5G communication and security in connected vehicles

Antonio Imbruglia, Daniela Cancila, Marina Settembre

5G Communication and Security in Connected Vehicles

Antonio Imbruglia
STMicroelectronics, Stradale Primosole 50, 95121, Catania, Italy; email:antonio.imbruglia@st.com

Daniela Cancila
Université Paris-Saclay, CEA, List, F-91120, Palaiseau, France; email: daniela.cancila@cea.fr

Marina Settembre
Fondazione Ugo Bordoni, Viale del Policlinico 147, 00161, Roma, Italy; email:msettembre@fub.it

Abstract

The widespread diffusion of Cyber-Physical Systems and their capability to interact with the physical world depend also on the availability of 5G network. The exponential development of intelligent and interconnected IoT and autonomous systems, combined with the development of 5G networks, presents new challenges from a cyber-security perspective. The paper, without claiming to be exhaustive, offers insights and reflections on the very broad topic that integrates innovative devices, 5G and cybersecurity by illustrating the main European directions indicated by both the Strategic Research and Innovation Agenda for Electronic Component and Systems (ECS-SRIA) and the evolution of 5G network standards. Some of the afore-mentioned issues will be reanalysed through use cases based on Vehicles to X (V2X) scenario, where connectivity, safety and cybersecurity play a key interworking.

Keywords: ECS-SRIA, 5G, Cybersecurity, Safety, V2X

1 Introduction

The exponential development of IoT systems, electric embedded devices and cyber-physical systems (CPS), with stronger intelligence and interconnection requirements, takes advantage of the development of 5G networks. In spite of new emerging application scenarios, new thorny issues in cyber-security should be considered due to an increased attack surface and evolving threat landscape. These systems are going to operate in a more dynamic and open environment respect to traditional systems, with increasing needs to exchange information with other systems. Consider electric and autonomous vehicles, where the connection with both other vehicles and the environment (e.g. infrastructure, roads, traffic lights pedestrians) can improve road safety, reduce environmental impact, and provide a new driving experience. However, if susceptible to cyber-attacks, these systems could have catastrophic consequence. Moreover, in traditional systems, specialized operators manage the system. For example, in the railway application domain, a team of experts manages the system (including train maintenance). In this new scenario, the actors involved in the management can be more heterogenous, belonging to different organizations and not always so specialized to recognize the nominal or degraded behavior of the system, following for example a cyber-attack.

The paper, without claiming to be exhaustive, offers insights and reflections on the very broad topic that integrates innovative devices, 5G and cybersecurity by illustrating the main European directions indicated by both the Strategic Research and Innovation Agenda for Electronic Component and Systems (ECS-SRIA), [1] and some insights into the evolution of 5G network standards. For the sake of concreteness, some considerations will be reanalyzed in Vehicles to X (V2X) case studies.

2 ECS-SRIA

The Strategic Research and Innovation Agenda for Electronic Component and Systems (ECS-SRIA) aims at describing the "Major Challenges, and the necessary Research & Development & Innovation efforts to tackle them, in micro- and nanoelectronics for smart systems integration all the way up to embedded and cyber physical systems, and System of Systems" [1].

ECS-SRIA is developed by three industrial associations: AENEAS [2], Inside Industry Association [3] and EPOSS [4], with the support of a European team of experts in the discipline coming from European industries, Research and Technology Organizations and Academics in Europe.

ECS-SRIA is based on three main areas (see Figure 1):

- Key application areas, such as Mobility, (Green colour)
- Fundamental Technologies, such as Embedded software and Beyond, (Blue colour)
- Cross-Sectional technologies, such as cybersecurity, safety, connectivity, (purple colour).

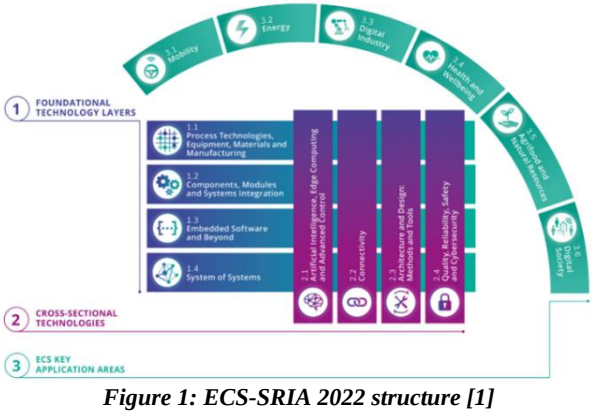

Figure 1: ECS-SRIA 2022 structure [1]

Some of the main ECS-SRIA objectives address:

- To boost industrial competitiveness through interdisciplinary technology innovations [1]
- To ensure EU digital autonomy through secure, safe and reliable ECS supporting key European application domains [1]
- To establish and strengthen sustainable and resilient ECS value chains supporting the Green Deal [1].

The following sections discuss some insights related to the chapters of the ECS SRIA in which the authors are more active.

3.1 The Cyber-Security and Privacy Challenge

The new generation of CPS are closed to the non-expert human via societal applications. For example, CPS may be customized to individual, including an embedded combination of heterogeneous subsystems of different quality, artificial Intelligence (AI) and connectivity functionality. In this context, ECS-SRIA identifies the cyber-attacks risks and the potential leakage of sensitive data, highlighting a research direction towards a "robust root of trust system, with unique identification enabling security without interruption from the hardware level right up to the applications, including AI involved in the accomplishment of the system's mission in dynamic unknown environments" [1]. A particular emphasis is placed on trustworthiness and the hardware security of such systems. Many organizations in Europe, including the IC and Digital System Division, at CEA LIST, and STMicroelectronics, are working in this direction.

The challenge also highlights the need to achieve a common recognized certification scheme under the composition of modular trusted hardware and trusted software. Electric and autonomous vehicles, for example, include several heterogeneous sensors, actuators and embedded devices, that can change or updated over time. Evolution of certification dealing with system changing in some parts over time is a challenge both in terms of cost and security, and, hence, competitiveness.

Ensuring privacy is another relevant theme in the challenge. This focus includes not only privacy-by-design approach, but also of quantum-safe cryptography modules everywhere in the system.

Finally, the challenge addresses "ensuring both security and safety" properties. In the case of autonomous vehicle, enhanced connectivity can be useful for driving safety, but, if susceptible to cyber security attacks, may have catastrophic consequences. Ensuring both safety and security requirements has been also capital during the Covid-19 pandemic. Then, in order to achieve a greater level of trustworthiness, it is necessary to properly manage safety and cyber-security issues in the same system.

3.2 The Connectivity Challenge

The main ECS SRIA challenges to ensure European leadership in terms of connectivity technologies as well as associated hardware technology supporting the development of connectivity solutions can be summarized as follows:

- Strengthening the EU connectivity technology portfolio to maintain leadership, secure sovereignty and offer an independent supply chain.
- Investigate innovative connectivity technology (new spectrum or medium) and new approaches to improving existing connectivity technology to maintain the EU's long-term leadership
- Autonomous interoperability translation for communication protocol, data encoding, compression, security and information semantics.
- Architectures and reference implementations of interoperable, secure, scalable, smart and evolvable IoT and SoS connectivity
- Network virtualisation enabling run-time engineering, deployment and management of edge and cloud network architectures

Finally, secure communication and control by powerful computation system applying AI are fundamental.

4. Innovation Aspects in the 3GPP 5G Standard Evolution

The innovative aspects of 5G networks are not only evolutionary in nature, basically characterized by performance improvements (e.g. capacity, mobility management, connection density, spectral efficiency, latency, energy efficiency), but also present many revolutionary elements (e.g., network softwerization and programmability, network slicing, cloud native approach, more flexible and expanded use of frequencies, artificial intelligence, new approach to cybersecurity). 5G can be considered as a multiplicity of dedicated, flexible, and intelligent networks open to new actors to connect anything and to dynamically serve different verticals, exploiting the concept of slicing. In such a complex scenario the standardization, regulatory and institutional bodies, vendors, and operators should face many challenges to ensure security, safety, privacy, net neutrality and transparency for all users [6]. The third-generation partnership project, 3GPP [6], which is the reference standard for mobile communications, identifies three phases in 5G evolution [7]. During phase 1, the first set of 5G specifications on the new radio have been completed both for non-standalone solutions, when the new radio interacts with an existing 4G/LTE core network, and for the standalone solution, when the new radio interconnects within a 5G core network. The new radio truly represents a step forward from previous generations of radios both in terms of flexibility, throughput, latency, and reliability to meet even mission critical service requirements, exploiting a frequency spectrum that expands from low frequencies below 1 GHz to mmWave, flexible subcarrier spacing up-to 400MHz Channel bandwidths for a single-component (CC) carrier, 3D beamforming for improvement of spectral efficiency, dynamic time-division duplexing (TDD). New radio plays an important role in the autonomous driving application scenario that we will consider in the Section 4. In Phase 2, 3GPP introduced the new concept of Service Base Architecture (SBA) for the 5G

core network (Release 16) [8], aiming at providing unprecedented flexibility agilityrespect to the traditional architecture. In Phase 3, Release 17 and beyond, new 5G enhancements are considered both on the radio part (e.g., MIMO, positioning, side-link) and on the core network and slicing, extending it to the access part [9]. New security features have been introduced compared to previous generations, such as a stronger cryptographic algorithm for 256-bit encryption, better air interface security, user privacy protection and enhanced roaming security, but SBA is a completely new concept and leads to completely new security challenges. The SBA is composed of services. Each Network Function (NF) can be regarded as a service [6]. In the upper green part of the Fig. 2 are represented the NFs of the control plane, while the lower part represents the user plane and access networks. It is out of the scope of the present paper entering into details of each network function, (a detailed description can be found in [9]), but for improving the understanding the NFs are, schematically and not rigorously, grouped by functionality.

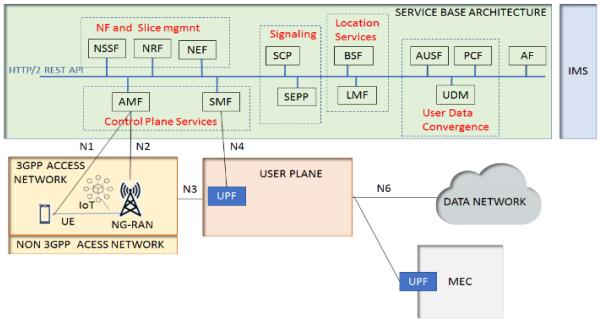

Fig.2 SBA architecture view, [6]

NFs are self-contained, independent and can be connected to a service bus, using common Internet protocol, [10-12]. Each NF is a software running on virtual machines or containers efficiently deployed as a Virtual Network Function (VNF) by exploiting cloud computing. NFV and SDN allow the implementation and automation of customized services on a fully programmable platform. Several NFs can be combined to form a logical block, named slice, addressing a specific purpose, with specific QoS and latency features. 3GPP has already standardized some specific slices as massive Machine Type (mMTC), enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency (URLLC) and Vehicle-to-X (V2X) communications, but many others can be defined as well. It is undoubtable that the integration of network slicing, NFs, NFV, SDN allows a powerful, flexible, fast, and dynamic service deployment, but its management is complex, and the security should be properly addressed,[6]. 5G threat landscape is complex and continuously evolving, [12]. Potential source of attacks (threat actors) could come from end devices, untrusted networks, roaming networks, internet application service providers or insider attack. These attacks constitute different threats to network assets, that can be schematically categorized as loss of availability, confidentiality, integrity, and control [13].

4.1 V2X scenario: communication, safety, and security issues

The automotive industry is at the center of a real revolution. 5G with its low latency, higher bandwidth and great flexibility can provide many previously unachievable features to automotive sector. In recent years vehicles have been equipped with an increasing number of electronic Advanced Driver Assistance Systems (ADAS) developed to increase the level of safety and driving comfort, exploiting four types of sensors: radar, lidar, camera and ultrasonic shortrange sensors, [14]. However, these sensors have limitations. They are unable to see a pedestrian around the corner or to alert drivers to hazards or slowdowns before they meet on the road: they do not communicate. To complement ADAS systems there are systems called Vehicle to X (V2X) overcoming intrinsic limitation of ADAS systems and, hence, providing features of 360° vision, Non-Light of Sight view, extended range, and the ability to communicate between vehicles, [15]. There are basically two types of communication for connected vehicles. Dedicated short-range communication (DRSC) is the first standard of V2X technology, based on the IEEE 802.11p standard and operating at 5.9 GHz. It provides the ability for vehicles to communicate with other vehicles and infrastructure around them, exchanging basic safety messages to prevent collisions, but it is not a system for long range communications (about 300 m). Subsequently, 3GPP has introduced the cellular V2X (C-V2X) starting with Release 14, which in turn was based on Release 12 related to Device to Device (D2D) communications. 3GPP specifies four types of C-V2X communication: Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Network (V2N), and Vehicle to Pedestrians (V2P). The 3GPP's C-V2X standard supports two complementary communication methods: a cellular network-based communication, that uses the air LTE Uu interface and uses the cellular communication bands for long-range transmissions to connect to the network and thus to services; and a direct or side-link that uses the PC5 interface for short-range (less than 1 km) V2V and V2I communications. 3GPP Release 14 defines the foundations of C-V2X communication for basic security message exchange. New features are added in Release 15, but a real step forward is possible with Release16 with the use of 5G New Radio. 5G NR V2X provides lower latency, ultra-reliable communication, and high data rate useful for addressing challenging autonomous driving requirements (e.g. high throughput sensor sharing, intent/trajectory sharing, real time local updates to build detailed maps and share them, coordinated driving etc.), [15]. In the connected vehicles scenario some critical challenges and possible C-V2X solutions are:

- high relative speed of two vehicles driving in opposite directions causes a Doppler shift and frequency offset. C-V2X provides an improved signal design and additional reference signal symbols for better channel estimation.
- high vehicle density can lead to radio resource congestion. C-V2X can adopt algorithms that detect available resources, selecting the least congested ones.

- Loss of out-of-coverage synchronization. C-V2X is inherently a synchronous system using GNSS.

An application scenario for connected vehicles with challenging requirements on the radio component is platooning, where the lead vehicle of a convoy relays information to the vehicles behind it. Platooning offers many advantages for long-distance travel since vehicles can drive at a constant speed with a short distance in between, reduced air resistance and, hence, a reduction in fuel consumption and CO2 emissions. Moreover, platooning improves safety by, reducing response times and minimizing the risk or, at least, the impact of accidents. ETSI (European TLC Standards Institute) define, the requirements in terms of end-to-end latency, reliability, and data rate, for enhanced V2X scenarios, (e.g. platooning, as driving with high or full automation, remote driving, sharing large amounts of sensor data). It results that 5G NR V2X represents the most suitable solution for Advanced Safety Automated Driving scenarios, as reported in [15], but the increased connectivity and automation expose them to several cyber threats. [17]. ITU-T Recommendation X.1372 provides security guidelines for different V2X scenarios, some depicted in Fig. 3, [18]. Specifically, ITU-T Recommendation X.1372 identifies cybersecurity threats, security requirements to mitigate these threats and describes possible implementations of secure V2X communications. Security issues deal with: i) identification, authenticity to authorize access to services and information, ii) message integrity to ensure that information is accurate and reliable, iii) availability of services and information, iv) confidentiality & privacy of users, their data and their actions from eavesdropping and exploitation and v) non-repudiation and accountability of the source of information. In the case of identification, authenticity, and integrity the main threats to be considered are message manipulation by an attacker providing false information, credential manipulation allowing access to information without authorization, manipulation of sensor data and information, causing traffic congestion, accidents etc., and interception of message and malicious reply in place of the authorized user. In the case of availability, the main threats consist of i) jamming and distributed denial of service (DDoS) attacks caused malicious service requests congesting the channel capacity and so impacting the reliability or availability of C-V2X services, ii) timing attack aiming at delaying the delivery of a safety message to other vehicles and iii) hacking of sensors providing incorrect values determining transient or permanent faults. For confidentiality and privacy issues, the main threats are due to eavesdropping of V2V, V2I, V2P, and V2D messages or leaking of personally identifiable information as identity, position, actions, trajectories of a user of the V2X service. Finally, for non-repudiation case main threats may occur if an attacker manipulates the certification database or accesses the private key to a certificate without authorization. The analysis of possible mitigations to the above-mentioned threats for C- V2X is out of the scope of the presen paper.

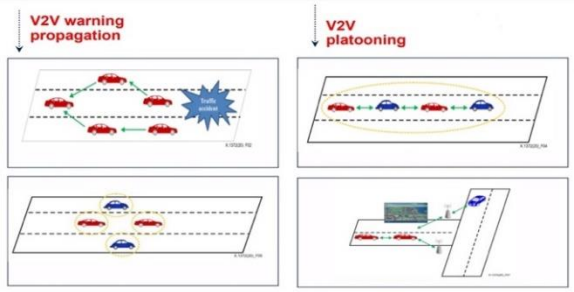

Fig.3 V2X communication scenarios, [18]

5. Conclusions

In this paper, without claiming to be exhaustive, some insights from the ECS-SRIA and the evolution on 5G networks have been discussed focusing mainly on connectivity, cybersecurity, and safety issues. The cellular-V2X scenario has been analysed as a relevant use case where connectivity, safety and security have a key interwork.

Acknowledgment

This paper has been originated from a lecture the authors gave in the framework of the course 0921SIC10, organized by AMES Society - AEIT (Italian Association of Electrical, Electronics, Automation, Information and Communication Technology). The authors wish to thank AMES -AEIT for supporting this activity.

References

[1] ECS-SRIA. Electronic Components and Systems - Strategic Research and Innovation Agenda, 2022.
[2] https://aeneas-office.org/
[3] Home | Inside (inside-association.eu)
[4] EPoSS (smart-systems-integration.org)
[5] M. Settembre, "A 5G Core Network Challenge: Combining Flexibility and Security", 2021 AEIT International Annual Conference 2021, pp. 1-6.
[6] https://www.3gpp.org/
[7] https://www.3gpp.org/release-16
[8] https://www.3gpp.org/release-17
[9] 3GPP TS 23.501, "System architecture for the 5G System (5GS)", version 17.4.0, March 23, 2022.
[10] NGMN Alliance, "Service Based Architecture in 5G", (Final deliverable (approved-P Public), January 2018.
[11] D. Borsatti, L. Spinacci, C. Grasselli, M. Settembre, W. Cerroni, F. Callegati, "A Network Slicing Architecture for Mission Critical Communications", IEEE WiMob 2020 Workshop on ICT Systems for PPRR, Oct. 2020.
[12] ENISA Report "Threat Landscape for 5G Networks", update December 2020.
[13] ENISA Report - Security in 5G Specifications, Feb. 2021.
[14] M. Duncan, A. Imbruglia, S. Gligerini, "The way forward and opportunities towards autonomous driving, AEIT, March, pp. 50-55, 2019.
[15] NGMN Alliance, "V2X: white paper ", 2019.
[16] 3GPP TS 22.186 version 15.3.0 Release 15.
[17] ENISA Report "ENISA good practices for security of smart cars", November 2019.
[18] Recomm. ITU-T X.1372 "Security guidelines for vehicle-to-everything (V2X) communication", March 2020