D7.3 Technology watch report

Project number:	644080
Project acronym:	SAFURE
Project title:	SAFURE: SAFety and secURity by dEsign for interconnected mixed-critical cyber-physical systems
Start date of the project:	1st February, 2015
Duration:	36 months
Programme:	H2020-ICT-2014-1

Deliverable type:	Report
Deliverable reference number:	ICT-644080 / D7.3/ 1.0
Work package	WP7
Due date:	July 2017 – M30
Actual submission date:	2nd August, 2017

Responsible organisation:	TCS
Editor:	L.Chibi, D.Ragot, E.Gureghian, E.Leveugle.
Dissemination level:	PU
Revision:	FINAL I 1.0

Abstract:	This document performs a technology watch report related to the SAFURE Framework methodology to build Safe and Secure solutions on multi-core platforms for mixed-criticality markets
Keywords:	Security, Safety, Telecommunication, Automotive, RTOS

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.

Editor

Lounes Chibi, main editor (TCS)

Dominique Ragot, reviewer (TCS)

Emmanuel Gureghian, security editor, reviewer (TCS)

Elodie Leveugle, editor, reviewer (TCS)

Contributors/Reviewer (ordered according to beneficiary numbers)

Martin Deutschmann, Oleksandr Tomashchuk (TEC)

André Osterhues, Cheng Lu (ESCR)

Stefania Botta, Luigi Santamato, Fabrizio Lussiana (MAG)

Carolina Reyes, Edin Arnautovic (TTT)

Mikalai Krasikau, Sergey Tverdyshev (SYSG)

Jonas Diemer (SYM)

Sylvain Girbal (TRT)

Daniel Thiele (TUBS)

Jaume Abella (BSC)

Marco Di Natale (SSSA)

Philipp Miedl, Rehan Ahmed (ETHZ)

Disclaimer

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 uses the information at its sole risk and liability.

Executive Summary

This document provides a technology watch report for safe and secure solutions on multi-core platforms for mixed-criticality.

In Chapter 2, competitive platforms addressing safety and security properties will be presented. A focus will be on the following fields: telecommunication, automotive, IMD, aeronautical, space.

RTOS and hypervisors commonly used to ensure safety and/or security are described in Chapter 3.

Communication interfaces addressing issues concerning either or both security and safety are outlined in Chapter 4.

Chapter 5 provides a brief summary regarding standards and guidelines related to security and safety.

Finally, a summary and a conclusion of the document are given in Chapter 6 .

Contents

List of Figures & Tables

Chapter 1 Introduction

The current approach for security on safety-critical embedded systems is generally to keep subsystems separated, but this approach is now being challenged by technological evolution towards openness, increased communications and use of multi-core architectures. Therefore, the consortium found together and formulated a proposal to advance the technology by proposing the H2020 idea of SAFURE.

The mission of SAFURE is to design a cyber-physical system by implementing a methodology that ensures safety and security by construction without keeping subsystems separated. This methodology is enabled by a framework developed to extend system capabilities so as to control the concurrent effects of security suppliers of safety-critical embedded products and to develop more cost and energy-aware solutions.

This document provides a technology watch report of the platforms, safety measures and technologies addressing safety and security.

In Chapter 2, competitive platforms addressing safety and/or security properties are presented with a focus on hardware and software features. These features sometimes can only be inferred from the amount and availability of the information. A focus is on the devices which are used in the following fields: telecommunication, automotive, IMD, aeronautics and space.

RTOS and hypervisors commonly used to ensure safety and/or security. The most popular and technologically advanced of them are described in Chapter 3. A brief description of the properties ensuring safety and/or security is given as well.

Communication interfaces, addressing issues concerning either or both security and safety, are outlined in Chapter 4. The list of described interfaces is not exhaustive but it contains the most relevant ones for SAFURE.

Chapter 5 provides a brief summary regarding standards and guidelines related to security and safety.

Finally, a summary and a conclusion of the document are given in Chapter 6.

Chapter 2 Competitive platforms

The classification of the platforms will be made by the target market. Depending on the market, the focus is made on either security first or safety first. The platforms (hardware and software) used for a specific field share common requirements.

Examples of such requirements could be found in the SAFURE-D1.2-PU-M06. The reasons why these requirements are needed are also described for both telecommunication and automotive field. In subchapters of Chapter 3 and Chapter 4, the RTOS and different types of communication interfaces coping with safety and/or security are described. Some of them will be used by SAFURE demonstrator.

2.1 Telecommunication devices

The Figure 1 shows the targets of the telecommunication market involved in the field of security and/or safety. Currently, most of the competitors of TCS only deal with security requirements. However, with emerging market of eHealth, safety requirements are also needed. The market, as shown on the figure, is destined to four groups with different level of security requirements/needs: government, steering committee, companies operating in strategic or sensitive areas and public. TCS is currently addressing both the government market with *Teorem* and other custom solutions and the public market with *Teopad* and Citadel. In the following, the software and hardware characteristics of each of these devices will be described such that comparisons among them can be established.

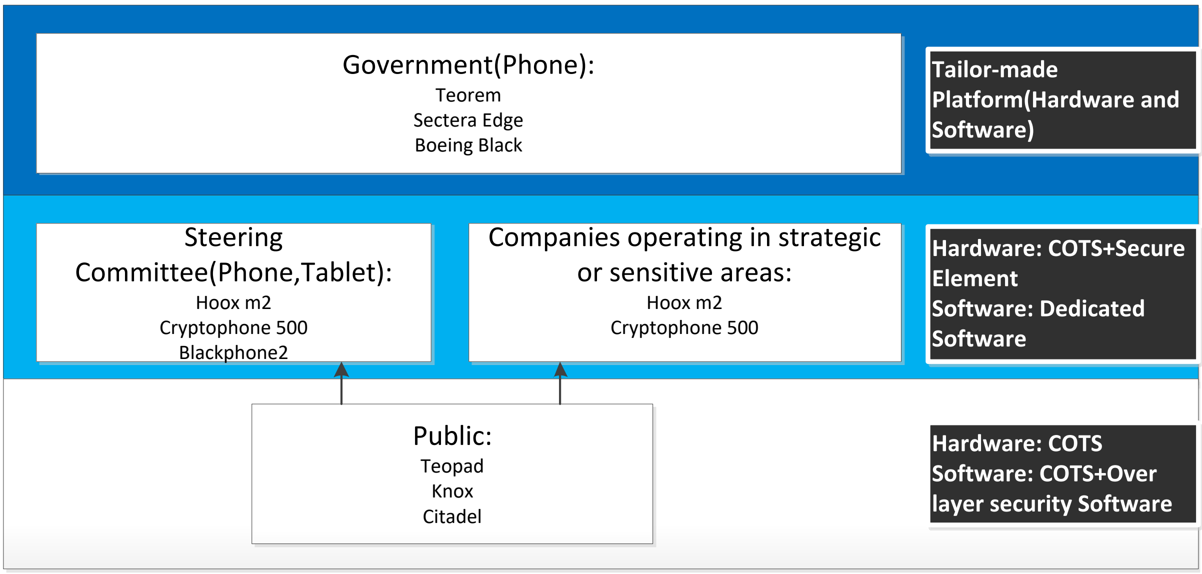
Government(Phone):
Teorem
Sectera Edge
Boeing Black
Tailor-made Platform(Hardware and Software)
Steering Committee(Phone,Tablet):
Hoox m2
Cryptophone 500
Blackphone2
Companies operating in strategic or sensitive areas:
Hoox m2
Cryptophone 500
Hardware: COTS+Secure Element
Software: Dedicated Software
Public:
Teopad
Knox
Citadel
Hardware: COTS
Software: COTS+Over layer security Software

Figure 1: Telecommunication market

2.1.1 Teorem by TCS

Teorem is a secure mobile phone made by a French company Thales targeting high level government officials (e.g. president, ministers…). This phone is designed for critical communications such as governmental officers or VIPs like CEOs of big companies.

Features:

- Dedicated Security processor
- Strong authentication with dedicated PIN code
- Certifications and agreement:

  - Voice and data protection up to SECRET level in France
- Others:
  - Security screen showing the level of security

2.1.2 Sectéra Edge

Sectéra Edge [7] is a mobile phone made by General Dynamics destined to governments (president, ministers…). The phone has been developed for the National Security Agency's Secure Mobile Environment Portable Electronic Device (SME PED) program.

General Dynamics Corporation [8] is an American defense and aerospace company found in 1899.

Software Features:

- Secure communication:
  - Secure and non-secure wireless phone, e-mail and web browsing
- DoD PKI enabled Common Access Card (CAC) support
- Supports DoD 8100.2 requirements
- Secure wireless access to the SIPRNET and NIPRNET
- Storage:
  - Type 1 [9] encrypted storage of classified data
- OS:
  - Microsoft Windows Platform
- Certifications and agreement :
  - NSA certified, DISA approved
- Interoperability:
  - U.S. Type 1 and Homeland Security (Suite B)
  - NATO, Coalition, Australia, New Zealand, Canada, U.K.
  - SCIP
  - HAIPE
- Others:
  - Separation of Classified and Unclassified applications
  - One-touch switching between classified and unclassified PDA functions

Hardware Features:

- Memory:
  - RAM : 128 MB RAM (64MB classified, 64MB unclassified),
  - Internal Flash Memory: 192 MB Flash Memory (128 MB classified, 64 MB classified),
  - External Flash Memory: microSD expansion slot up to 2GB
- Radio: The wireless communication modules are interchangeable
  - GSM quad-band 850/900/1800/1900 MHz, 3G/3G+ 2100-1900-850 MHz

  - Or CDMA 800/1900 MHz
  - Or Wi-Fi b/g
- Miscellaneous:
  - Environment :
    - MIL-STD-810F
    - Operating Temp between -23° and 60°
    - Storage Temp -55° and 75°

2.1.3 Boeing Black Smartphone by Boeing

Boeing Black [38] is a mobile phone made by Boeing destined to governments (president, ministers…). Boeing is an US multinational corporation specialized on aeronautics, aerospace and defense.

Software Features:

- Embedded FIPS 140-2 Key StorageSecure and non-secure wireless phone, e-mail and web browsing.
- Storage:
  - Secure access to unclassified and classified data
- OS:
  - Android OS with enhanced software security policy
- Others:
  - Configurable OS Security Policies
  - Integration of the BYOD (Bring Your Own Device) solution of BlackBerry(BES12)

Hardware Features:

- CPU:
  - Dual 1.2GHz ARM Cortex-A9
- Memory:
  - External Flash Memory: microSD expansion slot
- Radio:
  - LTE 700/1700/2100
  - GSM quad-band 850/900/1800/1900 MHz
  - WCDMA 850/1900/2100 MHz
  - Bluetooth 2.1
- Miscellaneous:
  - Dual Sim

2.1.4 Cryptophone 500 (CP500i) by GSMK

The CryptoPhone 500 [1] is a secure mobile phone made by a German company GSMK destined to steering committee members and companies operating in strategic or sensitive

areas. The company develops and produces satellites and phones (mobile and desktop) that provide end-to-end voice encryption.
All GSMK CryptoPhone products come with their full source code published.

Software Features:

- Secure end-to-end encrypted voice over IP calls :
  - 4096 bit Diffie-Hellman key exchange with SHA256 hash function
  - AES256 and Twofish, counter mode used
  - Encryption keys are destroyed as soon as the call ends
- Storage:
  - Encrypted storage system for contacts, messages, and notes with smart folders protects data at rest against unauthorized access
- OS:
  - Secure Android OS built from source code with granular security management and streamlined, security-optimized components and communication stacks
  - Configurable OS security profiles: Hardware module controller and permission enforcement module control access to network, data and sensors (camera, microphone, etc.).
- Baseband firewall:
  - Protection against over-the-air attacks with constant monitoring of baseband processor activity
  - Baseband attack detection and initiation of countermeasures
  - IMSI-Catcher

Hardware Features:

- Radio:
  - GSM quad-band 850/900/1800/1900 MHz
  - UMTS HSDPA / W-CDMA 850/900/1900/2100 MHz with HSUPA and HSPA+ support
  - Wi-Fi a/b/g/n/ac

2.1.5 Hoox m2 by Bull (ATOS)

The Hoox m2 [2][3][4] is a secure mobile phone made by a French company ATOS destined to steering committee members and companies operating in strategic or sensitive areas. This phone has been approved for French, NATO and EU Restricted communication level.

Software Features:

- Authentication with remote card (2048-bit RSA)
- G&D smartcard - EAL5+ certified (ISO15408)
- Secure end-to-end encrypted voice over IP calls:
  - AES256
  - Single-use session keys for voice, SMS and data

    - 2048 bits Diffie-Hellman key exchange
- OS:
    - Android OS
- Certifications and agreement [2]:
    - ANSSI: for protection of the information marked “Diffusion Restreinte”:
        - Classified “Spécial France”
        - Classified “Diffusion Restreinte OTAN”
        - Classified UE/UE Restricted
        - Classified EUROCOR Restricted
- Others:
    - Cryptosmart™ applet - EAL4+ certified (ISO15408)
    - Integration with existing PKI (X.509 standard)
    - Store enterprise
    - Protection against “man in the middle” attacks
    - 2 modes :
        - Installed mode : the whole solution is installed at the customer
        - Hosted mode : the central system is installed in Bull Data Center in France

Hardware Features:

- CPU:
    - Quad Core 1.2GHz Cortex A5
- Memory:
    - RAM : 1GB
- Radio:
    - GSM quad-band 850/900/1800/1900 MHz
    - 3G/3G+ (2100-1900-900 MHz)
    - Wi-Fi b/g/n
    - Bluetooth 3.0
- Miscellaneous:
    - Fingerprint reader

2.1.6 Blackphone 2 by Silent Circle

The Blackphone [5] is made by the Swiss company Silent Circle destined to public. It is based on a modified version of Android named Silent OS.

The company [6] has been founded recently in October 2011. The company focuses on providing secure mobile phones for publics. Their products enable encrypted phone calls, text messaging and video chat.

Software Features:

- OS:
  - Silent OS based on Android OS
- Baseband firewall:
  - No
- Certifications and agreement:
  - No

Hardware Features:

- CPU:
  - Qualcomm Snapdragon 615, 1.7GHz octo-core (Cortex A53)
- Memory:
  - RAM : 3 GB,
  - Internal Flash Memory: 32GB
- Radio:
  - GSM (No details)
  - 3G/3G+ (No details)
  - Wi-Fi b/g/n/ac
  - Bluetooth 4.0 LE
- Display: 5.5” Full HD

2.1.7 Teopad by TCS

Teopad [23] is not a mobile phone but a software solution made by Thales destined to steering committee members and companies operating in strategic or sensitive areas. Teopad creates a dedicated trusted professional workspace on the terminal that is completely separate from the user's personal space. This environment, which is encrypted and protected by strong authentication, contains all the applications, data and settings required by the user for their professional activities. The professional workspace has no effect on the user’s personal settings and in doesn’t restricts the use of personal applications.

Software Features:

- Strong authentication
- X.509 V2 and V3 support
- Secure end-to-end encrypted telephone communication, text messages and video conferences:
  - SIP-TLS
  - SRTP
  - Open solution compatible with third-party terminals
- Storage:
  - Encryption of all professional user data and of the data generated by the professional applications OS
    - AES 128 ou 256 bits en mode GCM.

- Baseband firewall:
    - No
- Certifications and agreement [22]:
    - Voice and data protection up to “SECRET DEFENSE” in France
    - « Certification de sécurité de premier niveau » by ANSSI in France
- Others:
    - Secure application store
    - Compatible with all types of consumer and business applications

Hardware Features:

- Compatible with all Android devices.

2.1.8 The workplay tablet by InZero Systems

The workplay [17][18] tablet is a solution for securing a tablet made by InZero System. The solution is based on the hardware separation using the ARM TrustZone [19] Technology.

The company creates and develops innovative security technology that addresses the vulnerabilities of software-based security solutions.

InZero focused on security problems caused by the use of mobile devices for both enterprise and personal activity. The user’s personal activity in casual browsing, social media, emails, etc. This behaviour increases the risk of the introduction of malware that will eventually be able to access and compromise company data.
By using the TrustZone technology, the company achieved to provide two-hardware separated Android OSs in a single device, one will be only dedicated to personal activity and the other one will be dedicated to professional activity.

The hardware-separated OSs are respectively called the “WorkZone” Tablet and the “PlayZone” Tablet, in acknowledgment of typical tablet use for both such purposes. When one Zone is activated, the other Zone is simultaneously deactivated and placed in hibernation. Switching between Zones is done instantaneously by touching an icon.

Software Features:

- Storage:
    - Separation between the 2 OSs using the TrustZone technology
- Others:
    - Solution based on TrustZone technology

Hardware Features:

- CPU:
    - Freescale iMX6 quad-core CPU.
- Memory:
    - Internal Flash Memory: 16GB,32GB,64GB or 128GB depending on the version,
    - A separation between memory areas is made equally between the memories dedicated to each zone (WorkZone and PlayZone).

2.1.9 Knox by Samsung

Knox [20][21] is a solution of securing tablets and Galaxy mobile phones made by Samsung destined to public. One of the main features of this solution is to create a dedicated trusted professional workspace on the terminal that is completely separated from the user's personal space.

Samsung is a South Korean multinational conglomerate company. Samsung Electronics, a Samsung subsidiary, is one of the world’s largest information technology companies.

Software Features:

- Strong authentication
- Secure end-to-end encrypted telephone communication, text messages and video conferences :
    - SIP-TLS
    - SRTP
    - Open solution compatible with third-party terminals
- Storage:
    - Encryption of all professional and user data (the decryption key is stored encrypted by a Device-Unique Hardware key)
- Certifications and agreement [21] :
    - Certification from the Department of Defense(US) STIG
    - CESG(UK)
    - NIST FIPS 140-2 for the VPN
    - DISA APL under Common Criteria

Hardware Features:

- Compatible with Galaxy Android devices (recent ones only)

2.1.10 Citadel Team

Citadel Team is a tool made by Thales for collaborative work that brings together: private messages, group chat and content sharing (files, pictures, positioning).

Software Features:

- OS:
    - iOS
    - Android (At least version 5.0)
- Encrypted telephone communication between endpoint and infrastructure :
    - SIPS(TLS-TLS 1.2 with AES 256 bits)
- Secured key negotiation from endpoint to endpoint :
    - ZRTP AES 128 bits
- Others:
    - SaaS service hosted and operated by Thales with high availability (SLA 99.7%)

2.1.11 Citadel Phone

Citadel Phone is a software solution made by Thales destined to steering committee members and companies wanting to communicate securely. The application is present in both Android and iOS. The application permits HD Calls (voice, video) and instant messaging securely.

2.1.12 KATIM Phone

This secure phone is made by DarkMatter [138][139] which is a cyber-security company based in UAE. According to DarkMatter, KATIM uses a hardened Android 7.x (Nougat) operating system to safeguard against vulnerabilities, and features end-to-end data encryption and secure storage for keys. Its multilevel tamper protection also provides high assurance against physical threats, and frequent security patches protect against evolving vulnerabilities.
It has four levels of security protection - the phone, its operating system, applications and a cyber-command center.
The phone is preloaded with apps that have security in mind, such as encrypting voice calls and a messenger that automatically secures photos and expires after a time limit.
The Katim operating system is said to be compatible with almost any smartphone running Google's Android, and is apparently secure against unauthorised modifications.

Software Features[145]:

- OS:
  - Hardened Android 7
- Secure communication:
  - Encrypted one-to-one voice call and ephemeral messages
- Others:
  - Bootloader: secured against unauthorized modifications and it is encrypted
  - Multilevel tamper protection and detection
  - Locked Mode: Microphones and Camera disabled in this state by using a hardware switch
  - Two-factor authentication by using fingerprint sensor
  - USB interface blocking
  - Secure App store containing a collection of vetted apps

Hardware Features:

- CPU:
  - Qualcomm Snapdragon 821 octo-core (4x Qualcomm Kryo CPU).
- Memory:
  - RAM : 4 GB,
  - Internal Flash Memory: 64GB
- Radio:
  - GSM

    - 3G/3G+/4G
    - Wi-Fi
- Bluetooth 4.2
- Display: 5.5” IPS LCD Full HD

2.1.13 Solarin Phone

This phone is made by Sirin Labs, founded in 2013 with the purpose of providing a secure smartphone for CEOs and billionaries [140][141][142]. Sirin labs claims that the Solarin phone provide a military grade security because of the hardware 256-bit AES encryption. This feature is provided by another company (KoolSpan [143]) providing secure communication solutions.

Software Features:

- OS:
    - Android 5.1 Lollipop
- Secure end-to-end encrypted telephone communication, text messages and video conferences using 256-bit AES encryption
- Others:
    - Security Switch button is used to switch to an encrypted communication

Hardware Features:

- CPU:
    - Qualcomm Snapdragon 810 octo-core (4x Cortex A57 + 4x Cortex A53)
- Memory:
    - RAM : 4 GB,
    - Internal Flash Memory: 128GB
- Radio:
    - GSM
    - 3G/3G+/4G
    - Wi-Fi
    - Bluetooth 4.1 LE

2.1.14 BlackBerry DTEK 50

This phone is made by BlackBerry, the Canadian phone-maker company. This smartphone is based on an enhanced version of Android 6.0 and is destined to steering committee members and companies operating in strategic or sensitive areas.

DTEK is a security feature added by BlackBerry to the smartphone. It automatically monitors the OS and the applications. It gives an overall security rating of the phone and advices to improve it (no exact detail is given about this functionality). DTEK tracks applications and notifies when someone is:

- Taking pictures or videos without your knowledge
- Turning your microphone on

- Sending a text message
- Accessing your contacts or location

Software Features:

- OS:
  - Android OS 6.0 Marshmallow
- Baseband firewall:
  - No
- Certifications and agreement :
  - No
- Others:
  - DTEK - OS monitoring application

Hardware Features:

- CPU:
  - Qualcomm Snapdragon 617 octo-core (Cortex A53)
- Memory:
  - RAM : 3 GB,
  - Internal Flash Memory: 128GB
- Radio:
  - GSM
  - 3G/3G+
  - Wi-Fi
  - Bluetooth 4.1 LE

2.1.15 Summary and usability in SAFURE

The concepts developed for SAFURE project in WP4 regarding the security aspects could be applied to all telecommunication devices. Such possible security aspects could be secure boot, secure update, secure storage, spatial isolation provided by the high assurance separation kernel.

Specifically, safety aspects in WP4 could be applied in telecommunication devices when they are used as IMD devices. Such possible safety mechanism could be the timing-integrity by using new protection mechanisms supporting dynamic resource sharing (such as priority-based task scheduling) as well as new analytical verification methods considering the specific effects of errors and attacks already at design time.

Therefore, by applying these aspects, it could be demonstrated that COTS platforms such as smartphones or tablets are suitable devices that can handle both information body sensors and e-health IT systems hub services and end-user terminal services.

2.2 Automotive devices

Here, the main ECU platforms that belong to the actual automotive market are addressed. In the following paragraph, we will consider Magneti Marelli S.p.A [61], Robert Bosch S.p.A [106], and Continental AG [107], as the major automotive components providers.

2.2.1 Magneti Marelli - Gasoline GDI ECU [131]

The main control functions are:

- Complete torque management, Magneti Marelli has been producing a system based on torque control with three-level supervision called “safety” since 1999
- Blend control
- Ignition management
- Management of swirl/tumble actuators (flaps and variable geometry)
- Turbo boost management (turbocharger and/or volumetric compressor)
- Fuel composition and volatility recognition
- Valve opening management (VVA- Variable Valve Actuation, VVT- Variable Valve Timing)
- EGR (Exhaust Gas Recirculation) management
- CO_2 reduction control (fuel consumption reduction)

The hardware component of the ECU is designed to allow excellent architectural flexibility, resulting in optimized costs and performances.

In fact, the hardware composition can be adapted to the various engine/vehicle configurations through a “scalar” approach, thanks to which it is possible to start from a full version of the same logic core and arrive at optimized versions depending on market specifications.

The GDI software is developed through robust design based on:

- Modular type Software architecture, compliant with AUTOSAR European standard [123]
- Automatic generation and optimization of the Software code through specific tools
- SPICE 2-certified development process [116]
- Safety standard ISO 26262 [50]

The Time-to-Market is reduced thanks to the possibility of carrying out a preliminary calibration in a simulated environment. Due to the modular approach, the GDI software can be fully customized for different customer requests. The automatic code generation also allows the co-design software prototyping approach.

2.2.2 Magneti Marelli - Gasoline PFI ECU [132]

The main control functions are:

- Complete torque management, Magneti Marelli has been producing a system based on torque control with three-level supervision since 1999
- Blend control
- Ignition management
- Management of swirl/tumble actuators (flaps and variable geometry)
- Turbo boost management (turbocharger and/or volumetric compressor)
- Fuel composition and volatility recognition

- Valve opening management (VVA- Variable Valve Actuation, VVT- Variable Valve Timing)
- EGR (Exhaust Gas Recirculation) management
- Control of polluting gas emission according to regulations in force in the different countries where the products are marketed; catalytic converter activation and control strategies
- Control of CO2 emissions (fuel consumption management)

The hardware component of the Electronic Control Unit (ECU) is designed to allow excellent architectural flexibility, resulting in optimized performances depending on the application (2/4/6-cylinder engines).

In fact, the hardware structure can be adapted to the various engine/vehicle configurations through a "scalar" approach, thanks to which it is possible to start from a full version of the same logic core to arrive at reduced versions for simpler vehicles or for different market needs. The specific management software for Port Fuel Injection (PFI) engines is developed through a design based on:

- Modular type, model-based software architecture for a reutilization that crosses over different applications
- Automatic generation and optimization of the software code
- SPICE 2 certified development process [116]
- AUTOSAR compliant [82]
- ISO 26262 compliant [50]
- Pre-calibration in a simulated environment
- Immobilizer
- Management of communication protocols: CAN, LIN, K line

The Time-to-Market is reduced as a consequence of the fast prototyping which also allows customization according to the customer's requests.

Magneti Marelli supplies "turnkey" systems. In other words, systems that are completely optimized from the calibration standpoint based on the specific skills developed over the last decades at different facilities located in Europe, China, United States, India and South America. These systems are developed specifically depending on the different needs of the markets addresses by Magneti Marelli.

2.2.3 Magneti Marelli - AMT Gearbox [133]

The robotized gearbox is a type of gearbox for automotive use whose name comes from the "robotization". This entails the substitution of manual drives of a regular manual gearbox with automatic drives. The ECU independently carries out the clutch and gear engagement movements by means of specific actuators. This control unit carries out the clutch disengagement process, the change in gear ratio and the subsequent clutch re-engagement.

During this operation, a message is sent to the engine control unit, through the CAN bus network, to 1) ignore the drive torque request coming from the accelerator pedal so that the revolutions decrease while upshifting or 2) to accelerate the engine while downshifting, with an appreciable "double-clutching" effect.

The Magneti Marelli robotized gearboxes feature hydraulic actuation of the movements, which is characterized by faster actuation speed and consequently improved sports performances and greater vehicle comfort.

Strong of a longstanding experience in this sector, which began with the first robotized gearbox created for the Formula 1, Magneti Marelli supplies its robotized gearboxes to all manufacturers of super sports cars (Ferrari, Maserati, Aston Martin, Lamborghini and Audi), compact cars and commercial vehicles.

Through a process of constant technological evolution, today it has reached the “mechatronics” generation, which for the first time integrates in a single kit the electronic control part with the hydraulic transmission part, allowing a significant improvement in performances, both in terms of gearshift speed and comfort

Magneti Marelli’s robotized gearboxes also offer a dual operating mode: manual or automatic. In the completely automatic mode, the control unit is responsible for deciding on the gear change. In the manual mode, the driver chooses the gear to be engaged using a lever similar to the traditional one or by means of steering wheel controls or paddles.

ADVANTAGES

This type of transmission offers the following advantages:

- POSSIBILITY OF CHOICE: With the Magneti Marelli robotized gearbox, drivers choose the driving style, as a light touch of the gearshift lever is all it takes to switch from automatic mode to manual mode and vice versa, all without having to take their foot off the accelerator. Even in automatic mode, drivers maintain control by acting on the gearshift lever they can instruct the system on the desired gear. In addition, all the relevant information can be displayed on the dashboard to allow drivers to have control over the situation at all times.
- COMFORT: the Magneti Marelli robotized gearbox makes driving less stressful. In automatic mode, the driver can concentrate on driving without having to worry about shifting gears, while in manual mode its gearshifts are made easier since a simple touch of the lever is all that is needed, without having to engage the clutch pedal and without taking the foot off the accelerator.
- SAVINGS: Thanks to the electronic control unit, the Magneti Marelli robotized gearbox saves fuel by carrying out an optima gear change in relation to driving conditions, speed-engine revolutions. The system is based on a technology that is very different from the traditional automatic transmission which, on the contrary, tends to significantly increase fuel consumption. In fact, FreeChoice [137], allows a 4% savings in fuel on country roads and motorways and over 10% in city traffic.
- FOCUS ON THE ENVIRONMENT: lower consumption also means reduced CO2 emissions: the Magneti Marelli robotized gearbox is eco-friendly, as it allows a reduction of up to 5% in the emissions of polluting gases compared to vehicles fitted with a manual transmission.
- SAFETY: the robotized gearbox constantly monitors the transmission system. It also prevents possible driver mistakes and avoids improper maneuvers and unwanted engine stops. Since drivers do not have to worry about shifting gears, they can fully concentrate on driving, always keeping both hands on the steering wheel. For all-round safety.

2.2.4 Bosch – Gasoline GDI ECU [134]

The main control functions are:

- Inward-opening solenoid injector
- Multihole injector (MHI) with high variability concerning spray angle and spray shape
- For variable system pressure up to 20 MPa nominal
- Suitable for highly integrated power stage (65 V booster voltage)
- Easy assembly and fixing for central or side installation at the cylinder head
- Option: variable lengths

By its flexibility regarding spray shape as well as flow rate the high-pressure injector is qualified for various engine types. Today, the injector is applied worldwide in a 1.0 3-cylinder as well as a V8 with turbocharging, both for consumption (e.g. downsizing) and fun-to-drive concepts (e.g. in combination with turbocharging).

Thereby the high-pressure injector supports different engine operating points – from high-pressure start with catalyst heating and multiple injection to homogeneous full load.

2.2.5 Bosch – PFI ECU [135]

Port fuel injection is the most widely used powertrain system for gasoline engines in the world. This proven technology still retains a great amount of potential to further reduce fuel consumption and emissions.

When used in engines with a specific power of approximately 60 kW/liter and downsizing concepts of up to 25%, gasoline port fuel injection offers significant cost advantages over systems with high-pressure direct injection. As a low-pressure system (system pressure: approx. 6 bar), gasoline port fuel injection has a comparably straightforward operating strategy: simple injection control based on degrees of freedom with the injection time window. This does away with the complex requirements of high-pressure control (system pressure: approx. 150 bar) along with the high-pressure pump, the high-pressure sensor, the control system for the fuel-supply control valve, and the high-pressure injectors for multiple injections.

Gasoline port fuel injection's robust combustion process tolerates even lower-quality fuels. Its reduced range of functions compared to systems with high-pressure direct injection allows simple software to be used, with a corresponding reduction in expenditure on system diagnostics.

Bosch develops and manufactures innovative powertrain technology for vehicles with gasoline port fuel injection. Bosch's portfolio includes components for fuel supply, fuel injection, intake air adjustment, ignition, engine management, and exhaust gas treatment, which are available worldwide either individually or as part of coordinated systems

2.2.6 Continental - TCU [136]

Continental actively drives forward the integration of control units inside the transmission. Since the control unit is immersed in transmission fluid, this system profits considerably from our extensive expertise in electronics design and manufacturing, ranging from Printed Circuit Boards (PCBs) to extremely shock and temperature resistant ceramic substrate technology, e.g. Low Temperature Co-fired Ceramics (LTCCs) or Thickfilm Ceramics. The latest milestone in this area is a new high temperature capable organic substrate technology (BD-HDI), an innovation of the Business Unit Transmission.

This innovative transmission technology has been in series production since 2003; with its smooth gearshifts and no shuddering or traction torque interruption, the DCT combines the ease of an automatic transmission with the dynamism of a manual gearshift, saving fuel and reducing emissions. The heart of the DCT is Continental‘s control unit – one of their development highlights, which proofs their expertise and innovative strength.

2.2.7 Summary and usability in SAFURE

The concepts developed for SAFURE project in WP4 regarding the safety aspect such as memory protection and timing protection can be applied for all ECU Software for automotive project. So, the benefits are that they can guarantee the ISO26262 requirements also for legacy OS and avoid possible faults in Q.M. system cause failure on safety relevant part of a system. Furthermore, the secure communication avoids intrusions such as malicious attacks into the system.

2.3 IMD (Implantable Medical Devices)

Implantable medical devices are used to augment and monitor health conditions. IMDs usually comprise of energy efficient, low-performance processing platforms that perform simple operations. However, IMDs have strict safety and security requirements which can make some of the results in SAFURE relevant for their development.

2.3.1 Insulin Pumps

The company Debiotech [51][52] developed the insulin pumps "JewelPUMP" and the "JewelPUMP2" based on the use of microfluidic Micro-Electro-Mechanical Systems Technology in order to treat diabetes patients. This pump is waterproof and can be placed on a disposable skin patch guaranteeing a continuous supply of insulin. The dosage of the insulin delivery is regulated by a corresponding smartphone device – the "JewelCOM" - including a blood-glucose metre.

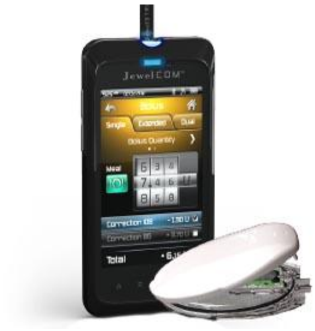

Figure 2: JewelPUMP and JewelCOM [51]

Debiotech is an innovative Swiss company that was founded in 1990 and specialized in the development of affordable and highly innovative medical devices.

Features of the JewelPUMP [51]

- Reservoir size: 5 mL (500U)
- Dimensions: approx. 70 x 40 x12 mm
- Weight: 25 grams (incl. battery)
- Water Resistant (IPX7)

The JewelCOM [51]

- Touch-screen and colour display interface
- Integrated BGM (according to ISO 15197:2013)
- Bolus calculator
- 5 editable Basal Profiles
- 5 editable Temporary Adjustment Profiles
- Customizable reminders
- 3G and GPRS communication

As another example, the Swiss company Ypsomed also developed an insulin pump device – the OmniPod - and a Personal Diabetes Manager (PDM) displayed in Figure 3.

Figure 3: OmniPod insulin pump and PDM

Features of the OmniPod [53]

- Reservoir size: 200U
- Dimensions: approx. 39 x 52 x 255 mm
- Weight: 25 grams
- Water Resistant (IPX8)

Modern insulin delivery systems typically include [54]:

- An insulin infusion system with a wireless interface that delivers the insulin subcutaneously
- A glucose monitor with a subcutaneous sensor for glucose measurement and a wireless transmitter
- An Insulin management system that allows the patient to remotely change pump settings or manually trigger insulin delivery

The glucose monitor thereby transmits the collected data to the display of the management system. In response to the measured data, medical personnel can adjust the settings of the pump in the management system that passes the new settings to the insulin pump.

2.3.2 Cochlear Implants [55]

A cochlear implant is an implanted medical device that enables persons who are profoundly deaf to have a sense of sound. In contrast to a hearing aid that amplifies sounds at the outer ear, this implant bypasses the damaged part of the ear.

The US American company Cochlear developed the world's first[1] multi-channel cochlear implant called Cochlear Nucleus System about 30 years ago. Today there exists a variety of wireless features to suit the needs of individuals. A remote control is available in order to adjust settings on the sound processor like volume and sensitivity. Additionally, there exist wireless features like mini microphones to improve sound quality in busy places and phone clips that use Bluetooth in order to facilitate phone calls [55].

[1] However in France, Bertin holds the first patent for such system and an Austrian team developed the first multi-channel system … back in 1977.

Figure 4: Cochlear Nucleus System [55]

Figure 5: Wireless accessories for the Cochlear and the Baha Implant [55]

In addition to cochlear implants, there are also Bone Conduction Implants available on the market. Cochlear issued the Baha Bone Conduction Implant [124] that uses the body's natural ability to bypass the damaged outer or middle ear in order to send clear sends directly to the inner ear. For the Baha implant the same wireless features as for the Colchea Nucleus System as well as a remote control implant exist, however the Baha 5 sound processor can stream directly from an iPhone, iPad and iPod touch using a dedicated app.

2.3.3 Implantable cardiac defibrillator device

A pacemaker is used to regulate a patient's cardiac rhythm by applying electrical impulses. However, an Implantable Cardiac Defibrillator (ICD) extends the capabilities of a pacemaker in that way that it can generate larger shocks to reset an unsustainable heart rhythm. Commonly IMDs have a single-use battery, where they get the power from. These are sealed inside the device to prevent heating up of the tissue around. Therefore, there is a stringent need to for ultra-low power consumption, as the battery has to last for at least 5 years.

In case of an implantable cardiac defibrillator, there is a radio interface for clinical adjustments and status reports. ICDs may be connected with a monitoring device where the status is recorded or with an ICD programming device for new configurations.

Medronic developed the Conexus Wireless Telemetry System (Figure 6: Conexus Wireless Telemetry system) that uses a Medical Implant Communications Service radio frequency band that is designed for medical devices worldwide and protected against interference. The radio frequency lies between 402 – 405 MHz for this type of implant [56].

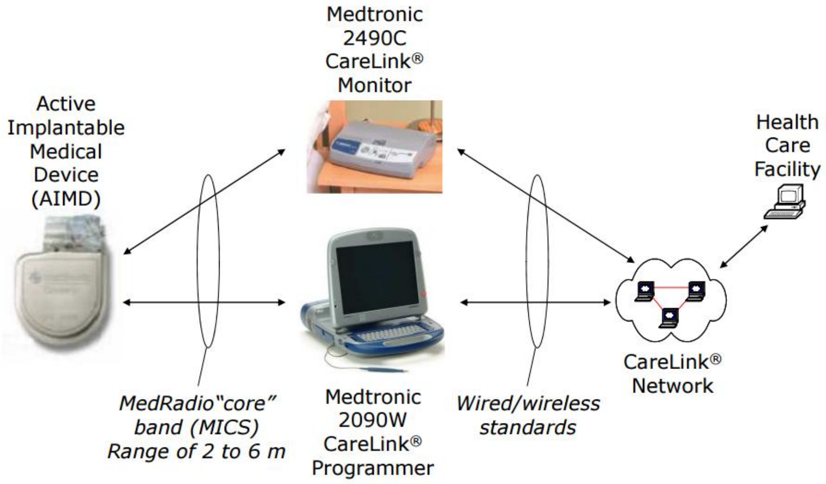

Figure 6: Conexus Wireless Telemetry system

2.3.4 Deep brain stimulators

Deep brain stimulators are brain implants that send electric signals to specific regions of the brain for treatment of movement and neuropsychiatric disorders. Deep brain stimulators have been specifically useful in improving the quality of life for people with Parkinson's disease.

The deep brain stimulator (Figure 7: Mediatronic deep brain stimulator) has three essential parts: 1) Electrode, which is inserted through a small opening in the skull, 2) extension, which is an insulated wire connection the electrode with neurotransmitter 3) Neurotransmitter, which generates the signals and also serves as the battery pack.

Mediatronic [57] is a USA based company which makes deep brain stimulators. Their devices are FDA approved for MRI scans and provide solutions for people with Parkinson's disease, essential tremor and dystonia

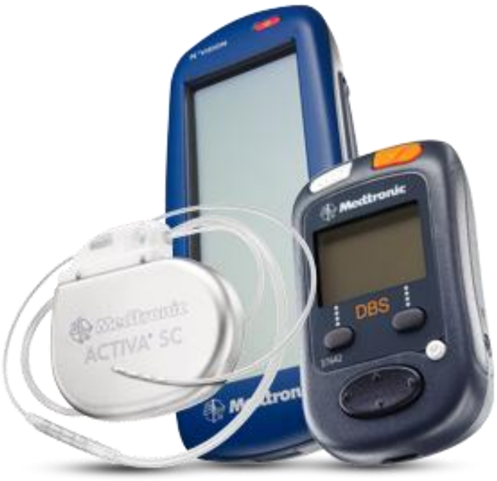

Figure 7: Mediatronic deep brain stimulator

2.3.5 Gastric Stimulator

Gastric stimulator (Figure 8) is a device used to decrease nausea and vomiting in some patients with gastroparesis. Gastric stimulator device is implanted in the abdomen region and sends mild electrical signals to control the effects of gastroparesis.

Mediatronic also makes gastric stimulators. The use of these devices is recommended for patients with refractory symptoms of gastroparesis.

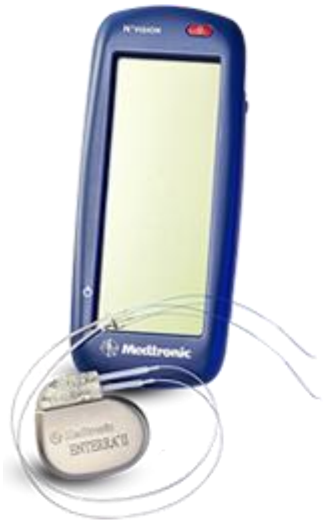

Figure 8: Mediatronic gastric stimulator [58]

2.3.6 Foot drop implants

Foot drop implants are designed to help people with drop foot condition that may be caused due to a stroke. This condition is a gait abnormality in which the forefoot drops. It causes impaired ability to raise toes, or raise foot from the ankle. As a result, walking requires high concentration and walking speed, efficiency and balance are affected. These implants use Functional electrical stimulation to stimulate the serves which help correct drop foot.

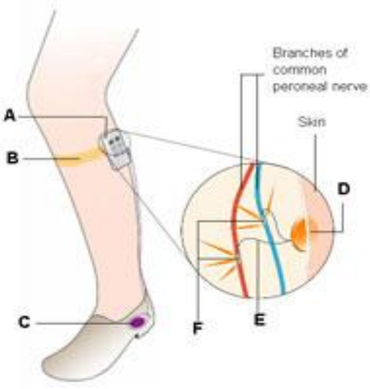

Figure 9: Finetechmedical foot drop implant

Finetech medical [125], which is a UK based company, makes foot drop implants. Their solution has four components: The external Controller (A) is positioned over the site of the Implant Receiver (D) using the Leg Strap (B). The Footswitch (C) is placed under the heel of the foot inside the shoe and plugged into the Controller.

2.3.7 MINIMED 670 system

Recently, Madiatronic has developed the MINIMED670 System [157] which constitutes the first and only glucose monitor sensor which is FDA approved and trusted to control insulin dosage. As a result of this sensor, MINIMED670 system is able to closely monitor and regulate blood glucose levels. This enables “auto mode” of the device in which the MINMED670 automatically adjusts insulin delivery every five minutes such that blood glucose level is within a specified target range. The system is also waterproof, to enable underwater activities.

Figure 10: MINIMED 670 system

2.3.8 Summary and usability in SAFURE

Since the processing platforms used IMDs are not required to provide multi-usage capabilities within a single device, the timing integrity results of SAFURE will likely not be relevant here. However, IMDs usually contain sensitive information (patient history, programming of dosage in case of insulin pumps etc.). Due to this sensitive information, the data integrity results of SAFURE are expected to be relevant. The sensibility of the information manipulated by IMD devices requires a high level of security to ensure confidentiality and safety of the patient.

2.4 Aeronautical devices

Unlike other domains, where the number of interconnected systems is the topmost design constraint, the avionic domain is handling a variety of systems with different level of criticality. The interconnections are possible only within a given level of criticality and serve different purposes, depending on the level of criticality. For higher levels, redundancy is the key to reliability. The aircraft itself is a single device running a wide variety of systems with different levels of criticality.

Criticality in avionics:

In the RTCA DO-178B and RTCA DO-254 standards, safety levels are represented with Design Assurance Level (DAL) and are defined in terms of the impact and maximum probability of a failure on the flight. The safety levels range from DAL-A where the effect of a failure will lead to catastrophic consequences such as plane crash or loss of life, to DAL-E where the effect of a failure will have no impact on the plane such as impacting the on-flight video of the passengers. Safety levels are presented in Figure 11 together with examples of systems running at each safety level.

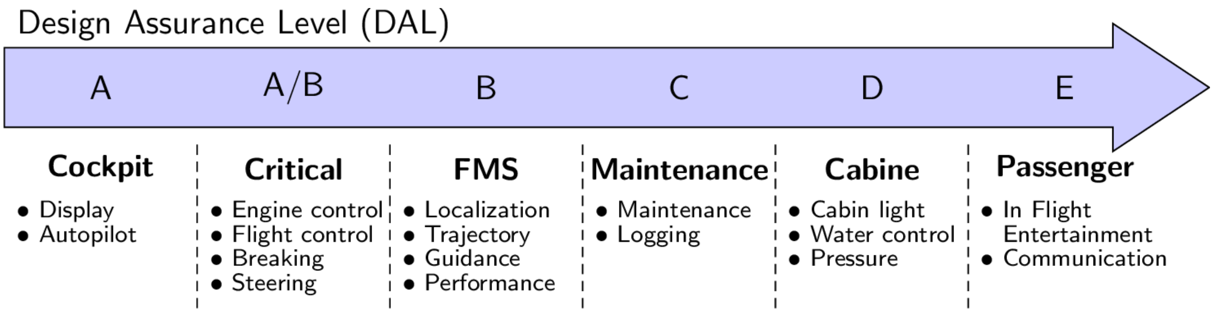

Figure 11: Safety in avionics: Design Assurance Levels

Mixed-criticality in avionics:

Bringing mixed-criticality to avionics could involve running applications with different DAL level in the same system. It is still quite unlikely to mix DAL-A application with DAL-E application due to the high certification and requirements of DAL-A systems. However, for DAL-C and below systems, it could be a viable solution.

Specific requirements of avionic systems:

Multi-core architectures possess the required inherent performance level for future avionic applications, but bring some predictability issues that may endanger the certification processes in avionics. Beside the predictability requirement, some other properties are also critical for the avionic applications:

- The performance requirement reflects the expected requirements in term of performance for next generations of the system. It is correlated with how well the solution requires the extra performance of the multi-core platform.
- The legacy requirement illustrates the necessity for legacy support. Considering the high certification cost of high-critical applications, it is important to avoid any modification to such a system, as it would involve to re-certify the system again.
- The partitioning requirement indicates how much the system relies on robust spatial and time partitioning.
- The integration requirement indicates how much the system fits into a multi-actor integration process. It has to be evaluated against the integration into an industry process property.
- The application complexity reflects the complexity of the source code. It has a significant impact on the easiness to port this application to a multi-core environment.
- The certification costs estimates the overall cost when certifying the system. This is tied both with the DAL level of the application and its complexity.
- The diversification requirement reflects the requirements for replication and diversification. It is a common practice in avionics to replicate most critical systems to protect against faults and decrease failure probability.

It is quite hard to rank the above-defined requirements. In fact, the ranking depend on the system. In the remaining of this subsection, we consider five different systems by decreasing level of criticality; we evaluate each of these requirement properties, and conclude if the solutions proposed in SAFURE could be considered for such a system.

2.4.1 Full Authority Digital Engine Control (FADEC)

The Full Authority Digital Engine Control (FADEC) [126] is a critical subsystem in charge of controlling all aspects of the aircraft engine performance. Its purpose is to provide optimum engine efficiency for a given flight condition.

The flight crew has usually no means of manually overriding the FADEC engine control, and in case of a total FADEC failure occurs, the engine fails. Safety is therefore of prime concern, and redundancy with diversification is a common practice.

For such a high-critical control-command system, the equipment provider manages simultaneously the development of the hardware platform and the software applications. In this condition, the equipment designer can introduce mechanisms managing all the shared resources accesses at the application level. Therefore, proof of determinism for certifiability is performed at design time.

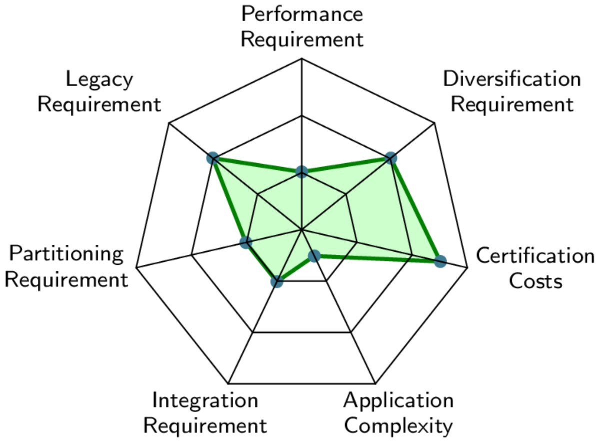

Figure 12: FADEC requirements

Figure 12 summarizes the requirements of the FADEC subsystem with regards to the requirements defined earlier. Being a control-command application, the application complexity remains low with average future requirements in performance. However, the certification costs and the ability to diversify are of prime concern for a DAL-A subsystem.

Applicability of the solutions proposed in the SAFURE project: The high level of certification requirements of DAL-A applications will enforce the usage control solution guaranteeing the absence of interferences, rather than reactive solutions has like the ones developed in the SAFURE project.

2.4.2 Integrated Modular Avionics (IMA)

Integrated Modular Avionics (IMA) [127] systems were introduced to run several high performance missions computing software on the same hardware component. IMA subsystems safety requirements can range from DAL-A down to DAL-D.

Their purpose is to: 1) reduce weight, space and energy requirements by sharing the same hardware; 2) reduce conception and certification costs with an incremental certification process; 3) reduce maintenance and upgrade costs during the aircraft lifespan.

The DO-197 standard organizes IMA development though three different actors: The *platform supplier* developing the hardware platform and kernel software services, the *system integrator* performing shared resource allocation for the different software functions to integrate, and several *application suppliers* developing the avionic functions.

IMA modularity simplifies the development process of avionics software, enabling concurrent and independent conception and certification of different avionic functions.

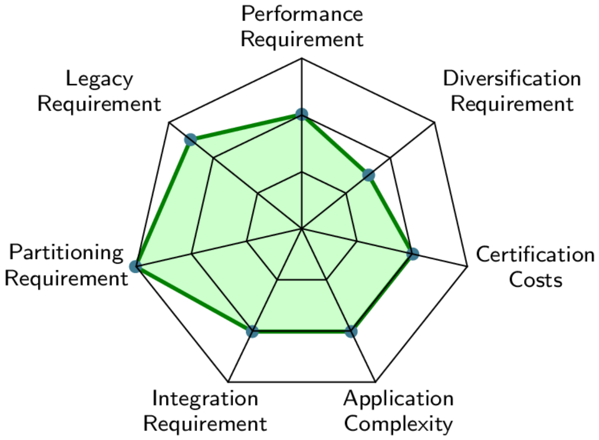

Figure 13: IMA requirements

To deal with resource sharing, IMA subsystems are strongly relying on robust partitioning, as shown in Figure 13. Running several software components on the same hardware also makes it very sensitive to legacy support.

Applicability of the solutions proposed in the SAFURE project: Integrated Modular Avionic is perfectly adapted to support mixed criticality. The high level of partitioning requirements will not allow the usage of reactive solutions developed in SAFURE. DAL-B systems will need more deterministic solutions. Secure deterministic networks, as developed by TTTech, can for example offer these features.

2.4.3 Data server subsystem

The data server subsystem is in charge of the management of the communication with satellites using SATCOM, of the crew communication and of the maintenance interface. The associated computing platform should be capable of hosting communications management services, performing some network management, and acting as a network server or file server. Having less stringent requirements in term of real-time constraints this subsystem is typically a DAL-C or a DAL-D application.

For such a system, throughput performance is more important than pure computation performance or memory bandwidth. As a consequence, most of the multi-core related interferences will occur while accessing I/Os. Otherwise, all the requirements along the other identified axes are low to average as depicted in Figure 14.

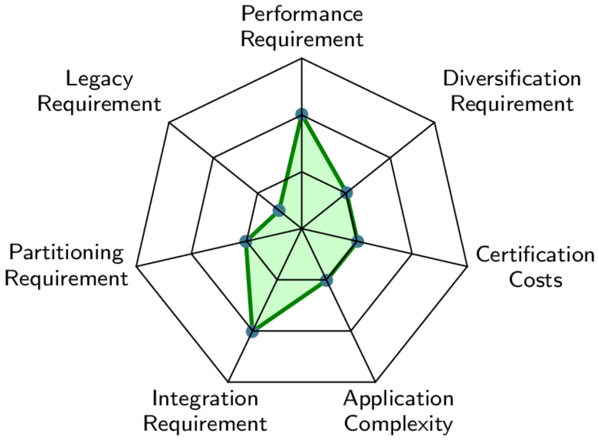

Figure 14: Data server requirement

Applicability of the solutions proposed in the SAFURE project: DAL-C and DAL-D systems are good candidates for high-critical systems for regulation-based solutions as the ones developed in the SAFURE project.

Integrated Modular Avionic is perfectly adapted to support mixed criticality. However, the high level of partitioning requirements will not allow the usage of reactive solutions as developed in SAFURE. DAL-B systems will need more deterministic solutions. Secure deterministic networks, as developed by TTTech, can for example offer these features.

2.4.4 In-Flight Entertainment subsystem (IFE)

The In-Flight Entertainment subsystem (IFE), running at DAL-E, is dedicated to the passengers' entertainment with no safety-critical requirements but an important demand for processing and communication efficiency.

The IFE subsystem is hosting multimedia applications that are very demanding in terms of performance and that can achieve a high level of complexity.

While not being purely safety-critical, IFE systems are frequently managed by external content service providers. Beyond cost efficiency, system safety and reliability remains a design issue for these systems: To contain any possible issues, IFE systems are typically isolated from the other systems of the aircraft. However, such systems usually involve miles of wiring with added weight and associated risks of voltage arcing or current leaks.

In recent years, IFE has been expanded to include Wi-Fi connectivity services through satellite networking or an air-to-ground networking, encompassing new safety / security concerns.

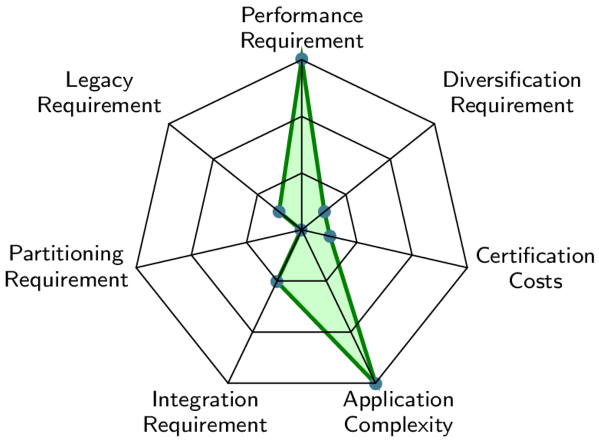

Figure 15: IFE requirements

Figure 15 summarizes the requirements of the IFE subsystem with regards to the requirement properties defined earlier. Involving mostly best-effort applications similarly to the consumer electronic market, performance is a key property. Application complexity can also be quite high, while the other properties could be relaxed.

2.4.5 Summary and usability in SAFURE

The low level of certification requirement of DAL-E applications makes them a perfect candidate for low critical application in a regulation-based system such as the one developed in SAFURE as part of WP3 and WP4. They are also very good candidates to become QoS aware applications, but it can be costly due the high application complexity to drive the application by the availability of the hardware resources.

2.5 Space devices

A number of space missions of the European Space Agency (ESA) and NASA build upon general-purpose microprocessors delivered by Cobham Gaisler, a Swedish SME, which is specialized in the development of IP technology for the Space domain. This technology has a number of properties particularly relevant for SAFURE, in particular those related to reliability (and thus safety) since Space devices are designed and validated to operate in harsh environments.

For instance, a component of a recent space mission, the Mobile Asteroid Surface Scout (MASCOT) for the Hayabusa-2 mission, builds upon the Gaisler GR712RC microprocessor. MASCOT is intended to study the near-Earth 1999JU3 asteroid as part of an ESA mission.

2.5.1 The GR712RC space device

The GR712RC is a dual-core LEON3FT processor implementing the SPARC V8 Instruction Set Architecture. It includes a number of advanced interface protocols specifically designed for radiation-hardened (Rad-Hard) aerospace applications where high reliability is a must. The GR712RC is fabricated with standard 180nm CMOS technology using a number of methods that make the processor Rad-Hard by design while keeping power low.

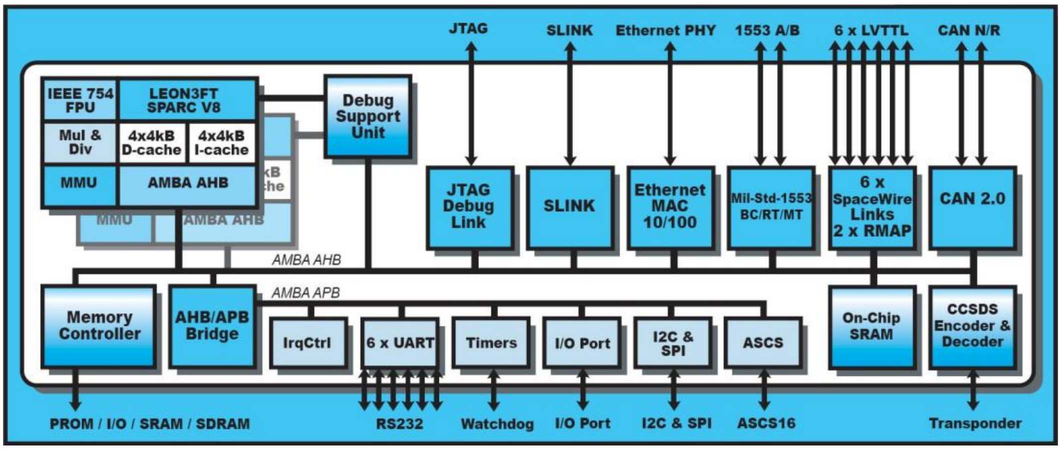

Figure 16: Schematic of the GR712RC SoC

The key features of the GR712RC are as follows:

- Abundant communication interfaces for higher flexibility to make the device usable in many applications requiring only changing interface drivers.
- Use of the AMBA Advanced High-speed Bus (AHB), to which the two LEON3FT cores are connected, together with all remaining devices with high-bandwidth requirements. AMBA is a communication protocol by ARM that defines a number of communication interfaces.
- Use of the AMBA Advanced Peripheral Bus (APB) for low-bandwidth devices. The APB is connected to the AHB through a bridge.
- Cache coherency support across the LEON3FT cores. Also, each core includes a Memory Management Unit (MMU) and an IEEE754-compliant double-precision floating point unit.
- The two LEON3FT cores can be used for asymmetric or symmetric (redundant execution) multiprocessing mode.

The GR712RC dual-Core SoC operates at 100MHz and delivers 200 Dhrystone MIPS of performance.

2.5.2 The LEON3FT microprocessor

The LEON3FT core is a fault-tolerant version of the standard LEON3 SPARC V8 core with enhancements to make it suitable for Space operation. The additional features included with regard to the standard LEON3 core relate mostly to the detection and correction of single-event upsets (SEU) in all on-chip RAM blocks:

- Transparent SEU error detection and correction in the register file and cache memories of up to 4 errors per 32-bit word or tag
- Error detection and correction introduces no performance degradation and is managed transparently with hardware-only means

On the other hand, a number of features available in the LEON3 are not available in the LEON3FT such as local data and instruction scratchpads and cache locking capabilities.

Error detection and correction in RAM blocks is performed by means of Error Correction Codes (ECC). Those ECC codes are tuned to the particular characteristics of each RAM block so that they provide error detection and correction if data are not replicated elsewhere (e.g., register files) and provide error detection only when data are mirrored elsewhere (e.g., cache memories are mirrored in RAM memory). In the latter case, correction requires reloading faulty data from the mirror location (e.g., cache line invalidation and re-fetch). ECC implementation is tuned also to not harm performance, particularly in the register file. Thus, fast encoding/decoding times are had despite this increases the number of ECC bits required. This way the LEON3FT can operate at the same maximum frequency as the standard LEON3 core. Other RAM blocks out of the LEON3FT core such as the FIFOs in the SpaceWire IP core and the buffer RAM in the CAN-2.0 IP core are also ECC protected.

The LEON3FT has a 15% higher area cost than the standard LEON3 core and can be obtained in ASIC and RTAX (on FPGA) technologies.

Since LEON3FT is functionally identical to the LEON3 core, the software development environment is the same in both cases. Thus, eCos, RTEMS and VxWorks operating systems are supported, and the LEON3 simulators (TSIM and GRSIM) can also be used for the LEON3FT. GRMON debug facility is also fully compatible with the LEON3FT.

2.5.3 The GR740 space device

Recently, Cobham Gaisler has developed an enhanced multicore for the Space domain: the GR740 SoC. As for the GR712RC, the GR740 is a Rad-Hard SoC. The GR740 SoC is a fault-tolerant quad-core LEON4 SPARC V8 processor including a number of interfaces such as an 8-port SpaceWire router, PCI initiator/target interface, CAN 2.0 interfaces and 10/100/1000 Mbit Ethernet interfaces. The GR740 has been designed as part of the ESA Next Generation Microprocessor (NGMP) programme.

Gaisler has released the GR-CPCI-GR740 Quad-Core LEON4FT Development Board including the GR740 SOC.

The main specification parameters for the GR740 device are as follows:

- Operating frequency: 250 MHz
- CLGA625 package
- Four LEON4 SPARC V8 cores with 7-stage pipeline, 8 register windows, 16KB 4-way data and instruction caches
- Double-precision IEEE754 floating point units
- 2 MB 4-way shared second level (L2) cache. It can be partitioned across cores (1-way per core)
- Main memory: 64-bit PC100 SDRAM memory interface with Reed-Solomon EDAC
- 8/16-bit PROM/IO interface with EDAC

- SpaceWire router with eight SpaceWire links 200 Mbit/s minimum
- 2x 10/100/1000 Mbit Ethernet interfaces
- 33/66 MHz (TBC) PCI 2.3 initiator/target interface
- MIL-STD-1553B interface
- 2x CAN 2.0 controller interface
- 2x UART, SPI, timers and watchdog, 16+22 pin GPIO
- CPU and I/O memory management units (MMU and IOMMU)
- Multi-processor interrupt controller with support for asymmetric and symmetric multiprocessing
- SpaceWire TDP controller and support for time synchronisation

By comparing the GR740 with the GR712RC, it can be seen that the GR740 is intended to deliver much higher performance due to the higher operating frequency (250MHz vs 100MHz) as well as the microarchitecture features (4 cores vs 2 cores, L2 cache, more powerful cores, high-speed interfaces, etc.). Both, the GR740 and the GR712RC allow symmetric and asymmetric multiprocessing.

The GR740 device also operates with the GRMON software debugger and is compatible with a number of compilers and operating systems. A development board (GR-CPCI-GR740) has been designed to allow the evaluation of the GR740 device [129].

2.5.4 LEON3/LEON4 multicore extensions

As part of some projects funded by the ESA and the FP7 PROXIMA project, a number of developments have been integrated into LEON3 and LEON4 multicore RTL implementations, which have been delivered for FPGAs, but not yet for ASICs. Some of these enhancements are particularly devised to monitor multicore contention by means of an extended Performance Monitoring Unit (PMU), which monitors at fine grain how much each core is stalled due to contention in shared resources and between which elements the contention occurred [154]. This support has been proven highly effective to provide reliable and tight execution time bounds due to multicore contention. However, there is an alternative. Some enhancements built upon time randomization result in probabilistic behaviour of contention effects in shared resources and cache effects. Hence, they can also be accounted with appropriate timing analysis tools requiring almost no intervention from the end user. This relieves the end user from having to monitor detailed information and to exercise fine-grained control on some execution conditions[152] [153]. Some of these enhancements have been already integrated in a commercial LEON3 multicore for the Space domain available through Gaisler website (http://gaisler.com/leon3).

2.5.5 Summary and usability in SAFURE

In principle, the GR712RC and GR740 SoCs are unlikely to fit the needs of SAFURE “as they are”. However, they deliver a number of features, such as transparent fault tolerance, compatibility with the SPARC V8 ISA, multicore operation, multicore contention monitoring support and time-randomization for probabilistic modelling of multicore contention, which may be of interest for some end users. On the other hand, relatively low performance (100MHz and 250MHz maximum frequency respectively) and over-designed fault tolerance for the domains of interest of SAFURE make this design unattractive for direct use. Still, given that Cobham Gaisler is an IP vendor, it may consider producing ASIC implementations with lighter fault tolerance and higher performance ASIC implementations if commercial opportunities arise in domains beyond Space.

Chapter 3 RTOS and hypervisors

The following section represents RTOS and hypervisors which are available on the market. The representation form is a brief description and key features highlights.

3.1 VxWorks

Provided by Wind River, VxWorks [101] Real Time Operation System (RTOS) is well known on the market. It supports a lot of 32 and 64-bit processor architectures both single and multicore including x86, PowerPC and ARM. The kernel of VxWorks is separated from other packages (like protocols, applications, add-ons etc.) which triggers scalability. There is also a possibility to use VxWorks as a Type 1 (hardware) hypervisor. However, VxWorks versions are not always based on the same base regarding to end-user needs.

The key points of VxWorks are:

- Scalable footprint
- Safety and security
- Virtualization facilities
- Guaranteed RT performance
- Multicore support
- Memory protection
- Certifiable

3.2 QNX Neutrino RTOS

The QNX Neutrino RTOS [100] provides wide facilities for building complete operating systems on different platforms. It is a microkernel-based system that runs other modules (like drivers, network stack, file system, graphical interface, etc.) in the safe memory-protected user space. Virtually any component can fail — and be automatically restarted — without affecting other components or the kernel. It is available for most of existing architectures including 32/64 x86, PowerPC and ARM. The key points of QNX Neutrino RTOS are:

- Microkernel architecture
- Scalability
- High availability (fault isolation and recovery)
- Wide networking and file system support
- Graphics
- Time partitioning
- Multicore support

3.3 Xen

Xen [102][103] is a type 2 hypervisor based on Linux, providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently. The University of Cambridge Computer Laboratory developed the first versions of Xen. The Xen Project community develops and maintains Xen Project as free and open-source software, subject to the requirements of the GNU General Public License (GPL), version 2. Xen Project is currently available for the IA-32, x86-64 and ARM instruction sets.

The key points are:

- Small footprint and interface
- Open source

- Operating system agnostic
- Driver Isolation
- 4 types of virtualization whom some of them are native
- Domain0, which is a "host" operating system, dedicated for critical code. Xen is not usable without it.

3.4 seL4

SeL4 [104] is a L4 family microkernel OS and hypervisor. SeL4 claimed to be an operating-system kernel with an end-to-end proof of implementation correctness and security enforcement. It supports x86 and ARM architectures.

The key points are:

- L4 microkernel architecture
- Verified microkernel
- Open Source
- Academic project

3.5 PikeOS

SYSGO's PikeOS [105] combines RTOS and hypervisor build upon the safe and secure virtualization. It provides timing and resource isolation (partitioning) and allows different operation system interfaces (like PikeOS Native, ARINC 653, Linux, POSIX, certified POSIX, Android, RTEMS, AUTOSAR, iTRON and others) to work within a single machine. PikeOS is based on L4 microkernel architecture that allows its usage in even resource constrained devices. It supports a number of architectures including x86, PowerPC and ARM for 32 bit as well as for 64 bit.

PikeOS is the only operating system that achieved a SIL4 certification for SMP usage on multi-core platforms.

The Key points of PikeOS are:

- Microkernel architecture
- Multi-core and hardware virtualization support
- Safety and security
- Scalability
- Time partitioning
- Resource partitioning
- Hard real-time support
- Certifiability to multiple industrial standarts
- Certified for the following standards:
  - IEC 61508
  - DO-178B
  - ISO 26262
  - IEC 62304
  - EN 50128

3.6 Summary and usability in SAFURE

The current concept of hypervisors and separation kernels created the base for mixed-critical design by separating applications into confined memory/computing time domains. The future CPS systems require further properties such as timing integrity, communication integrity and temperature, security. These requirements will stimulate development of different classes of operating systems with foreseen goal to "partition everything", i.e. creating a truly SW abstraction layer for the underlying hardware. The SAFURE approach addresses these requirements and demonstrates how some of these requirements will be implemented in the real-time hypervisor PikeOS.

SAFURE project delivers PikeOS support on novel ARM architectures (CPUs and SoC), new hardware platforms, secure communication, and a new type of a scheduler. These results have been assessed in joint collaborative case studies and demonstrators with focus on satisfying complex mixed-critical requirements on multi-core processors. The project has also provided methods and tools to perform the mentioned assessments. These extensions provide greater flexibility for system design than the solutions available on the market.

Chapter 4 Communication interfaces

Some interfaces are specifically used to address issues concerning either or both security and safety. Therefore, some of them could be relevant in the case of SAFURE and could be probably used by the demonstrators that would be developed in WP6. We will describe some of these interfaces without being exhaustive below.

4.1 External software communications (between terminal and system)

4.1.1 Network stacks

SAFURE will provide a certain level of safety and security in the network stacks that will imply information flow control from the input and output data. It will allow networks that previously had to be physically isolated to exchange information with each other, even when their security levels are different. Moreover, SAFURE will allow network operators and designers to consider SAFURE's paradigm by evaluating how to create, update, and manage available network resources.

Each network protocol, such as Ethernet or different CAN protocols, covers a specified number of layers from the OSI (*Open Systems Interconnection Model*). The network or protocol stack of a protocol refers to the implementation of the interfaces this protocol utilises. In case of a network, involving several protocols, messages have to converted from one format to another via their corresponding stacks. It is the case for instance whenever CAN frames are to be transported over an Ethernet network,. To do this, the corresponding network stacks are traversed in reversed order, as indicated in Figure 17.

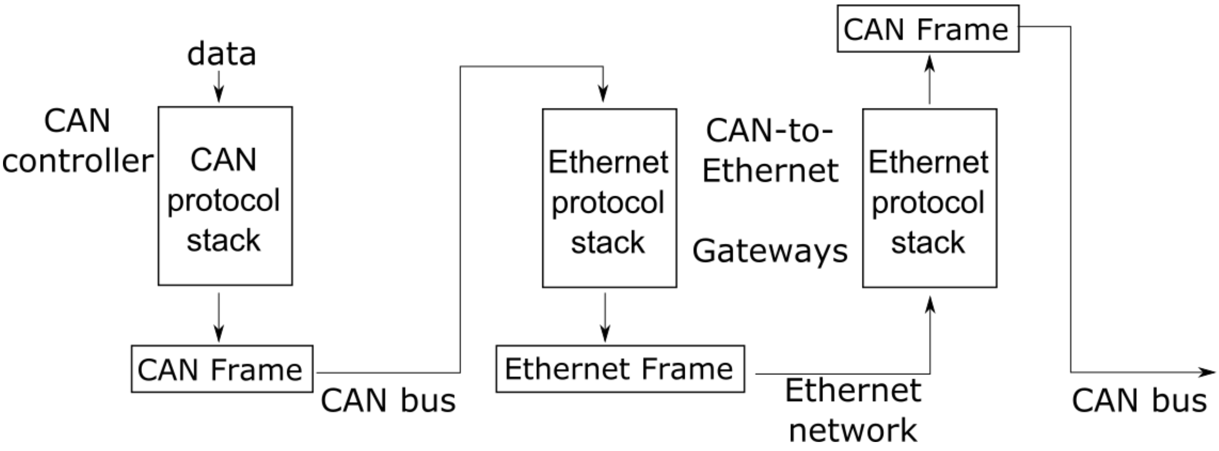

Figure 17: CAN frames are packed into Ethernet frames via the Ethernet protocol stack in a gateway. To retrieve the original CAN frames, the Ethernet stack has to be traversed in reserved order.

4.1.1.1 CAN

The Controlled Area Network Bus (CAN-Bus) is a communication system used in modern vehicles that allow:

- Data communication among the various electrical components
- Control of other car parts
- Receiving feedback from sensors

From the safety point of view, the error detection capabilities and operational safety of the standard CAN protocol are debated in [65][66][67]. CAN with Flexible Fata-rate (CAN FD) keeps all of CAN's fault confinement mechanisms such as error frames, error counters, error-active/ -passive modes, and positive acknowledging for fault-free messages, while providing support for higher bit rates (>1 Mbps) and for payloads larger than 8 byte per frame.

With the recurring evidence of automotive system vulnerabilities and the likelihood of CAN to continue being significantly used in upcoming in-vehicle architectures, several academic and industry partners are putting tremendous efforts in addressing safety and security aspects. CAN poses a big challenge in this respect, as it does not inherently support any kind of security.

Some of the explored mechanisms to improve CAN security regard the use of controller authentication [69][70]. This means that the controllers running in a CAN bus shall implement security measures e.g., authentication mechanisms to identify and communicate with each other within the bus system. Every controller needs a certificate to authenticate itself against the gateway as a valid sender.

As opening up a CAN network to the outside world requires more stringent security, the encryption of all vehicular data transmissions has been identified as a way to address these points [71]. Nevertheless, retrofitting CAN with new security mechanisms would lead to higher data traffic in a network characterized by ECUs with limited processing power and limited bandwidth.

Different cryptographic schemes such as the Advance Encryption Standard (AES) have been used in order to face this challenge [62] [73] [74]. AES, considered as cryptographically secure block cipher, involves symmetrical block encryption with a block length of 128 bits. It generates 16 bytes or a multiple of 16 bytes, which is transmitted from the sender to the receiver. Unfortunately, when standard CAN frames of 8 bytes are used, a 16-byte block cipher means that two CAN messages are required for each original message, effectively doubling the message time compared to using no cryptographic approach at all. A Japanese start-up has recently claimed to have developed a CAN bus encryption and key management system for protecting payloads with less than 8 bytes [75][2]. In this case, a whole CAN payload could be encrypted (64 bits length) without using a 128-bit block algorithm needed for AES-based encryptions.

Another approach regards stream cipher methods, also for eliminating the problem of additional messages generated when using a block cipher. As stream cipher effectively encrypts the data in a byte-by-byte fashion, meaning that the encrypted payload and the original data have the same size. The work in [72][74] provide an insight on the implementation of RC4 for the encryption of CAN data frames as well as recommendations about the use of public key cryptosystem for refreshing the keys.

An overview on security CAN-bus communication, considering AES and RC4 encryption, HMAC message authentication, and authenticated encryption, is analysed and compared in [74]. Here, the experimental results verify that the security of the CAN bus can be improved by means of cryptographic methods, and that there are consequences with respect to message times as a result of using these methods. Moreover, it is shown that the effects of any cryptographic approach will be different for each CAN network, depending on the underlying hardware capacity of that network.

4.1.1.2 Ethernet

The following layers [77] of the OSI model will be discussed in the context of network security protocols:

[2] Usually when cleartext space if smaller than key space, cryptography becomes more tricky.

- Application Layer is where services such as HTTP, FTP, telnet, SSH and TSL/SSL reside. The Transport Layer Security (TLS) and its predecessor, the Secure Sockets Layer (SSL) are protocols that provide data encryption and authentication between applications and servers in scenarios where data is being sent across an insecure network. This works by setting up an encrypted tunnel between a browser and a Web server over which secured data packets can travel, namely, by having HTTP over SSL (HTTPS).

  An alternative protocol to HTTPS is the Secure HTTP (SHTTP). Here, instead of encrypting the whole tunnel, only individual messages will be secured before being transmitted.

  SSL can be used for other TCP/IP protocols such as FTP and TELNET. The File Transfer Protocol (FTP) is utilized for transferring computer files between a client and a server within a computer network. FTP users may authenticate themselves with a clear-text sign-in protocol, by means of a username and password. Nevertheless, the users can establish an anonymous connection with the server, if the latter is configured to allow so. FTP makes use of SSL/TLS (FTPS) to secure both the username and the password.

  Telnet has been known as the pioneer of all security application protocols [76]. It was created in 1969 and since then various vulnerabilities have been discovered that have led to experts recommendation to discontinue its use [78]. The Secure Shell (SSH) protocol emerged as an alternative to Telnet. Here, the idea is to secure an SSH client with an SSH server (both running SSH protocol), further protocol details can be found in [79].

- Network Layer is where IP and ICMP reside. The Network Layer cares only about the IP address associated with the packet. The IPsec lays within this layer and when implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. IPsec is below the transport layer and so is transparent to applications. One of its advantages relies on the fact that, when implemented in a firewall or router, a user or server system does not need to change software. This means that it is not necessary to train users, issue keying material on a per-user basis, or revoke keying material when users leave the organization.

  Moreover, IPsec can provide security to individual users if needed and plays a vital role in the routing architecture as it can ensure that: 1) router and neighbour advertisements come from authorized routers, 2) a redirect message comes from the router to which the initial packet was sent and 3) a routing update is not forged.

  There are two types of IPsec protocols: 1) the Authentication Header (AH) protocol [e], which provides source authentication and data integrity, but no confidentiality and 2) the Encapsulation Security Protocol (ESP) [81], which provides source authentication, data integrity and confidentiality. Therefore, the latter has been more widely used.

4.1.1.3 CAN to Ethernet

As car connectivity will become an essential part in the future transportation technologies, new security requirements must be considered. Some security mechanisms are already being designed, for instance in the AUTOSAR environment [82]. Here, it is possible to distinct between two main groups of BSW modules (see Figure 18). Namely,

- CAL and CSM: Basic cryptographic primitives for BSW and application
- SecOC: Authenticated communication seamlessly integrated into the AUTOSAR communication stack

CAL and CSM consist of following modules, which include abstract definitions of cryptographic services:

- Crypto Abstraction Library – CAL
- Crypto Primitive Library – CPL
- Crypto Service Manager – CSM
- Crypto library module – CRY

These modules shall provide synchronous or asynchronous services to enable a unique access to basic cryptographic functionalities for all software modules. The standard does not specify which cryptographic algorithm shall be used. Nevertheless, by enabling the use of well-defined interfaces, it is possible to seamlessly change from one implementation to another.

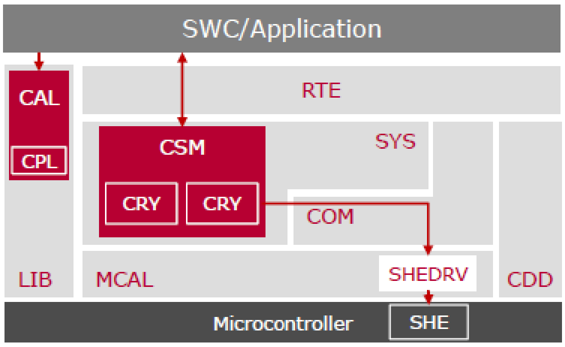

Figure 18: Scheme with Basic Software Modules

4.1.1.4 SecOC (Secure Onboard Communication)

SecOC sends and receives secured PDUs, which are protected against manipulation, random errors and replays. These PDUs are routed through SecOC (see Figure 19) while using security mechanisms from CAL or CSM.

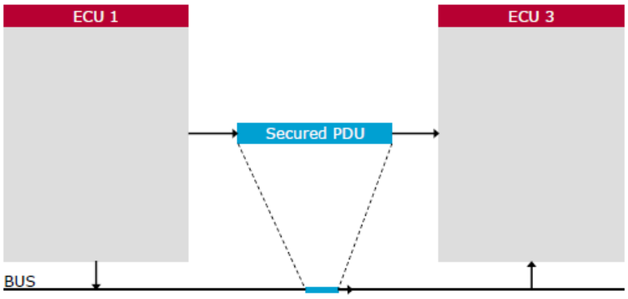

Figure 19: Secure Onboard Communication

4.2 Hardware communication interfaces

SAFURE will enhance the safety and security aspects of the existing hardware by adding specific anti-counterfeiting measures. This means that the implementation of data integrity algorithms and functions such as encryption, decryption, generation of keys and hashing into the physical devices will provide certain level of physical tamper resistance, which will be of great advantage for all types of safety and secure real-time applications.

4.2.1 TTEthernet

The TTEthernet paradigm is characterized by its capability to detect failures and irregularities within a network. To achieve certain level of safety, availability and fault tolerance, TTEthernet can be deployed in a network with multiple redundant end systems, switches and segments, as depicted in Figure 20. This allows the system to continue operating even if a fault occurs. It means that the failure of a single system or message can be tolerated without affecting a whole application.

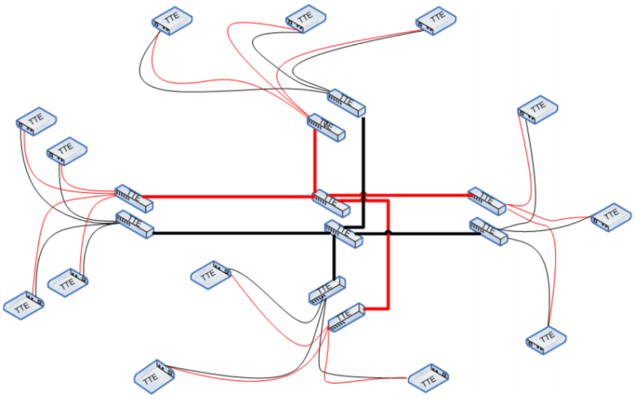

Figure 20: TTEthernet provides implicit fault tolerance mechanisms

The SAE AS6802 [83] protocol allows the integration of guardians in switches and end-systems. The guardians are in charge of supervising the well-functioning of the network, in other words, they must control that the network works in compliance with the predefined parameters. In case faulty systems block network or segments are detected, the guardian disconnects the respective network segment or port. Several redundant guardians can be implemented such that the highest safety requirements are met.

TTEthernet tolerates arbitrary transient disturbances even in presence of permanent failures: In addition to fault tolerance, it also provides self-stabilization properties, e.g., the synchronization will be re-established even after transient upsets in a multitude of devices in the distributed computer system. TTEthernet stabilizes from an arbitrary system state to a synchronized system state. This self-stabilizing property becomes more and more important with decreasing feature sizes of computer chips and, therefore, resulting increase in transient upsets.

As mentioned in D5.1 “Alpha Communication Prototypes”, various safety aspects are covered and used by TTEthernet protocols (typically running over the same network) in order to configure, manage, control the access and administer the networks.

4.2.2 MACSec

Embedded systems and local area networks are often used to transfer sensitive or critical data. Such networks often contain components of different developers or customers. In general, it is not feasible to secure the complete network against physical access by intruders and attackers. Instead, in order to prevent an attacker from accessing sensitive or manipulate critical data, the communication between components has to be secured. MACSec [60] can offer a solution against certain kinds of attacks and data corruption. It can prevent passive wiretapping and denial of service, intrusion, man-in-the-middle and playback attacks.

MACSec (*MAC Security*) [60] is defined in the IEEE 802.1ae standard and provides connectionless frame data integrity and data origin authenticity on layer 2 of the OSI model. The integrity check is always performed when MACSec is configured but encryption is optional. The security is achieved by providing secure point-to-point Ethernet links between nodes on a frame-by-frame basis. This means that each transferred frame is individually secured by added integrity tags. This hop-by-hop security allows data inspection on each node within a connection and reduces the number of keys to be stored.

MACSec transforms a standard Ethernet packet by adding an 8-byte header (SecTAG) and a 16-byte tail (ICV or Integrity Check Value) to the Ethernet packet, which forms a MACsec Protocol Data Unit (MPDU) as shown in Figure 21. On arrival, an integrity check is performed on each packet with the ICV and any packets that do not pass this check are discarded.

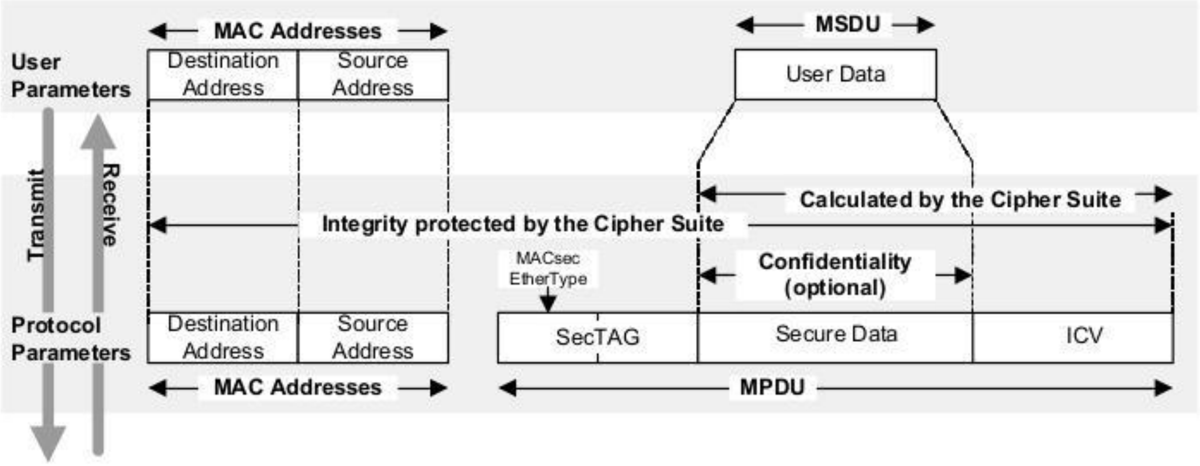

Figure 21: The MACSec protocol.

The MACSec protocol will transform the user data into the MPDU. The user data can be encrypted optionally. The SecTAG describes (amongst other) the Ethertype and packet number of the packet. The ICV provides integrity checks for the whole packet and therefore depends on the encryption suite.

The SecTAG is a protocol header and contains the MACSec Ethertype. It defines the active MACSec services, and it contains a packet number to prevent replay attacks as well. The ICV field contains a checksum to verify the packet integrity.

The encryption of the user data and computation of the ICV is done via a cipher suit and a session key called SAK (secure association key). The default cipher suite is GCM-AES-128 (Galois/Counter mode, turning the AES block cipher stream cipher like). For each session, a new key is used. These keys are created via a MACSec Key Agreement (MKA) protocol that utilised a Connectivity Association Key (CAK), which needs to be statically preinstalled for each Ethernet connection on a device, i.e. each port.

MACSec can provide secure Ethernet links between two devices in a network by adding a cipher-based check sum and the option to encrypt the payload of an Ethernet packet.

4.2.3 ZigBee

4.2.3.1 Introduction

The Zigbee [24] is an IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small and low-power digital radios.

The technology defined by the ZigBee specification is intended to be simpler and less expensive than other wireless personal area networks (WPANs), such as Bluetooth or Wi-Fi.

The ZigBee network layer natively supports both star and tree networks, and generic mesh networking. Every network must have one device-coordinator, tasked with its creation, the control of its parameters and basic maintenance. Within star networks, the coordinator must be the central node. Both trees and meshes allow the use of ZigBee routers to extend communication at the network level.

A ZigBee network allows up to more than 65000 nodes and the nominal distance is between 10m to 100m.

ZigBee is typically used in low data rate (256 Kbit/s) applications that require long battery life and secure networking (ZigBee networks are secured by 128-bit symmetric encryption keys). The security suite used is AES_CCM.

An integrity mechanism is also used by adding a Message Integrity Code (MIC) to be transported along with the data to be protected. The MIC is also bound to the identity (IEEE address) of the originator and thus provides origin authenticity.

4.2.3.1 Usage

The demand of using smart wireless sensing for health, safety and surveillance applications is growing rapidly and the ZigBee technology is one of the favourite technologies to build a wireless sensor network.

Health applications:

For example, a proof of the concept of a health care platform [25] using Zigbee wireless sensor network has been done. Based on a wireless sensor network, the platform incorporates Zigbee-based wireless transmission combined with an electronic humidity sensor and emergency event report system integration platform. The platform uses the advantages of a wireless network based on ZigBee, which are: economical, simple and capable of large scale monitoring.

Another example [26] is a real-time monitoring system for in-patient. The system is made up of two sub-systems:

- A patient physical states data acquisition and communication system based on Zigbee technology
- A hospital monitoring and control center

The patient's physical state data acquisition and communication system monitors the main physical parameters and movement status continuously by using various sensors: cardiac sound, pulse, temperature, blood pressure.

The information from the sensors is processed by an MCU and sent by a ZigBee wireless communication module.

The monitoring center receives the information from each patient and save them to database by the ZigBee central node and then judges the states of patients by fuzzy reasoning.
The scheme structure of monitoring system is shown as Figure 22: The monitoring system for cardiac patient.

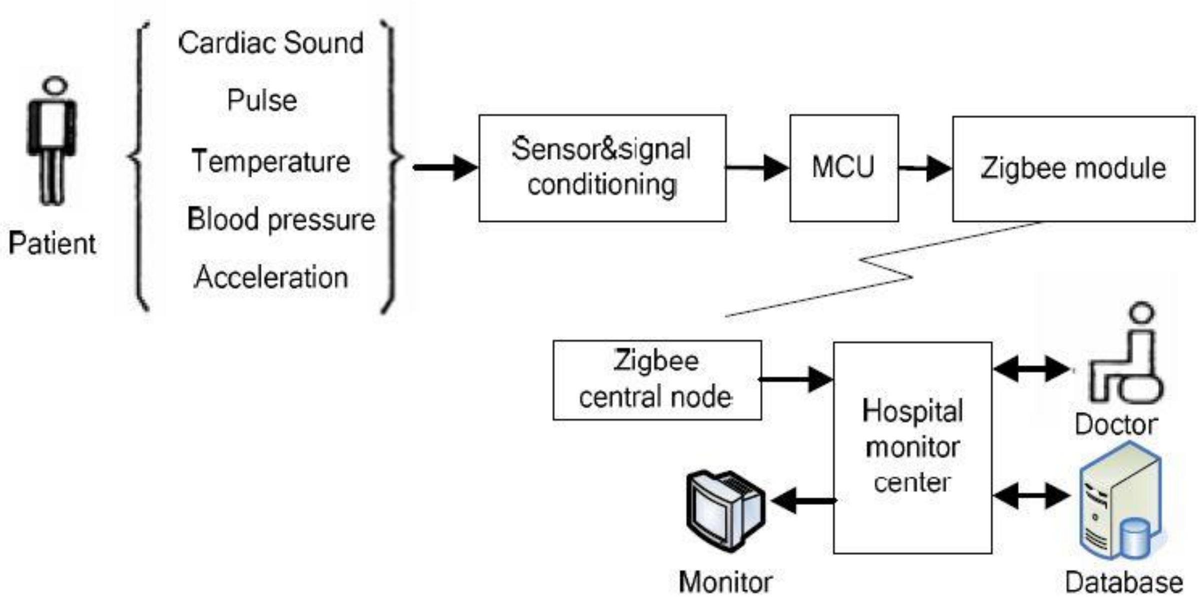

Figure 22: The monitoring system for cardiac patient

4.2.4 Bluetooth

4.2.4.1 Introduction

Bluetooth [27] is a wireless technology standard for exchanging data over short distances (nominal distance around 10m). Bluetooth was primarily designed for low-power consumption, with a short range based on low-cost transceiver microchips in each device.

Bluetooth operates at frequencies between 2400 MHz and 2483.5 MHz. This is in the globally unlicensed (but not unregulated) Industrial, Scientific and Medical (ISM) 2.4 GHz short-range radio frequency band.

The Bluetooth data rate varies from 1Mbit/s with the version 1.2 of the protocol to 24 Mbit/s with the version 4.0. The Bluetooth SIG officially unveiled Bluetooth 5 during a media event in London on 16 June 2016. Its new features are mainly focused on emerging Internet of Things technology.

Bluetooth is a packet-based protocol with a master-slave structure. One master may communicate with up to seven slaves in a “piconet”. All devices share the master's clock. Sometimes, by an agreement, an initiator could initiate the connection with a device. In this case, it operates as a master. After the connection is made with the device, the initiator operates as a slave. Such device operating as a master and slave is a headset.

The Bluetooth Core Specification provides for the connection of two or more “piconets” to form a “scatternet”, in which certain devices simultaneously play the master role in one piconet and the slave role in another.

A baseband error correction is made depending on packet type. Furthermore, packets with CRC will be retransmitted until acknowledged by Automatic Repeat Request (ARQ).

There are essentially two pairing mechanisms used:

- Legacy pairing: It is a method used in Bluetooth v2.0 and before. The pairing is used by entering a PIN code by both the devices. This method of pairing was not providing a real level of security against sniffing [39].

- Secure Simple Pairing (SSP): this method uses a public/private key and a Diffie-Hellman algorithm for exchanging public keys. This method is considered more secure [39].

4.2.4.1 Usage

Bluetooth technology is one of the favourite wireless technologies used by health equipment manufacturers. One of the major reasons for its success is that it is a widespread technology used in smartphones.

Health applications:

Many examples of health care applications could be found in the “Google Play” or the “App Store”. These applications connect to different devices by Bluetooth measuring the following body parameters: blood pressure, heart rate, body temperature, ECG, breathe rate, and the biochemical parameters such as blood sugar.

Experimental results showed that a smartphone based on Android could interact with up to 7 Bluetooth sensors simultaneously [40].This limitation to only 7 simultaneous connections could be a major drawback for the Bluetooth comparing to other protocols like ZigBee.

4.2.5 WIFI

4.2.5.1 Introduction

Wifi [40] is one of the most popular data transmission technologies available today. It is a widespread technology and available nearly everywhere (residential homes, public places, etc.).

The widespread use of the technology has made it a convenient choice for a health monitoring system usage. It is principally used to transmit the collected data to a distant server.

Wi-Fi compatible devices can connect to the Internet via a WLAN network and a wireless access point. A hotspot (or access point) has a range of about 20 meters indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometres achieved by using multiple overlapping access points.

Wi-Fi [42] operates at 2.4 GHz (802.11b and 802.11g), 3.6 GHz, 5 GHz, and 60 GHz (802.11ad).

Various encryption methods have been used: WEP that is nearly not used anymore, WPA and WPA2.

The Wi-Fi [42] data rate depends on the version of the protocol used. For example, the data rate in the 802.11g protocol is 54 Mbit/s.

4.2.5.2 Usage

Wi-Fi technology in the case of health equipment is used as a relay to transmit wirelessly information from different devices of eventually different patients. The typical use in telemedicine is gathering information by different low power microcontrollers and RF transceivers that perform the measurements and transmit them to the patient monitoring device. The patient monitoring device, in form of a PDA or a smartphone that runs medical monitoring (heart, blood sugar, blood pressure…) application. The value could therefore be transmitted periodically to a central monitoring server by using a Wi-Fi connection.

With this means, the patient can achieve medical assistance of a chronic condition, or can be supervised during recovery from an acute event or surgical procedure.

4.2.6 2G/3G/4G/5G

4.2.6.1 Introduction

2G/3G/4G/5G refer to different generations of wireless technologies. In Figure 23, a short comparison between these technologies is presented.

The nomenclature of the generations generally refers to a change in the fundamental nature of the service, non-backwards-compatible transmission technology, higher peak bit rates, new frequency bands, wider channel frequency bandwidth in Hertz, and higher capacity for many simultaneous data transfers (higher system spectral efficiency in bit/second/Hertz/site).

Each of these generations could refer to multiple technologies depending on the country and evolutions introduced regularly.

Most of the technologies used in these generations are standardized by 2 groups:

- 3GPP[147]: for GSM (2G), GPRS, EDGE, UMTS(3G) , HSDPA (3G release 5), HSUPA (3G release 6), HSPA (3G+), HSPA+ (3G++), LTE (4G).
- 3GPP2: for CDMA2000[46].

Gener-ations	Launch date	Main Technologies/standards	Transmission capacity(max theorical /practise) in downstream
2G[44]	1991 in Finland	GSM cdmaOne (referred as CDMA in US) D-AMPS (referred as TDMA in US) Evolutions: GPRS(2.5G) EDGE(2.75G)	50 Kbit/s 1 Mbit/s

3G[45]	1998 (by NTT DoCoMo in Japan)	CDMA2000/EV-DO(Release 0, Rev A, Rev B)
		WCDMA(UMTS standard)
		HSPA(UMTS standard)
		HSPA+(UMTS standard)
		TD-SCDMA(UMTS standard , used only on China)
			up to 384kbit/s
			up to 7.2Mbit/sec
			up to 21.6 Mbit/s

4G	-2007 for the mobile WiMAX -2009 for LTE in Norway and Sweden	Mobile WiMAX: -rel 1 -rel 1.5 -rel 2 LTE(Long Term Evolution)	-Up to 37 Mbit/s -Up to 83 Mbit/s -Up to 110 Mbit/s -Up to 100 Mbit/s Cat 3 -Up to 150 Mbit/s Cat 4 -Up to 300 Mbit/s Cat 5

Figure 23 : Comparison between 2G/3G/4G

5G[49] is the next generation of wireless technologies but there is no standard defined right now. The official standard for 5G should be rolled out by 2020 to meet business and consumer demands. This technology [148] aims to become the primary mean of network for person-to-person and person-to-machine connectivity by matching the diversity of service requirements and service characteristics (Figure 24). Examples include extreme broadband, ultra-low latency, massive connection and ultra-high reliability etc., along with the ability to accommodate various use cases. It will provide higher data rates (cell data rate ~10 Gb/s), enhance end-user quality-of-experience (QoE), reduce end-to-end latency(2 to 5ms end-to-end), and lower energy consumption comparing to the 4G technology.

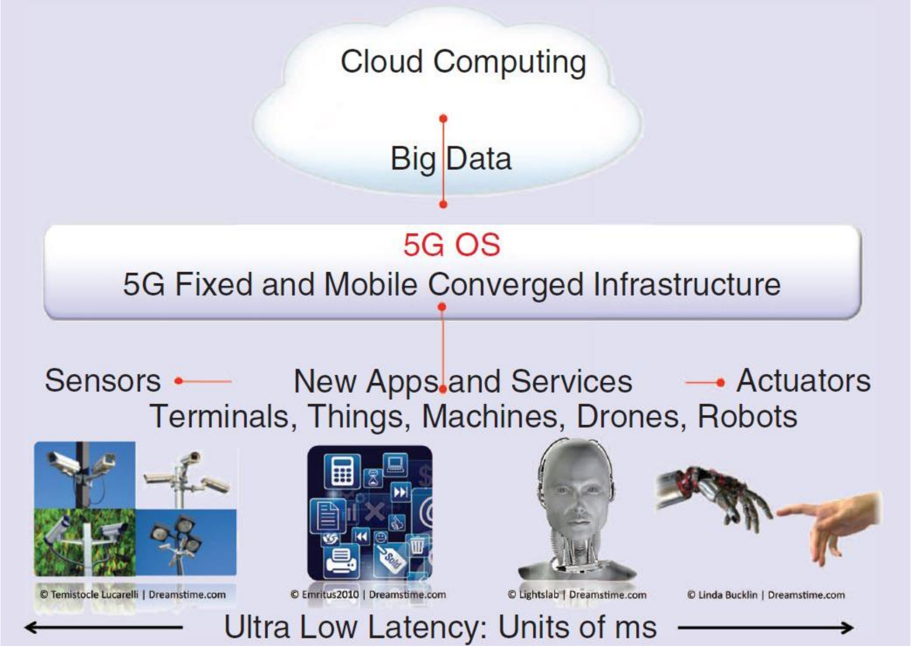
Cloud Computing
Big Data
5G OS
5G Fixed and Mobile Converged Infrastructure
Sensors
New Apps and Services
Actuators
Terminals, Things, Machines, Drones, Robots
© Temistocle Lucarelli | Dreamstime.com
© Emritus2010 | Dreamstime.com
© Lightslab | Dreamstime.com
© Linda Bucklin | Dreamstime.com
Ultra Low Latency: Units of ms

Figure 24: The new ecosystems based on 5G

4.2.6.1 Usage

3G and 4G technologies in the case of health equipment could be used as the WiFi technology to transmit information wirelessly from different devices of eventually different patients.

The typical use is the same as the one used in WiFi. Gathering information by different captors and transmitting them periodically to a central monitoring server by using a 3G or 4G connection.

With this means, the patient can achieve medical assistance of a chronic condition, or can be supervised during recovery from an acute event or surgical procedure.

Chapter 5 Standards and guidelines

5.1 Overview

In this chapter, some of the most used or well spread standards of security (section 5.2) and safety (section 5.3) will be presented. Figure 25 depicts some of the standards used for security assurance, according to application (military and civil) and by country.

Thereafter, a diagram with structuration of standards and identification of those relevant for SAFURE (see blue boxes) is presented.

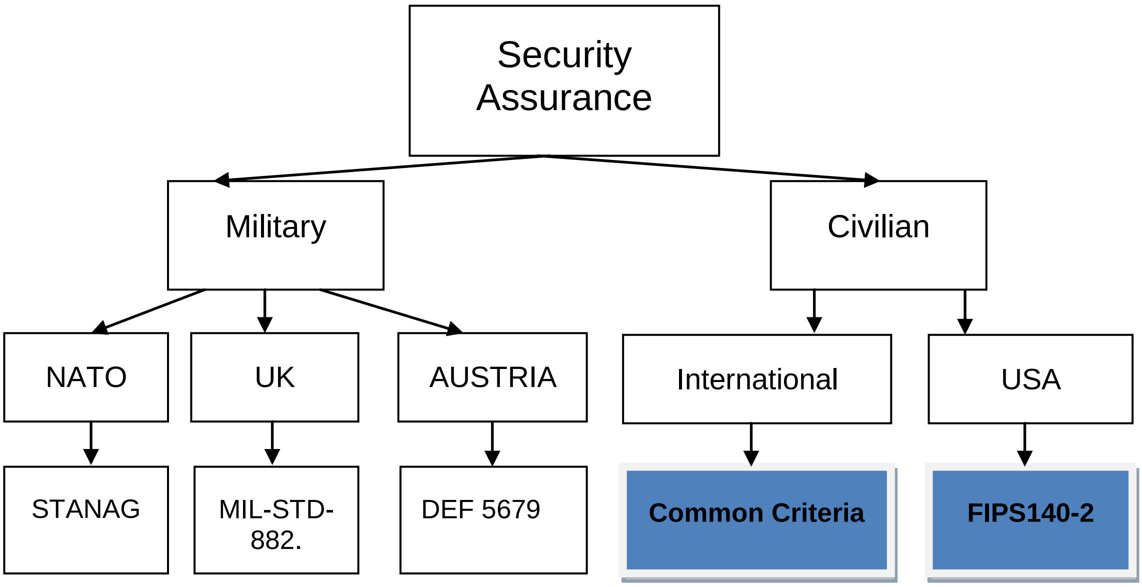

Figure 25: Security standards

The diagram below presents security standard mechanisms and identification of relevant ones (blue ones) for SAFURE.

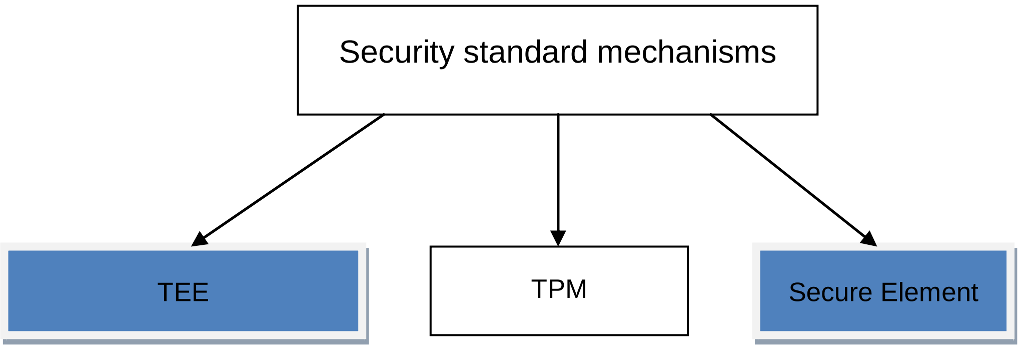

Figure 26: Security standard mechanisms

5.2 Security

5.2.1 MILS COMPLIANCE

MILS (Multiple Independent Level of Security) is an architecture for high-security computer systems, which relies on 4 principles: data isolation, control of information flow, periods processing, and damage limitation [99].

Currently there is no formal certification infrastructure for MILS, in the sense that you can go with product X to someone, and get a certificate that product X is MILS-compliant. In this section, we describe the state of the art on MILS compliance.

Open Group “Mils” for any MILS products

The Open Group has acquired a trademark for “Mils” (in that spelling, intentionally distinct from “MILS”). In [92], the Open Group member Rance Delong explains a view of software architecture consisting of components and interactions [97], and proceeds that Mils™ is “*now used as a proper noun, rather than an acronym, “Mils” refers to the refined (and still in the process of refinement) set of concept definitions, architecture, doctrine, standards, practices and support for the development, evaluation, certification and deployment of Mils components and systems intended to achieve the MILS goals.* “.[92] envisions a “*marketplace of COTS products developed according to Mils standards and evaluated to Mils protection profiles*”. However, as of now, to the best of our knowledge, the Open Group has not yet published a more formal definition of “Mils” or its sub concepts, nor any Mils protection profile. Similarly there are not yet any guidelines to check whether a product is “Mils”-compliant that would pave the way for certification.

Common Criteria Protection Profiles for separation kernels

Additionally, it is possible to certify (any) component of a MILS system according to the technology-agnostic IT security standard Common Criteria (CC) for Information Technology Security [91]. (Any) CC certification can opt to use a protection profile, to simplify the generation of a security target that is part of a CC certification. For the MILS component of a separation kernel, there exist two protection profiles:

- SKPP[98] is a US-based protection profile published in 2007. It has been used to certify two versions of the Green Hills Integrity Operating system in 2008 and 2010. However, the protection profile has subsequently been revoked (“sunsetted”) by NSA/NIAP in 2010.Igor Furgel, Viola Saftig, EURO-MILS project, EURO-MILS proposal for Projection Profile (PP) for a Highly Robust OS in Europe: project deliverable D12.3, http://dx.doi.org/10.5281/zenodo.51582
- [93] is a draft of a protection profile originating from the EURO-MILS project. A user of [93] would have to formally evaluate the protection profile draft at certification body.

EURO-MILS “MILS Architecture Template” for any separation kernels and MILS systems

EURO-MILS has developed a MILS Architecture Template [99] (Section 3.1). [99] is a document that gives more detailed definitions of the components of a MILS system, and defines the policies that a MILS system can enforce. The two prototypes of EURO-MILS (avionics and automotive, described in [94] Sections 4 and 5) made meaningful use of a separation kernel and provided a description in terms of the MILS Architecture Template. EURO-MILS definition for MILS compliance would be:

- Usage of the MILS Architecture Template and conforms to the definition of separation kernel in [99]
- Usage of a separation kernel

- The used separation kernel implement functionality defined in a one of Protection Profiles (PP) for separation kernels, i.e. SKPP or [93]
    - Since these PPs are not binding, SKPP does not exist officially, and [FS16] is still work in progress, we don't expect any formal compliance according these PPs.

No formal certification infrastructure exists yet for measuring either of the compliance claims. In future the MILS community (http://mils-community.euromils.eu/) possibly could be forum for providing an infrastructure for assessment of "MILS compliance".

5.2.2 Common Criteria

Common Criteria is the predominant certification scheme in the security market. The "*Common Criteria for Information Technology Security Evaluation*" (CC) is an international standard for the evaluation of the security of systems. Standardization began in the 1990s to reconcile different existing national or, in the case of the European input, supranational, standards. Version 1.0 came out in 1996; the current version is 3.1 from 2009. Nowadays, worldwide, there are about 200 evaluations published annually. The idea is to ensure the security of a product by forcing developers to undergo an evaluation process by an accredited evaluation laboratory. Practically, the evaluation process consists of developers providing artefacts about the system under evaluation and an evaluation laboratory reviewing those artefacts possibly accompanied by some testing and on-site visits. To be CC-compliant, it is possible to take an existing system and to certify it according to the CC. Examples of CC-certified operating systems (up to different levels of criticality) are Microsoft Windows, Oracle Solaris, Red Hat Linux.

The CC core document for products is called *Security Target* (ST). Predefined assurance of the CC is graded on a scale of 1 (lowest) to 7 (highest). Assurance levels on that scale are called EALs (Evaluation Assurance Levels). In order to ease the description of products by the CC, the author of an ST may decide to base it on a *protection profile* (PP). A PP is a document that serves as a template for many security targets in a class of products such as for example firewalls, smart cards, or, as in our case, operating systems. PPs can not only be generated by a national or international central authority, but also be generated by companies and industry groups, therefore in different domains a competition of PPs exists (this is the case in operating systems). An ST writer also may opt *not* to base the ST onto an existing PP.

One portion of a security target is "how" security is achieved from a software process point of view, such as adherence to design, testing and life cycle standards. A security target also mandates the developer to identify a set of *assets*, *threats* and *security objectives* to describe the specific system that is protected: threats increase risks to assets that are of value ("what" is protected). Security objectives act as countermeasures to reduce the risk to assets. In addition, the security target requires to make a selection of *security functional requirements* (SFRs) from a template of 134 pre-written CC *components* providing text blocks (that each may be adapted). The intent of the SFR selection is to describe the mechanisms for implementing the countermeasures and to improve comparability with other products.

The MILS Community has selected an assurance approach based on Common Criteria.

5.3 Safety

There is a range of system safety standards in use today. Military standards such as Def Stan 00-56 (UK) [10], MIL STD 882 (USA) [11], and DEF(AUST)5679 (Australia) [12] give requirements and guidance for defense systems.

There are also civilian standards, most prominent of which are the generic industry standard IEC 61508 [13] and its sector specific instantiations, such as the CENELEC Standard EN 50126 [14] for railways and the ISO 26262 standard for automotive safety.

5.3.1 IEC 61508

IEC 61508 [15] is an international standard published by the International Electrotechnical Commission of rules applied in industry. It is titled: *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems* (E/E/PE or E/E/PES).

IEC 61508 is intended to be a basic functional safety standard applicable to all kinds of industry. It defines functional safety as "part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities". The standard was created with rapidly developing technology in mind. The framework in this standard is considered to be sufficiently robust and comprehensive to cater to future developments. The standard covers the complete safety life cycle, and may need interpretation to develop sector specific standards. It has its origins in the process control industry.

The safety life cycle has 16 phases that roughly can be divided into three groups as follows:

1. Phases 1-5 address analysis
2. Phases 6-13 address realisation
3. Phases 14-16 address operation

All phases are concerned with the safety function of the system.

The standard has seven parts:

- Parts 1-3 contain the requirements of the standard (normative)
- Parts 4-7 are guidelines and examples for development and thus informative

The concepts of risk and safety function are central to the standard. The risk is a function of frequency (or likelihood) of the hazardous event and the event consequence severity. The risk is reduced to a tolerable level by applying safety functions that may consist of E/E/PES and/or other technologies. While other technologies may be employed in reducing the risk, only those safety functions relying on E/E/PES are covered by the detailed requirements of IEC 61508.

IEC 61508 has the following views on risks:

- Zero risk can never be reached
- Safety must be considered from the beginning
- Non-tolerable risks must be reduced

The safety integrity level (SIL) provides a target to attain in regards to a system's development. A risk assessment effort yields a target SIL, which thus becomes a requirement for the final system. The requirement informs how to set up the development process (using appropriate quality control, management processes, validation and verification techniques, failure analysis, etc.) so that one can reasonably justify that the final system attains the required SIL. Part 2 and 3 of IEC 61508 give guidance on activities to perform in order to attain a SIL.

The meaning of the SIL varies depending on whether the functional component will be exposed to high or low demand:

- For systems that operate continuously (continuous mode) or systems that operate more than once per year (high demand mode), SIL specifies an allowable frequency of dangerous failure.
- For systems that operate intermittently and at most once a year (low demand mode), SIL specifies an allowable probability that the system will fail to respond on demand.

SIL	Low demand mode: average probability of failure on demand	High demand or continuous mode: probability of dangerous failure per hour
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$ (1 dangerous failure in 1140 years)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$

Many variants of the standards exist, such as:

- ISO 26262 in automotive software.
- IEC 62279 in rail software: it provides a specific interpretation of IEC 61508 for railway applications. It is intended to cover the development of software for railway control and protection including communications, signaling and processing systems.
- IEC 61511 in process industry (refineries, petrochemical, chemical, power): it is a technical standard which sets out practices in the engineering of systems that ensure the safety of an industrial process through the use of instrumentation.
- IEC 61513 in nuclear power plants: provides requirements and recommendations for the instrumentation and control for systems important to safety of nuclear power plants. It indicates the general requirements for systems that contain conventional hardwired equipment, computer-based equipment or a combination of both types of equipment.

5.3.2 RTCA-EUROCAE DO-178C

Software Considerations in Airborne Systems and Equipment Certification is the title of the published document from RTCA (Radio Technical Commission for Aeronautics) in a joint effort with EUROCAE (the European Organisation for Civil Aviation Equipment). The D0-178C [16] replaces D0178B as the primary document by which the certification authorities such as FAA (Federal Aviation Administration of USA), EASA (European Aviation Safety Agency of European Union) and Transport Canada will approve all commercial software-based aerospace systems.

The software safety requirements are inputs to the software lifecycle process. To ensure that safety requirements are properly implemented, the system requirements typically include or reference:

- The system description and hardware definition
- Certification requirements, including Federal Aviation Regulations (United States), Joint Aviation Regulations (Europe), and Advisory Circulars (United States)
- System requirements allocated to software, including functional requirements, performance requirements, and software safety requirements
- Software level(s) and data substantiating determinations, failure conditions, Hazard Risk Index categories, and related functions allocated to software
- Software strategies and design constraints, including design methods such as partitioning, dissimilarity, redundancy, and safety monitoring
- The software safety requirements and failure conditions if the system is a component of another system

5.3.3 RTCA-EUROCAE DO-254

Hardware Considerations in Airborne Systems and Equipment Certification is a similar document targeting the hardware part of avionic components rather than the software part. With DO-254, the FAA has indicated that avionics equipment contains both hardware and software, and each is critical to safe operation of aircraft.

Similarly to DO-178, the hardware safety requirements are inputs to the software lifecycle process, and the associated safety process typically includes:

- A Plan for Hardware Aspects of Certification (PHAC)
- A Hardware Verification Plan (HVP)
- A Top-Level Drawing, and a Hardware Accomplishment Summary (HAS)
- A Planning process defining the approach towards the certification
- Some Hardware design processes
- A Validation and verification process that provides the conformity assurance

5.3.4 RTCA-EUROCAE DO-297

DO-297 [130] contains guidance for IMA (Integrated Modular Avionics) developers, application developers, integrators, certification applicants, and those involved in the approval and continued airworthiness of IMA systems in civil certification projects. It is focused on IMA-specific aspects of design assurance.

IMA is described as a shared set of flexible, reusable, and interoperable hardware and software resources that, when integrated, form a platform that provides services, designed and verified to a defined set of requirements, to host applications performing aircraft functions. The primary industry-accepted guidance for satisfying airworthiness requirements for IMA components is included and it describes application properties as they relate to their integration with a platform.

Robust partitioning enforcement is a mandatory requirement in IMA systems. Robust partitioning allows independent applications to share resources without any unintended interactions, meaning that isolation and independence are guaranteed in all circumstances (including hardware failures, hardware and software design errors, or anomalous behavior). Robust partitioning ensures that:

- A partition should not be allowed to contaminate the code, I/O, or data storage areas of another partition
- A partition should be allowed to consume shared processor resources only during its allocated time
- A partition should be allowed to consume only its allocation of shared I/O resources
- Failures of hardware unique to a partition should not cause adverse effects on other partitions

5.3.5 Def Stan 00-56 (military UK)

United Kingdom Defence Standard (DEF-STAN) 00-56, *Safety Management Requirements for Defence Systems*, Issue 4, June 2007, supersedes and combines DEF-STANs 00-56, 00-54, and 00-55. The standard provides requirements and guidelines for the development of all defense systems, not solely computer-based systems. Like MIL-STD-882D, DEF-STAN 00-56 provides broad guidance on the requirements for a system safety program to achieve a level of safety risk that is as low as reasonably practicable. The DEF-STAN has a strong basis in UK law and notes that the system developer, as the duty holder, has the responsibility to exercise due diligence in the development of the system.

A key aspect of the DEF-STAN is the development of a safety case. The DEF-STAN requires the developer to provide a safety case at various stages of development. Early safety cases document the planned approach to risk evaluation and mitigation; latter safety cases provide the evidence of risk mitigation. The safety case should demonstrate how safety will be, is being, and has been achieved and maintained. The Safety Case should consist of a structured argument supported by a body of evidence. The quantity and quality of the evidence depends on the systems risks, complexity, and unfamiliarity of the circumstances involved. The unfamiliarity criteria are aimed at novel systems or unusual environments. The standard requires the developer to work closely with the Ministry of Defense and stakeholders throughout the development process to ensure that the delivered system achieves the stated requirements.

The aspects of software are dealt with in part 2 of the standard. The concept of complex electronic elements, which includes software and custom hardware (e.g. firmware is treated the same as software), is used.

5.3.6 MIL-STD-882 (military USA)

Standard Practice for System Safety is an American military standard. This Standard [11] is approved for use by all Military Departments and Defense Agencies within the Department of Defense (DOD).

It requires from the system developers to document the approach to:

- Identify hazards in the system through a systematic analysis approach
- Assess the severity of the hazards
- Identify mitigation techniques
- Reduce mishap risk to an acceptable level
- Verify and validate mishap risk reduction
- Report residual risk to the PM

5.3.7 DEF (AUSTRALIA) 5679

DEF (AUST) 5679, published by the Australian Department of Defense in March 1999, is a standard for the procurement of safety-critical systems with an emphasis on computer-based systems. The standard focuses on safety management and the phased production of safety assurance throughout the system development lifecycle, with emphasis on software and software-like processes. A safety case provides auditable evidence of the safety assurance argument.

Software risk and integrity assessments are based on the concept of development integrity levels. Probabilistic interpretations of risk are excluded because of the scope for error or corruption in the quantitative analysis process, and because it is currently impossible to interpret or assess low targets of failure rates for software or complex designs.

For each potential accident identified by the PHA, a severity category (Catastrophic, Fatal, Severe, or Minor) is allocated, based on the level of injury incurred. Sequences of events that could lead to each accident are identified and are assigned a probability where estimation is possible.

The Defense Standard uses Level of Trust (LOT) definitions. One of seven LOTs is allocated to each system safety requirement, depending on the severity category of the accidents that may result from the corresponding system hazard. The LOT may be reduced if each accident sequence can be shown to be sufficiently improbable. Each LOT defines the desired level of confidence that the corresponding system safety requirement will be met.

Next, one of seven SILs is assigned to each Component Safety Requirement (CSR), indicating the level of rigor required for meeting the CSR. By default, the SIL level of the CSR is the same as the LOT of the system safety requirement corresponding to the CSR. However, the default SIL may be reduced by up to two levels by implementing fault-tolerant measures in the design to reduce the likelihood of the corresponding hazard.

5.3.8 ISO 26262

In automotive systems, safety analysis is based on the ISO 26262 [50] standard. The standard consists of nine normative parts and a guideline for the ISO 26262 as the 10th part. Here some extracts from ISO 26262 are provided, that describe different safety analysis area covered by ISO-26262, for details please refer to the full ISO 26262 documentation.

ISO 26262 is intended to be applied to safety-related systems that include one or more E/E systems and that are installed in series production passenger cars with a max gross weight up to 3,5 t. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities. Systems developed prior to the publication date of ISO 26262 are exempted from the scope.

ISO 26262 addresses possible hazards caused by malfunctioning behavior of E/E safety-related systems including interaction of these systems. It does not address hazards as electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy, and similar hazards unless directly caused by malfunctioning behavior of E/E safety-related systems.

ISO 26262 does not address the nominal performance of E/E systems, even if dedicated functional performance standards exist for these systems (for example active and passive safety systems, brake systems, ACC).

Shortly, ISO 26262:

- Provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases
- Provides an automotive specific risk-based approach for determining risk classes (Automotive Safety Integrity Levels, ASILs)
- Uses ASILs for specifying the item's necessary safety requirements for achieving an acceptable residual risk; and provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved

ISO 26262 gives requirements and guidelines for Safety Analysis at:

- Product Development: System Level
- Hardware Level
- Software Level

Freedom from interference by software partitioning

ISO-26262 provides design guidelines to accomplish at SW level “Freedom of Interference”, thus allowing to avoid that safety-relevant components and data could be corrupted by non-ASIL components.

Automotive Scenario related to SAFURE Project will implement protection mechanisms aligned to these ISO guidelines.

The following text is taken from ISO-26262 and is about **Freedom of Interference**,

<u>Appendix D of ISO-26262 norm:</u>

Objectives

The objective is to prevent propagation of a failure in one software partition to another software partition.

<u>NOTE</u>: Errors in the state of the executing software can occur due to systematic software faults or due to random as well as systematic hardware faults. Such errors in one partition could disturb the operation of other software partitions either due to shared resources or due to error propagation.

General

***D.2.1** Software partitioning allows the co-existence of software partitions that use the same resources. It allows*

a) software components to be free from interference from other software components; and
<u>NOTE:</u> Different software partitions can be assigned different values of ASIL or a value of QM (see ISO 26262-9:—, Clause 5).

b) changes to be made to one software partition without the need to re-verify the unmodified software partitions.

<u>Impact on system and software design</u>
Depending on the system architecture, two approaches can be used:

c) several software partitions within a single microcontroller (see Figure D.1) with shared resources such as CPU time, memory, I/O-devices; and

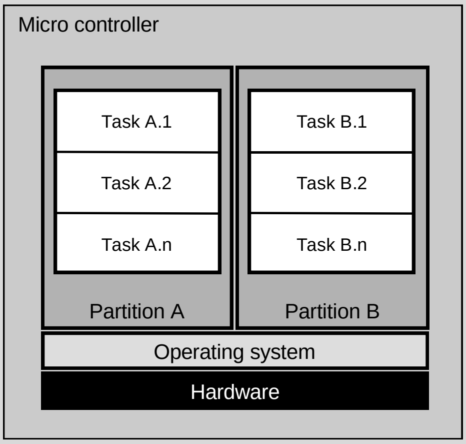

Figure 27: Several software partitions within a single microcontroller

d) several software partitions within the scope of a micro controller network (see Figures D.2 and D.3) with shared resources such as I/O-devices, especially internal and external data buses.

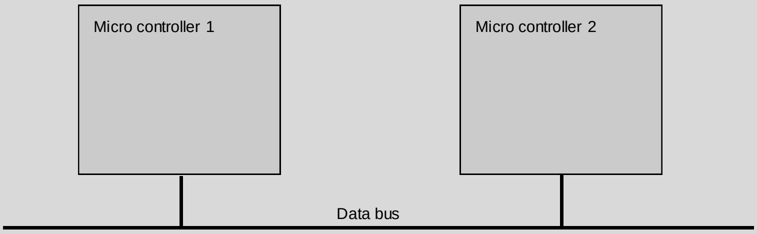

Figure 28: Several partitions within the scope of a micro controller network

<u>NOTE:</u> The micro controller network can consist of several processors in a single electronic control unit communicating via an internal data bus (intra processor communication). This is illustrated in figure D.3.

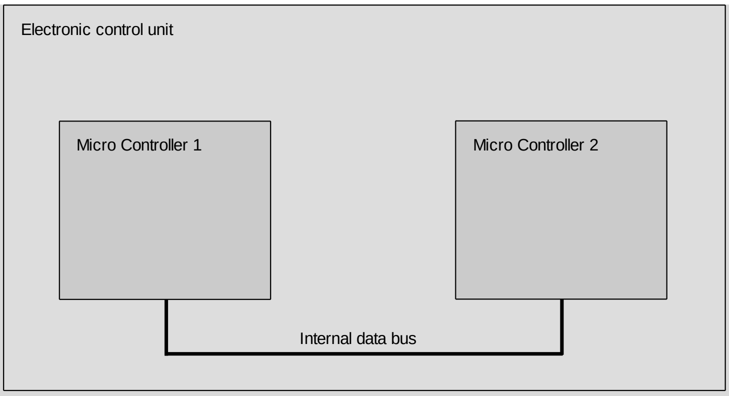

Figure 29: Several partitions within the scope of a multi-processor electronic control unit

Software components are executed within their respective software partition on their respective microcontroller as illustrated in Figures D.2 and D.3.

Impact on shared resources

Software partitioning requires adequate support by system resources.

In order to isolate multiple software partitions in a shared resource environment, the hardware has to provide the operating system with the ability to restrict access to shared resources for each software partition.

CPU time

To ensure freedom from interference of software partitions within a single microcontroller, the fault effects

- *blocking of partitions due to communication deadlocks; and*
- *wrong allocation of processor execution time*

are to be prevented by:

e) time triggered scheduling;

NOTE 1: Software partitions are considered coequally in allocating processor execution time and the same priority is assigned to all of them.
NOTE 2: Regarding the allocation of processor time, spare time is allocated in each processing cycle because of incoming interrupts.
NOTE 3: Time triggered scheduling is considered to have effectiveness “high” against protection against the fault effect “wrong processor execution time”.

f) cycling execution scheduling policy;

NOTE 4: The time triggered scheduling method specifies a scheduling algorithm based on a predetermined fixed schedule, repetitive with a fixed periodicity.
NOTE 5: Using the time triggered scheduling method the allocation of processor execution time takes place through a static allocation table. Thus, for each task, a fixed point in time is predetermined for activating the task. Usage of time triggered scheduling method precludes priority-based scheduling.

g) fixed priority based scheduling;
h) monitoring of processor execution time of software partitions in accordance with the allocation;

NOTE 6: Monitoring of each partition by software checks if all partitions are executed in conformance with the predefined static allocation table.

i) program sequence monitoring;

NOTE 7: Program sequence monitoring is based on a hardware device (see ISO 26262-5:—, Table D.10).

j) arrival rate monitoring.

NOTE 8: Monitoring of processor execution is an additive method of Program sequence monitoring. If both methods are combined the effectiveness is "high" protection against the fault effect “wrong processor execution time”.

Memory

To ensure freedom from interference of software partitions within a single microcontroller, the fault effect memory corruption due to unintended writing to memory of another partition

is to be prevented by:

k) memory protection mechanisms;
NOTE 1: The memory protection mechanisms refer to processors with Memory Management Unit or Memory Protection Unit.
NOTE 2: A Memory Management Unit enables the concept of virtual address space. This prevents a task of one partition corrupting the memory space of another task by unintended writing into that memory space, since every partition has its own address space.
NOTE 3: Usage of a Memory Management Unit requires support of the operating system.
NOTE 4: Provisions are made that the Memory Management Unit cannot be ignored, i.e. tasks are executed in a so-called user mode and the real addressing mode is not to be used.

l) verification of safety-related data;
NOTE 5: RAM locations containing safety-related data are verified by additional methods. This can be accomplished for example by using parity bits, Error Correcting/Correction Code (ECC), Cyclic Redundancy Checksum (CRC) or redundant storage.
NOTE 6: The effectiveness of these methods depends very heavily on the verification quality.
NOTE 7: Verification of safety-related data is done at run time.

m) offline analysis of code and data of other partitions;
n) restricted access to memory;
o) static analysis; and
NOTE 8: Static analysis methods defined in Table 10 can be used for reviewing pieces of code that access memory locations containing safety-related data.

p) static allocation.
NOTE 9: Static allocation means that resources are allocated statically during initialisation.

I/O-devices (communication)

To ensure freedom from interference of software partitions in communication microcontrollers, the fault effects

- *loss of peer to peer communication;*
- *unintended message repetition due to the same message being unintentionally sent again;*
- *message loss during transmission;*
- *insertion of messages due to receiver unintentionally receiving an additional message, which is interpreted to have correct source and destination addresses;*
- *re-sequencing due to the order of the data being changed during transmission, i.e. the data is not received in the same order as in which it was been sent;*
- *message corruption due to one or more data bits in the message being changed during transmission;*
- *message delay due to the message being received correctly, but not in time;*
- *blocking access to data bus due to a faulty node not adhering to the expected patterns of use and making excessive demands for service, thereby reducing its availability to other nodes, e.g. while wrongly waiting for non existing data; and*
- *constant transmission of messages by a faulty node, thereby compromising the operation of the entire bus.*

are to be prevented by:

q) identifier for communication objects;
r) keep alive messages;

NOTE 1: Keep alive messages is considered "high" effectiveness for detection of "Failure of communication peer".

s) alive counter;
NOTE 2: Alive counter is considered "high" protection against "Unintended message repetition" and "medium" protection against "Message loss", "Insertion of messages" and "Constant transmission of messages".

t) sequence number;
NOTE 3: Sequence number is considered "high" protection against "Unintended message repetition", "Message loss", "Insertion of messages", "Re-sequencing" and "Medium" protection against "Constant transmission of messages".

u) error detection codes;
NOTE 4: Cyclic Redundancy Checks are used as error detection codes if the residual error rate of the CRC implemented in the bus system is considered not to be sufficient. In this case an additional CRC at the application level is recommended.
NOTE 5: Alive Counter and CRC are transmitted (embedded in the frame for instance) and checked by the receiver.

v) error correction code;
w) message repetition;
NOTE 6: Message repetition is considered "high" protection against "Message loss", "Medium" protection against "Re-sequencing", and "Message corruption".

x) loop back;
y) acknowledge;
NOTE 7: Acknowledge is considered "high" effectiveness protection against the fault effect "Wrong communication peer".

z) separated point-to-point unidirectional communication objects;
NOTE 8: Exactly two uni-directional communication objects are used between two partitions respectively for data exchange.
NOTE 9: Method j) is considered "Medium" effectiveness protection against the fault effect "Wrong communication peer".

aa) unambiguous bidirectional communication object;
NOTE 10: Unambiguous bidirectional communication object uses unique numbers for identifying communication peers and/or acknowledges receipt of messages by the communication peer.
NOTE 11: Method k) is considered "medium" effectiveness protection against the fault effect "Wrong communication peer".

bb) asynchronous data communication; and
NOTE 12: In using asynchronous data communication there is no waiting state completed by the communication itself.
NOTE 13: Method l) is considered "high" effectiveness protection against the fault effect "Blocking of partitions".

cc) synchronous data communication.
NOTE 14: Access is synchronised between both software partitions using shared memory for communication. This can be done e.g. using semaphores.
NOTE 15: Communication objects in a) and j) between software partitions are e.g. pipes, message queues, shared memory. These communication objects cannot to be used for synchronizing partitions.
NOTE 16: Blocking read or write access is to be avoided by design when using message queues.

For bus allocation within a microcontroller network the following methods have to be considered:

dd) time-triggered data bus;
NOTE 1: Time-triggered data bus is considered "high" protection against "Failure of communication peer", "Insertion of messages", "Message delay", and "Medium" protection against "Blocking access to data bus".

ee) event-triggered data bus;
ff) event-triggered data bus with time-triggered access;
gg) mini-slotting;

NOTE 2: Mini slotting is considered "high" protection against "Constant transmission of messages" and "Medium" protection against "Message delay".
NOTE 3: Mini-slotting (see [ARINC 629]) requires each micro controller connected to the bus to wait a certain period before it is permitted to access the bus again.

hh) bus arbitration by priority;
ii) bus guardian.
NOTE 4: Bus guardian is considered "high" protection against "Blocking access to data bus", "Constant transmission of messages" and "Medium" protection against "Message corruption".

5.3.9 Autosar

With respect to the AUTOSAR modelling extensions and the examples of safety and security models in AUTOSAR and the related analysis methods, the possible exploitation is along three main directions.

The first possible exploitation channel is purely academic. Our aim is to describe the results of the project in research papers in conferences and journals. As a result of WP2 there are currently three topics that are promising and are currently being documented in research papers to be submitted

- The use of modeling extensions in AUTOSAR to describe input-output functional dependencies and the related possibilities for the purpose of safety and security analysis
- The use of modeling extensions for the specification of security requirements in application-level communications and the possibility for automatically generating components and RTE code from them
- The general framework of modelling extensions developed in WP2 for safety and security

Within the time period of this intermediate plan, we published one workshop paper with the preliminary results on the synthesis of security components from AUTOSAR models, but we plan for further submissions of research papers documenting the results to international conferences on modelling, security and timing analysis.

The second possible exploitation is on the example models and pertains to their possible evaluation by carmakers for improving the description of products.

The third exploitation option is the possibility of having the AUTOSAR consortium adopt some of the modelling recommendations or considering some of the issues that are raised in WP2 and planning for extensions to the standard in order to cope with them.

Chapter 6 Summary and conclusion

The SAFURE methodology targets the design of safe and secure cyber-physical system. The present document performs a technology watch report related to the SAFURE Framework methodology to build safe and secure solutions on multi-core platforms for mixed-criticality markets.

The focus is mainly on the current products in the market with the technologies used to ensure safety and security. The outcomes clearly show that the concepts of SAFURE could be applied to all telecommunication devices. The data integrity results of the project are expected to be relevant for IMD too. Thus, security of solutions, where COTS platforms (e.g. smartphones) and IMD are used together, can be significantly improved by the outcomes of SAFURE. Memory and timing protection concepts of the project can be applied for all ECU devices from the automotive domain, which can guarantee fulfilment of the standards and avoidance of malicious attacks. Due to the fact that the foundings showed the low level of certification requirement of DAL-E applications, aeronautical devices are seen as a perfect candidate for implementation of main SAFURE concepts. However, devices from the space domain are unlikely to fit the needs of the project “as they are”, but they deliver a number of features, which may be of interest for some end users. Moreover, potential technologies of interest for SAFURE requirements, such as RTOS, hypervisors and different communication interfaces, are described and will be watched continuously. The relevant standard of safety and security for SAFURE are also presented and taken into account.

In the current context, the SAFURE project is considered fully relevant in terms of the technologies it is developing. Most of them were found to be not systematically addressed in the current products on the market.

Chapter 7 List of Abbreviations

Abbreviation	Explanation
AMOLED	Active-Matrix Organic Light-Emitting Diode
AMT	Automated Manual Transmission (Also called Freechoice)
ANSSI	Agence nationale de la sécurité des systèmes d'information (French Network and Information Security Agency)
ASIL	Automotive Safety Integrity Level : classification scheme defined by the ISO26262
BGM	Blood glucose monitoring
CAL	Crypto Abstraction Library
CDMA	Code Division Multiple Access
COTS	Commercial Off-The-Shelf
CPL	Crypto Primitive Library
CRY	Crypto library module
CSM	Crypto Service Manager
DoD	Department of Defense
E/E	Electrical/Electronic
E/E/PES	Electrical/Electronic/Programmable Electronic Safety-related Systems
ECU	Engine Control Unit
ECU	Electronic Control Unit
EGR	Exhaust Gas Recirculation
ESP	Encapsulation Security Protocol
FCA	Fiat Chrysler Automobiles
FDA	Food and Drug Administration: The FDA is a federal agency responsible for the safety of drugs, medical devices, food and cosmetics.
FTP	File Transfer Protocol
GSM	Global System for Mobile
HD	High-definition
HSDPA	High Speed Downlink Packet Access
HSM	Hardware Security Module
HSPA	Evolved High Speed Packet Access
HSUPA	High-Speed Uplink Packet Access
HTTPS	Hypertext Transfer Protocol over TLS
IMA	Integrated modular avionics
IMD	Implantable Medical Device
IT	Information technology
LOT	Level Of Trust
LTCCs	Low Temperature Co-fired Ceramics
MDM	Mobile Device Management
NIPRNet	Non-Secure Internet Protocol Router Network

Abbreviation	Explanation
OSI	Open Systems Interconnection model
PCB	Printed Circuit Board
PDM	Personal Diabetes Manager
PEST	Political, Economic, Social, Technological; PEST analysis describes a framework of macro-environmental factors used in the environmental scanning component of strategic management
PIN	Personal identification number
PP	Protection Profile
QHD	Quad HD : 2560x1440 pixels
RSA	Rivest-Shamir-Adleman
SIPRNet	Secret Internet Protocol Router Network
SIP-TLS	Session Initiation Protocol TLS
SOTA	State Of The Art
SRTP	Secure Real-time Transport Protocol
SRTP	Secure Real-time Transport Protocol
SSL	Secure Sockets Layer
STIG	Security Technical Implementation Guide
SWOT	Strengths, Weaknesses, Opportunites et Threats : is a structured planning method that evaluates those four elements of a project or business venture
TCS	Thales Communications & Security
TCU	Transmission Control Unit
TLS	Transport Layer Security
VVA	Variable Valve Actuation
SLA	service level agreement
SaaS	Software as a Service

Table 1: List of Abbreviations

Chapter 8 Bibliography

[1] http://www.cryptophone.de/upload/files/42/original/CP500-Brochure.pdf

[2] http://www.ssi.gouv.fr/administration/qualification/hoox-m2/

[3] http://www.bull.com/sites/default/files/docs-dl/s-hoox_on_premises-en.pdf

[4] http://www.bull.com/sites/default/files/docs-dl/s-hoox_as_a_sevice-en_0.pdf

[5] https://www.silentcircle.com/uploads/misc/SilentCircleMarketingResources_Sep2015.pdf

[6] https://en.wikipedia.org/wiki/Silent_Circle_%28software%29

[7] https://gdmissionsystems.com/wp-content/uploads/2015/12/D-SMEPED-02-1115.pdf

[8] https://en.wikipedia.org/wiki/General_Dynamics#Information_Systems_and_Technology

[9] https://en.wikipedia.org/wiki/NSA_product_types

[10] Ministry of Defence. Safety Management Requirements for Defence Systems, Part 1 Requirements. Defence Standard 00-56 Issue 4, British Government, June 2007.

[11] Department of Defense. System Safety Program Requirements. Military Standard MIL-STD-882E, United States of America, 11 May 2012. http://www.system-safety.org/Documents/MIL-STD-882E.pdf

[12] Department of Defence. Safety Engineering for Defence Systems. Australian Defence Standard DEF(AUST)5679/Issue 2, Australian Government, 14 October 2008.

[13] Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. International Standard 61508, International Electrotechnical Commission, 2010.

[14] Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS). Draft Standard prEN 50126, European Committee for Electrotechnical Standardization (CENELEC), 2012.

[15] https://en.wikipedia.org/wiki/IEC_61508

[16] https://en.wikipedia.org/wiki/DO-178C

[17] http://www.workplaytechnology.com/downloads/WorkPlay-Technology-Discussion-Paper.pdf

[18] http://www.workplaytechnology.com/technology/

[19] http://www.arm.com/products/processors/technologies/trustzone/

[20] http://www.samsung.com/us/business/security/knox/

[21] http://www.samsung.com/us/system/b2b/resource/2015/06/26/KNOX_Brochure_Final_062515.pdf

[22] http://www.ssi.gouv.fr/administration/certification_cspn/teopad-version-1-1-06/

[23] https://www.thalesgroup.com/sites/default/files/asset/document/COM_WHITE%20PAPER%20TEOPAD_EN_V3.pdf

[24] https://en.wikipedia.org/wiki/ZigBee

[25] Mei-Yu Wu and Wen-Yen Huang, Chung Hua University, Hsinchu, Taiwan, Health Care Platform with Safety Monitoring for Long-Term Care Institutions. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5967567&tag=1

[26] Ping Wan, China, The real-time monitoring system for in-patient based on Zigbee. Intelligent Information Technology Application, 2008. IITA '08. Second International Symposium on (Volume:1) http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4739640

[27] https://en.wikipedia.org/wiki/Bluetooth

[28] https://fr.wikipedia.org/wiki/Chronologie_du_t%C3%A9l%C3%A9phone#Ann.C3.A9es_1990.2C_les_t.C3.A9l.C3.A9phones_sans_fil

[29] https://en.wikipedia.org/wiki/Smartphone

[30] “Opportunities and challenges for smartphone applications in supporting health behavior change: qualitative study” by Laura Dennison, Leanne Morrison, Gemma Conway, Lucy Yardley, Academic Unit of Psychology, University of Southampton, Southampton, United Kingdom. Published on 18.04.13 in the Journal of Medical Internet Research http://www.jmir.org/2013/4/e86/

[31] Financial Times, Health apps run into privacy snags, 1.09.2013

[32] Research2Guidance (2013), "The mobile health global market report 2013-2017: the commercialisation of mHealth apps" (Vol. 3).

[33] The New England Center for Investigative Reporting, Boston University, "Lacking regulation, many medical apps questionable at best", 18.11.2012.

[34] Catharine Paddock, Mobile medical apps: FDA issues final guidance, 24/09/2013, medical news today http://www.medicalnewstoday.com/articles/266479.php

[35] Modahi M. Telehealth index: 2015 consumer survey. American Well. January 2015. http://cdn2.hubspot.net/hub/214366/file-2374840622-pdf/TelehealthConsumerSurvey_eBook_NDF_Electronic_Version_(2).pdf?submissionGuid=a6b4e527-37a1-4d71-b035-446b73ebe6f1

[36] The European Commission, Green Paper on mobile health ("mHealth"), 10.4.2014 http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5147

[37] https://safure.eu/

[38] http://www.boeing.com/defense/boeing-black/index.page#/tech-spec

[39] Secure Simple Pairing Explained, Ellisys Bluetooth Expert Notes, 05/16/2011/ http://www.ellisys.com/technology/een_bt07.pdf

[40] Xiaojing Tang, Chao Hu, WeiXing Lin, Android Bluetooth Multi-Source Signal Acquisition For Multi-Parameter Health Monitoring Devices, August 2015, Proceeding of the 2015 IEEE International Conference on Information and Automation Lijiang, China http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7279577&tag=1

[41] https://en.wikipedia.org/wiki/Wi-Fi

[42] https://en.wikipedia.org/wiki/IEEE_802.11#802.11b

[43] Cristian Rotariu,, Alexandru Pasarica, Hariton Costin, Felix Adochiei and Razvan Ciobotariu, Telemedicine System for Remote Blood Pressure and Heart Rate Monitoring, 4th-26th November, 2011. Proceedings of the 3rd International Conference on E-Health and Bioengineering. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6150342&tag=1

[44] https://en.wikipedia.org/wiki/2G#cite_note-Radiolinja.27s_History-1

[45] https://en.wikipedia.org/wiki/3G

[46] https://en.wikipedia.org/wiki/CDMA2000

[47] https://en.wikipedia.org/wiki/UMTS_%28telecommunication%29

[48] https://en.wikipedia.org/wiki/WiMAX#Mobile_phones

[49] https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf

[50] International Organization for Standardization (ISO). ISO 26262: Road Vehicles - Functional Safety, 2011.

[51] http://www.debiotech.com/ (accessed: 2016/05/31)

[52] http://www.valtronic.com/current/articles/swiss-companies-debiotech-and-valtronic-announce-partnership-agreement-jewelpump (accessed: 2016/05/31)

[53] http://www.mylife-diabetescare.at/ (accessed: 2016/05/31)

[54] Burleson, Wayne, et al. "Design challenges for secure implantable medical devices." Proceedings of the 49th Annual Design Automation Conference. ACM, 2012

[55] http://www.cochlear.com/wps/wcm/connect/us/home (accessed: 2016/05/31)

[56] http://www.cwins.wpi.edu/workshop11/ppt/business_Charles.pdf (accessed: 2016/06/01)

[57] http://professional.medtronic.com/pt/neuro/dbs-md/index.htm#.V2F1FWJ96L4 (accessed: 2016/06/15)

[58] http://professional.medtronic.com/pt/gastro/ges/prod/index.htm#.V2F4cGJ96L5 (accessed: 2016/06/15)

[59] http://finetech-medical.co.uk/en-us/medicalprofessionals/footdropmanagement,poststroke.aspx (accessed: 2016/06/15)

[60] IEEE Std 802.1AE TM -2006 https://standards.ieee.org/getieee802/download/802.1AE-2006.pdf

[61] Magneti Marelli: Homepage http://www.magnetimarelli.com/

[62] “Announcing the ADVANCED ENCRYPTION STANDARD (AES)”. Federal Information Processing Standards Publication 197 November 26, 2001.

[63] https://itsecuritything.com/how-real-car-hacking/

[64] https://www.wired.com/2014/08/car-hacking-chart/

[65] J. Unruh, H.-J. Mathony, K.-H. Kaiser; Error Detection Analysis of Automotive Communication Protocols; SAE Paper 900699, Detroit, USA, 1990

[66] J. Charzinski; Performance of the Error Detection Mechanisms in CAN; Proceedings of the 1st international CAN Conference, Mainz, Germany, September 1994, pp. 1.20-1.29.

[67] E. Tran; Multi-Bit Error Vulnerabilities in the Controller Area Network Protocol; Thesis, Dept. of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, Pa, 1999.

[68] “CAN with Flexible Data-Rate”. Florian Hartwich (Florian.Hartwic@de.bosch.com), Germany.

[69] Final Project A Public-Key Authentication Scheme for Controller Area Networks. Nicolas Bravo (nbravo@mit.edu) Skanda Koppula (skoppula@mit.edu) Matthew Chang (m chang@mit.edu), May 2015.

[70] “Security Authentication System for In-Vehicle Network”. Hiroshi UEDA, Ryo KURACHI, Hiroaki TAKADA, Tomohiro MIZUTANI, Masayuki INOUE and Satoshi HORIHATA. SEI Technical review, number 81, October 2015

[71] ”Car2X Communication: Securing the Last Meter“. H. Schweppe, Y. Roudier, B. Weyl, L. Apvrille, and D. Scheuermann. WIVEC 2011, 4th IEEE International Symposium on

Wireless Vehicular Communications, 5-6 September 2011, San Francisco, CA, United States, pages 1–5, June 2011.

[72] M. Chavez, C. Rosete, and F. Henriquez. Achieving Confidentiality Security Service for CAN. In Electronics, Communications and Computers, 2005. CONIELECOMP 2005. Proceedings. 15th International Conference on, pages 166–170, 2005.

[73] "Secure communication for CAN FD". Armin Happel, CAN Newsletter 4/2014.

[74] "Securing CAN Bus Communication: An Analysis of Cryptographic Approaches". Jennifer Ann Bruton, Master Thesis, National University of Ireland, Galway. August 2014.

[75] http://www.eetimes.com/document.asp?doc_id=1328081

[76] IEEE Internet Computing. "TELNET: THE MOTHER OF ALL (APPLICATION) PROTOCOLS". Rohit Khare, University of California, Irvine • www.ics.uci.edu/~rohit/. Volume 2, Issue 3, May 1998, page 88-91.

[77] "Fundamentals_of_network_security" John E. Canavan. Artech House. Boston, London, UK. (Khare, 1998)

[78] https://en.wikipedia.org/wiki/Telnet

[79] Network Working Group of the IETF, January 2006, RFC 4251, The Secure Shell (SSH) Protocol Architecture

[80] https://tools.ietf.org/html/rfc4302

[81] https://tools.ietf.org/html/rfc4303

[82] AUTOSAR Security Modules Lecture. ESCAR 2015.

[83] http://standards.sae.org/as6802/

[84] Strategic Outlook of Global Autonomous Driving Market in 2016 - Frost & Sullivan

[85] Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99-120.

[86] Duncan, H. (2006). Ranking Models for the opportunities and threats of projects management. Gower Technical Press Limited.

[87] Foss, N. J., Klein, P. G., Kor, Y. Y., & Mahoney, J. T. (2008). Entrepreneurship, subjectivism, and the resource-based view: toward a new synthesis. Strategic Entrepreneurship Journal, 2(1), 73-94.

[88] Osterwalder, A., and Pigneur, Y. (2010). „Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers".

[89] Thomas, H. (2007). An Analysis of the Environment and Competitive Dynamics of Management Education, Journal of Management Development, Volume 6 (1), p. 9-21.

[90] Symonds, M. (2009). Brainstorming A SWOT Analysis, the Steps involved. McGraw – Hill inc; New York.

[91] [CC] Common Criteria Sponsoring Organizations, Common Criteria for Information Technology Security Evaluation. Version 3.1, revision 4, vol. 1--3, September, 2012, http://www.commoncriteriaportal.org/cc/

[92] Rance Delong, The MilsTM Architecture -- a Foundation for Dependable Systems, The Open Group Conference: Real-Time & Embedded Systems Forum, 2012, http://www.opengroup.org/public/member/proceedings/q212/23RT.htm (slides; only open to members of the Open Group).

[93] Igor Furgel, Viola Saftig, EURO-MILS project, EURO-MILS proposal for Projection Profile (PP) for a Highly Robust OS in Europe: project deliverable D12.3, http://dx.doi.org/10.5281/zenodo.51582

[94] Igor Furgel, Viola Saftig, Tobias Wagner, Kevin Müller, Reinhard Schwarz, Axel Söding-Freiherr Blomberg, Non-Interfering Composed Evaluation, MILS Workshop at HiPEAC 2016, http://dx.doi.org/10.5281/zenodo.47979

[95] [GH08] Green Hills Software, INTEGRITY-178B Separation Kernel Security Target, no. IN-ICR750-0100-GH01ST, May, 2008, http://www.niap-ccevs.org/cc-scheme/st/st_vid10119.pdf

[96] [GH10] Green Hills Software, INTEGRITY-178B Separation Kernel Security Target, no. IN-ICR750-0402-GH01ST, May, 2010, http://www.niap-ccevs.org/cc-scheme/st/vid10362/

[97] [SG95] Shaw, Mary, Garlan, David, Formulations and formalisms in software architecture, Computer Science Today, p. 307-323, 1995, Springer, http://www-2.cs.cmu.edu/~Compose/ProgCodif.pdf.

[98] Information Assurance Directorate, U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness. Version 1.03, June, 2007, http://www.niap-ccevs.org/cc-scheme/pp/pp_skpp_hr_v1.03/

[99] Tverdyshev, Sergey, Blasum, Holger, Langenstein, Bruno, Maebe, Jonas, De Sutter, Bjorn, Leconte, Bertrand, Triquet, Benoît, Müller, Kevin, Paulitsch, Michael, Söding-Freiherr von Blomberg, Axel, Tillequin, Axel, MILS Architecture, 2013, EURO-MILS, http://dx.doi.org/10.5281/zenodo.45164.

[100] [qnxrtos] http://www.qnx.com/products/neutrino-rtos/neutrino-rtos.html

[101] [vxwprod] http://windriver.com/products/product-overviews/2691-VxWorks-Product-Overview/

[102] [wikixen] https://en.wikipedia.org/wiki/Xen

[103] [xenprjwiki] http://wiki.xenproject.org/wiki/Xen_Overview

[104] [wwwsel4] http://sel4.systems/

[105] [PikeOS] https://www.sysgo.com/products/pikeos-hypervisor/

[106] [BOSCH] http://www.bosch-mobility-solutions.com/en/powertrain-electrified-mobility/

[107] [Continental] http://www.continental-automotive.com

[108] [ra_paper] Ross Anderson. On the security of digital tachographs. In Computer Security - ESORICS 98, pages 111-125. Springer, 1998.

[109] [scdabk_paper] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al. Comprehensive experimental analyses of automotive attack surfaces. In USENIX Security Symposium. San Francisco, 2011.

[110] [klcpmw_paper] Kerstin Lemke, Christof Paar, and Marko Wolf. Embedded security in cars. Springer, 2006.

[111] [EVITA] http://www.evita-project.org

[112] [wssrmm_paper] Winfried Stephan, Solveig Richter, and Markus Müller. Aspects of secure vehicle software ashing. In Embedded Security in Cars, pages 17-26. Springer, 2006.

[113] [aauhars_paper] André Adelsbach, Ulrich Huber, and Ahmad-Reza Sadeghi. Secure software delivery and installation in embedded systems. In Embedded Security in Cars, pages 27-49. Springer, 2006.

[114] [HSM] https://en.wikipedia.org/wiki/Hardware_security_module

[115] [EGAS] ”Standardized ETC Monitoring Concept for Gasoline and Diesel Engine Control Systems” v 6.0.

[116] [SPICE] http://www.automotivespice.com/

[117] E-Health « Des acteurs innatendus, quelle évolution du modèle commercial ? » , Paris, September 24, 2014, ROland

[118] NHS Data Breaches, A Big Brother Watch Report, NHS Data Breaches November 2014. EMBARGO 00:01 FRIDAY 14 NOVEMBER

[119] Rapport d’activité 2014, ASIPSANTE, agence des systèmes d’information partagés de santé

[120] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009R0661

[121] https://www.grandviewresearch.com/press-release/global-e-health-market

[122] http://www.sinus-institut.de/sinus-loesungen/sinus-meta-milieus-weltweit/

[123] https://fr.wikipedia.org/wiki/AUTOSAR

[124] http://www.cochlear.com/wps/wcm/connect/uk/home/discover/baha-bone-conduction-implants

[125] http://finetech-medical.co.uk/en-us/aboutus.aspx

[126] https://en.wikipedia.org/wiki/FADEC

[127] https://en.wikipedia.org/wiki/Integrated_modular_avionics

[128] http://www.gaisler.com/index.php/products/processors/leon3ft?task=view&id=364 (accessed: 2016/06/17)

[129] http://www.gaisler.com/index.php/products/boards/gr-cpci-gr740 (accessed 2016/06/17)

[130] http://www.rtca.org/store_product.asp?prodid=617

[131] http://www.magnetimarelli.com/business_areas/powertrain/gasoline-system-gdi/ecu

[132] http://www.magnetimarelli.com/business_areas/powertrain/gasoline-system-pfi/ecu

[133] http://www.magnetimarelli.com/business_areas/powertrain/transmission/amt-hydr

[134] http://products.bosch-mobility-solutions.com/media/en/ubk_europe/db_application/downloads/pdf/antrieb/de_5/Bosch_di_folder.pdf

[135] https://www.boschautoparts.com/en/auto/fuel-injectors/port-fuel-injection

[136] http://www.continental-automotive.com/www/automotive_de_en/themes/passenger_cars/powertrain/ProductInfo_CMArticletransmission_en_1.html

[137] http://www.magnetimarelli.com/excellence/technological-excellences/amt

[138] http://www.standard.co.uk/news/techandgadgets/darkmatter-katim-ultrasecure-smartphone-for-worlds-elites-unveiled-in-barcelona-a3477501.html

[139] http://www.forbesmiddleeast.com/en/darkmatter-says-that-its-katim-phone-is-the-worlds-most-secured/

[140] http://www.zdnet.com/article/sirin-labs-launches-ultra-secure-ultra-expensive-solarin-smartphone/

[141] http://www.01net.com/actualites/solarin-le-smartphone-android-ultra-securise-a-17-000-dollars-979390.html

[142] http://www.androidauthority.com/solarin-phone-756894/

[143] https://koolspan.com/about/

[144] http://economictimes.indiatimes.com/slideshows/tech-life/5-most-secure-smartphones-in-the-world/solarin/slideshow/53883184.cms

[145] http://katim.com/katim-phone/

[146] https://play.google.com/store/apps/details?id=im.team&hl=fr

[147] https://www.youtube.com/watch?v=2nsEAw_SirQ

[148] “5G Cellular: Key Enabling Technologies and Research Challenges” byEkram Hossain and Monowar Hasan. IEEE Instrumentation & Measurement Magazine(June 2015).

[149] Huawei Whitepaper, “5G: A Technology Vision,” Nov. 2013. http://www.huawei.com/ilink/en/download/HW_314849

[150] 5G: New Air Interface and Radio Access Virtualization - Huawei WHITE PAPER 2015

[151] “Horizon 2020 and Beyond_2015”, IEEE vehicular technology magazine MARCH 2015

[152] Mikel Fernandez, David Morales, Leonidas Kosmidis, Alen Bardizbanyan, Ian Broster, Carles Hernandez, Eduardo Quiñones, Jaume Abella, Francisco J. Cazorla, Paulo Machado, Luca Fossati, "Probabilistic Timing Analysis on Time-Randomized Platforms for the Space Domain", 20th Design, Automation and Test in Europe Conference (DATE), March 2017.

[153] Carles Hernandez, Nils-Johan Wessman, Leonidas Kosmidis, Alen Bardizbanyan, Jaume Abella, Jan Andersson, Francisco J. Cazorla, "EFL: Enabling Timing Guarantees in Multi-core Processors with Shared Caches", 22nd Data Systems In Aerospace Conference (DASIA), May 2017.

[154] Javier Jalle, Mikel Fernandez, Jaume Abella, Jan Andersson, Matthieu Patte, Luca Fossati, Marco Zulianello, Francisco J. Cazorla, "Contention-Aware Performance Monitoring Counter Support for Real-Time MPSoCs", 11th IEEE International Symposium on Industrial Embedded Systems (SIES), May 2016.

[155] Burleson, Wayne, et al. "Design challenges for secure implantable medical devices." Proceedings of the 49th Annual Design Automation Conference. ACM, 2012

[156] R. William Beckwith, W. Mark Vanfleet, Lee MacLaren. “High Assurance Security/Safety for Deeply Embedded, Real-time Systems”, Embedded Systems Conference 2004.

[157] MINIMED 670G System: https://www.medtronicdiabetes.com/products/minimed-670g-insulin-pump-system