Driver-vehicle Interface (AIDE)**
  - Adaptation of the HMI-output to the strain state of the driver
  - Access to the car sensors, ACC, traffic and road data in the different car domains is needed

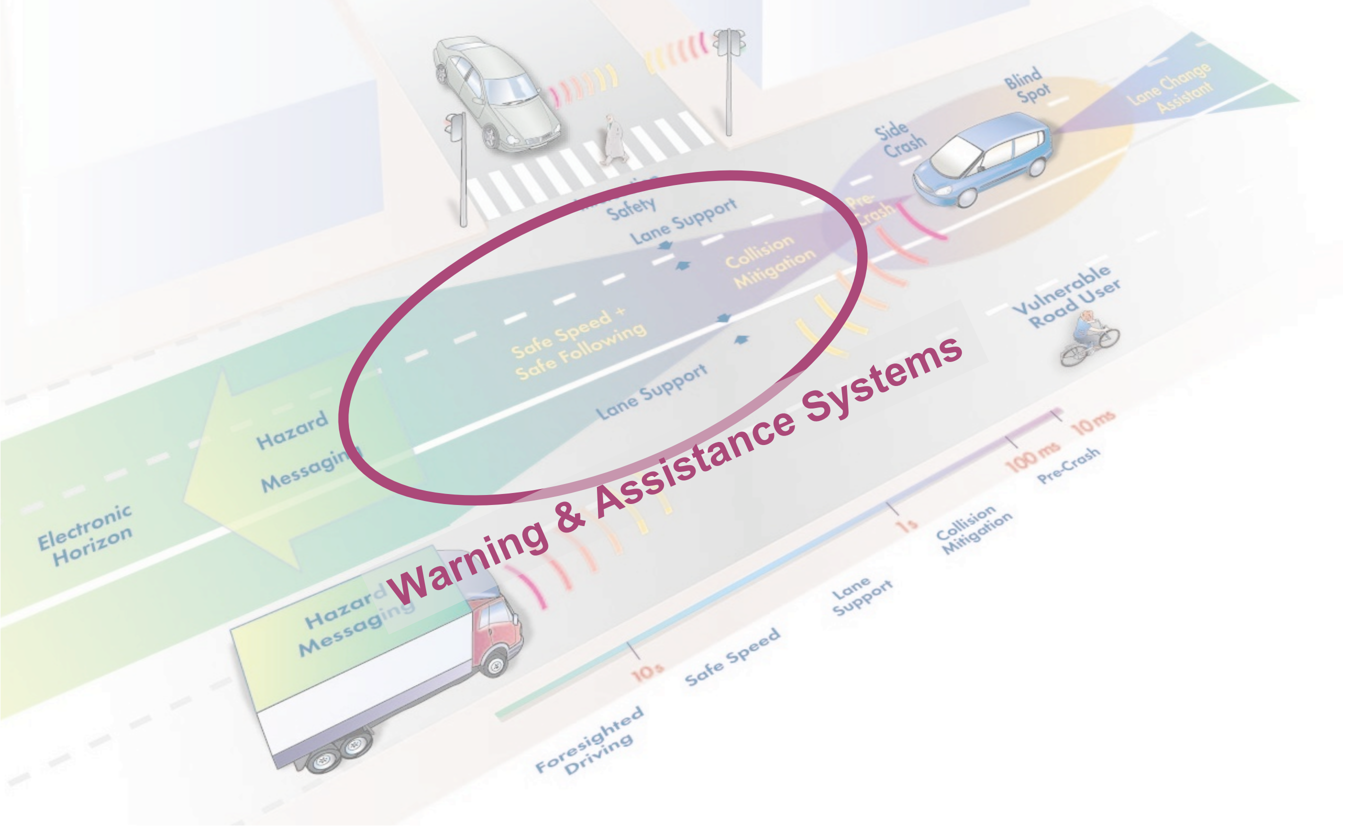
⇨ Safe and reliable communication is needed



Application II

➢ PReVENT sub-project Willwarn (Wireless Local Danger Warning)

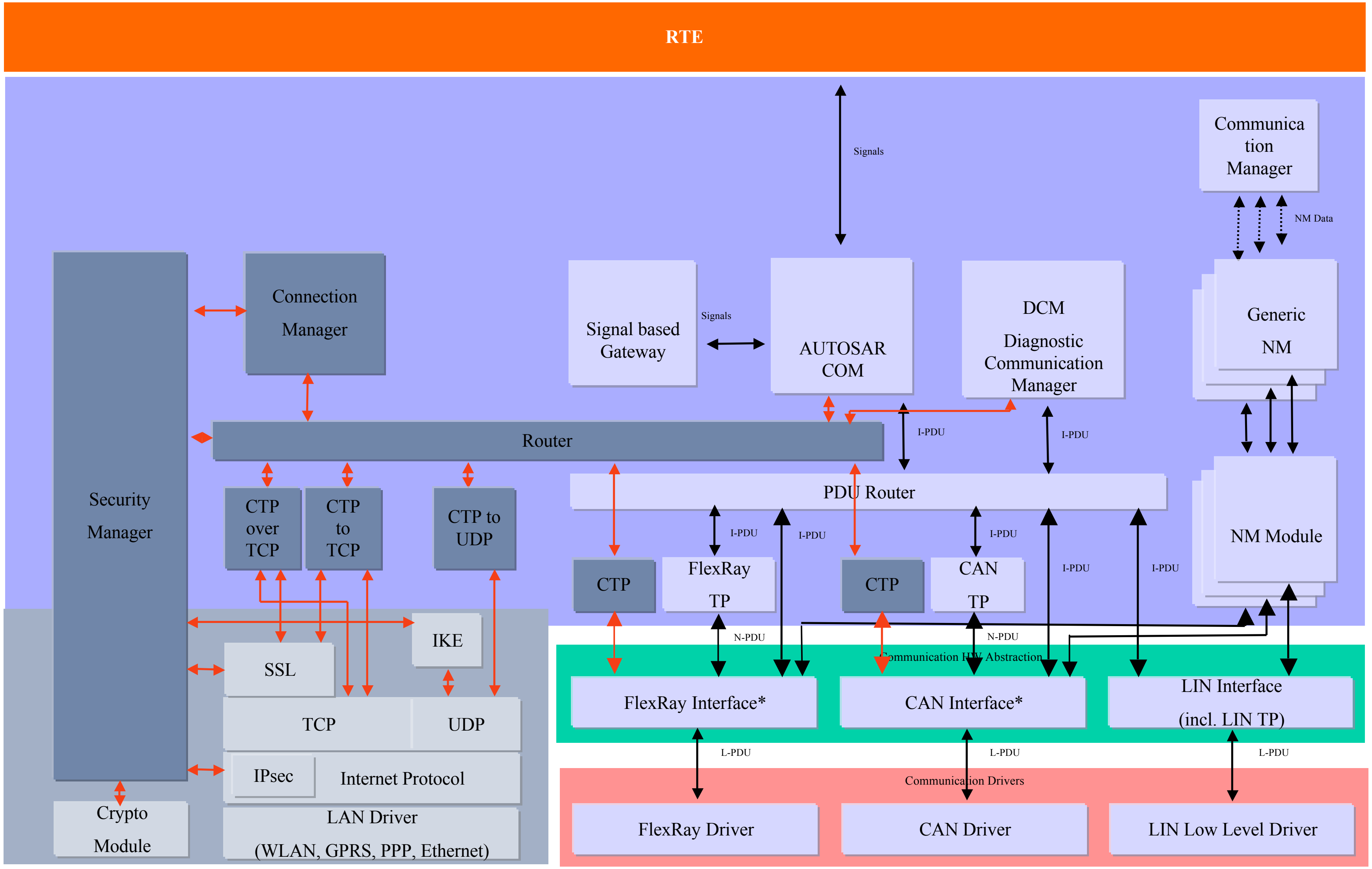
- Expansion of the detection horizon of the driver thank to warning about danger sources



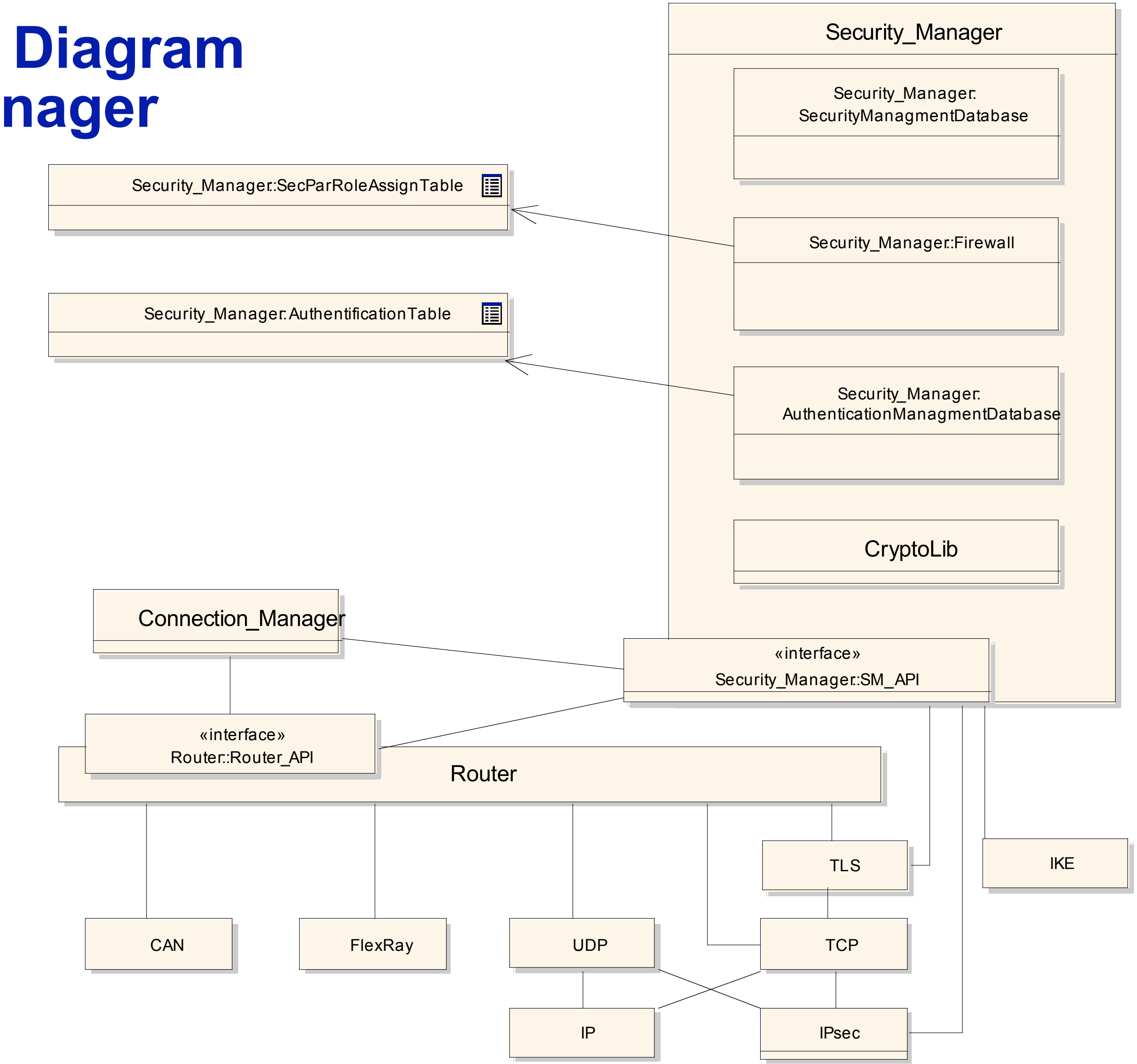
Attacks

- Eavesdropping
  - Eavesdropping and recording of a warning message (warning about emergency vehicles)
- Denial of Service
  - Accessibility of a service is restricted
- Bogus information attack
  - Faking of a warning message
- Spoofing
  - Take over of the identity of an authorised device (cone, speed limit)
- ID disclosure of other vehicles
  - Surveillance of the vehicle motions by using the V2V and V2I infrastructure

EASIS Gateway Architecture

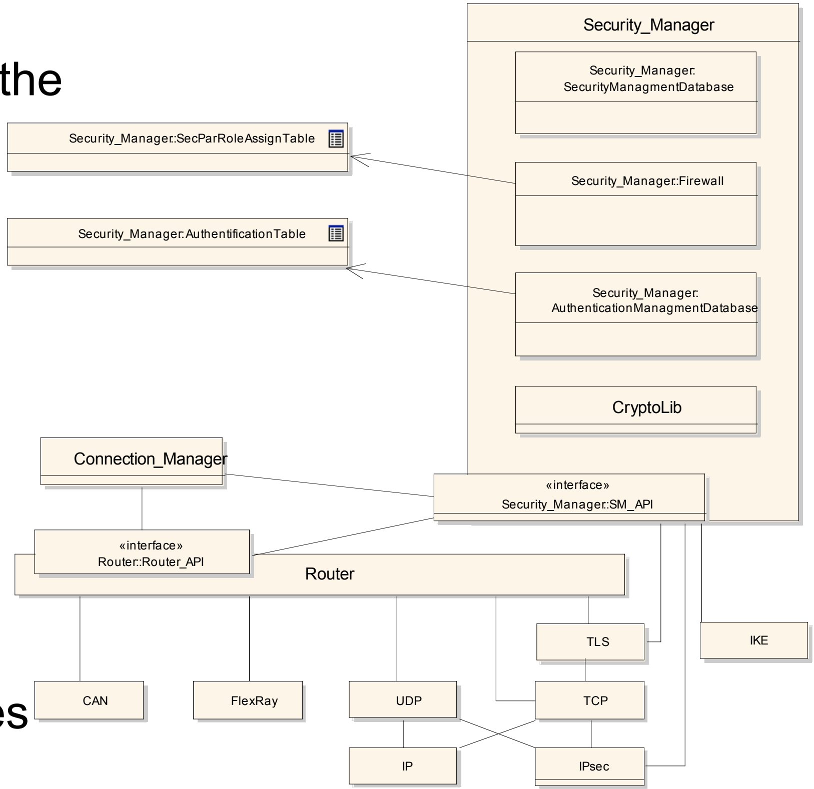


Component Diagram
Security Manager



Component Diagram Security Manager (1)

- **Firewall**
  - Provides filtering rules for the access control to car-internal communication entities
  - Determines the required security processes for the external connection establishment
- **Security Parameter Assign Table** (SecParRuleAssignTable)
  - Assignment of the security parameters to a role
  - Parameters: protocol type, min. authentication, hash and encoding process, target and source address
- **CryptoLib**
  - Wrapper in order to use different Crypto modules


Security_Manager
Security_Manager: SecurityManagmentDatabase
Security_Manager:SecParRoleAssignTable
Security_Manager:Firewall
Security_Manager:AuthentificationTable
Security_Manager: AuthenticationManagmentDatabase
CryptoLib
Connection_Manager
«interface» Security_Manager:SM_API
«interface» Router::Router_API
Router
TLS
IKE
CAN
FlexRay
UDP
TCP
IP
IPsec

Component Diagram Security Manager (2)

Authentication Management Database (AMD)

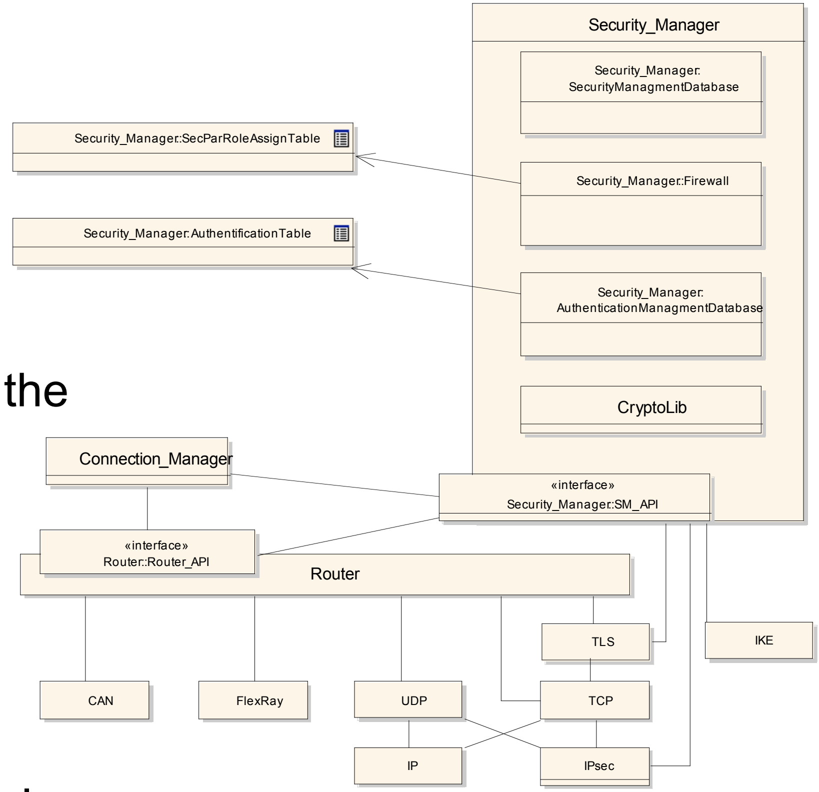
- Management of the own certificates
- Reliable recording of root certificates
- User database incl. roles, public keys etc.

Security Management Database (SMD)

- Management of current connection data and of the security parameters
    - Communication partners
    - Authentication method
    - User and current role

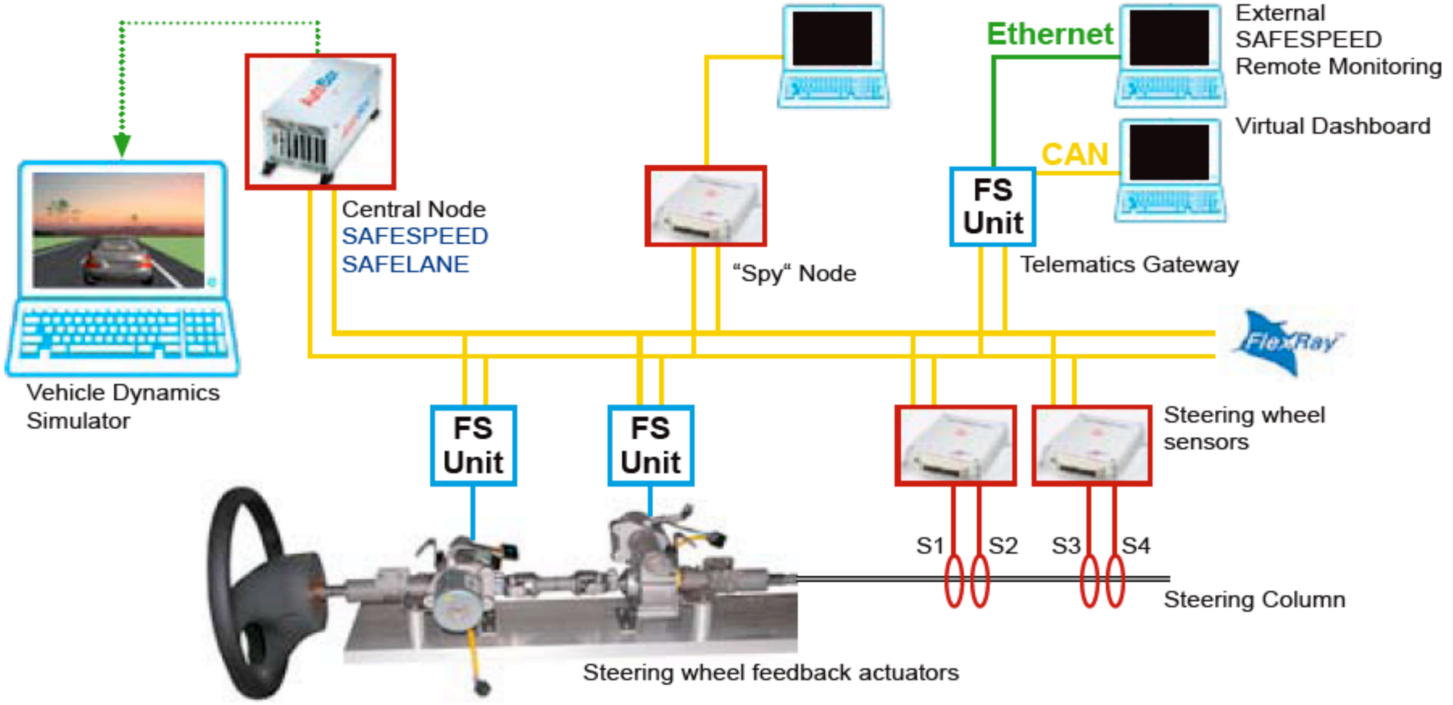
Security Management API (SM_API)

- interface between security manager and external components



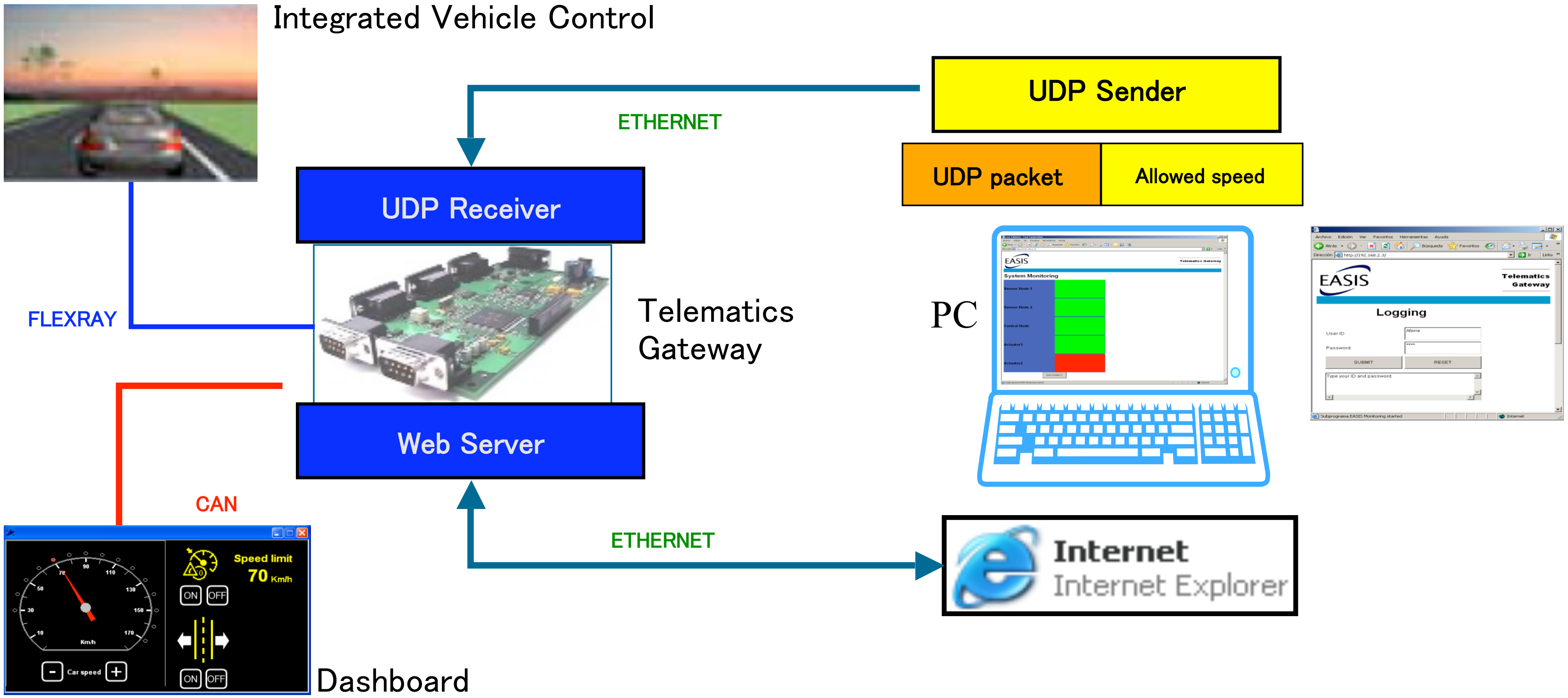
EASIS Validator:

- It includes a Telematics Gateway between internal buses (fault-tolerant FlexRay network and CAN network) and external Telematics network (WLAN/Ethernet) with protocol conversion and security services
- It includes two demonstrative applications:
  - SAFESPEED (adaptive vehicle speed to maximum allowed speed)
  - REMOTE MONITORING (web server delivering information such as vehicle speed or vehicle status to authorized users)



Telematics Gateway:

- It integrates an scalable implementation of TCP/IP protocol
- It integrates a UDP sender / receiver for SAFESPEED
- It integrates a WEB server for REMOTE MONITORING with authentication & authorization
- It integrates a gateway with automotive buses **FlexRay** and **CAN**



Information Society Technologies

Summary

- Integrated safety systems and similar applications require reliable communication over the domains

- A security management Architecture based on the AUTOSAR approach has been presented:
  - Use of a rule-based access control for internal and external communication
  - Protection of the external communication by means of the standards IPsec, IKE und TLS/SSL, established in the internet.
  - Protection of the internal communication at the transport layer level is made possible (CTP protocol)
  - Modular architecture allows a simple expansion of security standards (e.g. for V2V, V2I)

- Basic concepts has been demonstrated by the EASIS validator

Thank you very much for your attention

Are there any questions?