IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 1, 2021, accepted January 25, 2022, date of publication January 27, 2022, date of current version February 14, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3147323

Cyber-Physical Systems Enabled Transport Networks in Smart Cities: Challenges and Enabling Technologies of the New Mobility Era

AMIT PUNDIR[1], (Member, IEEE), SANJEEV SINGH[2], (Member, IEEE), MANISH KUMAR[3], ANIL BAFILA[2], AND GEETIKA J. SAXENA[1], (Senior Member, IEEE)

[1]Department of Electronics, Maharaja Agrasen College, University of Delhi, New Delhi 110021, India
[2]Institute of Informatics and Communication, University of Delhi, New Delhi 110021, India
[3]School of Computer and Information Sciences, Indira Gandhi National Open University, New Delhi 110068, India

Corresponding author: Geetika J. Saxena (gsaxena@mac.du.ac.in)

ABSTRACT Wireless communication technologies, smart sensors, enormously enhanced computational capabilities, intelligent controls merge to form Cyber-Physical Systems (CPSs). The synergy achieved due to this integration will considerably transform how humans' interaction with engineered systems in future smart cities. Such cities will leverage technologies to design, develop, and implement intelligent solutions to provide inclusive development, efficient community infrastructure, and a clean and sustainable environment. One of the domains likely to witness paradigm- shift in future smart cities is transport. The development of urban structures, functionality, and prosperity are intricately connected to how the city designs its mobility infrastructure. Shortly, all vehicles and roadside infrastructures in a city-wide ITS will be enabled with integrated smart sensors, edge computing devices and communication units to provide diversified and inclusive services to its residents. Nonetheless, due to the high heterogeneity and complexity of cross-cutting aspects of CPS, the transportation domain is susceptible to cyber vulnerabilities, threats, illegal access, cyber-attacks, unauthorized information sharing, and so on. This paper attempts to understand smart CPS-enabled transportation systems, it's conceptual framework, the connected and automated vehicles and other associated technologies and communication networks. Finally, we present the expected demands of the transportation domain in a future smart city and the capabilities of CPS in a demand-supply framework. However, the major intellectual challenge lies in effectively designing-developing-deploying models and algorithms to harness the powers of the integrated TCPS system implemented in the intended environment.

INDEX TERMS Actuators and actuation, CPS, computational capabilities, cyber systems, cyber security, physical systems, sensors and sensing, smart home, smart cities, TCPS architecture.

I. INTRODUCTION

The next milestone in the inexorable march of digital technologies would be 'Cyber-Physical Systems' (CPS). The world is fast embracing CPS, and the integration of intelligent cyber-science and physical processes is happening at an alacritous pace. Cyber-science was described as ''procedural epistemology'' by Abelson and Sussman (1996) [1], where instructions are executed according to a procedure, for example, the software working sequentially. In physical systems, many processes take place parallelly with their intrinsic uncertainties. Measuring, monitoring, and controlling the dynamics of physical systems with the help of cyber systems requires advanced computational capabilities to make real-time decisions, implement proper feedback systems, and integrate computation and networks. Nowadays, with highly enhanced computational capabilities and considerably developed artificial intelligence, it is possible to acquire deep

The associate editor coordinating the review of this manuscript and approving it for publication was Ghufran Ahmed.

knowledge of physical systems to be monitored and design more responsive, accurate, efficient, and dependable systems. The orchestration of the two worlds, virtual and the physical, is known as Cyber-Physical Systems. The synergy achieved due to this integration will significantly transform the way people interact with engineered systems in the future. CPS can initiate a revolution of intelligent devices and strategies vital for shaping our future smart cities [2], [3].

The emergence of CPSs is to provide, redesign, and create numerous new approaches in resource management, intelligent transportation systems, business management, energy management (large-scale smart grid management systems), education, commerce, industries, smart manufacturing, and environmental monitoring, to name a few. Due to the seamless integration of various intricate interdependencies of smart computing and pervasive physical processes, CPSs hold tremendous promise to transform the transportation sector in future smart cities [4], [5].

The ongoing research to integrate intelligent algorithms-based cyber abstractions and network/infrastructure will soon develop enhanced capabilities and scalability [6]. However, despite tremendous advancements in the development of CPSs, the reliability, automated operations, efficiency, and maintenance of the systems are still a matter of research as networked systems are becoming increasingly complex. CPSs promise to transform the world into a better place with efficient and robust systems. Still, the security of the newly developed cyber world is one of the most significant research challenges [7]. Furthermore, the large-scale adoption of CPS in the transport sector introduces new risks as purely mechanical elements are less likely to fail than a system of sensors and actuators highly susceptible to failure due to software mistakes, hardware malfunction, or cyber security attacks.

In this paper, an attempt has been made to present evidence of the worldwide developments, suggesting a framework for the Transport system in smart cities of the future. This paper is divided into five sections, including the introduction. Section II presents CPS background, including the conceptual framework, the design parameters and deployment life-cycle. Section III discusses the concept of smart cities, identifying critical research statements related to transport cyber-physical systems (TCPS) and the detailed review of the statements. Section IV details the challenges and future requirements, highlighting the critical CPS cyber threats, attacks, and vulnerabilities. Finally, section V includes essential suggestions and recommendations for a future smart city's, safe, and secure TCPS environment.

II. BACKGROUND AND CONCEPTUAL FRAMEWORK

A. CPS-CONCEPT, CHARACTERISTICS AND DEFINITIONS

Coined in 2006 by Helen Gill, the term ''cyber-physical systems'' stems from ''cybernetics.'' The integration of cyber and physical processes is fast becoming complex. The rapidly diminishing gap between cyber and physical systems justifies the coining of a new term that explains them as inseparable.

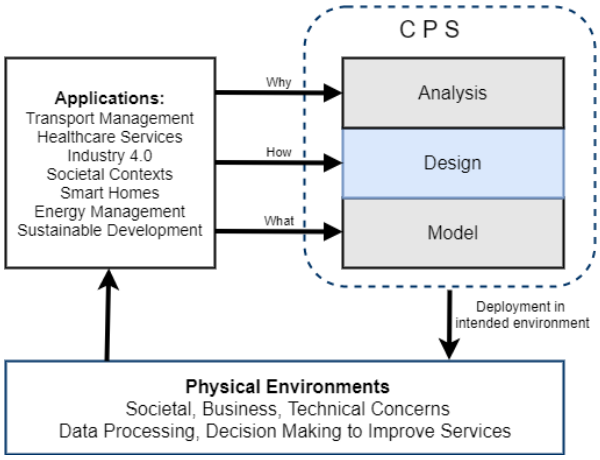


FIGURE 1. Why-How-What analogy-based conceptual framework of CPS.

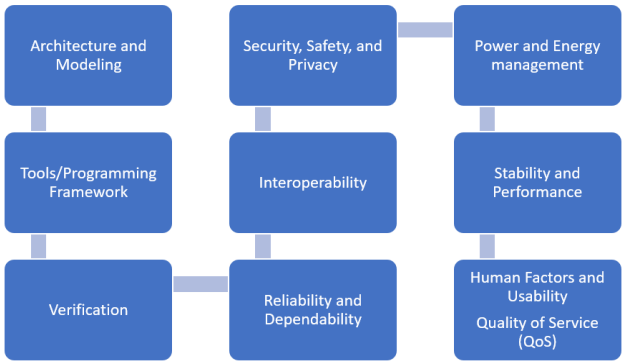


FIGURE 2. The chain model of design parameters of a CPS.

The conceptual framework of CPS, based on the why-how-what analogy, is shown in Fig. 1 [8], [9]. In 2010, Acatech (German National Academy of Science and Engineering) provided a more detailed definition: ''*A CPS is a system with embedded software (as part of devices, buildings, means of transport, production systems, medical processes, logistic processes, coordination processes, and management processes), which records data using sensors and affect physical processes, evaluates and saves recorded data, interacts in real-time with both the physical and digital world via digital communication networks (wireless or wired, local or global), in a series of dedicated, multi-modal human-machine interfaces.*'' [10].

The process to design reliable cyber-physical systems (CPSs) is inherently collaborative, involving diverse disciplines. The design parameters, arranged in the development chain that support the cross-cutting aspects, manages complexity and scale, co-modeling, simulation and testing and deployment are shown in Fig 2. The life-cycle integration of such a developed CPS system is shown in Fig 3.

III. SMART CITIES AND TCPS

A. CPS ENABLED FUTURE SMART CITIES

Cities that leverage technologies to design, develop, and implement intelligent solutions to provide inclusive

development, efficient community infrastructure, a clean and sustainable environment, and other resources to give citizens decent quality of life are termed smart cities. Digital technologies and their interaction with physical systems, like the amalgamation of cyber services with city health services, provide intelligent solutions that may drive economic growth by improving infrastructure and services, creating employment, and enhancing the quality of life in smart cities. As many of these smart city applications are based on intelligent sensing and real-time monitoring, controls, data analysis, and decision making, it is imminent that future cities will depend considerably on CPSs. [11]–[14].

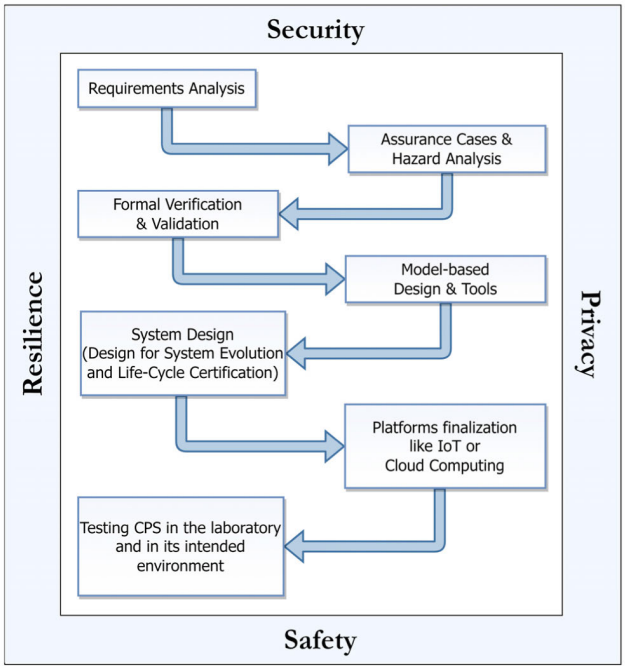


FIGURE 3. The life-cycle integration model of deployment of a CPS. The other aspects not covered in this figure are management, services, data management and models' capability to upgrade.

Transport Cyber-Physical System (TCPS): One of the domains likely to witness a paradigm- shift in future smart cities is transport. The development of urban structures, functionality, and prosperity are intricately connected to how the city designs its mobility infrastructure [15]. Artificial intelligence holds the promise to transform transport systems worldwide, addressing extensive data integration, user-driven solutions, making decisions in real-time and using the learning to develop better adaptive solutions [16]–[18].

The connected vehicle is already a realized mainstream reality and the world is fast moving towards the 'always connected' transport paradigm. We are now looking an ecosystem of city mobility that ensures zero road collisions reduces air pollution, emissions and ensures a more predictable travel. Today's vehicles are more autonomous than ever before, more intelligent, safer, use green fuel and always connected. Today's roads are no longer a simple physical infrastructure but 'empowered' with info-communications, intelligence and sensing capabilities and can harvest energy, weigh vehicles in motion, collect tolls, etc. *Therefore, the connected mobility system designed to handle congestion and environmental degradation and to provide better, faster, cleaner and cheaper services in rail-road-air transportation by taking advantage of the advances in communications networks, IoT, cloud and edge computing, scalable storage, and data-empowered insights can be termed as Transport Cyber-Physical System (TCPS).* It is the new autonomous system of connected vehicles and infrastructure, shared and data-driven mobility paradigm of future urban settings [19], [20].

B. ADOPTED METHODOLOGY FOR TCPS REVIEW

Systematic reviews of the published work have been undertaken following a predefined search strategy making every effort to identify research that supports the current research basis. The most critical issue in any systematic review protocol is formulating the proper research statements [21]. We identified the following statements, in the context of this paper that can be addressed by systematic review:

1. *Significance of Transport Cyber-Physical Systems (TCPS)in the context of future smart cities.*
2. *The current status of connected and automated vehicles.*
3. *Formulation of TCPS Framework for future smart cities.*
4. *TCPS technologies in terms of architectures, reliability, performance, and safety, and security.*
5. *Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and Vehicle-to-Everything (V2X) wireless communication networks.*
6. *Present Intelligent Transport Systems (ITS) communication standards.*
7. *Present status and future of Mobility-as-a-Service (MaaS) in TCPS.*

1) SIGNIFICANCE OF TCPS

The rapidly changing landscapes of urban mobility in a smart city shall deliver mobility solutions that are innovative, collaborative, and sustainable in terms of services like traffic management, drive-sharing, ride-sharing, parking management and autonomous driving. The TCPSs have evolved into very complex systems having various forms of data streams, processing massive amounts of data, and providing a wide range of services. The TCPSs have robust data analytics capabilities to perform real-time and static data processing, handle V2V, V2I and V2X communications data, road infrastructure, road-rail-air transportation data, smart vehicles and traffic monitoring networks, to decide in real-time. These CPS-enabled interventions have significantly transformed intelligent transport systems worldwide [22]–[28]. Some of the applications, potential benefits to society of TCPS in future smart cities are

- Driverless cars communicate securely and perform tasks to provide safety to passengers and make travel far more relaxing.

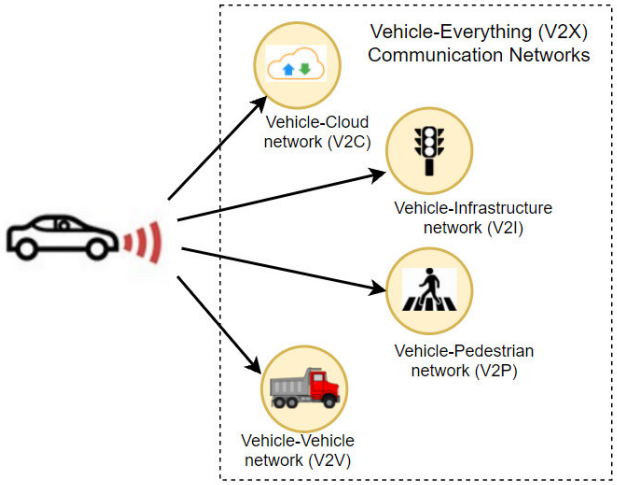


FIGURE 4. Various communication networks CAVs interact with in real-world scenarios.

- Smart roads infrastructure that coordinates to reduce delays using route optimizations.
- Adaptive and demand-responsive traffic system with huge drive-share and ride-share potential.
- Minimization of human error factors.
- Easier surveillance, monitoring and regulation of traffic conditions in the city.
- Efficient routing optimizations to minimize traffic congestion, parking woes and traffic policing.
- Easy implementation of unified models of traffic flow and communication standards.
- Drones for infrastructure management and provide Wi-Fi access during disaster management.
- User-centric adaptive, secure, efficient, and cost-effective transport system.
- Huge potential to design and implement an inclusive transport ecosystem. People with certain benchmarked disabilities will be able to drive in the new ecosystem.
- Cost minimization and better efficiencies with renewable fuels.
- Environmental benefits include reduced carbon emission and noise levels.
- Devise human-scaled measurements to study the areas around metro stations, railway stations etc., for Transit oriented development, addressing the interaction between the physical environment and human activities.

2) CONNECTED AND AUTOMATED VEHICLES (CAVS)

CAVs are among the most heavily researched automotive technologies. Vehicles that can communicate with other vehicles on the road, with the driver, on-road and roadside infrastructure, collect, share data with cloud services to improve on-road safety and security, vehicle efficiency, and environment friendly are connected vehicles. A few of the types of communication networks are shown in Fig 4.

TABLE 1. The six levels of automation describe autonomous vehicles, as per the National Highway Traffic Safety Administration (NHTSA).

Level 0	**No Automation:** The human driver is in complete control of all aspects of driving.
Level 1	**Minimal Driver Assistance:** ADAS on the vehicle can assist the human driver with either steering, braking or accelerating.
Level 2	**Low Automation:** ADAS controls steering, braking and accelerating under certain circumstances. The human driver must perform the remaining driving tasks.
Level 3	**Medium Automation:** On-board automated driving system (ADS) performs most of the driving tasks under some circumstances. In all other cases, the human driver performs the driving task.
Level 4	**High Automation:** On-board ADS can perform and monitor all driving tasks in real-world scenarios. The human need not pay attention in those scenarios.
Level 5	**Full Automation:** On-board ADS can do all the driving in all circumstances. The human occupants are just passengers and need not be involved in driving.

The CAVs, one of the ultimate manifestations of AI-based CPSs, would bring revolutionary mobility changes by minimizing human intervention [17]–[19], [29]–[31]. In addition, these vehicles are trustworthy, secure, robust, reliable, interactive, have real-time decision-making capabilities and are likely to enhance safety, accessibility, inclusivity [29], [30], [32], [33].

The technologies for CAVs and advanced driver assistance systems (ADAS) overlap vastly, though an emerging sector. Table 1 describes autonomous vehicles through six levels of driver assistance technology advancements [34].

CAVs Challenges: Although adding connectivity to vehicles has its benefits, it also has challenges. Due to the large volume of information being accessed and shared, there are numerous security, privacy, data analytics, and aggregation issues. In addition, there are concerns about the system vulnerabilities towards cyber-attacks, software and hardware malfunctioning and privacy data exploitation issues [29], [31], [35]–[40]. CAVs can effectively solve real-life transportation problems by improving transportation safety and ITS standards and legislative, legal, moral, business and social engagement frameworks. However, formulations of standards acceptable worldwide are a significant challenge. Few organizations are actively involved in developing such standards. For example, The ITS program of the US Department of Transportation (USDOT) facilitates the research for the adoption of intelligent vehicles, intelligent infrastructure, and the entire ecosystem of a smart transportation system, as shown in Table 2.

CAVs will coexist with older AVs, semi-autonomous and conventional vehicles during the transition period.

During that time behavioral adaptation, situational awareness, and user resistance problems will be paramount. In addition, combining earlier technology with the latest communication networks to increase connectivity and integrate information across domains is another challenge.

TABLE 2. Development of ITS standards for deployment of CAVs by the US Department of Transportation (USDOT).

The ITS standards are used to deploy Connected Vehicles.	IEEE 802.11 - 2012	The standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks
	IEEE 1609.2-2016	The standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages
	IEEE 1609.3-2016	The standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services
	IEEE 1609.4-2016	The standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation
	IEEE 1609.12-2016	The standard for Wireless Access in Vehicular Environments (WAVE) - Identifier Allocations
	SAE J2735	Dedicated Short-Range Communications (DSRC) Message Set Dictionary
	SAE J2945/1	On-board Minimum Performance Requirements for V2V Safety Communications

Automated vehicles (AVs) in an ITS are analogous to computers on wheels, running on data and communicating with intelligent societal infrastructure around them. Therefore, data engineering to decide the type, quality and, amount of data to be collected, safety security and storage for effective fleet learning is also a significant challenge [32], [33], [41], [42].

3) TCPS FRAMEWORK FOR FUTURE SMART CITIES

The framework is the fundamental structure of a TCPS system. It presents conceptual connections of the relationships among the modules that provide the basic behavior of the suggested approach. A framework is proposed, connecting various modules of many related problems in any real-world scenario, although with variations. Each module is driven by algorithms that absorb much of these variabilities, follow unified standards, have different architectures, different performance characteristics with high degree of reliability and safety. In this section, a framework is suggested for TCPS, as shown in Fig. 5, that shall provide a platform to design-develop-deploy a TCPS system and evaluate the system's performance in the context of actual applications.

4) TCPS TECHNOLOGIES IN TERMS OF ARCHITECTURES, RELIABILITY AND PERFORMANCE

The paper by Mollor *et al.* [43] focuses on the requirements of conjoined intelligent transport and IT systems for the effective implementation of CPS to on-road transport systems. Traffic flow analysis, remote access lab, and simulation studies consisting of vehicles and roads conducted in the natural world transportation system were able to extract constraints of CPS implementation. Limitations regarding sensing, actuating, and communicating in networks specifically to intelligent traffic light systems in congested and uncongested traffic flow scenarios and travel time prediction are investigated and reported in this paper.

From innovative tires to intelligent transport systems or roads, trains, air connected by communication networks, transportation systems today are a cross-domain integration that demands coordination across sectors like transportation infrastructure, logistics, automotive, capacity, and governance. The integration has led to the emergence of logistics as the most vital part of industrial and societal processes, and the 'mobility as a service is fast accelerating.' Modern transport solutions developed on highly automated integrated systems addressing top concerns provide the best services to the society with minimum human interactions. However, adaptation to new transport services, especially by an increasingly aging population, largely depends on quality, reliability, security, accessibility for persons with reduced mobility, and safety. On the other hand, the customization, variability of transport system architecture, inherent deep level complexities, ever-increasing requirements for enhanced capabilities, changing landscapes, safety and security and real-time pattern analysis of accident statistics, continuous updates to vehicles, or avoiding inappropriate driver behavior remain challenges till today [44].

The paper [45] presents a parallel execution methodology to conjoin artificial systems with physical-social systems. Stepwise control, computational experiment-based validation realizes a CPS-based intelligent transport system. The method consists of modeling and representation, analysis and evaluation through computational experiments, and control and management through parallel execution. The methodology effectively represents aspects of complex engineering and social complexity elements, paving the way for intelligent traffic cyber systems to become more powerful, ITS 5.0 and offering several advantages over traditional approaches.

The students' smartphone data is analyzed to determine wait time for the bus using Media Access Control (MAC) addresses and conduct route optimization to identify the best route available uniquely. The various security threats to the systems were identified, like data collection, transmission, fake data generation, and flooding of cloud storage [46]. Maintaining the transport infrastructure with the help of intelligent systems is another critical aspect of any Intelligent transport system.

The paper presents a structured health monitoring mechanism to measure the road infrastructure conditions, like bridges, by correlating traffic loads to bridge responses. A CPS framework is suggested to monitor truckloads, trigger SHM systems, record bridge responses, and link the data with truckloads collected by weigh-in-motion (WIM) stations but not on bridges [47].

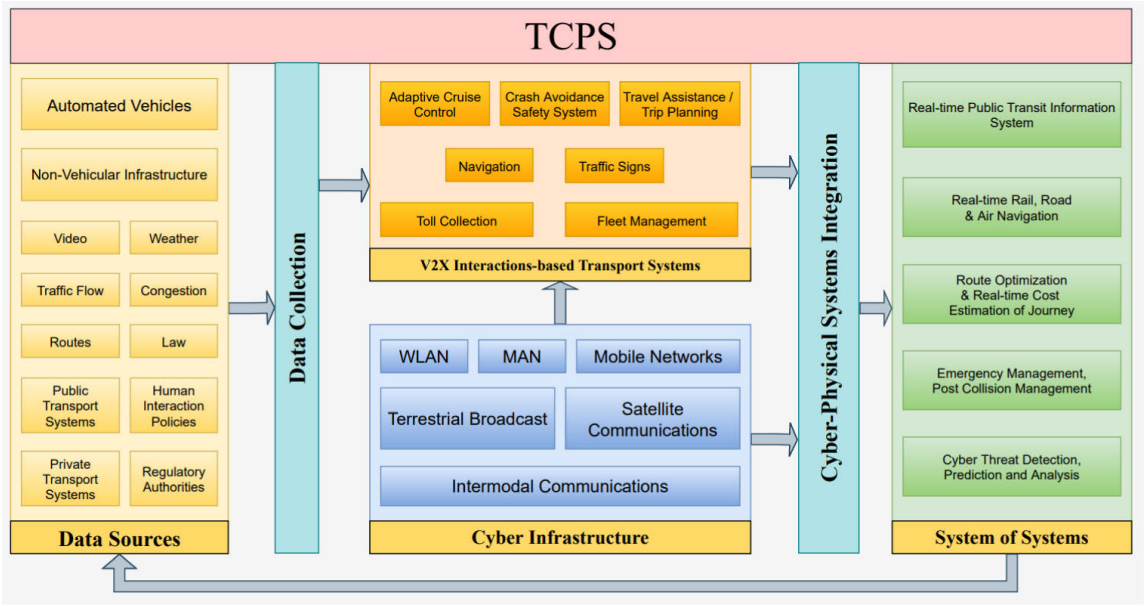
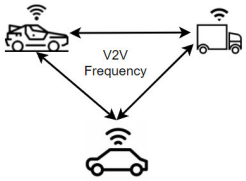
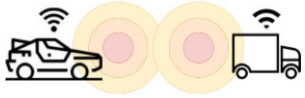
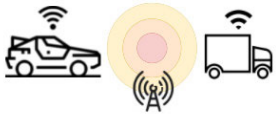
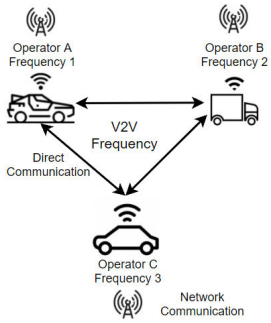


FIGURE 5. Suggested framework of TCPS for future smart cities.

TABLE 3. Direct and network communication networks, few of the use cases and challenges in ITS.

Direct & Network Communication	Use Cases	V2X Challenges
Direct Communication (V2V)  Proximal direct communications (100s of meters) considering for high speeds / high Doppler, high density, improved synchronization and low latency	 • Prevention of Collision • Latency-sensitive use cases, e.g., V2V safety • Operates both in- and out-of-coverage network areas	High relative speeds: Lead to significant Doppler shift/frequency offset. Therefore, the TCPS design should consider relative speeds up to 500km/h. High node densities: Random resource allocation results in excessive resource collisions. The TCPS design for the future calls for more efficient resource selection and allocation and new sensing methods. Time synchronization: Lack of synchronization source when out-of-coverage. The capabilities of TCPS should have enhancements to use satellites for out-of-coverage area communication.
Network Communication  To broadcast messages from a V2X server to vehicles and beyond. Vehicles can send messages to servers.	 • Wide area networks communications • More latency tolerant use cases, e.g., V2N situational awareness	

5) VEHICLE-TO-VEHICLE (V2V) AND VEHICLE-TO-INFRASTRUCTURE (V2I) WIRELESS COMMUNICATION NETWORKS

In TCPS, vehicles are responsible for sending, receiving, processing information and broadcasting to intelligent transport service providers, ensuring safe, congestion-free traffic management. The onboard units (OBU) in smart vehicles enable this and use available wireless technologies to form Vehicles-based networks known as Vehicular-AdHoc-Networks (VANETs). With technological advancements in AI, wireless communications with high bandwidth, high-reliability links, mobile services and enhanced capabilities of OBUs, enable vehicles to communicate with other vehicles and roadside units (RSUs). It improves their performance,

perception area and allows the execution of joint maneuvers. Vehicle ability to correctly interpret data, to learn from it and to use learning in various driving situations have made the demand for Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) Communication and Vehicle-to-Everything (V2X) very high. Today, vehicles interact in real-time with multiple V2V and V2I networks with high reliability and accuracy for object detection and collision avoidance mechanisms. For this, the vehicles need heterogeneous connectivity environments and high OBU-device intelligence and these days, they have both.

V2X communication is a critical component of TCPS as it enables vehicles to communicate effectively with other vehicles and beyond. It encompasses vehicle-to-network, vehicle-to-vehicle, vehicle-to-infrastructure and vehicle-to-pedestrian communications and brings substantial value to advanced driver assistance systems (ADAS). The implementation of V2X communication with interconnectivity and interoperability requires the use of standards and protocols. Dedicated short-range communications (DSRC), a short to medium-range service with high data transfers and low latency, supports V2V and V2X communications and covers various applications such as safety messages, congestion information, and toll collection. The DSRC spectrum has seven channels, each 10 MHz wide. One channel is restricted for safety communications only, while two other channels are reserved for critical safety of life and high power public safety. The remaining channels are service channels that can be used for non-safety applications [48]–[50].

Vehicular traffic scenarios have more significant challenges than fixed wireless networks caused by varying driving speeds, traffic patterns, and driving environments. For instance, to ensure timely vehicular safety communications, fast data exchanges are required. In these circumstances, scanning channels and multiple handshakes necessary to establish communication are associated with too much complexity and high overheads. The DSRC was changed to IEEE 802.11p Wireless Access in Vehicular Environments (WAVE) to address these challenging requirements and is universally adopted [51]–[53]. The various communication networks, a few of the use cases and the challenges are shown in Table 3.

Routing, Broadcasting, and Security in VANET: The vehicle, a self-driving car, for example, is loaded with several independent and overlapping CPSs for controls of cruise control, anti-lock braking, temperature, tire pressure, crankshaft position, light, collision sensors, etc. and are primarily wired to ensure safety, security, and 100% availability [54]. More and more functionalities are being handled by these interlinked CPSs enhancing autonomy and complexities while reducing human intervention requirements. However, following current wireline standards, the wired communication network is still susceptible to security breaches [55]–[57], making a solid case for secure, highly reliable, short-range standards to replace the wired connections in the future.

Sensors, cameras, loop detectors, collaborative sensors, cooperative cruise control, and cross-domain communications (vehicle to infrastructure, V2I, and vehicle-to-vehicle, V2V) are some of the elements of an Intelligent transport vehicle and the physical systems in which it operates. The paper [58] compares the detection of malicious data nodes by defining a data-specific or node-specific taxonomy of misbehavior. The security-technique analysis and a comparative analysis identify the attacks that a particular technique can prevent. Comparing security check mechanisms in ITs is challenging due to the agility problems, scalability and real-time operations [59] and lack of nomenclature of subdomains.

In VANETs, monitoring the vehicle in motion in real-time and communicating with other vehicles is a critical issue [60], [61]. Automated collision avoidance and route optimization through intelligent decision-making are achieved if the network has real-time information dissemination capability. Communication between vehicle and roadside stationary units connected to other back-end networks is thus critical.

Designing and implementing a collaborative system capable of real-time control requires a three-pillar approach. Abstract intelligent transportation systems processes, web services, and sensors form a pillar in the suggested approach. The other two are creating an integrated service execution engine to enable its creation and a prototype implementation that employs the framework. The Greater Toronto Area (GTA), Ontario model, which stitches 790 on-the-fly heterogeneous dynamic ITS services to execute ITSoS operations and integrates services by dispersed stakeholders for the benefit of end-users, is discussed in detail in the paper [62].

6) ITS COMMUNICATION STANDARDS

It is a fact that connected vehicles, also known as Cooperative Intelligent Transportation Systems (C-ITS), will improve the transportation system's safety, mobility, sustainability, and efficiency. However, deployment of this technology is challenging as the connected systems should have standard hardware and software modules to minimize market deviations. Presently, stakeholders are trying to harmonize the equipment and architectures to develop and deploy the CV technology globally with unified standards and communication protocols. In addition, it may reduce the cost as the manufacturer could use the same systems for vehicles sold worldwide. CVs technologies include various communication and data standards for multiple applications as they require central coordination between vehicles and infrastructure. The communication-based automotive applications can be broadly characterized as safety orientated (stopped or slow vehicle advisor, emergency brake light, V2V post-crash notification, road feature notification, and cooperative collision warning), convenience-oriented (parking availability, locating parking location, on-road congestion, and tolls) and commercial oriented (real-time broadcasts, vehicle diagnostics, and personalization). The requirements of networking criteria and attributes are different for different applications. The attention has been focused on vehicle/infrastructure (V2X) based applications from various governments and industries

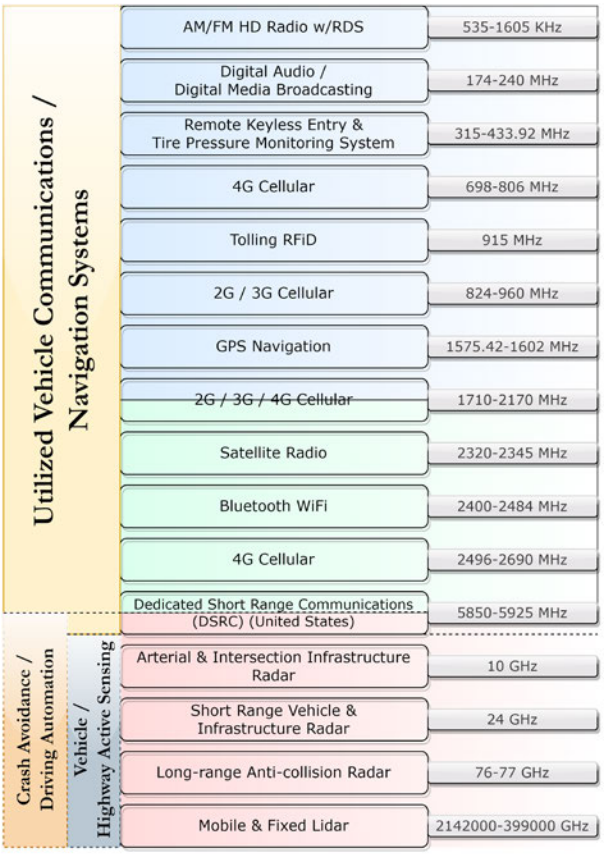


FIGURE 6. Spectrum utilization for vehicle communications, navigation, and active sensors technologies.

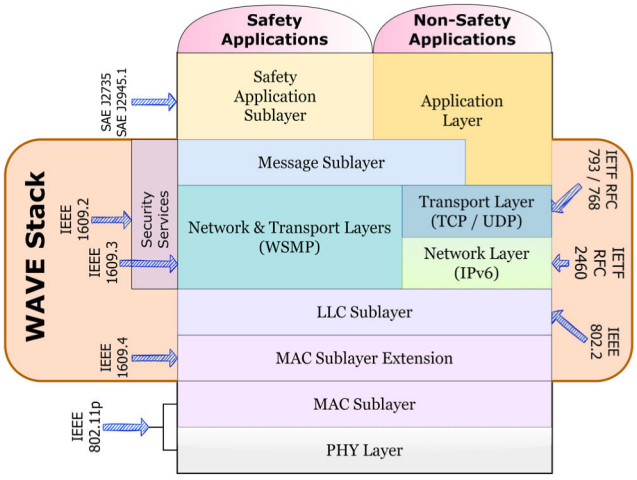


FIGURE 7. Multiple stack layers framework of DSRC.

because of its unprecedented capability to address vehicle safety, mobility, interoperability, and other commercial applications [63].

Many wireless technologies are being employed in modern vehicles, such as Wireless FM/AM, multimedia USB, Wi-Fi, Bluetooth, and remote direct access telematics. In addition, DSRC (Dedicated Short Range Communication) supports V2V and V2I applications exchanging BSMs (Basic Safety Messages) for collision avoidance. Fig. 6 shows the spectrum utilization for vehicle communications, navigation, and active sensors technologies. The spectrum requirements of conventional wireless networks and DSRC networks differ substantially. Consequently, the DSRC band requirements for different countries also vary, as shown in Table 4. DSRC is based on the IEEE 802.11p standard and operates in the 5.9GHz spectrum. The US and EU scenarios concentrate on 5.9 GHz communications; however, the EU scenario appears to be more integrated and scalable. DSRC is composed of multiple stack layers, as depicted in Fig. 7 [64]–[76].

WAVE (Wireless Access in Vehicular Environment) consists of an application, security, network, upper MAC, lower MAC, and physical layers. The SAE (Society of Automotive Engineers) J2735 dictionary is used by applications to exchange data over DSRC/WAVE and other communication protocols defining the data frames and elements for exchange. Networking and transport layers are implemented based on IEEE 1609.3 standards, and security services are implemented based on IEEE 1609.2 standards. It is also composed of the MAC sublayer based on IEEE 1609.4 standard. The PHY and MAC layers are based on the IEEE 802.11p standard. DSRC/WAVE faces several challenges, mainly channel congestion in dense vehicular environments, self-interference due to inadequate spectrum mask, and lack of ability to receive broadcast messages, no internet connectivity, and no evolution path.

An alternative technology, Cellular V2X, provides over-the-top cloud services, representing a novel interface termed PC5 for V2V, V2I, and V2N (Vehicle to Network) communication over the LTE Uu interface. Message transmission and reception in the RF environment are challenges experienced by vehicles moving at high speeds. A discernable Doppler shift and perceptible frequency offset are observed when relative speed approaches 500Km/hr. This issue is addressed by C-V2X technology with a more suitable signal design. Furthermore, in heavy traffic situations, there might be pressure in the allocation of radio resources.

In C-V2X, elaborate algorithms are developed which perceive the available resources, order them, choose the least congested resources and transmit using a semi-persistent resource allocation methodology. The C-V2X is implicitly a synchronous technology employing GPS timing using GNSS-timing in out-of-coverage situations. All these techniques allow forward-compatible progression to 5G. Work is on to harmonize global communication standards by outlining the gaps and areas of overlap for various parameters like privacy, safety, and security, authenticity-related parameters protocol for the exchange of information between ITS and other regulatory authorities [77].

TABLE 4. Spectrum requirements of DSRC communication bands in various countries.

	Region	Standard	Frequency	Remarks
1.	USA	ASTM E2213-02	5.850-5.925 GHz	5.850-5.925 GHz as DSRC band for ITS (IEEE 802.11p for base layers, IEEE 1609 for middle layers, and SAE J2735 for message set).
2.	Europe	EN 12253	5.795-5.815 GHz	5.9 GHz to be used across the European Union. Though not the same as North America, it is sufficiently close to use the same chipset.
3	Japan	ARIB T55	5.770-5.850	Japan's Association of Radio Industries and Businesses (ARIB) is using 5.8 GHz as well as 700 MHz bands for V2V. Therefore, ARIB's standards are significantly different from US and EU standards.
4	China	ISO/TC204	5.795-5.815GHz	For ETC, traveler information systems, traffic operation, and fleet management. CV standards lag behind the rapid market growth driven by global auto manufactures and domestic telecommunication service providers
5	Australia and New Zealand		50 MHz of the 5.9 GHz band	in line with the EU allocation

7) MOBILITY-AS-A- SERVICE (MAAS) IN TCPS

MaaS integrates mobility services into a single service accessible on demand. This platform facilitates integrating public transport, private transport, ride-share, vehicles on lease, or any combination to meet a customer's need [78]–[80]. Though still in the embryonic stage of its development, MaaS, once implemented in an all-in-one smart online platform, will offer beneficial services in the form of digital packages of personalized multi-modal mobility. In addition, MaaS is likely to substantially reduce private vehicles on roads worldwide by providing integrated journey planning, booking, ticketing and information services support to the commuters on an as-needed basis [81]–[89].

The literature survey reveals that MaaS is not yet clearly defined and contextualized. The demand for MaaS will soon increase substantially and hence it is a matter of active research. Therefore, it is essential to assign a globally uniform definition of MaaS as a whole and its component services. It will show a minor route to researchers to develop a unified protocol, standard, governing policy acceptable worldwide. Two key points of concern for a MaaS system are negotiating with the pervasive influence of cultural mobility practices, not only for the more tech-savvy millennial generation but also for all people [90]. The change in attitudes towards owning versus leasing, renting and sharing transport vehicles [91] because of sustainability pressures and increasing environmental awareness makes MaaS more acceptable. As the MaaS is multi-modal and scalable to the global level, involving many countries, the complexity of stitching up collaborations between states responsible for its operations and management [92] is an impediment that needs to be dealt with immediately. Researchers and policymakers can best handle the complex nature of the issue by providing definitive answers through a unified policy framework [93].

IV. CHALLENGES AND FUTURE REQUIREMENTS IN TCPS

A. CHALLENGES IN TCPS DOMAIN

The challenges of TCPS include big data analytics, faster executions/inferences, charging infrastructure, real-time communications and security. Handling multiple data sources, such as geospatial data, traffic network data, and connected vehicle data in a heterogeneous system is a significant time-consuming and costly challenge. In the TCPs domain, it is critical to process the data that leads to intelligent decision-making in real-time in varying environments and scenarios.

According to Nikitas (2020) [94], the areas of priority for CAVs policy and planning for a smooth transition are *technology, legislation, crisis and employment ethics, road infrastructure and land use, integration, traffic safety, cybersecurity and privacy, business models, traffic congestion and travel behavior and finally acceptability, trust and customer readiness*. The various demands of an ITS in a smart city regarding intelligent applications and the characteristics of CPS that shall enable, provide supply to fulfill such demands are shown in Fig. 8.

In addition, other significant challenges are as follows:

- ADAS may only enhance driving safety, comfort, and efficiency in certain operating conditions, like speed, light, road conditions, and high-speed communication networks. Many of its most promising applications are still being refined and reverted to manual mode and outside those boundary conditions.
- When the vehicle is driving autonomously, the drivers may get engaged in other activities. In case of any safety alert, they would need to quickly re-engage in driving or take action as per the vehicles' request. It depends a lot on the physical and cognitive ability of the driver and is a significant challenge in TCPS.
- The TCPS design, particularly the architecture, should consider that if a part of the system fails in the middle

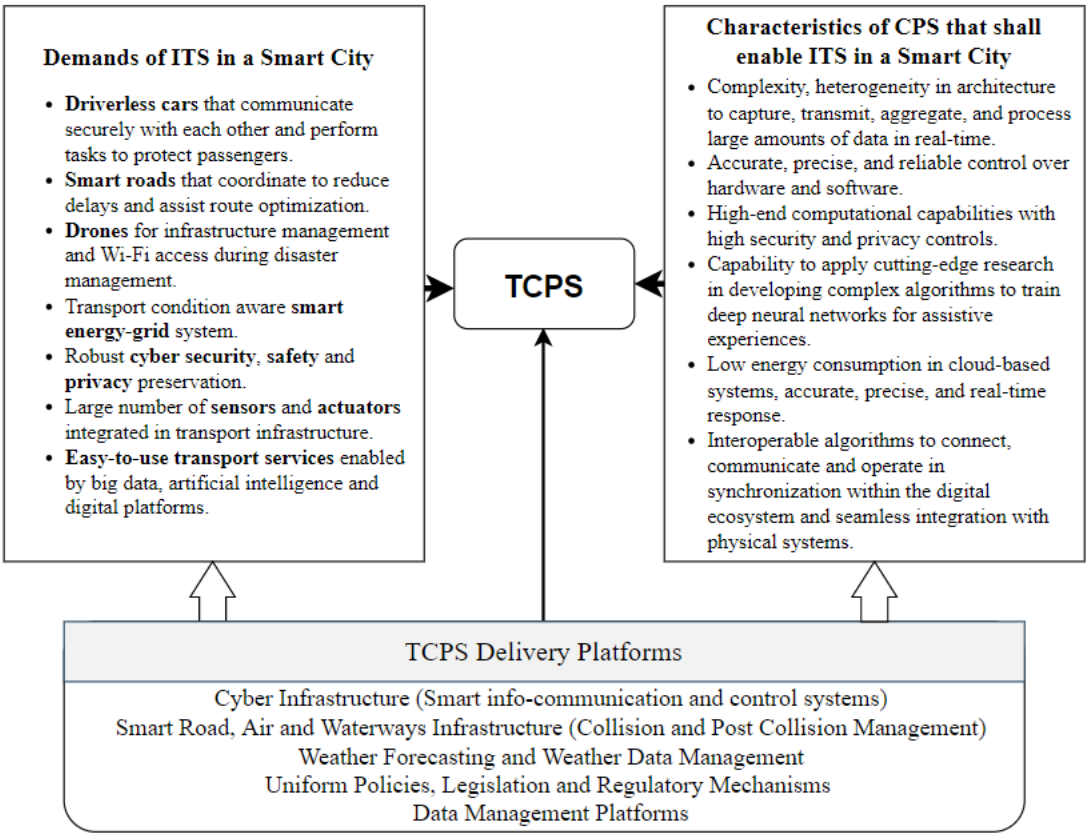


FIGURE 8. A framework highlighting the demands of ITS in future smart cities and the capabilities of CPS that shall enable the supply.

of a highway or busy traffic, it must have an excellent backup plan so that the vehicle can reach a safe point.

- As TCPS is a complex network of communication using diverse platforms, operating systems, updating and upgrading the software with high reliability is a challenge.
- System security is a big concern. The consequences of a hacker's interference with steering, braking, or other vehicle functions could be catastrophic. Already, there have been some hacks on vehicle systems, such as those that locate, unlock, and start cars.
- Unified standards and regulations are required to address safety, security, cross-domain communications, and policy for global implementation and enforcement by governments worldwide.

B. CYBERSECURITY, SAFETY AND PRIVACY CONCERNS IN TCPS

Few general safeties, security and privacy concerns in the TCPS domain are:

- TCPS are complex systems with increased vulnerability to software flaws and cyber threats.
- In V2V communications, fully autonomous vehicles may face issues in communicating with partially autonomous vehicles.
- Susceptibility of the vehicles' navigation system to adverse weather conditions.
- Re-skilling and upskilling of drivers regarding cyber threats are critical.

Due to their heterogeneous nature, dependence on large amounts of data and cross domains communication networks, CPS systems are highly prone to various cyber security threats and attacks.

Table 5 shows various aspects of Cybersecurity, safety and privacy, vulnerabilities and threats, and security certification of CPS systems as cited in literature. TCPS-based AI models can be compromised using model extraction, inversion, poisoning, and evasion. Attackers extract information regarding drivers' and passengers' location and other privacy issues, the vehicle's components and systems and exploit it for security breaches. Methods for defense against them are considerable research problems. Thus, any CPS vulnerability in different security aspects, including confidentiality, integrity, and availability, can be targeted to conduct dangerous attacks. The CPS architecture in general consists of three layers; perception, transmission and application layers.

Making CPSs immune to cyber-attacks requires robust and reliable security testing to detect security-related flaws [130]–[134]. According to National Institute of Standards and Technology (NIST) guidelines [135], [136], a well-designed,

TABLE 5. Cybersecurity, safety and privacy, vulnerabilities and threats, and security certification of CPS systems.

CPS Architecture layer	Layer Function	Security Concern
The perception layer includes equipment such as sensors, actuators, aggregators, RFID tags, GPS, and various other devices.	Collect real-time data to monitor, track and interpret the physical world.	Securing sensors, actuators to ensure authorized sources for feedback and control commands.
The transmission layer includes Internet/LANs/WANs, Bluetooth, 4G/5G, IR, ZigBee, Wi-Fi, and other technologies. In addition, it uses cloud computing platforms, routing devices, switching and internet gateways, firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) for data transmission [95]-[96].	Acts as an interface between perception and application layers. It interchanges and processes data between them.	For secure transmission of data is to be safeguarded against intrusions and malicious attacks such as malware, malicious code injection [97], Denial of Service/Distributed Denial of Service (DoS/DDoS), eavesdropping, and unauthorized access attacks [98].
Application Layer Services include healthcare, energy grid management, intelligent transport systems, water management, industrial manufacturing, environmental, and many more.	Most interactive layer. It processes the received information from the data transmission layer and issues and executes commands with complex decision-making algorithms.	Protecting and preserving the privacy of users generally through approaches such as anonymization, data masking (camouflage) [99]-[100], privacy-preserving, and secret sharing [101]. In addition, the security of big data is a critical issue [102].
CPS Threats: Exploitation of wireless networks [103]-[104], Jamming [105], Reconnaissance [106]-[107], industrial data thefts and espionage [108]- [109], Disclosure of Information [110]-[111], interception [103], unauthorized access [112], GPS network exploitation [103] [113]-[114].		
CPS Vulnerabilities: They can be broadly divided into three categories • Network Vulnerabilities: weak security measures at open wired/wireless communication and connections leading to man-in-the-middle, eavesdropping, replay, sniffing, spoofing and communication-stack (network/transport/application layer) [115], back-doors [56], DoS/DDoS and packet manipulation attacks [116]. • Platform Vulnerabilities: include hardware, software, configuration, and database vulnerabilities [97]. • Management Vulnerabilities: include lack of security guidelines, procedures and policies.		
Reasons for CPS Vulnerabilities: ● Increasing Connectivity [117], ● Heterogeneity [118]. ● USB Usage ● Bad Practice ● Spying ● Homogeneity: similar cyber-physical system types suffer from the same vulnerabilities, affecting all the devices within their vicinity once exploited. [119]. ● Suspicious Employees		
CPS Attacks: Eavesdropping, Cross-Site Scripting, SQL Injection [120], Password Cracking [121]- [122], DoS/DDoS [123]-[124], Malicious Third Party, Watering-hole Attack, Malware (Botnets, Trojan, Virus, Worms, Rootkit, polymorphic malware, spyware, ransomware)		
CPS Failures: Content Failures, Timing Failures, Sensor failures [125], Silent Failures, Babbling Failures, Schedule Failures, Service Failures		
Securing CPSs - Certification: WST Achilles Certification [126] Exida Certification [127] ISA Secure EDSA Certification [128] MuDynamics MUSIC Certification [129]		

reliable, secure, robust and reliable system ensures trust between IoT and CPS based on various multi-factors such as safety, security, privacy, consistency, dependability, resiliency, reliability, interaction and coordination. Several CPS testing tools are used to evaluate the protection of the CPSs based on these factors [137]. For example, a testing mechanism suggested by Zhou *et al.* [138], [139] using novel lightweight encryption for real-time processing in Vehicular ad hoc networks (VANETs) found the system secure, reliable and efficient.

V. CONCLUSION, VISION, OPPORTUNITIES AND CHALLENGES

Smart cities have tremendous potential to offer better living standards for future generations. A well-designed smart city framework should comfortably negate the negative impacts of urbanization. The initial step towards developing such a framework involves the identification of appropriate policy and appropriate technology. The paper has presented a comprehensive overview of the smart city aspects and its most essential domain, transport. It suggested the CPS-enabled

transport framework, the technologies available and the policies and standards.

Every revolution promises a spirit of optimism and significant changes and CPSs enabled transport systems for future smart cities are a prime example of this. They offer numerous benefits, such as car-sharing and ride-sharing, traffic safety and accident prevention, minimizing social exclusion for current non-drivers, enhancing electric vehicles adoption, and improving accessibility and interconnectivity between cities and in-vehicle riding experience. Moreover, TCPS may alleviate significant problems such as road traffic congestion, number of private cars, environmental degradation, noise pollution, accident rate, automatic fare collection and traffic congestion.

At the same time, in TCPS, there are also some concerns about the increased vulnerability to hacking, software and hardware flaws, loss of privacy, and travel data exploitation. In addition, cyber-attacks on TCPS may increase traffic accidents, congestion and emission rates. Finally, behavioral adaptation is also critical during the transition period when CAVs coexist with simpler AVs, semi-autonomous and conventional vehicles.

The world has started implementing TCPS. Shortly, almost all major cities will adopt models that can provide advanced information to the driver and traveler, enhanced vehicle control and backed by a robust transportation management system of systems functioning on globally accepted unified policies and regulations. Thus, the era of CPS-enabled transport systems has already begun.

ACKNOWLEDGMENT

The authors would like to thank the University of Delhi, FRP, Institute of Eminence and the team of Project Samarth, an initiative of the Ministry of Education, India, at the University of Delhi South Campus (UDSC), for their support.

REFERENCES

[1] H. Abelson and G. J. Sussman, *Structure and Interpretation of Computer Programs*, 2nd ed. Cambridge, MA, USA: MIT Press, 1996.

[2] X. Zhou, F. C. Delicato, K. I.-K. Wang, and R. Huang, "Smart computing and cyber technology for cyberization," *World Wide Web*, vol. 23, no. 2, pp. 1089–1100, Mar. 2020, doi: 10.1007/s11280-019-00773-y.

[3] A. Kaplan and M. Haenlein, "Siri, siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence," *Bus. Horizons*, vol. 62, no. 1, pp. 15–25, Jan. 2019.

[4] A. Puliafito, G. Tricomi, A. Zafeiropoulos, and *S. Papavassiliou*, "Smart cities of the future as cyber physical systems: Challenges and enabling technologies," *Sensors*, vol. 21, no. 10, p. 3349, May 2021, doi: 10.3390/s21103349.

[5] S. Paiva, M. Ahad, G. Tripathi, N. Feroz, and G. Casalino, "Enabling technologies for urban smart mobility: Recent trends, opportunities and challenges," *Sensors*, vol. 21, no. 6, p. 2143, Mar. 2021, doi: 10.3390/s21062143.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013, doi: 10.1016/j.future.2013.01.010.

[7] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and challenges for realizing the Internet of Things," *Cluster Eur. Res. Projects Internet Things, Eur. Commision*, vol. 3, no. 3, pp. 34–36, 2010.

[8] National Science Foundation—Cyber–Physical Systems. *Enabling a Smart and Connected World*. Accessed: Dec. 2, 2021. [Online]. Available: https://www.nsf.gov/news/special_reports/cyber-physical/

[9] I. Lee, *Department of Computer and Information Science School of Engineering and Applied Science University of Pennsylvania*. Accessed: Dec. 2, 2021. [Online]. Available: https://www.cis.upenn.edu/~lee/

[10] V. Cengarle, S. Bensalem, J. McDermid, R. Passerone, A. Sangiovanni-Vincentelli, and M. Torngren. (Nov. 2013). *Characteristics, Capabilities, Potential Applications of Cyber–Physical Systems: A Preliminary Analysis*. Deliverable D2.1 of the CyPhERS FP7 project. [Online]. Available: http://www.cyphers.eu/sites/default/files/D2.1.pdf

[11] V. Albino, U. Berardi, and R. M. Dangelico, "Smart cities: Definitions, dimensions, performance, and initiatives," *J. Urban Technol.*, vol. 22, no. 1, pp. 3–21, 2015.

[12] H. Ahvenniemi, A. Huovila, I. Pinto-Seppä, and M. Airaksinen, "What are the differences between sustainable and smart cities?" *Cities*, vol. 60, pp. 234–245, Feb. 2017.

[13] N. Komninos, P. Tsarchopoulos, and C. Kakderi, "New services design for smart cities: A planning roadmap for user-driven innovation," in *Proc. ACM Int. Workshop Wireless Mobile Technol. Smart Cities*, Philadelphia, PA, USA, 2014, pp. 11–14.

[14] I. Docherty, G. Marsden, and J. Anable, "The governance of smart mobility," *Transp. Res. A, Policy Pract.*, vol. 115, pp. 114–125, Oct. 2018.

[15] K. T. Chai, A. S. Julio, C. C. Juan, and J. M. Francisco, "Advances in smart roads for future smart cities," *Proc. Royal. Soc. A*, vol. 476, no. 2233, pp. 1–24, 2020, doi: 10.1098/rspa.2019.0439.

[16] (Sep. 2012). *Energy Information Administration. Annual Energy Review 2011. DOE/EIA-0384(2011)*. [Online]. Available: http://qrowd-project.eu/the-future-of-smart-transport/U.S.

[17] Future Transport Technology. (2016). *An Overview Roadmap, Transport for New South Wales, Australia*. [Online]. Available: https://future.transport.nsw.gov.au/sites/default/files/media/documents/2018/Future-Transport-Technology-Overview-Roadmap-2016.pdf

[18] *Future Transport Summary*. Accessed: Dec. 1, 2021. [Online]. Available: https://future.transport.nsw.gov.au/sites/default/files/media/documents/2018/Future-Transport-Technology-Roadmap_2016__.pdf

[19] (2017). *The Telegraph: Autonomous Cars in Smart Cities*. Accessed: Aug. 25, 2021. [Online]. Available: https://www.telegraph.co.U.K./business/risk-insights/autonomous-cars-in-smart-cities/

[20] Y. Yuan, D. Zhang, F. Miao, J. A. Stankovic, T. He, G. Pappas, and S. Lin, "eRoute: Mobility-driven integration of heterogeneous urban cyber–physical systems under disruptive events," *IEEE Trans. Mobile Comput.*, early access, Jun. 22, 2021, doi: 10.1109/TMC.2021.3091324.

[21] B. Kitchenham, "Procedures for performing systematic reviews, joint technical report, software engineering group," Department of Computer Science, Keele University Technical Report, Tech. Rep. TR/SE-0401, 2004. [Online]. Available: http://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf

[22] A. Nikitas, K. Michalakopoulou, E. T. Njoya, and D. Karampatzakis, "Artificial intelligence, transport and the smart city: Definitions and dimensions of a new mobility era," *Sustainability*, vol. 12, no. 7, p. 2789, Apr. 2020, doi: 10.3390/su12072789.

[23] J. Iskanderov and M. A. Guvensan, "Breaking the limits of transportation mode detection: Applying deep learning approach with knowledge-based features," *IEEE Sensors J.*, vol. 20, no. 21, pp. 12871–12884, Nov. 2020, doi: 10.1109/JSEN.2020.3001803.

[24] R. D. Knowles, F. Ferbrache, and A. Nikitas, "Transport's historical, contemporary and future role in shaping urban development: Re-evaluating transit oriented development," *Cities*, vol. 99, Apr. 2020, Art. no. 102607.

[25] W. Lang, E. C. M. Hui, T. Chen, and X. Li, "Understanding livable dense urban form for social activities in transit-oriented development through human-scale measurements," *Habitat Int.*, vol. 104, Oct. 2020, Art. no. 102238, doi: 10.1016/j.habitatint.2020.102238.

[26] A. Alessandrini, A. Campagna, P. D. Site, F. Filippi, and L. Persia, "Automated vehicles and the rethinking of mobility and cities," *Transp. Res. Proc.*, vol. 5, pp. 145–160, Nov. 2016.

[27] A. Amditis and P. Lytrivis, "Towards automated transport systems: European initiatives, challenges and the way forward," in *Proc. Road Veh. Automat.*, in Lecture Notes in Mobility. Cham, Switzerland: Springer, 2015.

[28] G. Lyons, "Getting smart about urban mobility–aligning the paradigms of smart and sustainable," *Transp. Res. A, Policy Pract.*, vol. 115, pp. 4–14, Sep. 2018.

[29] D. Milakis, B. Van Arem, and B. van Wee, "Policy and society related implications of automated driving: A review of literature and directions for future research," *J. Intell. Transp. Syst. Technol. Planning, Oper.*, vol. 21, no. 4, pp. 324–348, 2017.
[30] E. Papa and A. Ferreira, "Sustainable accessibility and the implementation of automated vehicles: Identifying critical decisions," *Urban Sci.*, vol. 2, no. 1, p. 5, Jan. 2018.
[31] N. Thomopoulos and A. Nikitas, "Smart urban mobility futures: Editorial for special issue," *Int. J. Automot. Technol. Manage.*, vol. 19, no. 1–2, pp. 1–9, 2019.
[32] R. M. Gandia, F. Antonialli, B. H. Cavazza, A. M. Neto, D. A. D. Lima, J. Y. Sugano, I. Nicolai, and A. L. Zambalde, "Autonomous vehicles: Scientometric and bibliometric review," *Transp. Rev.*, vol. 39, no. 1, pp. 9–28, 2017.
[33] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, "Connected vehicles: Solutions and challenges," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 289–299, Aug. 2014.
[34] *National Highway Traffic Safety Administration (NHTSA)*. Accessed: Dec. 2, 2021. [Online]. Available: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety#:~:text=Automated%20vehicles%20and%20driver%20assisting,prevent%20injuries%2C%20and%20save%20lives.&text=Fully%20automated%20vehicles%20that%20can,resulting%20crashes%2C%20and%20their%20toll
[35] A. Nikitas, E. T. Njoya, and S. Dani, "Examining the myths of connected and autonomous vehicles: Analysing the pathway to a driverless mobility paradigm," *Int. J. Automot. Technol. Manage.*, vol. 19, nos. 1–2, pp. 10–30, 2019.
[36] A. Nikitas, I. Kougias, E. Alyavina, and E. N. Tchouamou, "How can autonomous and connected vehicles, electromobility, BRT, hyperloop, shared use mobility and mobility-as-a-service shape transport futures for the context of smart cities?" *Urban Sci.*, vol. 1, no. 4, p. 36, 2017.
[37] D. J. Fagnant and K. Kockelman, "Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations," *Transp. Res. A, Policy Pract.*, vol. 77, pp. 167–181, Jul. 2015.
[38] N. Thomopoulos and M. Givoni, "The autonomous car—A blessing or a curse for the future of low carbon mobility? An exploration of likely vs. desirable outcomes," *Eur. J. Futures Res.*, vol. 3, no. 1, p. 14, Dec. 2015.
[39] N. Gavanas, "Autonomous road vehicles: Challenges for urban planning in European cities," *Urban Sci.*, vol. 3, no. 2, p. 61, Jun. 2019.
[40] G. H. De Almeida Correia, D. Milakis, B. van Arem, and R. Hoogendoorn, "Vehicle automation and transport system performance," in *Handbook on Transport and Urban Planning in the Developed World*. Cheltenham, U.K.: Edward Elgar Publishing, 2016, pp. 498–516.
[41] J. Firnkorn and M. Müller, "Free-floating electric carsharing-fleets in smart cities: The dawning of a post-private car era in urban environments?" *Environ. Sci. Policy*, vol. 45, pp. 30–40, Jan. 2015.
[42] A. Chehri and H. T. Mouftah, "Autonomous vehicles in the sustainable cities, the beginning of a green adventure," *Sustain. Cities Soc.*, vol. 51, Nov. 2019, Art. no. 101751.
[43] D. P. F. Moller and H. Vakilzadian, "Cyber–physical systems in smart transportation," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, May 2016, pp. 776–781.
[44] M. Törngren, F. Asplund, S. Bensalem, J. McDermid, R. Passerone, H. Pfeifer, A. Sangiovanni-Vincentelli, and B. Schätz, "Characterization, analysis, and recommendations for exploiting the opportunities of cyber–physical systems," *Cyber–Physical Systems*. New York, NY, USA: Academic, 2017, pp. 3–14, doi: 10.1016/B978-0-12-803801-7.00001-8.
[45] G. Xiong, F. Zhu, X. Liu, X. Dong, W. Huang, S. Chen, and K. Zhao, "Cyber–physical-social system in intelligent transportation," *IEEE/CAA J. Autom. Sinica*, vol. 2, no. 3, pp. 320–333, Jul. 2015, doi: 10.1109/JAS.2015.7152667.
[46] R. Gifty, R. Bharathi, and P. Krishnakumar, "Privacy and security of big data in cyber physical systems using Weibull distribution-based intrusion detection," *Neural Comput. Appl.*, vol. 31, no. S1, pp. 23–34, Jan. 2019.
[47] R. Hou, S. Jeong, J. P. Lynch, and K. H. Law, "Cyber–physical system architecture for automating the mapping of truck loads to bridge behavior using computer vision in connected highway corridors," *Transp. Res. C, Emerg. Technol.*, vol. 111, pp. 547–571, Feb. 2020.
[48] *Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems-5 GHz Band Dedicated Short-Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. Standard ASTM E2213-03, 2003.
[49] Y. Kudoh, "DSRC standards for multiple applications," in *Proc. 11th World Congr. ITS*, Nagoya, Japan, 2004, pp. 1–19.
[50] J. Yin, T. Elbatt, and S. Habermas, "Performance evaluation of safety applications over DSRC vehicular ad hoc networks," in *Proc. VANET*, Philadelphia, PA, USA, Oct. 2004, pp. 1–9.
[51] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," in *Proc. VTC Spring-IEEE Veh. Technol. Conf.*, 2008, pp. 2036–2040, doi: 10.1109/VETECS.2008.458.
[52] K. Z. Ghafoor, M. Guizani, L. Kong, H. S. Maghdid, and K. F. Jasim, "Enabling efficient coexistence of DSRC and C-V2X in vehicular networks," *IEEE Wireless Commun.*, vol. 27, no. 2, pp. 134–140, Apr. 2020, doi: 10.1109/MWC.001.1900219.
[53] S. Zeadally, M. A. Javed, and E. B. Hamida, "Vehicular communications for ITS: Standardization and challenges," *IEEE Commun. Standards Mag.*, vol. 4, no. 1, pp. 11–17, Dec. 2020, doi: 10.1109/MCOMSTD.001.1900044.
[54] A. Burg, A. Chattopadhyay, and K. Y. Lam, "Wireless communication and security issues for cyber–physical systems and the Internet-of-Things," *Proc. IEEE*, vol. 106, no. 1, pp. 38–60, Jan. 2018, doi: 10.1109/JPROC.2017.2780172.
[55] S. Checkoway, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX Conf. Secur.*, 2011, pp. 1–16.
[56] D. K. Nilsson, U. E. Larson, F. Picasso, and E. Jonsson, "A first simulation of attacks in the automotive network communications protocol FlexRay," in *Proc. Int. Workshop Comput. Intell. Secur. Inf. Syst.* Berlin, Germany: Springer-Verlag, 2009, pp. 84–91.
[57] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 12, pp. 3893–3902, Dec. 2018, doi: 10.1109/TITS.2018.2791484.
[58] J. Giraldo, E. Sarkar, A. A. Cárdenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber–physical systems: A survey of surveys," *IEEE Design Test*, vol. 34, no. 4, pp. 7–17, Aug. 2017, doi: 10.1109/MDAT.2017.2709310.
[59] F. Sakiz and S. Sen, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Netw.*, vol. 61, pp. 33–50, Jun. 2017.
[60] A. Gokhale, S. Tambe, L. Dowdy, and G. Biswas, "Towards high confidence cyberphysical systems for intelligent transportation systems," in *Proc. Nat. Workshop High-Confidence Automot. Cyber-Phys. Syst.*, 2008, pp. 1–3.
[61] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015, doi: 10.1109/TITS.2015.2439292.
[62] M. Elshenawy, B. Abdulhai, and M. El-Darieby, "Towards a service-oriented cyber–physical systems of systems for smart city mobility applications," *Future Gener. Comput. Syst.*, vol. 79, pp. 575–587, Feb. 2018, doi: 10.1016/j.future.2017.09.047.
[63] Q. Hong, E. P. Dennis, R. Wallace, and J. Cregger, "Global harmonization of connected vehicle communication standards," MDOT and CAR, Lansing, MI, USA, Tech. Rep., 2016. [Online]. Available: https://tinyurl.com/y42rqhcp
[64] M. Hasan, S. Mohan, T. Shimizu, and H. Lu, "Securing vehicle-to-everything (V2X) communication platforms," 2020, *arXiv:2003.07191*.
[65] M. Saini, A. Alelaiwi, and A. E. Saddik, "How close are we to realizing a pragmatic VANET solution? A meta-survey," *ACM Comput. Surveys*, vol. 48, no. 2, p. 29, 2015.
[66] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Dec. 2011.
[67] A. Festag, "Cooperative intelligent transport systems standards in Europe," *IEEE Commun. Mag.*, vol. 52, no. 12, pp. 166–172, Dec. 2014.
[68] *Intelligent Transport Systems (ITS) Usage*, document Rec. ITU-R M.2445-0, 2018.
[69] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Secur. Symp.*, 2011, pp. 1–16.
[70] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2X access technologies: Regulation, research, and remaining challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1858–1877, 3rd Quart., 2018.
[71] *IEEE Standard for Information Technology—Local and Metropolitan Area Networks—Specific Requirements—Part 11*, Standard IEEE 802.11p2010, 2010, pp. 1–51.

[72] S. Belcher, E. Merlis, J. McNew, and M. Wright, "Roadmap to vehicle connectivity," SFB Consulting, Washington, DC, USA, Tech. Rep., Sep. 2018. [Online]. Available: https://www.atssa.com/Portals/0/Roadmap-to-Vehicle-Connectivity.pdf

[73] C. Suthaputchakun and Z. Sun, "Routing protocol in intervehicle communication systems: A survey," *IEEE Commun. Mag.*, vol. 49, no. 12, pp. 150–156, Dec. 2011.

[74] M. Seredynski, D. Khadraoui, and F. Viti, "Signal phase and timing (SPaT) for cooperative public transport priority measures," in *Proc. 22nd ITS World Congr.*, 2015, pp. 1–10.

[75] *700 MHz Band Intelligent Transport Systems*, Standard ARIB STD-T109, V1.3, 2017. [Online]. Available: https://tinyurl.com/y49ae6dy

[76] SAE International. *SAE J2945/1: On-Board System Requirements for V2V Safety Communications*. Accessed: Dec. 2, 2021. [Online]. Available: https://saemobilus.sae.org/content/j2945/1201603

[77] L. Miao, J. J. Virtusio, and K.-L. Hua, "PC5-based cellular-V2X evolution and deployment," *Sensors*, vol. 21, no. 3, p. 843, Jan. 2021, doi: 10.3390/s21030843.

[78] I. C. M. Karlsson, J. Sochor, and H. Strömberg, "Developing the 'service' in mobility as a service: Experiences from a field trial of an innovative travel brokerage," *Transp. Res. Proc.*, vol. 14, pp. 3265–3273, 2016.

[79] J. Sochor, H. Strömberg, and I. C. M. Karlsson, "Implementing mobility as a service: Challenges in integrating user, commercial, and societal perspectives," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2536, no. 1, pp. 1–9, Jan. 2015.

[80] J. Sochor, I. C. M. Karlsson, and H. Strömberg, "Trying out mobility as a service: Experiences from a field trial and implications for understanding demand," *Transp. Res. Rec., J. Transp. Res. Board*, vol. 2542, no. 1, pp. 57–64, Jan. 2016.

[81] F. Hirschhorn, A. Paulsson, C. H. Sørensen, and W. Veeneman, "Public transport regimes and mobility as a service: Governance approaches in Amsterdam, Birmingham, and Helsinki," *Transp. Res. A, Policy Pract.*, vol. 130, pp. 178–191, Dec. 2019.

[82] G. Smith, J. Sochor, and I. C. M. Karlsson, "Mobility as a service: Development scenarios and implications for public transport," *Res. Transp. Econ.*, vol. 69, pp. 592–599, Sep. 2018.

[83] D. A. Hensher, "Future bus transport contracts under a mobility as a service (MaaS) regime in the digital age: Are they likely to change?" *Transp. Res. A, Policy Pract.*, vol. 98, pp. 86–96, Apr. 2017.

[84] A. Polydoropoulou, I. Pagoni, A. Tsirimpa, A. Roumboutsos, M. Kamargianni, and I. Tsouros, "Prototype business models for mobility-as-a-service," *Transp. Res. A, Policy Pract.*, vol. 131, pp. 149–162, Jan. 2020.

[85] M. Matyas and M. Kamargianni, "The potential of mobility as a service bundles as a mobility management tool," *Transportation*, vol. 46, no. 5, pp. 1951–1968, Oct. 2019.

[86] Y. Xie, M. Danaf, C. L. Azevedo, A. P. Akkinepally, B. Atasoy, K. Jeong, R. Seshadri, and M. Ben-Akiva, "Behavioral modeling of on-demand mobility services: General framework and application to sustainable travel incentives," *Transportation*, vol. 46, no. 6, pp. 2017–2039, Dec. 2019.

[87] J. Schikofsky, T. Dannewald, and M. Kowald, "Exploring motivational mechanisms behind the intention to adopt mobility as a service (MaaS): Insights from Germany," *Transp. Res. A, Policy Pract.*, vol. 131, pp. 296–312, Jan. 2020.

[88] C. Mulley, C. Ho, C. Balbontin, D. Hensher, L. Stevens, J. D. Nelson, and S. Wright, "Mobility as a service in community transport in australia: Can it provide a sustainable future?" *Transp. Res. A, Policy Pract.*, vol. 131, pp. 107–122, Jan. 2020.

[89] D. Arias-Molinares and J. C. García-Palomares, "The Ws of MaaS: Understanding mobility as a service fromaliterature review," *IATSS Res.*, vol. 44, no. 3, pp. 253–263, Oct. 2020.

[90] C. Mulley, "Mobility as a services (MaaS)—Does it have critical mass?" *Transp. Rev.*, vol. 37, no. 3, pp. 247–251, May 2017.

[91] M. Tinnilä and J. Kallio, "Impact of future trends on personal mobility services," *Int. J. Automot. Technol. Manag.*, vol. 15, no. 4, pp. 401–417, 2015.

[92] P. Jittrapirom, V. Marchau, R. van der Heijden, and H. Meurs, "Future implementation of mobility as a service (MaaS): Results of an international Delphi study," *Travel Behav. Soc.*, vol. 21, pp. 281–294, Oct. 2020.

[93] K. Pangbourne, M. N. Mladenović, D. Stead, and D. Milakis, "Questioning mobility as a service: Unanticipated implications for society and governance," *Transp. Res. A, Policy Pract.*, vol. 131, pp. 35–49, Jan. 2020.

[94] A. Nikitas, "Connected and autonomous vehicles: Priorities for policy and planning," in *International Encyclopedia of Transportation*, R. Vickerman, Ed. Amsterdam, The Netherlands: Elsevier, 2020.

[95] T. Sommestad, G. N. Ericsson, and J. Nordlander, "SCADA system cyber security—A comparison of standards," in *Proc. IEEE PES Gen. Meeting*, Jul. 2010, pp. 1–8.

[96] B. Zhu and S. Sastry, "SCADA-specific intrusion detection/prevention systems: A survey and taxonomy," *Proc. 1st Workshop Secure Control Syst. (SCS)*, vol. 11, 2010, p. 7.

[97] V. Sridharan, "Cyber security in power systems," Ph.D. dissertation, School Elect. Comput. Eng., Georgia Inst. Technol., Atlanta, GA, USA, 2012.

[98] J. Weiss, *Protecting Industrial Control Systems from Electronic Threats*. New York, NY, USA: Momentum Press, 2010.

[99] J. Clause and A. Orso, "Camouflage: Automated anonymization of field data," in *Proc. 33rd Int. Conf. Softw. Eng.*, May 2011, pp. 21–30.

[100] S. P. Pomroy, R. R. Lake, and T. A. Dunn, "Data masking system and method," U.S. Patent 7 974 942 B2, Jul. 5, 2011.

[101] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, Nov. 2014.

[102] S. Raza, "Lightweight security solutions for the Internet of Things," Ph.D. dissertation, Dept. Comput. Sci. Eng., Mälardalen Univ., Västerås, Sweden, 2013.

[103] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. USENIX Secur. Symp.*, 2011, pp. 77–92.

[104] E. S. Dawam, X. Feng, and D. Li, "Autonomous arial vehicles in smart cities: Potential cyber–physical threats," in *Proc. IEEE 20th Int. Conf. High Perform. Comput. Commun., IEEE 16th Int. Conf. Smart City, IEEE 4th Int. Conf. Data Sci. Syst. (HPCC/SmartCity/DSS)*, Jun. 2018, pp. 1497–1505, doi: 10.1109/HPCC/SmartCity/DSS.2018.00247.

[105] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and privacy in implantable medical devices and body area networks," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 524–539.

[106] K. Munro, "Deconstructing flame: The limitations of traditional defences," *Comput. Fraud Secur.*, vol. 2012, no. 10, pp. 8–11, 2012.

[107] B. Miller and D. Rowe, "A survey SCADA of and critical infrastructure incidents," in *Proc. 1st Annu. Conf. Res. Inf. Technol.*, 2012, pp. 51–56.

[108] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy*, vol. 7, no. 3, pp. 75–77, Jun. 2009.

[109] J. Vavra and M. Hromada, "An evaluation of cyber threats to industrial control systems," in *Proc. Int. Conf. Mil. Technol. (ICMT)*, May 2015, pp. 1–5.

[110] C. Camara, P. Peris-Lopez, J. M. de Fuentes, and S. Marchal, "Access control for implantable medical devices," *IEEE Trans. Emerg. Topics Comput.*, vol. 9, no. 3, pp. 1126–1138, Jul. 2021, doi: 10.1109/TETC.2020.2982461.

[111] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou, "Cyber–physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies," *IEEE Access*, vol. 9, pp. 29775–29818, 2021, doi: 10.1109/ACCESS.2021.3058403.

[112] I. Lee, O. Sokolsky, S. Chen, J. Hatcliff, E. Jee, B. Kim, A. King, M. Mullen-Fortino, S. Park, A. Roederer, and K. K. Venkatasubramanian, "Challenges and research directions in medical cyber–physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 75–90, Jan. 2012.

[113] R. Brooks, S. Sander, J. Deng, and J. Taiber, "Automotive system security: Challenges and state-of-the-art," *Proc. ACM 4th Annu. Workshop Cyber Secur. Inf. Intell. Res., Developing Strategies Meet Cyber Secur. Inf. Intell. Challenges Ahead*, pp. 1–3, 2008.

[114] V. G. Garagad, N. C. Iyer, and H. G. Wali, "Data integrity: A security threat for Internet of Things and cyber–physical systems," in *Proc. Int. Conf. Comput. Perform. Eval. (ComPE)*, Jul. 2020, pp. 244–249, doi: 10.1109/ComPE49325.2020.9200170.

[115] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proc. Int. Conf. Internet Things 4th Int. Conf. Cyber, Phys. Soc. Comput.*, Oct. 2011, pp. 380–388.

[116] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1963–1970, Sep. 2013.

[117] R. E. Gillen and S. L. Scott, "Method for assessment of security-relevant settings in anomaly-based intrusion detection for industrial control systems," in *Proc. IEEE Conf. Ind. Cyberphys. Syst. (ICPS)*, Jun. 2020, pp. 156–161, doi: 10.1109/ICPS48405.2020.9274691.

[118] S. Amin, G. A. Schwartz, and A. Hussain, "In quest of benchmarking security risks to cyber–physical systems," *IEEE Netw.*, vol. 27, no. 1, pp. 19–24, Jan. 2013.
[119] E. Iasiello, "Cyber attack: A dull tool to shape foreign policy," *Proc. IEEE 5th Int. Conf. Cyber Conflict (CYCON)*, 2013, pp. 1–18.
[120] V. N. Gudivada, S. Ramaswamy, and S. Srinivasan, "Data management issues in cyber-physical systems," in *Transportation Cyber-Physical Systems*. Amsterdam, The Netherlands: Elsevier, 2018, pp. 173–200.
[121] P. Papantonakis, D. Pnevmatikatos, I. Papaefstathiou, and C. Manifavas, "Fast, FPGA-based rainbow table creation for attacking encrypted mobile communications," in *Proc. 23rd Int. Conf. Field Program. Log. Appl.*, Sep. 2013, pp. 1–6.
[122] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez, "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms," in *Proc. IEEE Symp. Secur. Privacy*, May 2012, pp. 523–537.
[123] P. Solankar, S. Pingale, and R. Parihar, "Denial of service attack and classification techniques for attack detection," *Int. J. Comput. Sci. Inf. Technol.*, vol. 6, no. 2, pp. 1096–1099, 2015.
[124] F. Yihunie, E. Abdelfattah, and A. Odeh, "Analysis of ping of death DoS and DDoS attacks," in *Proc. IEEE Long Island Syst., Appl. Technol. Conf. (LISAT)*, May 2018, pp. 1–4.
[125] Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity attacks in vehicular sensors," *IEEE Sensors J.*, vol. 20, no. 22, pp. 13752–13767, Nov. 2020, doi: 10.1109/JSEN.2020.3004275.
[126] D. Rhoades. *Achille—The World's First Man-in-the-Middle Web Security Tool*. Accessed: Dec. 2, 2021. [Online]. Available: https://www.mavensecurity.com/about/achilles
[127] (2015). *Exida Certification—IEC 61508, IEC 61511, IEC 62443, ISO 26262, CFSE*. [Online]. Available: https://www.exida.com/Certification
[128] (2018). *Isasecure—IEC 62443-4-2—EDSA Certification*. [Online]. Available: https://www.isasecure.org/en-U.S./Certification/IEC-62443-EDSA-Certification
[129] *Mu Studio Performance Suite*. Accessed: Dec. 2, 2021. [Online]. Available: https://www.slideshare.net/aquaphlex/mu-studio-performance-suite
[130] L. C. Silva, M. Perkusich, F. M. Bublitz, H. O. Almeida, and A. Perkusich, "A model-based architecture for testing medical cyber–physical systems," in *Proc. 29th Annu. ACM Symp. Appl. Comput.*, 2014, pp. 25–30.
[131] A. M. Kosek and O. Gehrke, "Ensemble regression model-based anomaly detection for cyber–physical intrusion detection in smart grids," in *Proc. EPEC*, 2016, pp. 1–7.
[132] A. Motii, A. Lanusse, B. Hamid, and J. M. Bruel, "Model-based real-time evaluation of security patterns: A SCADA system case study," in *Proc. Int. Conf. Comput. Saf., Rel., Secur.*, 2016, pp. 375–389.
[133] J.-P.-A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber–physical systems security: Limitations, issues and future trends," *Microprocessors Microsyst.*, vol. 77, Sep. 2020, Art. no. 103201, doi: 10.1016/j.micpro.2020.103201.
[134] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094, doi: 10.1016/j.comnet.2019.107094.
[135] L. Monostori, B. Kádár, T. Bauernhansl, S. Kondoh, S. Kumara, G. Reinhart, O. Sauer, G. Schuh, W. Sihn, and K. Ueda, "Cyber–physical systems in manufacturing," *CIRP Ann.*, vol. 65, no. 2, pp. 621–641, 2016.
[136] Z. Drias, A. Serhrouchni, and O. Vogel, "Analysis of cyber security for industrial control systems," in *Proc. Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. (SSIC)*, Aug. 2015, pp. 1–8.
[137] W. Zhao, F. Xie, Y. Peng, Y. Gao, X. Han, H. Gao, and D. Wang, "Security testing methods and techniques of industrial control devices," in *Proc. 9th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Oct. 2013, pp. 433–436.
[138] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, 2012.
[139] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.

AMIT PUNDIR (Member, IEEE) received the M.Phil. and Ph.D. degrees from the Department of Electronics Science, University of Delhi South Campus, in 1993 and 1998, respectively. From 2007 to 2008, he was at the Institute of Lifelong Learning as a Content Writer and developed e-resources for undergraduate students. He is currently an Associate Professor with the Electronics Science Department, Maharaja Agrasen College, University of Delhi, where he teaches electronics science. His research interests include artificial intelligence and cyber physical systems.

SANJEEV SINGH (Member, IEEE) received the Ph.D. degree in electronics from the Department of Electronics, University of Delhi, in 1998. He is currently a Professor and the Head of the Institute of Informatics and Communication, University of Delhi. He is also an Academic Leader in informatics and technology. His research interests include learning pedagogy, cyber physical system security, and health informatics.

MANISH KUMAR received the Ph.D. degree from the Institute of Informatics and Communication, University of Delhi, in 2019. He is currently an Assistant Professor with the School of Computer and Information Sciences, Indira Gandhi National Open University, Maidan Garhi, New Delhi, India. His research interests include cyber security, machine learning, and health informatics.

ANIL BAFILA is currently pursuing the Ph.D. degree with the IIC, University of Delhi, India. His research interests include machine learning and privacy-preservation with deep learning technologies.

GEETIKA J. SAXENA (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in electronics, in 1998 and 2000, respectively, and the Ph.D. degree in modeling and simulation of optical amplifiers from the University of Delhi, in 2010. She is currently an Associate Professor with the Department of Electronics, Maharaja Agrasen College, University of Delhi. She is also working on design, modeling, and simulation of optical components for optical communication systems. Her current research interests include digital image processing and machine learning applications.