CISTER

Research Centre in
Real-Time & Embedded
Computing Systems

Journal Paper

Wireless Communication Technologies for Safe Cooperative Cyber Physical Systems

Ali Balador

Anis Koubâa*

Dajana Cassioli

Fotis Foukalas

Ricardo Severino*

Daria Stepanova

Giovanni Agosta

Jing Xie

Luigi Pomante

Maurizio Mongelli

Pierluigi Pierini

Stig Petersen

Timo Sukuvaara

*CISTER Research Centre

CISTER-TR-181128

2018/11/21

Wireless Communication Technologies for Safe Cooperative Cyber Physical Systems

Ali Balador, Anis Koubâa*, Dajana Cassioli, Fotis Foukalas, Ricardo Severino*, Daria Stepanova, Giovanni Agosta, Jing Xie, Luigi Pomante, Maurizio Mongelli, Pierluigi Pierini, Stig Petersen, Timo Sukuvaara

*CISTER Research Centre

Polytechnic Institute of Porto (ISEP-IPP)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail: aska@isep.ipp.pt, rar@isep.ipp.pt

http://www.cister.isep.ipp.pt

Abstract

Cooperative Cyber-Physical Systems (Co-CPSs) can be enabled using wireless communication technologies, which in principle should address reliability and safety challenges. Safety for Co-CPS enabled by wireless communication technologies is a crucial aspect and requires new dedicated design approaches. In this paper, we provide an overview of five Co-CPS use cases, as introduced in our SafeCOP EU project, and analyze their safety design requirements. Next, we provide a comprehensive analysis of the main existing wireless communication technologies giving details about the protocols developed within particular standardization bodies. We also investigate to what extent they address the non-functional requirements in terms of safety, security and real time, in the different application domains of each use case. Finally, we discuss general recommendations about the use of different wireless communication technologies showing their potentials in the selected real-world use cases. The discussion is provided under consideration in the 5G standardization process within 3GPP, whose current efforts are inline to current gaps in wireless communications protocols for Co-CPSs including many future use cases.

© CISTER Research Center
www.cister.isep.ipp.pt

sensors

MDPI

Article

Wireless Communication Technologies for Safe Cooperative Cyber Physical Systems

Ali Balador [1,2,*], Anis Kouba [3], Dajana Cassioli [4], Fotis Foukalas [5], Ricardo Severino [3], Daria Stepanova [6], Giovanni Agosta [7], Jing Xie [8], Luigi Pomante [4], Maurizio Mongelli [9], Pierluigi Pierini [10], Stig Petersen [11] and Timo Sukuvaara [6]

1 Innovation, Design and Technology (IDT), Mälardalen University, 72123 Västerås, Sweden
2 RISE SICS Västerås, Stora Gatan 36, 722 12 Västerås, Sweden
3 CISTER Research Centre, ISEP, Polytechnic Institute of Porto, 4249-015 Porto, Portugal; aka@isep.ipp.pt (A.K.); rarss@isep.ipp.pt (R.S.)
4 The Department of Information Engineering, University of L'Aquila, 67100 L'Aquila, Italy; dajana.cassioli@univaq.it (D.C.); luigi.pomante@univaq.it (L.P.)
5 DTU Compute, Technical University of Denmark, 2800 Kongens Lyngby, Denmark; fotisf@dtu.dk
6 Space and Earth Observation Centre, Finnish Meteorological Institute, 99600 Sodankylä, Finland; daria.stepanova@fmi.fi (D.S.); timo.sukuvaara@fmi.fi (T.S.)
7 Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Via G. Ponzio 32, I-20133 Milano, Italy; agosta@acm.org
8 Group Technology & Research, DNV GL, Veritasveien 1, 1363 Høvik, Norway; jing.xie@dnvgl.com
9 CNR-IEIIT, via De Marini 6, 16149 Genova, Italy; maurizio.mongelli@ieiit.cnr.it
10 Innovation and Technological Services (ITS), Intecs S.p.A., 56121 Pisa, Italy; pierluigi.pierini@intecs.it
11 SINTEF ICT, 7465 Trondheim, Norway; Stig.Petersen@sintef.no
* Correspondence: ali.balador@mdh.se; Tel.: +46-73-662-1583

Received: 9 September 2018; Accepted: 12 November 2018; Published: 21 November 2018

Abstract: Cooperative Cyber-Physical Systems (Co-CPSs) can be enabled using wireless communication technologies, which in principle should address reliability and safety challenges. Safety for Co-CPS enabled by wireless communication technologies is a crucial aspect and requires new dedicated design approaches. In this paper, we provide an overview of five Co-CPS use cases, as introduced in our SafeCOP EU project, and analyze their safety design requirements. Next, we provide a comprehensive analysis of the main existing wireless communication technologies giving details about the protocols developed within particular standardization bodies. We also investigate to what extent they address the non-functional requirements in terms of safety, security and real time, in the different application domains of each use case. Finally, we discuss general recommendations about the use of different wireless communication technologies showing their potentials in the selected real-world use cases. The discussion is provided under consideration in the 5G standardization process within 3GPP, whose current efforts are inline to current gaps in wireless communications protocols for Co-CPSs including many future use cases.

Keywords: cooperative cyber-physical systems; wireless communication; safety; reliability; 5G

1. Introduction

Modern embedded systems, coupled with the advancements of digital communication technologies, have been enabling a new generation of systems, tightly interacting with the physical environment via sensing and actuating actions: Cyber Physical Systems (CPS) [1]. These systems, characterized by an unprecedented level of pervasiveness and ubiquity, have been increasingly relying on wireless communication technologies to provide seamless services for the Internet of Things (IoT) [2] and Industry 4.0 [3], via flexible cooperation. As these Cooperative CPS (Co-CPS) starts approaching

safety-critical application domains (e.g., automated vehicles platooning in the automotive and maritime domains, process control in hazardous industries, etc.), safety shows-up as a crucial topic that must be carefully analyzed because failures and errors might lead to hazardous situations, e.g., death, injuries or environmental damages. All these systems are required to perform specific safety functions to ensure that the risk of system's failure is maintained at an acceptable level. What makes the safety of these systems even more challenging is the fact that they heavily rely on wireless communication to exchange safety-critical information. For example, in automotive applications like vehicular platooning [4–6], the IEEE 802.11p standard is used as a communication protocol among vehicles, in a closed-loop control system where exchanged messages contribute to maintain the inter-vehicle safety distance. Message losses or delays may lead to serious crashes among the vehicles in the platoon with dramatic consequences. In this case, real-time and reliability are two important aspects for ensuring the safety of operation of the platoon. Furthermore, security is also very relevant as any possible attack on the platoon, such as for example false data injection, spoofing or jamming, would lead to disastrous consequences as well.

For several years, topics such as safety in Co-CPS have been mostly ignored to the point that, currently, the absence of a de-facto standard on safe and secure Co-CPS is becoming an impediment to their adoption. Security, on the other hand, has been investigated to some extent in several protocols like IEEE 802.11p, IEEE 802.15.4 [7,8] and its variants [9]. However, there are still several challenges in what concerns the impact analysis of several attacks upon cooperating functions, or the integration of security mechanisms with remaining Quality of Service (QoS) properties for safety assurance.

In this line, the ECSEL SafeCOP EU research project addresses these issues regarding the design of wireless safe and secure Co-CPS [10]. In fact, the SafeCOP project deals with safe cooperation of complex CPS that relies on wireless communications. The main objective is to provide a *safety assurance methodology* for these systems with emphasis on applications in the healthcare, maritime, automotive domains.

In this paper, we provide an overview on the safety requirements, challenges and solutions of Co-CPSs relying on wireless communications. We review the state-of-the-art of standard protocols used in Co-CPSs and assess their compliance to the requirements of safety, security and real-time for Co-CPSs. The main result provided by this survey is a collection of general recommendations for decision-making about the use of wireless technologies in Co-CPSs, which are illustrated through the application in relevant real-world use cases. In addition, given that currently 5G constitutes one of the most important areas of research in Europe towards enabling the interoperability and cooperation of heterogeneous radio technologies for the provision of innovative powerful services, we discuss how the current efforts in 5G standardization contribute to addressing the Co-CPSs challenges.

Several reviews of CPS are already presented in the literature, since 2011 [11], with focus on specific issues, such as: system design [12], open source [13], medical applications [14], testing [15], industry 4.0 [16], interoperability [17] and monitoring with formal verification [18]. Many others address security and inherent countermeasures, e.g., [19,20]. Some others focus on energy topics (smart grids and building, wind plants) [21–23]. Only two others are directly comparable to the work presented here as they concern safety [24,25]. Our focus is new as we address how to overcome impairments on safety due to the wireless channel with reference to real testbeds.

The rest of the paper is organized as follows: Section 2 provides the state of the art of Co-CPS as technical background. Section 2.5 outlines different Co-CPS use cases that are addressed in the SafeCOP project. Section 3 provides a survey on wireless communication technologies used in Co-CPSs pointing also out their safety issues, predicting how these could be overcome. Section 4 provides a survey about the safety and security protocols for the considered Co-CPS use cases. Finally, Section 5 explores the current 5G standardization efforts and shows to what extent new 5G standard proposals solve the Co-CPS challenges in each SafeCOP's use case, drawing out from the previous chapters. Section 6 concludes the paper.

2. Technical Background

In the SafeCOP project, we are interested in the class of "safety-critical Co-CPSs" [26,27] where any failure may provide damages of different types and severity (financial, environmental, health, human life, etc.). Thus, the concept of safety is related to the capability of controlling and mitigating hazardous situations. Such systems highlight significant challenges that are not adequately addressed by existing practices, related to their rapid design, development and integration, under (non-functional) requirements of safety, security and dependability. Furthermore, mechanisms and methods for efficiently upgrading and re-certifying systems are needed.

Dependability, as a general term, takes care of several aspects like performance, fault tolerance, adaptiveness to unpredictable environment evolution, CPS platea variability and reconfiguration, issues affecting the communications reliability, etc. There are many subtle interactions and interdependencies among safety, security and dependability (also mentioned as Quality of Service—QoS). Often, security is conflicting with safety and QoS, thus requiring to evaluate a quantifiable trade-off between the three. Security is a composite of several attributes including availability, confidentiality and integrity [28]. The introduction of security requirements into systems tends to modify the priorities of some other non-functional requirements. In addition, resource constraints may make it infeasible to guarantee absolute security in all circumstances.

Developing a safety critical system, thus, typically requires making design decisions that trade-off safety concerns, functionality, cost, and other considerations. Achieving adequately safe cooperative cyber-physical systems requires arriving at realising, and assuring a safe design even though participants in the design process are competitors reluctant to share all of their concerns or intricacies of designs with each other. Moreover, due to the cooperative and openness nature, many circumstances which have to be covered by the pre-release safety assurance are difficult to anticipate at design time in the case of Co-CPS.

2.1. Co-CPSs Safety Definitions

A wide variety of technical approaches and methods have been used or proposed to analyse system safety, hazards and risk over several decades. The concept of risk management is addressed by ISO 31000 [29] standard that provides a generic framework for assessing and managing risk across various industries. The aim is to obtain an understanding of the risk to inform decisions regarding whether risk is tolerable with respect to some criteria, to differentiate risk associated with different options/decisions, and to determine if (and which) risk treatment options should be implemented to control or modify risk. Barrier management is a safety philosophy widely used in the oil and gas industry [30]. The idea is to control risk by putting measures in place to prevent undesirable incidents from occurring and limit their effects if they occur. Barriers intended to reduce the likelihood of undesirable incidents are called preventive barriers, whereas barriers implemented to avoid escalation and reduce effects of incidents are called mitigating barriers. Systems-Theoretic Accident Model and Processes (STAMP) is a recent accident model, first introduced by [31], based on systems theory focusing on enforcing behavioural safety constraints rather than preventing failures. STAMP is able to assess complex sociotechnical systems by thinking of safety as a control problem rather than a reliability one. Failure Modes, Effects, and Criticality Analysis (FMECA) (a variant of FMEA adding the assessment of criticality) originated from the U.S. Military and was first described in a Military procedure MIL-P-1629A [32] and later used by NASA in the Apollo program. An FMECA involves reviewing components, sub-systems and assemblies to identify failure modes, causes and effects. The approach is described in [33]. Other significant approaches are the Fault Tree Analysis (FTA) and the Event Tree Analysis (ETA).

Looking at the industrial context, several standards are applied. The IEC61508 [34] is an international standard of rules applied in 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. Central to the standard are the concepts of risk and safety functions. The risk is a function of the 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. IEC 61508 defines safety integrity level (SIL) as a discrete level (one out of possible four), corresponding to a range of safety integrity values, where SIL 4 is the highest level of safety integrity and SIL 1 is the lowest. The standard has its origins in the process control industry. It covers the complete safety life cycle, and may need interpretation to develop sector-specific standards. In fact, the standard lies at the root of a number of specific domains e.g., IEC26262 for automotive, EN50128 for railway applications, IEC60601 for medical devices, etc.

2.2. Safety Approach in SafeCOP

The development of Co-CPS poses challenges on safety issues that are not adequately addressed by existing practices and standards exposed above. One of the primary objective of SafeCOP is to propose an approach to the safety assurance of Co-CPS which will facilitate their certification and market release.

The system's safety behavior is typically modeled through a set of "safety cases". A safety-case is a well-documented body of evidence, in the form of a clear argument, assuring that the system is acceptably safe. Building the safety case requires ensuring not only that identified failures have been addressed, but also that any unwanted interactions between the system parts as well as the environment have been managed. This is usually accomplished by gathering the risk assessment's results, i.e., the safety evidence during system development.

To obtain this result, we propose a combination of:

- a safety-assurance framework for Co-CPS,
- a reference "Runtime Manager" is able to detect at runtime abnormal behaviour, triggering, if needed, a safe degraded mode.

SafeCOP applies the Safety Assurance approach to manage functional safety activities during the life-cycle of the machine, i.e., the "assumption/guarantee contracts" that facilitates compositional verification and allows for independent development of components. As the contracts capture safety-relevant behaviors, they are used during system development for generating system-specific safety cases. It is necessary to assure that the system relates to the runtime assurance claim of whether the system is still sufficiently safe (whether the contracts are violated) in the current environment or not. A continuous Runtime Manager checks for contract violations. Since contracts are the specifications of the system's behavior, contract violations are seen as the system failures. Contracts must be always satisfied in any environment condition, thus their violation during runtime indicates that a failure occurred in the environment, i.e., the behavior guaranteed at design-time has been broken. On the other hand, if the contract assumptions are not violated, then the runtime manager should check if the system offers the promised guaranteed behavior. If the guaranteed behavior is not provided, then an internal failure exists.

2.3. Security vs. Wireless Communication

Beyond the safety, the overall system dependability relies on security: there are many subtle interactions and interdependencies among safety, QoS and security as introduced in previous sections. Often, security is conflicting with safety and performances, thus requiring to evaluate a quantifiable trade-off between the three. Security is a composite of several attributes including availability, confidentiality and integrity [28]. The introduction of security requirements into systems tends to modify the priorities of some other non-functional requirements. In addition, resource constraints may make it infeasible to guarantee absolute security in all circumstances. One of the key issues that allows the trade-off evaluation is the definition of a metric [35,36]. Metrics are also suitable for security assessment of services, applications, as well as users and communication channels. Several strategies

have been proposed in the area of communication channels security to secure protocols and messaging schema. The most widely used mechanism over TCP/IP networks is currently the Secure Socket Layer (SSL), a cryptographic protocol that provides data authentication, encryption and integrity. A SSL connection is established, between two pair nodes, exchanging identification parameters in the form of digital certificates. Defense mechanisms against possible threats, either malicious or due to environment, are also defined. In particular, wireless communications are subject to physical layer attacks, like, e.g., the well-known family of wireless jamming attacks (a noise burst that may result in a Denial of Service (DoS) attack on a wireless channel), or, the most common eavesdropping attacks. These require specific measures known as *physical layer security mechanisms* aimed at increasing the robustness and secrecy capacity of the wireless channel [37]. The main issues are related to the enhanced flexibility and scalability of the networks, especially in the case of Co-CPSs, where different systems could participate to a cooperative group with different roles and the group dimension can vary over time, like in vehicular use cases, where a platoon is a high dynamic set of cars continuously entering and exiting the platoon itself. Vision and details on these items are available in, e.g., [38–40]. While the security approaches proposed in the literature mainly focus on the trustiness of the information flowing through the network, enforcing the network access and utilization (e.g., user authentication, message integrity, etc.), the evolutionary scenarios for Co-CPSs require that the trustiness of services and users must also be guaranteed, extending the authentication mechanisms.

2.4. Security Approach in SafeCOP

SafeCOP aims to extend the current wireless protocols for both safe and secure cooperation. SafeCOP propose an application-level "safety layer" on top of existing protocols to ensure safe and secure cooperation such that Co-CPS can be certified.

The wireless communication channels considered in SafeCOP and addressed by Use Cases span from 802.11p (for automotive domain), 802.11 for generic communication support, 802.15x for short range communication, as well as mobile LTE. In general, such technologies have been designed to meet communication requirements and significant progress has been done to secure the channels, but they cannot satisfy the safety requirements imposed by the selected use cases. Therefore, SafeCOP is working to enhance current wireless communication protocols to ensure that safety requirements are preserved, together with security, in the highly dynamic scenarios envisaged for Co-CPSs, where traditional safety assurance methods may not be sufficient. Details on communication technologies adopted by each use case and the protocol enhancements proposed within SafeCOP project are presented in Sections 3 and 4.

However, attention is taken to the technology evolution of mobile networks since the future 5G technologies will address most of the challenging network issues, e.g., providing higher bandwidth, very low latency, specific priority schemes, device-to-device (D2D) communications, as well as more mobile-specific capabilities. Network virtualization increases the flexibility of 5G networks, and improves their adaptability to the specific communication requirements of Co-CPSs. While in the multi-provider environments of current mobile networks communication services are conveyed by different providers, the 5G ecosystem allows a further degree of flexibility through virtualization: application functions and services fall in the paradigm of "Everything as a Service" of cloud computing. Moreover, the storage capability of the cloud allows to collect a wide range of (sensors) data and to support the application logic with data analytics. A deeper discussion on 5G is available in Section 5.

2.5. SafeCOP Use Cases

The SafeCOP project aims to cover safety-crytical Co-CPS of a wide range of industrial domains. To reach this objective it is driven by five representative use cases that span from hospital applications with low-speed movements, vehicular applications with high speed movements, to maritime applications. In what follows, we briefly introduce the use cases addressed in the SafeCOP project.

(A) **Hospital Application: Autonomous Hospital Beds**

To reduce the risk of contamination and spread of disease, hospital beds are thoroughly cleaned before being used by a new patient. In most hospitals, the cleaning is performed manually on site in each patient room, even in hospitals where they have a centralized bed-washing facility (CBWF). This is because moving the bed to and from the CBWF takes about the same amount of time as cleaning the bed in the ward. Both manually cleaning a bed and transporting beds to the CBWF are tasks that require hard physical labor and non-ergonomic motions and positions. To avoid unnecessary strain on hospital workers, and to free up a large amount of their time, this use case proposes an automated solution using two small mobile robots, designated MiR00. After the discharge of a patient, the MiR100s will autonomously transport the bed from the ward to the CBWF for washing, and then bring a clean bed from the CBWF back to the ward. A MiR100 will be attached to each end of the bed, and coordinate and synchronize their movement through the use of safe communication. As the MiR100s are small, their vision is quite limited. To assist in navigation and obstacle detection, a network of cameras will be installed in the hospital hallways. These cameras will act as remote eyes, allowing the robots to maneuver in restricted spaces and keep out of peoples' way.

Figure 1 provides the layout of the hospital beds testbeds, where two individual mobile robots are moving in the corridor covered by wireless access points.

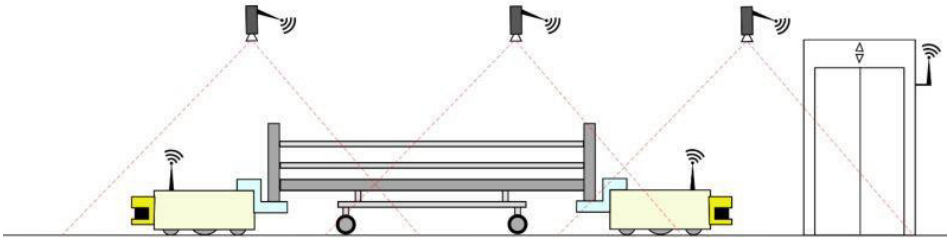

Figure 1. Layout of the use case "Autonomous Hospital Beds".

(B) **Maritime Application: Autonomous Boat Platoons**

Since international shipping is responsible for approximately 90% of world trade transportations, the safety of vessels is critical to the global economy. Human errors account for approximately 75% of the almost 15,000 marine liability insurance claims analyzed over five years, which correspond to over $1.6 bn [41]. Autonomous/semi-autonomous ships could improve maritime safety but revolutionize the movement of ships [42]. International Maritime Organization (IMO, London, UK) has received a proposal supported by a number of countries to include autonomous ships on its agenda. The IMO Maritime Safety Committee will establish a new international legal framework for the safe operation of autonomous vessels. It is evident that safety considerations are crucial in this respect. The main barrier to the development of autonomous shipping is represented by the concerns related to the risk of collision between manned and unmanned vessels. Moreover, as the number of cyber threats are increasing, a great concern is raised on specific cyber-attacks targeting the control of autonomous vessels [43]. To reduce inherent risk, cybersecurity should be taken at a high priority when developing autonomous ships.

Among various explorations of autonomous ships, bathymetry (Bathymetry is the study of underwater depth of lake or ocean floors. Bathymetric charts are typically produced to support geophysical exploration and environmental monitoring) is a very attractive application [44]. Bathymetry is usually performed by sailing a boat with a multi-beam sonar in a rather repetitive lawn-mover pattern. The data acquisition should ideally be going on 24/7, but when

using manned survey boats this possibility may be limited due to crew Health and Safety Executive (HSE) regulations. This is an ideal task for an unmanned surface vehicle (USV) that sails these repetitive patterns 24/7. USV application to bathymetry will result in a twofold gain: saving costs and reducing HSE risk for survey personnel [45]. This gain increases for bathymetry measurements in extreme conditions like the Arctic Ocean, where USV may replace a fully-crewed ship and shows better performance in adverse environments and inclement weather.

At the current stage, the USV has to be remotely controlled by a human operator who is located on another vessel. Such cooperation between the USV and the manned vessel can dramatically increase navigation safety while heavily relying on wireless communications between them, as illustrated in Figure 2. The USV and manned vessel have to periodically exchange critical information, such as vessel speed, course and position, to maintain a certain formation. The USV receives instructions and commands from the manned vessel to maneuver or stop. When safety-critical events occur (e.g., potential collisions), the manned vessel sends safety control commands to the USV, which has to respond within a certain time to avoid collisions. Therefore, packets carrying critical information and safety control commands are subject to *very low latency requirements*.

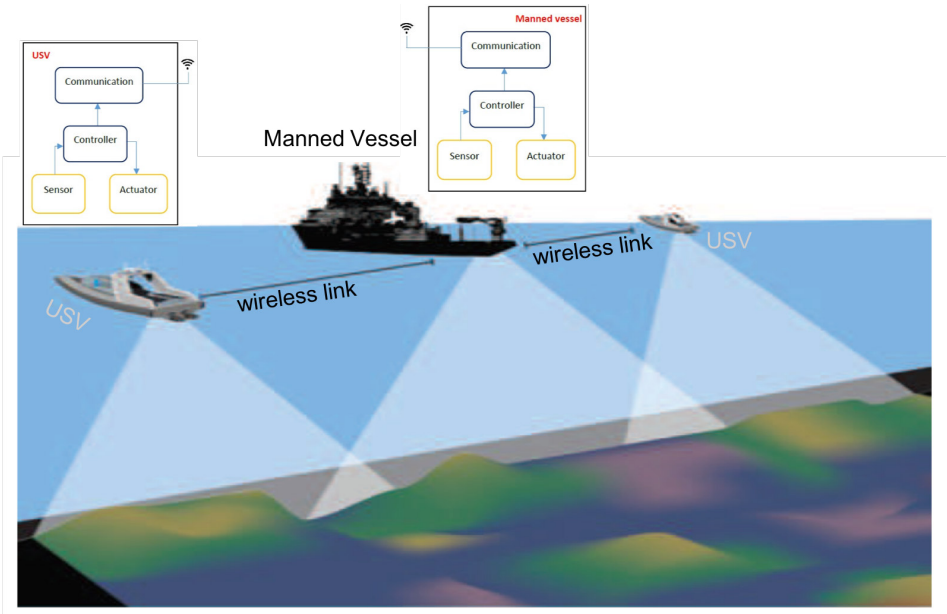

Figure 2. During the bathymetry measurements operation, the boats and the unmanned surface vehicle (USV) communicate wirelessly for coordination.

(C) Vehicular Applications

Safety, comfort and efficiency of both roads and vehicles have improved considerably over the last decade. However, our transportation system still suffers from many problems. The fast growth of urban areas causes an increasing trend of vehicular traffic and road accidents, resulting in serious socioeconomic problems. According to the latest report from the United States (U.S.) National Highway Traffic Safety Administration (NHTSA, Washington, DC, USA), the annual casualties of motor vehicle crashes was a total of 32,999 fatalities and 3.9 million injuries on the roadways of the U.S., which is equal to the annual economic loss to $836 billion [46]. Moreover, in 2014, highway users in the U.S. spend extra unnecessary 6.9 billion hours in traffic jams and consume an additional 3.1 billion gallons of fuel, adding up to an annual economic loss of $160 billion [47].

To address these problems, there have been worldwide efforts by automotive companies, universities, and governments to provide applications, services, and technologies that connect a vehicle to its surroundings. Examples of such applications and services may include adaptive cruise control, automate braking, remote vehicle diagnostics, hazards, and blind spot warnings. Typically, a connected vehicle (CV) includes interactive advanced driver-assistance systems (ADAS) and cooperative intelligent transport systems (C-ITS), where vehicle awareness concerning its current traffic context is aided by information exchange with surrounding vehicles through vehicle-to-vehicle (V2V) communication, close roadside units through vehicle-to-infrastructure (V2I) communication or people through vehicle-to-pedestrian (V2P) communication, collectively referred as V2X. The use of V2X communications can expand the horizon of on-board sensing systems, thereby eliminating 80% of the current road accidents and providing a smarter and safer ground transportation system [48]. These technologies are anticipated to offer significant benefits, including: reduced driver stress and possibility for passengers to rest and work while traveling; reduced driver costs of paid drivers for taxis and commercial transport; mobility for non-drivers including disabled people, therefore reducing the need for motorists to chauffeur non-drivers, and to subsidize public transport; increased road safety and therefore crash costs and insurance premiums; reduce high-risk driving, such as when impaired e.g., by alcohol consumption; efficient parking, increasing motorist convenience and reducing total parking costs; increase fuel efficiency and reduce pollution emissions. SafeCOP defined three use cases related to the vehicular applications, as described in the following.

- Vehicle Control Loss Warning

  The goal of this use case is to demonstrate how we can apply and extend wireless technologies to support automotive cooperative V2x-based systems such as auto-braking in vehicle platooning. Besides inter-vehicle networking, this use case is also exploring intra-vehicle communication. Therefore, we consider a scenario where a platoon of vehicles is traveling along a motorway, and Control Loss Warning (CLW) system should be able to detect any safety relevant occurrence that may compromise the vehicle's platooning ability, such as a braking system failure. Upon detection, the system should send a CLW alert to the other elements involved in the process, e.g., other cars in the platoon.

  The operation in this use case is illustrated in Figure 3. In case of control loss of any vehicle (the blue vehicle in the figure), CLW alert is delivered from car to car forward and backward using the V2V communication infrastructure, and eventually each vehicle gains knowledge about the CLW and can react in a pre-defined manner, by entering in a safe mode. In addition, a wireless network of in-vehicle sensors and actuators is exchanging data with the on-board unit to inform about the status of different automotive systems.

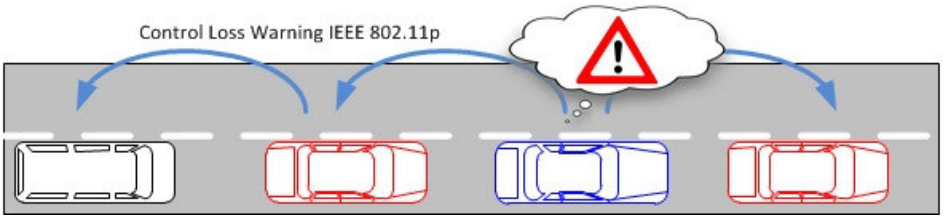

Figure 3. Vehicle control loss warning.

- Vehicles and Roadside Unit (RSU) interaction

  This use case has been built upon the data exchange between the roadside road weather station and a passing vehicle. Road weather stations (RWS) are typically installed to fixed

locations beside the road, collecting different measurement parameters related to weather and traffic, and delivering this data to a single data collection point, typically being the road administrator. Within its operative RWS and vehicular measurement entity, FMI demonstrates this operational environment [49]. During the RWS pass, the vehicle receives up-to-date local road weather information. As an exchange, vehicle can also deliver its own observational information back to RWS, to be used as local supporting data in meteorological services. In this vehicle-roadside unit interaction, we must ensure that the delivered data is not altered or violated by a third party or some communication malfunctioning.

The primary scenario in this use case is data exchange between vehicle and RWS, when and where the vehicle is passing the RWS. The basic scenario is introduced in [50]. This scenario is extended to cover also data exchange between two vehicles (scenario 2). In this case, both vehicles share the data received from the latest RWS, and as a result both vehicles will obtain up-to-date road weather data from the area ahead. The communication in this scenario is naturally local area communication. In the final extension (scenario 3), we employ an IoT cloud as communication entity, and instead of direct data exchanges between vehicles and RWSs, the IoT cloud shares the location-based relevant data with vehicles and RWSs. The architecture of these resulting three scenarios are presented in Figure 4. A vehicle and a roadside unit are participating in the first scenario (vehicle-to-infrastructure), two vehicles in the second scenario (vehicle-to-vehicle) and, finally, a service provider, a vehicle and a roadside unit to the final (third) IoT-cloud scenario.

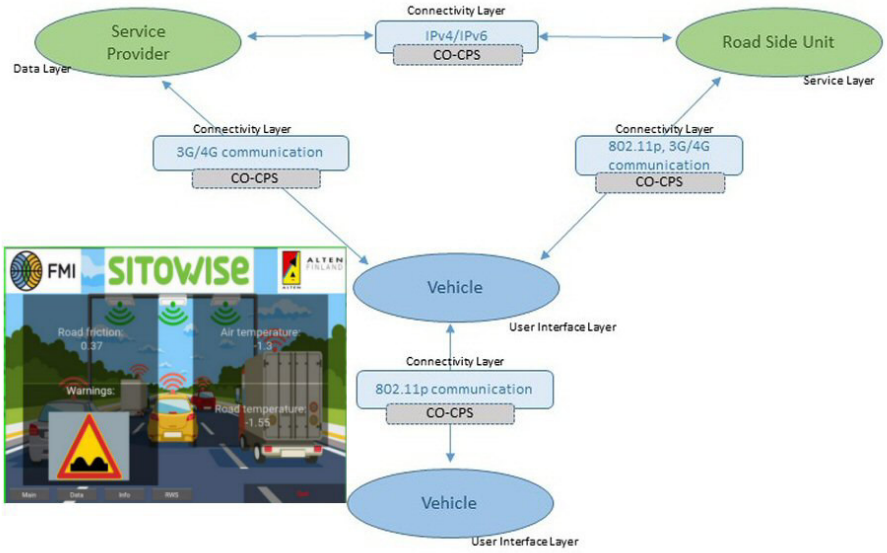

Figure 4. Operational structure of the use case "Vehicles and Roadside Unit (RSU) interaction" with communication to the cloud using 3G/4G, and IEEE 802.11p and 3G/4G for communication between vehicles and roadside units.

- V2I Cooperation for Traffic Management

  This use case aims at providing an innovative platform that integrates into the V2I network both traffic management (TM) and Video Content Analysis (VCA) functionalities, as shown in Figure 5. VCA consists in the acquisition from video cameras (referred to as RSU-C in Figure 5) and subsequent elaboration through appropriate algorithms. Active road safety

(ARS) programmes will strongly benefit from this integration, which enables, via VCA, the early-detection of possible dangerous road events/situations (e.g., vehicles slowing down, vehicles queue, motionless objects) and, via TM applications, the fast drivers' alert of such traffic anomalies [51,52].

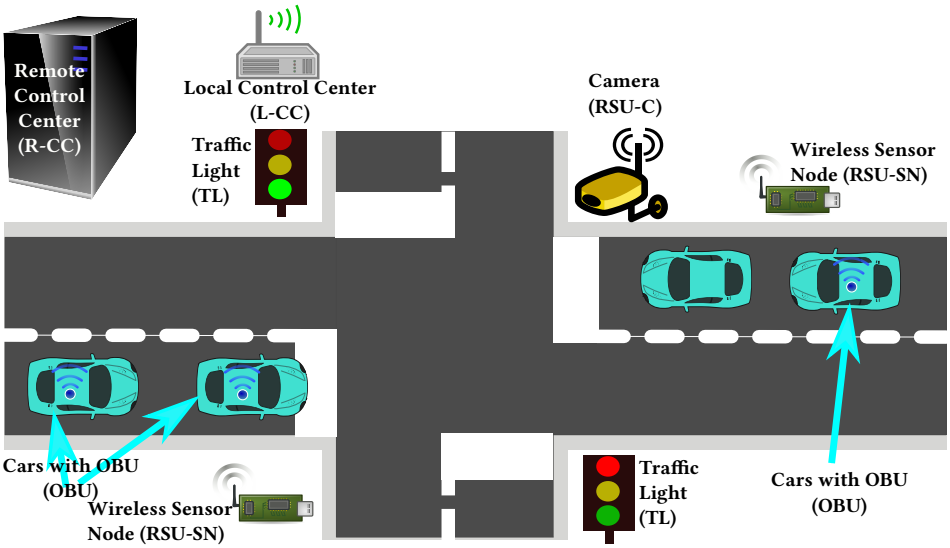

Figure 5. Typical scenario for a V2I cooperation system for traffic management.

The probability of traffic accidents will decrease by providing assistance to drivers exploiting both ARS (e.g., collision avoidance systems) and other management applications, like Adaptive Traffic Light Systems (A-TLSs) and dedicated wireless sensor networks (WSNs). A-TLSs change the traffic lights signaling plan (the duration of red, yellow and green phases) according to a set of control parameters, e.g., the time and the day. A-TLS improvements enabled by VCA allow the optimization of the signaling plan according to the changing traffic conditions, usually by extending the green phase when vehicles are closely spaced.

Figure 6 shows the architecture of the envisaged system. It integrates several SafeCOP framework components, including runtime mechanisms for safety assurance and distributed safety-critical cooperation techniques (based on extensions to IEEE 802.11p), into a Traffic Management Application, which runs in a distributed way. This system will represent one of the SafeCOP demonstrators. It is composed of on-board (OBU) and road side (RSU) units, and a server-based Control Center. Communications between the parts of the demonstrator system are performed through radio frequency front-ends which transmit and receive on-the-air, or through attenuators and noise generators for testing purposes. The OBU integrates radio communication and inertial sensors, allowing additional information on vehicle behavior to be received by the RSU. The RSU acquires video from the camera and performs the necessary initial elaboration to reduce communication times, aggregates information from vehicles in its operating range, and transmits the information over a wired connection to the remote Control Center.

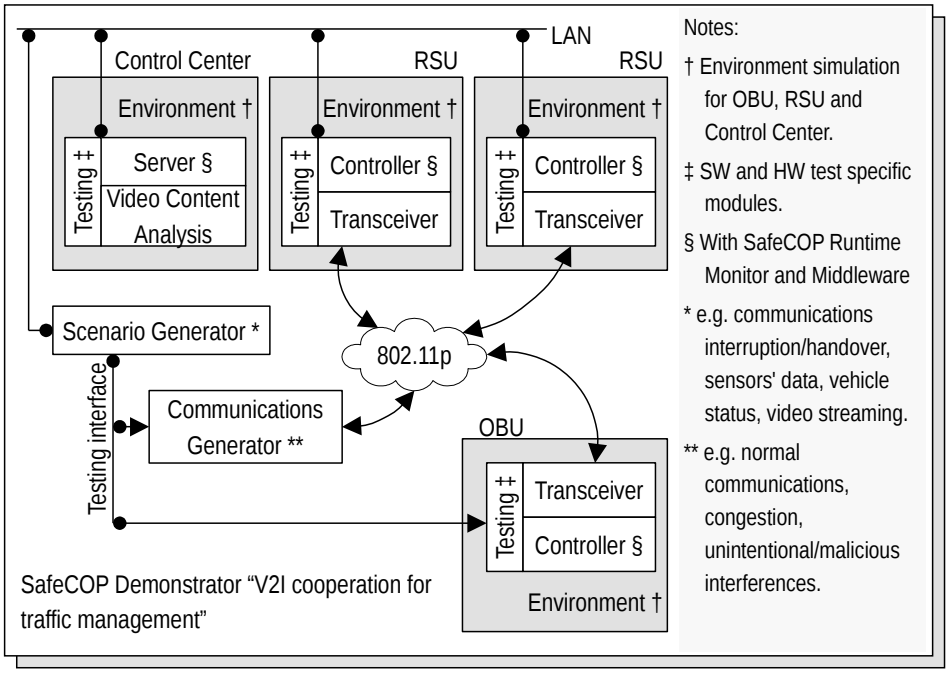

Figure 6. System architecture for the traffic management application through V2I cooperation.

3. Communication Technologies for SafeCOP Co-CPSs

Communication technologies vary for different Co-CPS use cases. For different use cases, we can use different protocols, open and proprietary, and technologies. Here, we give a brief overview of the most common communication technologies and protocols in each of the five use cases. Notably, we consider existing technologies that can be suitable candidates per use case because match the design requirements better.

3.1. Hospital Application

This use case will employ two different wireless protocols, namely Wi-Fi and XBee. The IEEE 802.11-based Wi-Fi protocol will primarily handle MiR100-to-camera communication. Wi-Fi infrastructure is already installed in some hospitals, and provides good coverage with relatively high data rates needed for transmission of live video streams. In addition, since both MiR100s are connected to the same network, non-safety related information and data will be transmitted between the MiR100s over the Wi-Fi connection. The Wi-Fi network can also be used for future communication between MiR100 and other hospital information systems of interest. For safety-critical MiR100-to-MiR100 communication, a small and inexpensive IEEE 802.15.4-based 2.4 GHz XBee-solution has been selected. This link will be used to safely coordinate and synchronize the movements of the two MiR100s. Although the over-the-air data rate of the XBee is limited to 256 kbps, this should be sufficient for this purpose.

The proposed setup of the autonomous hospital beds illustrated also in Figure 1 has been considered in some previous works that we discuss below. In [53], the authors provide an experimental testbed with mobile robots that can receive their position through a centralized camera. The images are processed in a central PC unit, which is able to send the position information to each robot over ZigBee standard. A distributed control algorithm based on event-triggered communications has been designed and implemented to bring the robots into the desired formation, where robots communicate to its neighbors only at event times. In [54], the authors provide a similar testbed setup that is used for localization and tracking using CMUcam3 modules mounted on static WSN nodes. A partially distributed approach was adopted and image segmentation was applied locally at each WSN camera node. The output of each WSN camera node, i.e., the location of the objects segmented on the image

plane, is sent to a central WSN node for sensor fusion using an Extended Information Filter (EIF). To a similar direction, authors in [55] proposed a testbed setup, where the images captured synchronously by the cameras are processed at each node with the objective of extracting the essential information of the object. To cope with the usual low bandwidth of WSN, only this distilled information is sent through the WSN. The measures from all the cameras are integrated using information fusion methods such as maximum likelihood and extended Kalman filters. Finally, in [56], the authors also provide a cooperative control system of multiple robots using infrared cameras and image processing to facilitate the cooperative formation control. The above mentioned works are benchmarked in terms of distance among the mobile robots and their estimated location in a formation control. Due to the heterogeneity of the considered formation controls for each case, we can not compare their results. However, a general outcome is that localization errors could exist depending on demanding formation control and in case of traveling longer distances [57].

3.2. Maritime Application

This use case sees a bathymetry system based on a set of USV in addition to a manned vessel that drives and controls the measurement campaign. The terrestrial radio-systems, including very high frequency (VHF), high frequency (HF) and medium frequency (MF), are well established in the maritime community and are cornerstones of the mandatory global maritime distress and safety system (GMDSS) requirements for Safety of Life at Sea (SOLARS) vessels. Since 1970s, the mobile satellite communication has been used to the maritime community as well. Taking into consideration the cost and signal coverage, the bathymetry platoon uses the VHF radios as the primary communication channel. To ensure the reliability of communication, both the USV and manned vessel are also equipped with the transceiver for communication via the mobile network.

The Maritime Robotics (Maritime Robotics is a leading provider of innovative unmanned solutions for maritime operations in harsh environments: https://maritimerobotics.com/), i.e., autonomous boat platoons provider, has developed a VHF protocol named next generation ham radio (NGHam (https://github.com/skagmo/ngham)) and the corresponding radio system: "Owl VHF".

NGHam specifies both physical (PHY) layer and media access control (MAC) layer functions [58]. The modulation schemes supported by NGHam are 2-GMSK (Gaussian Minimum Shift Keying) and 4-GMSK which result in different data rates of the channel, i.e., 9.6 Kbps and 19.2 Kbps, respectively. Although the available data rate of the VHF channel is low, it is sufficient when transmitting the critical information (e.g., vessel speed, position and course) in a regular periodic manner. However, the packet header does not include any field of packet type/priority. To distinguish the content of the packet, such as vessel voyage information or safety control command, some flag/type needs to be inserted into the payload field of the packet.

NGHam supports both carrier sense multiple access (CSMA) and time division multiple access (TDMA) schemes. Since message transmission between the USV and manned vessel requires the hard delay bound to ensure the safety of the cooperative bathymetry platoon, TDMA is a better option. It guarantees the worst-case end-to-end (E2E) delay through appropriately configuring the relevant parameters, such as TDMA frame length and slot size. TDMA requires synchronization among all users who access the shared channel to avoid interference caused by data transmission in consecutive slots. Synchronization can be realized referring to either some external clocks (e.g., global positioning system (e.g., GPS) or the internal clock of the master user.

3.3. Vehicular Applications

There are two potential solutions to support V2X communications: Dedicated Short Range Communication (DSRC)/Intelligent Transport Systems (ITS)-G5 and cellular network technologies such as 4G/5G. ITS-G5 generally refers to a wireless technology used for automotive and intelligent transportation system applications via short-range exchange of information among onboard units

(OBUs) located inside the vehicles, RSUs placed on the side of the road, or handheld devices carried by pedestrians.

Cellular networks provide an off-the-shelf solution for this type of communications. 4G cellular networks is a scheduled network: transmission rates are granted by network scheduler, collisions are avoided and mutual interference is minimized. Quality-of-Service (QoS) can also be guaranteed (e.g., bit rate or delay) by allocating radio resources. On the other hand, some drawbacks that have been recognized (e.g., increased latency in case of high user density, non-optimized channel for small data, unavailability for out of coverage areas, etc.) are addressed by the Proximity Services (ProSe) feature, being specified within 3GPP [59]. ProSe, similarly to ITS-G5, allows user equipment to discover and communicate with each other directly within communication range, regardless of whether they are in or out of network coverage.The ProSe specifications do not cover the whole V2X requirements (it has been designed with the requirements of public safety and commercial consumer applications in mind). Enhancements are required for high speeds (e.g., in highway scenarios), guaranteed QoS and support for broadcast and unicast communications.

5G will most likely integrate into a heterogeneous network the already available communication technologies like LTE ProSe and IEEE 802.11p and will provide the necessary extensions to enable the future V2X use cases. 5G, as a general objective, will exploit safety, security and privacy support both from the infrastructure and application point of view. From the application point of view, the 5G integrated architecture will allow new business models characterized by services and applications ensemble with an increasing interaction, cooperation and complexity level as well as a great level of flexibility for service tailoring on customer demands. At the infrastructure level, the research aims to satisfy most vertical use case requirements, improving and enhancing the current technologies in an evolutionary scenario, thus solving the foreseen weakness of LTE and ProSe for the vehicular use case.

To support the requirements of different vehicular applications, each vehicle must be aware of the position, status and intention of its surrounding vehicles through message broadcasting. The European Telecommunications Standards Institute (ETSI) defines two types of messages: periodic Cooperative Awareness Messages (CAM) [60], and event-triggered Decentralized Environmental Notification Messages (DENM) [61]. CAMs include information such as geographical location, speed, and acceleration, and are only sent to a close neighborhood, as the validity of the information they contain is very limited in time. A large variety of C-ITS based safety applications are built upon the periodic exchange of CAMs, and their timely and reliable transmission is vital as a vehicle that continuously fails to deliver its beacon becomes invisible to its neighbors, which may result in potentially hazardous situations. Based on American standardization, CAMs are periodically generated, while ETSI recently decided upon a set of kinematic CAM triggering rules that trigger beacons when needed rather than keeping it strictly periodic. On the other hand, DENMs are only generated when an event of common interest occurs, and it is spread within an area of interest for the duration of the event.

An IEEE 802.11p network contains no access points or base stations, and consequently, will not experience coverage problems. This is the main benefit of IEEE 802.11p compared to other WLAN technologies. The supported ad hoc mode reduces delay, as messages do not have to take the detour around the access point or base station. ETSI is responsible for developing the whole protocol stack including vehicle-centric road traffic safety applications, whereas applications orienting towards road traffic efficiency utilizing road infrastructure are under the responsibility of CEN. ETSI has standardized a profile of IEEE 802.11p adapted to the 30 MHz frequency spectrum at the 5.9 GHz band allocated in Europe that today comprises one control channel and two service channels. Non-safety related applications are directed to a 20 MHz band at 5.855–5.875 GHz. The dedicated frequency bands have been divided into 10 MHz frequency channels. Due to the proximity of these bands to the frequency band used for ETC in Europe (5.795–5.805 GHz), ETSI TC ITS must also develop mitigation techniques to avoid to interfere with the ETC systems. There is no cost associated with using this

frequency band (it is license free). However, EN 302 571 standard specifies requirements on output power limits, spectrum masks, etc.

A MAC protocol for a typical vehicular application has to be flexible enough to cope with high mobility and frequent topology changes. Therefore, the IEEE 802.11p MAC is based on a completely decentralized approach: the CSMA/CA random access MAC method used in IEEE 802.11 WLAN. The IEEE 802.11p MAC includes some enhanced features such as prioritized access to the channel by using queues with different arbitration interframe spaces (AIFS). This will ensure that data traffic with higher priority (e.g., video, IP telephony) has a higher probability of channel access compared to low priority traffic (e.g., background, best effort). However, the different QoS classes will not ensure timely channel access and thus, there will still be problems with collisions, especially during high utilization periods.

Regarding the intra-vehicle WSAN-(Wireless Sensor Actuator Network), the IEEE 802.15.4 first published in 2003 targeting low-rate WPANs, is perhaps the most paradigmatic technology supporting WSANs today. The protocol defines the physical and data-link layers and to complement it, several proposals such as the ZigBee, RPL, or 6loWPAN protocols were presented since its first release. More recently, to satisfy the requirements of emerging IoT applications, particularly in the industrial domain, the IEEE 802.15.4e amendment was proposed to complement the legacy IEEE 802.15.4-2011 standard. The IEEE 802.15.4e defines five MAC behaviors, instead of following a more conservative "one-size-fits-all" strategy. Hence, it improves its flexibility in accommodating different kinds of application requirements. In general, these new MAC behaviors are quite different from the ones considered in the legacy IEEE 802.15.4-2011. From the proposed MAC behaviors, the Deterministic Synchronous Multichannel Extension (DSME) is perhaps the closest to the legacy protocol, but nonetheless it brings significant enhancements to the IEEE 802.15.4 beacon-enabled mode by implementing multiple channel frequency hopping and Group Acknowledgments.

4. Safety and Security for SafeCOP Co-CPSs

SafeCOP use cases are representative of real application scenarios where safety and security play the key role. In the following, we analyze the safety and security requirements and solutions that are proposed for the five use cases of SafeCOP.

4.1. Autonomous Hospital Beds

An initial safety analysis of the concept has concluded that the network of external cameras is an enhancement to the basic functionality of the MiR100s, and should not be considered as part of the safety system. The MiR100-to-MiR100 communication, on the other hand, is an integral part of the safety system, and must be certified as safe according to the relevant safety communication standard. Unfortunately, there is currently no relevant safety standard for small, autonomous robots with wireless communication operating in a hospital environment. However, in the railway domain, there are similar challenges in signaling systems and train communication, where wires cannot be used due to the mobility of the application. The safe communication architecture will thus be based on the requirements of EN 50159 [62]. To avoid full safety certification of the communication protocol, it is proposed to use an end-to-end architecture with a safety layer inserted between the "black box" communication system and the safety application. In addition, since wireless communication by definition is an open communication system, which is vulnerable to attacks from actors with malicious intent, information security mechanisms (authentication, cryptography) are a prerequisite for achieving safe communication. The combination of threats random failures and external attacks will lead to one or more of the following basic message errors: repetition, deletion, insertion, resequence, corruption, delay and masquerade. In line with EN 50159, the XBee communication shall be enhanced with a safety layer implementing defenses against these threats. They consist of a protocol with the following parameters and functionalities: sequence number, time stamp, time-out, source and destination identifiers, feedback message, safety code, identification procedure, and cryptographic techniques.

4.2. Autonomous Boat Platoons

The primary scenario defined in this use case deals with one USV that is remotely controlled by a human operator located on another vessel. The wireless link connection between the USV and the manned vessel is maintained active by the continuous transmission of mode command messages from the manned vessel to the USV, to improve the reliability of the communication. If the message is not received within a given time-frame, the USV considers that the communication with the manned vessel is lost. Then, the USV will enter in fail-safe mode (e.g., stop). This mechanism is implemented at application level and independent of the underlying communication protocol.

A crucial safety requirement that the cooperative bathymetry platoon has to fulfill is to guarantee that a safe distance is maintained between the USV and the manned vessel. The acceptable distance between the USV and manned vessel is calculated as the maximum distance that allows messages carrying vessel voyage information be reliably and timely transmitted over the wireless network. Since the signal strength in maritime wireless networks is subject to perturbations due to the sea movement, safety messages are subject to packet loss at communication level. Therefore, sending messages in a periodic manner is applied to compensate packet loss. The vessels speed is typically slower than other transportation systems (e.g., cars, trains, etc.). Thus, missing one message is acceptable if the following one can be received correctly and timely.

Another safety requirement related to communication of safety-critical events emerges e.g., in the avoidance of potential collisions with obstacles such as another vessel, swimmer, or buoy. The manned vessel issues safety-control commands to the USV, which has to respond within a certain time to avoid collisions. To meet this requirement, the messages carrying control commands shall have higher priority than the messages sent out periodically. However, if a message carrying the safety-control command is lost during its transmission, the human operator may still have the chance to re-issue the same command if the message loss can be detected by timeout. It is worth noting that setting up a timeliness of the control command needs to take into account the movement of the USV and the distance to the obstacle. Thus, the timeliness of the control command may be varying from command to command.

Additional safety and security requirements have to be fulfilled to ensure safe USV operations [62,63]:

- *Messages authentication* ensures that the message is received in the same condition as it is sent out with no bits inserted, missing or modified. If the message is modified en route, then the receiver will certainly detect this. Without message authentication, the message, which is either corrupted or modified during transmission, carries the wrong information/command and may lead the USV to an unsafe-state, e.g., colliding with an obstacle.
- *Message timeliness* mechanism effectively limits the age of validly of delivered messages. Thus, if an attack diverts the validated messages for replay much later, the receiver can detect the delay introduced by this attack. Without timeliness constraint, the message which is not modified/corrupted but delayed may lead the USV to an unsafe-state. For example, if the command that the USV shall reduce the speed to avoid a potential collision is delivered to the USV too late, the USV may not have sufficient time to reduce its speed to avoid collision.
- *Message sequence* can be used to detect message loss, repetition and insertion. Without this mechanism, the attacker may intercept messages or insert malicious messages without being detected.

NGHam does not support any of the security mechanisms listed above. Therefore, the corresponding security functions need to be specified and implemented separately.

4.3. Vehicle Control Loss Warning

In the vehicle platooning scenarios, one vehicle may influence the behavior of other vehicles, and, since the consequences of a failure can harm human life, these systems are considered safety-critical

and must be designed according to relevant methodologies to ensure safety, also from a communication perspective. The main goal in vehicle platooning is finding the best trade-off between performance (i.e., maximize speed and minimize vehicles reciprocal distance) and safety (i.e., avoid collision). The largest part of the literature focuses on advanced control schemes, without modeling the communication medium properly. Delay of communication is typically considered as a fixed delay or through probabilistic models. This allows the analytical derivation of string stability models [64] under some hypotheses of the dynamical system, but it may be unreliable under realistic conditions. Two branches are evident from the literature in this respect: the derivation of simple models of the delay bound that guarantees safety (see, e.g., section IV.C of [65]) and brute force simulation with visualization of safety regions under a reduced set of parameters [66,67]. Ongoing research addresses formal verification to extract evidence of safety conditions [68]. Authors in [69] apply machine learning for sensitivity analysis of safety conditions in platooning, under the constraint of no false negative, i.e., avoiding to predict safety (no collision) while collision happens in reality.

Regarding communications, and in particular safety, we identified several concerns. An unexpected interruption of the communication between two nodes can have an extremely negative impact in the safety of the platooning. A proper defense mechanism against erasure must be in place. Furthermore, communication must support response to violations on time (before a deadline), thus delivery time, must be ensured to bound the delay. Finally, these systems must also cope with RF interference without loss of main functionality. Although generic, this requirement aims at guaranteeing that the communication system is resilient to wireless interference on one hand (accidental or not), and can be robust to cope with an eventual attack, such as a DoS attack. We believe that, by relying on the EN 50159 black-channel approach, we will be able to address most of the safety issues for inter-vehicular communication, while escaping the need to certify the whole communication protocol, easing the use of COTS communication stacks. While this approach can mitigate several (if not all) of these safety constraints, there are still others requirements that must be addressed, particularly in what concerns QoS performance, to support the expected behavior of the platoon.

In a vehicular platoon, a lead vehicle that is responsible for managing the platoon's moving directions and velocity, periodically disseminates control commands to following vehicles based on vehicle-to-vehicle communications. Inevitably, pushing vehicles to drive in close formation as the platoon requires low latency driving command transmission from the lead vehicle to the tail. Two critical challenges arise in the inter-vehicle wireless communication. The first challenge is that signal fading induces dynamic wireless channels, which causes command loss at the receiver. This command loss is especially crucial in vehicular platoons since command reception at each vehicle highly depends on the reception of its preceding vehicle. Moreover, command loss at preceding vehicles can impact the command dissemination due to retransmissions, which may lead to accidents due to lack of timely updates. The second challenge is the possibility of assigning the exact transmit rate to each vehicle in the platoon. Although a high transmit rate achieves low transmission latency for each vehicle, increasing the transmit rate results in increasing the receiver's bit error rate (BER) at a given Signal-to-Noise Ratio (SNR). Accordingly, the vehicle with high BER spends longer time on command retransmissions, which prolongs dissemination latency of the platoons. Therefore, allocating the transmit rate without a proper adaptivity leads to command dissemination latency performance degradation. In [70], we proposed a low-latency driving command dissemination (LCD) algorithm to adapt the transmit rate (i.e., modulation) allocation of vehicles as such that the latency of command dissemination in the platoon is minimized under guaranteed BER. We proved that the LCD algorithm achieves computation time complexity of O(NM2), where N and M are the number of vehicles and modulation levels, respectively. The simulation results show that LCD significantly improves the dissemination rate by 50.9% existing algorithms. Moreover, LCD also approximates the lower bound of dissemination latency with the maximum gap of up to 0.2 s.

Regarding security, each node's wireless communications must also be encrypted. Data exchange among nodes must be properly secured to prevent unauthorized access and alteration of the message

content for malicious purposes. Due to broadcast nature of radio channels, disseminating sensory data is vulnerable to eavesdropping, and message modification from an illegitimate eavesdropper. To improve communication security in CPS, using a shared secret key for data encryption/decryption is crucial to support data confidentiality, integrity, and sender authentication. Key generation based on the randomness in a wireless fading channel is a promising approach [71], where two sensor nodes extract secret bits from the inherently random spatial and temporal variations of the reciprocal wireless channel between them. However, while previous works on fading channel based secret key generation mainly focused on improving the secret bit generation rate between a pair of sensor nodes (by exploiting temporal and spatial variations of radio channel, multiple antenna diversity, or multiple frequencies), the problem of unanimity of the generated key for the real-time data dissemination remained a challenge. To address this, we presented in [72] a new data dissemination security protocol that quantizes the estimated received signal strength (RSS) measurements. The quantization intervals are cooperatively adapted to reduce secret bit mismatch rate (BMR). The secret key generated by our protocol is based on channel randomness over multiple hops, the eavesdropper at a different location experiences independent channel fading, which is not able to obtain the same key. In addition, the proposed protocol can be applied to more critical systems, as the secret key is generated in a distributed manner, eliminating a single point of failure.

In addition to inter-vehicular communications, its wireless intra-vehicular counterpart is also being addressed. In-vehicle wireless networks have been recently proposed with the goal of reducing manufacturing and maintenance cost of a large amount of wiring harnesses within vehicles [73,74]. The wiring harnesses used for the transmission of data and power delivery within current vehicles may have up to 4000 parts, weigh as much as 40 kg and contain up to 4 km of wiring. Eliminating these wires would additionally have the potential to improve fuel efficiency, greenhouse gas emission, and spur innovation by providing an open architecture to accommodate new systems and applications. Interestingly, in [75], Volvo group trucks technology presented a practical design of an in-vehicle WSN, using the IEEE 802.15.4 TSCH protocol as the MAC protocol. This work uses a network with only 10 nodes, while vehicles have the potential to use a much higher number of wireless sensors. DSME has better performance as the number of nodes increases and is probably the most flexible MAC behaviour from all the IEEE 802.15.4e proposals. Its multi-superframe structure allows for the transmission of both periodic as well sporadic traffic, while still supporting a fast reconfiguration of the DSME-GTS schedule. Several work has already been done regarding this protocol regarding the evaluation of its performance limits [76], and behavior [9], and some performance improvements are on the way [77].

4.4. Vehicles and Roadside Unit (RSU) Interaction

In this use case, safety and security risks are related to creating links and communication between different actors: service providers, vehicles and roadside units. Roadside unit is hosting the road weather station measurements and sensors, vehicle unit the embedded vehicular sensors and service provider the general service data. In each of the elements, the same security risks remain: identification of counterpart, validating the runtime operation of sensors and services and avoiding malfunctions due to interference with parallel communication. Other safety aspects are related to ensure the complete data exchange procedures in local area vehicular networking, when vehicles are passing each other or roadside unit. IEEE 802.11p operates in dedicated 5.875–5.905 GHz band in Europe. In 3G, the operator is hosting the communication parameters in each link, ensuring the quality of service. Therefore, the communication failures are typically caused by capacity overload. Communication can be disturbed by intentional interference as well, which must be taken into account when aiming to ensure safety and security.

4.5. V2I Cooperation for Traffic Management

Fundamental safety requirements for this use case are as follows:

- *Early detection of communication errors*, i.e., packet loss, packet insertion, packet replication, packet inversion.
- *Bounding to a known upper limit the WSN communication latency to the roadside unit*.
- *Executing image processing for VCA on two different HW components* (i.e., locally on the camera and remotely on the Network Video Recorder).

From the safety standpoint, a thorough hazard and risk analysis has been conducted, employing both ISO 26262 and STAMP [31] methodologies. The former identifies 35 hazard conditions, related to incorrect behaviours from a given subsystem. Since in ISO 26262 all components are considered in isolation, a safe state needs to be defined every time a component cannot guarantee an Automotive Safety Integrity Level at the "Quality Management" rank (i.e., the most safe). For the sake of brevity, we exemplify only the most dangerous condition identified, that of the on-board unit of the vehicle performing a braking action when no danger is actually present. Since this action could actually lead to accidents (ASIL-C), the runtime manager needs to inhibit the transmission of commands from the on-board unit to the control CAN bus. The latter identified 11 system-level risks. While it may appear that ISO 26262 provides a more detailed analysis of risks, it must be taken into account the fact that STAMP risks are system-level by nature, and are therefore relevant when considering the combined effects of multiple subsystems. As an example, the STAMP analysis highlighted as a key hazard the violation of integrity level of the V2I system, and led to the need to include appropriate detection tools (e.g., those developed in [78] at system level to preserve the operational status from external intrusion.

In terms of road safety, the most critical function provided in this use case is the image processing performed at the RSU-C and forwarded at the VCA platform, in order to detect dangerous situations and accidents in the monitored area and alert the LCU/RSU. This unit will apply then a specific countermeasure (GLOSA, ATL-S) over the relevant traffic zone. For this application, the requirements of latency and reliability of the wireless communication channel are of utmost importance, since the warning messages and countermeasures at the traffic lights should reach the destination at the due time. A full analysis of the computational workload is reported in [52]. It is worth noting, however, that such analysis is typically dependent on the specific road intersection scenario, and the resources available for the analysis must therefore be tuned to minimize the risk of exceeding the required latency.

From the security standpoint, authentication and encryption shall be applied to all communications; any non-authenticated and/or non-encrypted transmission cannot be automatically considered trustworthy. A non-authenticated communication may come to the control center from either a traffic light, a car or a WSN node. In the former case, the breach of authenticity is a critical issue, and the Co-CPS should switch to a safe mode. In the latter case, the non-authenticated information may simply be discarded, or be used in the decision process only if it is corroborated by coherent information coming from authenticated entities. Similar considerations apply for breaches of integrity. Regarding breaches of availability, the safety of the system clearly depends on the timeliness of the information. If breaches of availability are detected, the runtime manager should aptly react by moving to safer states. Therefore, we identify three service levels: (1) integrity, authenticity and availability are ensured for any message; (2) integrity, authenticity and availability are ensured for messages exchanged among infrastructure components only; (3) at least one infrastructure component cannot ensure integrity, authenticity and availability. ATL-S and GLOSA can be applied at service levels 1 and 2, but no cooperative activity can take place at level 3. The runtime manager will therefore inhibit transmissions from the control unit when level 3 is reached, returning the system to the safe state (i.e., the non-cooperative system). At level 1, functions beyond the current goals of the V2I scenario (e.g., platooning) could be supported as well.

In the V2I scenario, critical aspects of security are primarily related to ensuring that communications where one endpoint has limited computation capabilities, and is possibly exposed to attackers, are suitably protected while remaining within the resource and time budget. To this end, the WSN security mechanisms used for V2I cooperation in this use case employ a hybrid cryptography

scheme (TAKS) derived as extensions of the contributions in [7,8,79]. Furthermore, the trade-off between security and latency can be tuned by employing tools such as [80], which allow for selecting appropriate countermeasures to side-channel attacks.

5. 5G Open Challenges

In this section, the open challenges raised from the architectures of the SafeCOP use cases presented above are discussed in relation to 5G use cases. The reason to choose 5G to discuss about the technical challenges is the fact that 5G system can accommodate (from wireless communications standpoint) most of the SafeCOP use cases as identified from above discussion. Notably, 5G promises to facilitate new vertical industries through network slicing and network softwarization [81]. Our study below proves that 5G communications can facilitate most of the innovative CPS related use cases of SafeCop project. Safecop had as a major objective to provide cooperative safe CPS using wireless communications technologies and 5G could be considered the most promising candidate solution.

Work on 5G is currently in progress to meet the 2020 objectives of a ready-to-use technology. The European Union promoted the METIS project in 2012 [82,83], followed by the 5GPPP program [84], as well as other significant projects like e.g., CROWD [85]. The NGMN Alliance, which was founded by major mobile operators in 2006, provided an important contribution to 5G by publishing the NGMN 5G White Paper in March 2015 [86].

As the future cellular network's evolution, the 5G ecosystem is a multi-provider/multi-tenant environment. It is designed as a heterogeneous network supporting business and applications services [87]. It is structured in a set of layers divided into two basic groups:

1. *The higher service-centric layers* modeling the business implementations driven by the vertical use cases.
2. *The lower network-centric layers* representing the physical implementation and its abstraction based on software network technologies like software defined networking (SDN) and Network Function Virtualization (NFV).

The 5G protocol stack is based on IPv6, as defined in [88–90]. Network flexibility is obtained by the establishment of slices, configured for the purposes of specific application scenarios. Slicing allows the creation of multiple virtual networks on top of a shared physical infrastructure. They allow specific operators to offer ITS related services, ensuring the right prioritisation of communication channels (e.g., road monitoring for safety over other INTERNET traffic). Additional issues are network coverage and densification, where the latter consists in adding more cell sites to increase the available network capacity. Device-to-Device communications and the concept of virtual cells contribute to addressing both issues.

As 5G is designed according to specialized application requirements, its applicability to the SafeCOP use cases should be accurately discussed.

For the maritime use case, the radio high frequency transmission could suffer from hard degradation and interferences due to water surface and possible adverse weather conditions, challenging the use of 5G technology. Satellite communication is still possible, but latency and response time are generally not acceptable except for critical situations as a backup solution.

In case of a healthcare use case, the currently foreseen protocols like 802.15.4 and 802.11 are very suitable for indoor and intra-robot communications. 5G can be considered exploiting the "femtocell" indoor solution and integrating the system to a wider infrastructure for possible future expansion or effective service distribution.

The set of automotive use cases will take a great advantage by 5G evolution, since the research and improvement area of 5G aim to solve the limitations of current mobile and Ethernet-based technologies (i.e., LTE Proximity Service and 802.11p) [61,91–94].

Table 1 summarizes the 4G and 5G technology challenges related to SafeCOP use cases. We then outline how 5G standards may meet SafeCOP requirements and the open challenges ahead.

Table 1. 4G and 5G technology challenges in SafeCOP.

Use Case	4G	5G
Heathcare	Energy efficiency issue on radio interfaces	Femtocell solution for indoor comms Support scalability
Maritime	Radio signal degradation	Satellite transmission but latency concerns
Vehicle control loss warning	ProSe to be upgraded	natively supported
Vehicles and roadside units interaction	ProSe to be upgraded	natively supported
V2I cooperation for traffic management	latency concerns	natively supported

5.1. Autonomous Hospital Beds

With the idea of connecting different types of clinical devices to its network, 5G technology provides a pervasive environment in hospitals well beyond the one envisaged by this use case, specifically related to the automated management of hospital beds. In the health care sector, robots can be used to transport specimens, drugs, and bedlinen to wards, labs, pharmacies, and depositories, offloading repetitive low level tasks from skilled hospital staff as envisioned in [95]. Such a use case can be realized through the mission critical X (MCX) 3GPP services, like data and video introduced in [96,97]. The MCX 3GPP services apply to both aerial or terrestrial unmanned vehicles, including drones and robots. The Autonomous Hospital Beds use case focuses on robots that can be assimilated to terrestrial unmanned vehicles embedding 5G chipsets with MCX (MCData/MCVideo) air interface enabled. More ideas about robotics applications in healthcare within the 5G ecosystem can be found in [98], where robots are considered stand-alone configuration instead of a non-standalone new radio (i.e., 5G) application. To enable hospital bed use case in [96], the MCX 3GPP specifications integrates the following requirements:

1. MCData Service shall enable the control of robots;
2. MCData Service shall provide a common transmission framework to use and control robots;
3. MCData Service shall provide a default control latency depending on the robots type under (400 ms for a terrestrial unmanned vehicle).

The split between network latency and robot latency is left open for future research. Similar requirements can be found in [97] for video transmission, where MCVideo is coordinated with the MCData to give the most suitable priority to the control of the robots. It is evident that such design requirements can be used also to hospital beds, which can be equipped with both data/video transmission capabilities by implementing the MCX 5G interface. Since the 5G MCX interface is out of the scope of this paper, we refer the interested reader to the 3GPP web page in [99].

5.2. Autonomous Boat Platoons

Finding the right position for this use case in 3GPP standardization is not straightforward. In principle, we can make the assumption that autonomous shipping are enabled by a joint initiative of satellite operators and space agencies, where 5G satellite-related technology drive the autonomous shipping vision [100]. Enabling network availability to moving platforms such as passenger vehicles, aircraft ships, trains, buses, etc., is a requirement for the new radio interface for non-terrestrial networks (NTN) [101]. In [102], the authors discuss a sort of ship-mega constellation, which is similar to boat platooning, based on multi-hop communications enabled by both 5G and satellite communications. A clear vision towards autonomous shipping is presented in [100], based on satellite communications,

linked to the joint industry project called Advanced Autonomous Waterborne Applications (AAWA) led by Rolls Royce. Unfortunately, 5G is not included.

5.3. Vehicular Applications

5.3.1. Vehicle Control Loss Warning

In [103], the control loss warning is considered as a use case, where it enables a host vehicle to broadcast a self-generated control loss event to surrounding Remote Vehicles (RV). Upon receiving such event information, an RV determines the relevance of the event and provides a warning to the driver.

5.3.2. Vehicles and Roadside Unit (RSU) Interaction

A few V2X use cases towards 5G were initially introduced in [103,104] followed with details about enhanced V2X 5G services. In particular, requirements for use cases that rely on vehicles and roadside unit interaction such as platooning and advanced driving is provided in [104]. The following summary of requirements related to vehicles-RSU interaction is included:

- Between User Equipment (UE) supporting V2X application and RSU via another UE supporting V2X application with conditionally and fully automated driving, where the payload message could vary from 50–1200 bytes and latency to 20–50 ms.
- Between RSU and UE supporting V2X application with again partially or fully automated driving, where the payload message is lower around 100 bytes and latency to 10–50 ms.

A technology that could be useful for future 5G for most of the V2X services is network slicing [105]. The RSU can be also employed in Mobile Edge Computing (MEC), as a host of e.g., MEC server [106]. However, details are lacking in case of vehicles to RSU interaction and only high-level ideas are proposed towards the use cases reported in [104].

5.3.3. V2I Cooperation for Traffic Management

A mixed-use traffic management use case is proposed in [103], which includes various transportation modes (e.g., automobile, train, bicycle, and pedestrian), several traffic densities, and different environmental conditions. It is shown that a V2X system would need the flexibility to adapt to changing attributes such as vehicular traffic density, rates of speed, angles of approach, and weather conditions which all may impact the optimal range and transmission rate in a specific situation. However, the description of such a mixed-use case is not sufficiently detailed in [103,104]. Looking into the related research works, we have identified one recent contribution on traffic management [107]. It deals with urban traffic management to mitigate traffic congestion. A new architecture is defined, based on different layers, such as: environmental sensing, communication, mobile edge computing and remote core cloud server. 5G SDN and mobile edge computing are considered key enabling technologies. SDN offers high-bandwidth communication service with flexibility and programmability, thus providing agility to sensing operations. Other technologies are also listed for future research such as vehicle localization, data pre-fetching strategy, traffic prediction and traffic lights control.

6. Conclusions

This survey provides an overview of the technology requirements for future Co-CPS in terms of wireless communication and safety as analyzed within the framework of SafeCOP European project. We focused on highlighting the main wireless communication technologies currently available and evaluated their compliance to the safety requirements of Co-CPSs in terms of dependability, security and timeliness. The survey states the general recommendations deciding about the use of wireless communication technologies in Co-CPSs and illustrates them through real-world use

cases. Furthermore, the suitability of 5G technology to the SafeCOP use cases has been evaluated and discussed. Although its applicability is not straightforward, 5G technology offers clear benefits in several aspects but is challenging for some others. Through the presented analysis, the SafeCOP project is developing a reliable approach to safety assurance in cooperating cyber-physical systems. This approach is expected to represent a reference architecture able to fulfill the safety and security requirements proper for Co-CPSs as they have been individuated by the thorough analysis presented in this article.

Author Contributions: All authors contributed in writing the paper. A.B., D.C., R.S., A.K. and F.F. reviewed and finalized the paper.

Funding: This work was partially supported by the Knowledge Foundation (KKS) via the ELECTRA project, the SafeCOP project which is funded from the ECSEL Joint Undertaking under Grant No. 692529 and from National funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chaâri, R.; Ellouze, F.; Koubâa, A.; Qureshi, B.; Pereira, N.; Youssef, H.; Tovar, E. Cyber-physical systems clouds: A survey. *Comput. Netw.* **2016**, *108*, 260–278, doi:10.1016/j.comnet.2016.08.017.
2. Lin, J.; Yu, W.; Zhang, N.; Yang, X.; Zhang, H.; Zhao, W. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet Things J.* **2017**, *4*, 1125–1142, doi:10.1109/JIOT.2017.2683200.
3. Lu, Y. Industry 4.0: A survey on technologies, applications and open research issues. *J. Ind. Inf. Integr.* **2017**, *6*, 1–10, doi:10.1016/j.jii.2017.04.005.
4. Karoui, O.; Khalgui, M.; Koubâa, A.; Guerfala, E.; Li, Z.; Tovar, E. Dual mode for vehicular platoon safety: Simulation and formal verification. *Inf. Sci.* **2017**, *402*, 216–232, doi:10.1016/j.ins.2017.03.016.
5. Li, Z.; Karoui, O.; Koubaa, A.; Khalgui, M.; Guerfala, E.; Tovar, E.; Wu, N. System and Method for Operating a Follower Vehicle in a Vehicle Platoon. U.S. Patent US20170329348A1, 2017.
6. Balador, A.; Bohm, A.; Uhlemann, E.; Calafate, C.T.; Cano, J.C. A Reliable Token-Based MAC Protocol for Delay Sensitive Platooning Applications. In Proceedings of the 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), Boston, MA, USA, 6–9 September 2015; pp. 1–5, doi:10.1109/VTCFall.2015.7390813.
7. Pomante, L.; Marchesani, S.; Pugliese, M.; Santucci, F. A Middleware Approach to Provide Security in IEEE 802.15.4 Wireless Sensor Networks. In Proceedings of the Mobilware, Bologna, Italy, 11–13 November 2013.
8. Pomante, L.; Pugliese, M.; Tiberti, W.; Bozzi, L.; Santic, M.; Santucci, F.; Giuseppe, L.D. TinyWIDS: A WPM-based Intrusion Detection System for TinyOS2.x/802.15.4 Wireless Sensor Networks. In Proceedings of the HiPEAC Conference CS2 2018, Manchester, UK, 24 January 2018.
9. Kurunathan, H.; Severino, R.; Koubâa, A.; Tovar, E. IEEE 802.15.4e in a Nutshell: Survey and Performance Evaluation. *IEEE Commun. Surv. Tutor.* **2018**, *PP*, 1, doi:10.1109/COMST.2018.2800898.
10. SafeCOP Project's Website. Available online: http://www.safecop.eu/ (accessed on 14 November 2018).
11. Shi, J.; Wan, J.; Yan, H.; Suo, H. A survey of Cyber-Physical Systems. In Proceedings of the 2011 International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, China, 9–11 November 2011; pp. 1–6, doi:10.1109/WCSP.2011.6096958.
12. McKee, D.W. Survey of advances and challenges in intelligent autonomy for distributed cyber-physical systems. *CAAI Trans. Intell. Technol.* **2018**, *3*, 75–82.
13. Qutqut, M. A Survey of IoT Open Source Operating Systems. *IET Wirel. Sens. Syst.* **2018**, doi:10.1049/iet-wss.2018.5033.
14. Dey, N.; Ashour, A.S.; Shi, F.; Fong, S.J.; Tavares, J.M.R.S. Medical cyber-physical systems: A survey. *J. Med. Syst.* **2018**, *42*, 74, doi:10.1007/s10916-018-0921-x.
15. Abbaspour Asadollah, S.; Inam, R.; Hansson, H. A Survey on Testing for Cyber Physical System. In *Testing Software and Systems*; El-Fakih, K., Barlas, G., Yevtushenko, N., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 194–207.

16. Xu, L.D.; Duan, L. Big data for cyber physical systems in industry 4.0: A survey. *Enterp. Inf. Syst.* **2018**, 1–22, doi:10.1080/17517575.2018.1442934.
17. Gürdür, D.; Asplund, F. A systematic review to merge discourses: Interoperability, integration and cyber-physical systems. *J. Ind. Inf. Integr.* **2018**, *9*, 14–23, doi:10.1016/j.jii.2017.12.001.
18. Bartocci, E.; Deshmukh, J.; Donzé, A.; Fainekos, G.; Maler, O.; Ničković, D.; Sankaranarayanan, S. Specification-Based Monitoring of Cyber-Physical Systems: A Survey on Theory, Tools and Applications. In *Lectures on Runtime Verification: Introductory and Advanced Topics*; Bartocci, E., Falcone, Y., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 135–175, doi:10.1007/978-3-319-75632-5_5.
19. Giraldo, J.; Urbina, D.; Cardenas, A.; Valente, J.; Faisal, M.; Ruths, J.; Tippenhauer, N.O.; Sandberg, H.; Candell, R. A Survey of Physics-Based Attack Detection in Cyber-Physical Systems. *ACM Comput. Surv.* **2018**, *51*, 76:1–76:36, doi:10.1145/3203245.
20. Bou-Harb, E. A Brief Survey of Security Approaches for Cyber-Physical Systems. In Proceedings of the 2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Larnaca, Cyprus, 21–23 November 2016; pp. 1–5, doi:10.1109/NTMS.2016.7792424.
21. Shi, L.; Dai, Q.; Ni, Y. Cyber–physical interactions in power systems: A review of models, methods, and applications. *Electr. Power Syst. Res.* **2018**, *163*, 396–412, doi:10.1016/j.epsr.2018.07.015.
22. Schmidt, M.; Åhlund, C. Smart buildings as Cyber-Physical Systems: Data-driven predictive control strategies for energy efficiency. *Renew. Sustain. Energy Rev.* **2018**, *90*, 742–756, doi:10.1016/j.rser.2018.04.013.
23. Moness, M.; Moustafa, A.M. A Survey of Cyber-Physical Advances and Challenges of Wind Energy Conversion Systems: Prospects for Internet of Energy. *IEEE Internet Things J.* **2016**, *3*, 134–145, doi:10.1109/JIOT.2015.2478381.
24. Bolbot, V.; Theotokatos, G.; Bujorianu, M.L.; Boulougouris, E.; Vassalos, D. Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review. *Reliab. Eng. Syst. Saf.* **2018**, doi:10.1016/j.ress.2018.09.004.
25. Wolf, M.; Serpanos, D. Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems. *Proc. IEEE* **2018**, *106*, 9–20, doi:10.1109/JPROC.2017.2781198.
26. Rajkumar, R.; Lee, I.; Sha, L.; Stankovic, J. Cyber-physical systems: The next computing revolution. In Proceedings of the Design Automation Conference, Anaheim, CA, USA, 13–18 June 2010; pp. 731–736, doi:10.1145/1837274.1837461.
27. MÃŒller, H.A. The Rise of Intelligent Cyber-Physical Systems. *Computer* **2017**, *50*, 7–9, doi:10.1109/MC.2017.4451221.
28. Avizienis, A.; Laprie, J.; Randell, B.; Landwehr, C. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Trans. Dependable Secure Comput.* **2004**, *1*, 11–33.
29. *Risk Management—Guidelines*; ISO 31000:2018; Technical Report; ISO: Geneva, Switzerland, 2018.
30. *Principles for Barrier Management in the Petroleum Industry*; Technical Report; Petroleum Safety Authority Norway: Stavanger, Norway, 2013.
31. Leveson, N. A new accident model for engineering safer systems. *Saf. Sci.* **2004**, *42*, 237–270, doi:10.1016/S0925-7535(03)00047-X.
32. United States Department of Defense. *Procedures for Performing a Failure Mode, Effects and Criticality Analysis 1949;* MIL-P-1629A; Technical Report; United States Department of Defense: Arlington, VA, USA, 1980.
33. Rausand, M.A.H. *System Reliability Theory: Models, Statistical Methods, and Applications*; John Wiley and Sons: Hoboken, NJ, USA, 2004.
34. International Electrotechnical Commission. *Functional Safety of Electrical/ Electronic/Programmable Electronic Safety Related Systems—Part 3: Software Requirements, 65A/550/FDIS, IEC*; Technical Report IEC 61508; International Electrotechnical Commission: Geneva, Switzerland, 2009.
35. *The CIS Security Metrics*; Technical Report; The Center for Internet Security (CIS): East Greenbush, NY, USA, 2010.
36. Kert, M.J.; Lopez, E.B. *State-of-the-Art of Secure ICT Landscape*; Technical Report; Network Information Security (NIS) Platform WG3; 2014. Available online: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwj27v-GveTeAhUBzLwKHVhGB80QFjAAegQICRAC&url=https%3A%2F%2Fresilience.enisa.europa.eu%2Fnis-platform%2Fshared-documents%2Fwg3-documents%2Fstate-of-the-art-of-the-secure-ict-landscape%2Fat_download%2Ffile&usg=AOvVaw1_wGpwogadXeAgSaBYnClw (accessed on 20 November 2018).

37. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proc. IEEE* **2016**, *104*, 1727–1765, doi:10.1109/JPROC.2016.2558521.
38. Horn, G.P.S. Towards 5G Security, Nokia Networks. In Proceedings of the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communication, Helsinki, Finland, 20–22 August 2015.
39. Huawei. *5G Security: Forward Thinking, Huawei White Paper*; Huawei: Shenzhen, China, 2015.
40. Ericsson. *5G Security, Ericsson White Paper*; Ericsson: Stockholm, Sweden, 2015.
41. An Annual Review of Trends and Developments in Shipping Losses and Safety. Allianz Global Corporate & Specialty, 2018. Available online: http://www.agcs.allianz.com (accessed on 14 November 2018).
42. Rodseth, O.J.; Burmeister, H.C. Developments toward the Unmanned Ship. Available online: www.unmanned-ship.org/munin/wp-content/uploads/2012/08/R%C3%B8dseth-Burmeister-2012-Developments-toward-the-unmanned-ship.pdf (accessed on 21 November 2018).
43. Katsikas, S.K. Cyber Security of the Autonomous Ship. In Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, Abu Dhabi, UAE, 2 April 2017; pp. 55–56, doi:10.1145/3055186.3055191.
44. Suhari, K.T.; Karim, H.; Gunawan, P.H.; Purwanto, H. Small Rov Marine Boat for Bathymetry Surveys of Shallow Waters—Potential Implementation in Malaysia. *ISPRS Int. Arch. Photogramm. Remote Sens. Spat. Inf. Sci.* **2017**, *XLII-4/W5*, 201–208, doi:10.5194/isprs-archives-XLII-4-W5-201-2017.
45. Giordano, F.; Mattei, G.; Parente, C.; Peluso, F.; Santamaria, R. Integrating Sensors into a Marine Drone for Bathymetric 3D Surveys in Shallow Waters. *Sensors* **2016**, *16*, 41, doi:10.3390/s16010041.
46. Blincoe, L.; Miller, T.R.; Zaloshnja, E.; Lawrence, B. *The Economic and Societal Impact of Motor Vehicle Crashes, 2010 (Revised)*; Technical Report; U.S. National Highway Traffic Safety Administration (NHTSA): Washington, DC, USA, 2015.
47. Schrank, D.; Eisele, B.; Lomax, T.; Bak, J. *Urban Mobility Scorecard*; Technical Report; Texas A&M Transportation Institute: College Station, TX, USA, 2015.
48. Harding, J.; Powell, G.R.; Yoon, R.; Fikentscher, J.; Doyle, C.; Sade, D.; Lukuc, M.; Simons, J.; Wang, J. *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*; Technical Report, DOT HS 812 014; U.S. National Highway Traffic Safety Administration (NHTSA): Washington, DC, USA, 2014.
49. Sukuvaara, T. ITS-Enabled advanced road weather services and infrastructures for vehicle winter testing, professional traffic fleets and future automated driving. In Proceedings of the 2018 ITS World Congress, Copenhagen, Denmark, 17–21 September 2018.
50. Sukuvaara, T.; Ylitalo, R.; Katz, M. IEEE 802.11p Based Vehicular Networking Operational Pilot Field Measurement. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 409–417, doi:10.1109/JSAC.2013.SUP.0513037.
51. Agosta, G.; Barenghi, A.; Brandolese, C.; Fornaciari, W.; Pelosi, G.; Delucchi, S.; Massa, M.; Mongelli, M.; Ferrari, E.; Napoletani, L.; et al. V2I Cooperation for Traffic Management with SafeCop. In Proceedings of the 2016 Euromicro Conference on Digital System Design (DSD), Limassol, Cyprus, 31 August–2 September 2016; pp. 621–627, doi:10.1109/DSD.2016.18.
52. Agneessens, A.; Buemi, F.; Delucchi, S.; Massa, M.; Agosta, G.; Barenghi, A.; Brandolese, C.; Fornaciari, W.; Pelosi, G.; Ferrari, E.; et al. Safe cooperative CPS: A V2I traffic management scenario in the SafeCOP project. In Proceedings of the 2016 International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation (SAMOS), Samos, Greece, 15–19 July 2016; pp. 320–327, doi:10.1109/SAMOS.2016.7818365.
53. Guinaldo, M.; Fábregas, E.; Farias, G.; Dormido-Canto, S.; Chaos, D.; Sánchez, J.; Dormido, S. A Mobile Robots Experimental Environment with Event-Based Wireless Communication. *Sensors* **2013**, *13*, 9396–9413, doi:10.3390/s130709396.
54. Jiménez-González, A.; Martínez-de Dios, J.R.; Ollero, A. An Integrated Testbed for Cooperative Perception with Heterogeneous Mobile and Static Sensors. *Sensors* **2011**, *11*, 11516–11543, doi:10.3390/s111211516.
55. Sanchez-Matamoros, J.M.; de Dios, J.R.M.; Ollero, A. Cooperative localization and tracking with a camera-based WSN. In Proceedings of the 2009 IEEE International Conference on Mechatronics, Malaga, Spain, 14-17 April 2009; pp. 1–6, doi:10.1109/ICMECH.2009.4957244.
56. Jiang, Z.; Chen, S. Cooperative control system of multiple robots using visual location. In Proceedings of the 2017 Eighth International Conference on Intelligent Control and Information Processing (ICICIP), Hangzhou, China, 3–5 November 2017; pp. 168–172, doi:10.1109/ICICIP.2017.8113936.
57. Suh, J.; You, S.; Choi, S.; Oh, S. Vision-Based Coordinated Localization for Mobile Sensor Networks. *IEEE Trans. Autom. Sci. Eng.* **2016**, *13*, 611–620, doi:10.1109/TASE.2014.2362933.

58. Løfaldli, A.; Birkeland, R. Implementation of a Software Defined Radio Prototype Ground Station for CubeSats. In Proceedings of the ESA Small Satellites Systems and Services Symposium, Valletta, Malta, 30 May–3 June 2016; doi:10.13140/RG.2.1.1806.0408.
59. 3GPP. *X*; Technical Report. 2016. Available online: www.3gpp.org (accessed on 14 November 2018).
60. ETSI EN 302 637-2 V1.3.2. *Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service*; Technical Report; ETSI: Sophia Antipolis, France, 2014; Available online: www.etsi.org (accessed on 14 November 2018).
61. ETSI ES 302 637. *Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service*; Technical Report; ETSI: Sophia Antipolis, France, 2014; Available online: www.etsi.org (accessed on 14 November 2018).
62. EN 50159. *Railway Applications. Communication, Signaling and Processing Systems. Safety-Related Communication in Transmission Systems*; Technical Report; BSI: London, UK, 2010.
63. IEC 61784-3. *Industrial Communication Networks—Functional Safety Fieldbuses*; Technical Report; IEC: Geneva, Switzerland, 2016.
64. Oncu, S.; van de Wouw, N.; Nijmeijer, H. Cooperative adaptive cruise control: Tradeoffs between control and network specifications. In Proceedings of the 2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC), Washington, DC, USA, 5–7 October 2011; pp. 2051–2056, doi:10.1109/ITSC.2011.6082894.
65. Xu, L.; Wang, L.Y.; Yin, G.; Zhang, H. Communication Information Structures and Contents for Enhanced Safety of Highway Vehicle Platoons. *IEEE Trans. Veh. Technol.* **2014**, *63*, 4206–4220, doi:10.1109/TVT.2014.2311384.
66. Ge, J.; Orosz, G. Dynamics of connected vehicle systems with delayed acceleration feedback. *Transp. Res. Part C Emerg. Technol.* **2014**, *46*, 46–64, cited By 90, doi:10.1016/j.trc.2014.04.014.
67. Santini, S.; Salvi, A.; Valente, A.S.; PescapÃ, A.; Segata, M.; Cigno, R.L. A Consensus-Based Approach for Platooning with Intervehicular Communications and Its Validation in Realistic Scenarios. *IEEE Trans. Veh. Technol.* **2017**, *66*, 1985–1999, doi:10.1109/TVT.2016.2585018.
68. Meinke, K. Learning-Based Testing of Cyber-Physical Systems-of-Systems: A Platooning Study. *Computer Performance Engineering*; Reinecke, P., Di Marco, A., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 135–151.
69. Mongelli, M.; Ferrari, E.M.M.F.A. Performance validation of vehicle platooning via intelligible analytics. *IET Cyber-Phys. Syst. Theory Appl.* **2018**, doi:10.1049/iet-cps.2018.5055.
70. Li, K.; Ni, W.; Tovar, E.; Guizani, M. LCD: Low Latency Command Dissemination for a Platoon of Vehicles. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6, doi:10.1109/ICC.2018.8422933.
71. Trihinas, D.; Pallis, G.; Dikaiakos, M.D. ADMin: Adaptive monitoring dissemination for the Internet of Things. In Proceedings of the IEEE INFOCOM 2017- IEEE Conference on Computer Communications, Atlanta, GA, USA, 1–4 May 2017; pp. 1–9, doi:10.1109/INFOCOM.2017.8057144.
72. Li, K.; Kurunathan, H.; Severino, R.; Tovar, E. Cooperative Key Generation for Data Dissemination in Cyber-physical Systems. In Proceedings of the 9th ACM/IEEE International Conference on Cyber-Physical Systems, Porto, Portugal, 11–13 April 2018; pp. 331–332, doi:10.1109/ICCPS.2018.00039.
73. Sadi, Y.; Ergen, S.C. Optimal Power Control, Rate Adaptation, and Scheduling for UWB-Based Intravehicular Wireless Sensor Networks. *IEEE Trans. Veh. Technol.* **2013**, *62*, 219–234, doi:10.1109/TVT.2012.2217994.
74. Demir, U.; Ergen, S.C. ARIMA-based time variation model for beneath the chassis UWB channel. *EURASIP J. Wirel. Commun. Netw.* **2016**, *2016*, 178, doi:10.1186/s13638-016-0676-3.
75. Parthasarathy, D.; Whiton, R.; Hagerskans, J.; Gustafsson, T. An in-vehicle wireless sensor network for heavy vehicles. In Proceedings of the 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), Berlin, Germany, 6–9 September 2016; pp. 1–8, doi:10.1109/ETFA.2016.7733554.
76. Kurunathan, H.; Severino, R.; Koubâa, A.; Tovar, E. Worst-Case Bound Analysis for the Time-Critical MAC behaviors of IEEE 802.15. 4e. In Proceedings of the 13th IEEE International Workshop on Factory Communication Systems Communication in Automation (WFCS 2017), Limassol, Cyprus, 31 May–2 June 2017.

77. Kurunathan, H.; Severino, R.; Koubâa, A.; Tovar, E. An Efficient Approach to Multisuperframe Tuning for DSME Networks: Poster Abstract. In Proceedings of the 17th ACM/IEEE International Conference on Information Processing in Sensor Networks, Porto, Portugal, 11–13 April 2018; IEEE Press: Piscataway, NJ, USA, 2018; pp. 162–163, doi:10.1109/IPSN.2018.00044.
78. Mongelli, M.; Aiello, M.; Cambiaso, E.; Papaleo, G. Detection of DoS attacks through Fourier transform and mutual information. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 7204–7209.
79. Pomante, L.; Pugliese, M.; Marchesani, S.; Santucci, F. Definition and Development of a Topology-based Cryptographic Scheme for Wireless Sensor Networks. In *Sensor Systems and Software*; Springer: Cham, Switzerland, 2013.
80. Agosta, G.; Barenghi, A.; Maggi, M.; Pelosi, G. Design space extension for secure implementation of block ciphers. *IET Comput. Dig. Tech.* **2014**, *8*, 256–263, doi:10.1049/iet-cdt.2014.0037.
81. Kaloxylos, A. A Survey and an Analysis of Network Slicing in 5G Networks. *IEEE Commun. Stand. Mag.* **2018**, *2*, 60–65, doi:10.1109/MCOMSTD.2018.1700072.
82. Project, T.M. 2012. Available online: https://www.metis2020.com (accessed on 14 November 2018).
83. Consortium, M. *Scenarios, Requirements and KPIs for 5G Mobile and Wireless System*; ICT-317669 METIS; 2013.
84. 5G Infrastructure Public Private Partnership; 5GPPP; 2013. Available online: https://5g-ppp.eu/ (accessed on 14 November 2018).
85. ICT318115-CROWD. Connectivity Management for eneRgy Optimised Wireless Dense Networks. 2013. Available online: http://www.ict-crowd.eu/ (accessed on 14 November 2018).
86. NGMN 5G Initiative. *NGMN 5G White Paper*; NGMN Alliance: Frankfurt am Main, Germany, 2015.
87. *View on 5G Architecture*; 5GPPP; Technical Report; Available online: https://5g-ppp.eu/ (accessed on 14 November 2018).
88. *Detailed Specifications of the Terrestrial Radio Interfaces of International Mobile Telecommunications-Advanced*; ITU-R M.2012; Technical Report M.2012, ITU-R; 2015. Available online: www.itu.int (accessed on 14 November 2018).
89. *Access Layer Specification for Intelligent Transport Systems Operating in the 5 GHz Frequency Band*; ETSI ES 302 663; Technical Report; ETSI: Sophia Antipolis, France, 2012; Available online: www.etsi.org (accessed on 14 November 2018).
90. *European Profile Standard for the Physical and Medium Access Control Layer of Intelligent Transport Systems Operating in the 5 GHz Frequency Band*; ETSI ES 202 663; Technical Report; ETSI: Sophia Antipolis, France, 2009; Available online: www.etsi.org (accessed on 14 November 2018).
91. *5G Automotive Vision*; 5GPPP; Technical Report, 5GPPP; 2015. Available online: https://5g-ppp.eu/ (accessed on 14 November 2018).
92. *Vehicular Communications; GeoNetworking; Part 4: Geographical Addressing and Forwarding for Point-to-Point and Point-to-Multipoint Communications; Sub-Part 1: Media-Independent Functionality*; ETSI ES 302 636; Technical Report; ETSI: Sophia Antipolis, France, 2013; Available online: www.etsi.org (accessed on 14 November 2018).
93. ETSI ES 302 800. *Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM)*; Technical Report; ETSI: Sophia Antipolis, France, 2014; Available online: www.etsi.org (accessed on 14 November 2018).
94. ETSI ES 102 637. *Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements*; Technical Report; ETSI: Sophia Antipolis, France, 2009; Available online: www.etsi.org (accessed on 14 November 2018).
95. Puleri, M.; Sabella, R.; Osseiran, A. *Cloud Robotics: 5G Paves the Way for Mass-Market Automation*; Technical Report, Ericsson Technology Review. 2016. Available online: https://www.ericsson.com/en (accessed on 14 November 2018).
96. *3GPP TS 22.281. Mission Critical Video Services over LTE*; Technical Report; Rel. 14, v.14.3.0; 3GPP: Sophia Antipolis, France, 2017.
97. *3GPP TS 22.282. Mission Critical Video Services over LTE*; Technical Report; Rel. 14, v.14.3.0; 3GPP: Sophia Antipolis, France, 2017.

98. Soldani, D.; Fadini, F.; Rasanen, H.; Duran, J.; Niemela, T.; Chandramouli, D.; Hoglund, T.; Doppler, K.; Himanen, T.; Laiho, J.; et al. 5G Mobile Systems for Healthcare. In Proceedings of the IEEE VTC Spring, Sydney, NSW, Australia, 4–7 June 2017.
99. Mission Critical Services in 3GPP. Available online: http://www.3gpp.org/news-events/3gpp-news/1875-mc_services (accessed on 14 November 2018).
100. Levander, O. Autonomous ships on the high seas. *IEEE Spectr.* **2017**, *54*, 26–31.
101. *TR38.811. Study on New Radio (NR) to Support non Terrestrial Networks*; Technical Report; Rel. 15, v0.2.1; 3GPP: Sophia Antipolis, France, 2017.
102. Höyhtyä, M.; Huusko, J.; Kiviranta, M.; Solberg, K.; Rokka, J. Connectivity for autonomous ships: Architecture, use cases, and research challenges. In Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, 18–20 October 2017; pp. 345–350, doi:10.1109/ICTC.2017.8191000.
103. *TR22.885. Study on LTE Support for Vehicle to Everything (V2X) Services*; Technical Report; v14.0; 3GPP: Sophia Antipolis, France, 2015.
104. *TR 22.886. Study on Enhancement of 3GPP Support for 5G V2X Services*; Technical Report; v15.1.0; 3GPP: Sophia Antipolis, France, 2017.
105. Campolo, C.; Molinaro, A.; Iera, A.; Meninchella, F. 5G Network Slicing for vehicle-to-everything service. *IEEE Wirel. Commun.* **2017**, *24*, 38–45.
106. Shah, S.A.A.; Ahmed, E.; Imran, M.; Zeadally, S. 5G for Vehicular Communications. *IEEE Commun. Mag.* **2018**, *56*, 111–117, doi:10.1109/MCOM.2018.1700467.
107. Liu, J.; Wan, J.; Jia, D.B.Z.; Li, D.; Hsu, C.H.; Chen, H. High-Efficiency Urban Traffic Management in Context-Aware Computing and 5G Communication. *IEEE Commun. Mag.* **2017**, *55*, 34–40.

© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).