EMERGING CYBER-PHYSICAL LANDSCAPE OF TRANSPORTATION TECHNOLOGY

M.G. BERTOLLI
Consolidated Nuclear Security, Y-12 National Security Complex
Denver, United States
Email: mik@avrioanalytics.com

M.C. SHANNON
Oak Ridge National Laboratory
Oak Ridge, United States
Email: shannonmc@ornl.gov

Abstract

Technology is rapidly progressing in transportation and shipping industries across the globe, including the nuclear, radioactive and hazardous material transportation sectors. With this progress comes unprecedented opportunities for improved transparency, safety, and security in transportation, as well as novel threat surfaces and attack vectors. Therefore, the transport safety and security interface is affected through the application of these technologies. We provide an investigative overview of the developing fields of "trans-tech" or "freight- tech" with a look towards technology development and adoption over the next 3-5 years across three primary categories: Transportation IoT (Internet of Things), Smart Infrastructure, and digitization of transportation management. We also investigate the safety and security implications of utilizing these technologies. Each of these categories presents novel threats as well as opportunities. We examine the role of technology in each as an emerging cyber-physical threat to nuclear and radioactive material transportation security, and plausible mitigation considerations at both the state and operator levels in additional to opportunities for addressing the interface between safety and security.

1. INTRODUCTION

The International Atomic Energy Agency (IAEA) estimates 20 million shipments of radioactive materials each year [1], three million of which occur in the United States [2]. Movement of sensitive and dangerous assets – requiring complex, multi-modal logistics across state lines – face unique safety and security challenges including (i) management of sensitive information, (ensuring route information and details of security plan are only accessed by need-to-know stakeholders); (ii) securing nuclear materials while in transit (ensuring relevant parties that moving material is still in the right custody / have not been tampered); and (iii) proper execution of logistical processes (personnel authentication and process integrity especially during material hand-off) [3, 4]. Simultaneously, the development and adoption of transportation technology is rapidly progressing across the globe, including the transport of radioactive materials, other hazardous material, and high-impact novel medical technology, such as COVID-19 vaccinations.

This modernization trend, which is expected to continue over the next decade, both in adoption by vehicle manufacturers and adopted by carriers and implemented in Smart Cities, provides unprecedented opportunities for improved transportation monitoring, transparency across the entire supply chain, and transportation security, but adoption of the technology should be carefully evaluated, and best practices and appropriate protections established. For example, complete transportation transparency, distinct from monitoring in that it includes disclosure of all parts of a supply chain (see [5] for a full discussion), is possible thanks to technology. As supply chain attacks (i.e., compromising security by changing a component of a process before it comes under the control of the user, such as embedding malware in chip that is later used in a computer inside a secure facility) become of greater concern, any additional technology that presents opportunities for safety and security can be beneficial. This is particularly true for transportation security, as transportation plays an integral part in most supply chains, including often being when some supply is most at risk. However, the use of this technology as currently designed and implemented may introduce unknown vulnerabilities that adversaries might exploit either to gain access to critical systems or spoof the monitoring process. These vulnerabilities can exist from the individual sensors on cargo containers to cloud-based management software now in use throughout the shipping industry. This increases

the threat landscape for supply chain attacks, such that each new component to increase supply chain transparency can become compromised, adding additional risks.

These technologies present additional opportunities to adopt more robust monitoring of nuclear and radioactive material in transport. This can be done through use of numerous sensors, connected through wireless networks, such as cellular or wireless internet, which are monitored in real-time by both human experts and artificial intelligence driven solutions. Information may come from myriad sensors (e.g., cameras, radar, diagnostic sensors), a vehicle's on-board global positioning system (GPS) and performance sensors (e.g., the vehicle's controller area network (CAN bus)), or via the local infrastructure. Advances in these technologies even provide new monitoring capabilities. For example, multi-node mesh networks, where every device is interconnected with one another to provide a seamless connective "mesh" to increase efficiency and reduce fault tolerance, powered by ZigBee now allow direct radioactivity level monitoring of nuclear material [6] that could in principle be implemented for material transport, where radioactivity levels and signals are continually monitored in real time. This would provide further confidence in the safe, secure transport of nuclear materials.

The interplay between these devices gives not just data but may also provide context or situational awareness. For example, a vehicle's GPS might signal a departure from its planned primary route, but now common Department of Transportation traffic cameras could demonstrate that the departure was strategically sound. This means that as technology progresses, traffic monitoring will become a coordinated effort between the conveyance and monitoring center, with rerouting occurring before GPS indicates a departure from a route happens. Responses to unforeseen events, such as increased traffic, detours, and excessive breaks can ideally be determined in real time and accounted for, or later reviewed to increase performance metrics, such as travel time or cost, for future shipments.

The ability to identify a potential susceptibility early, before widespread adoption of this technology, is key to addressing emerging threats as the landscape evolves. This provides fertile ground for collaboration between the international community: stakeholders will benefit from the development and implementation of safety and security best-practices related to the use of this emerging technology. Many organizations may lack the resources or subject matter expertise to identify vulnerabilities. Even for those that do, the commercial market for this technology is rapidly growing, resulting in potential lack of support from vendors and an absence of accredited industry best-practices to ensure well-vetted offerings. Therefore, working together to encourage early adoption of appropriate security measures is critical.

Broadly, the categories considered herein are Internet of Vehicles (IoV), Smart City and Smart Infrastructure, and Cloud-based Transportation Management Software (TMS). Recent industry reviews cite technology adoption as the most significant factor for the continued health of this sector [7], and surveys suggest that most medium and large carriers identify updating technological infrastructure as one of the biggest and most important challenges [7, 8]. However, technology adoption is in the early stages, with the one exception of the recent United States federally mandated requirements to use Electronic Logging Devices (ELD) [9]. This rule became law in 2016, and ELD requirements mandated that older Automatic On-Board Recording Devices (AOBRDs) be replaced or upgraded by December 2019. The penetration of these technologies are expected to accelerate due to the widespread belief of providing more secure transportation through increased transparency of the supply chain, increased connectivity through Smart Cities, and bringing all shipping information under one roof via usage of Transportation Management Systems (TMS).

The transportation technologies ("TransTech") primarily influencing transportation modernization and for which this assessment is focused include the various sensors and connectivity needed for autonomous vehicles, the technology infrastructures being deployed for Smart Cities, and the digitization of transportation management to maintain fleets and provide evidence for accident litigation. In general, the adoption of TransTech is largely driven by transportation of goods and services in the commercial sector. Nevertheless, many nuclear and radioactive material carriers operate as commercial companies, rather than state-owned organizations. In fact, one of the largest international nuclear material shippers, Nuclear Transport Solutions, emphasizes that while their core business is transport services for the nuclear industry it is supported by a wide portfolio of "services for customers in other sectors, including retail and consumer goods." [10] As such, the adoption of the technology by commercial shippers is very relevant to the security of nuclear and radioactive material transportation. While providing an overview of recent advances in TransTech, we will also discuss the current status and adoption of TransTech within the industry markets. Projections will be made for future development and adoption in the 3-5-year time frame, as well as suggesting recommendations that will be high-impact during that time period.

Finally, despite all the technological advances discussed here, it is helpful to think through the entire supply chain from production of material, through packaging, transport (by truck, air or rail), and delivery to a destination. At each junction exists the prime opportunity to limit or expose a threat surface. Freight at rest is freight at risk; emerging technology deployed with the proper security can manage this risk while realizing the benefits.

This assessment has intentionally focused on those technologies that have, or are highly likely to, experience substantial market penetration and adoption. Each of these systems, from sensors to networks and cloud-based management software provides multiple areas for improved transparency and cybersecurity vulnerabilities. This paper will outline key insights to the benefits and emerging threats posed by this new technology and encourage the IAEA to address these emerging cyber-physical technologies and concerns by interacting with member states, training and workshop materials and publications.

2. ORIGINALITY, COPYRIGHT AND PUBLICATION

3. INTERNET OF VEHICLES

The Internet of Things (IoT) describes the networking of physical objects, and their seamless integration into the information network, so that physical objects become active participants in that network [11]. IoT has been seen largely through niche applications, such as wearable tech or smart consumer appliances. This has changed significantly over the past few years, where technology is being adopted to more wide-ranging applications. The shipping industry has been transformed with the emergence of the Internet of Vehicles (IoV). Like IoT, IoV describes the networking of vehicle-related physical objects: it encompasses everything from simple tire pressure gauge sensors to cameras which alert drivers to unsafe conditions or driving habits, to fully autonomous cars and trucks.

Internet of Vehicles consists of basic IoT combined with Vehicular Ad-Hoc Networks (VANETs). The primary difference between how IoT and VANET networks interact with a vehicle is that VANETs are specifically designed for safety and security of transport, as well as reduction in pollutants and reduction of travel time. Conversely, IoT also includes entertainment or commercial technologies. As a result, IoV uses additional communication protocols and is accessed in different ways than traditional IoT, with an additional network layer. Ultimately, this, coupled with being mobile, means that Smart Vehicles have different security implications than typical IoT devices. The architecture of these systems, and their interaction with external sources (via “smart cities”) is discussed in Section **Error! Reference source not found. Error! Reference source not found.**. Security and safety aspects are also discussed there.

Five types of IoV communication modalities are possible: Vehicle-to-Vehicle (V2V), Vehicle-to-Road Side Units (V2R), Vehicle-to-network Infrastructure (V2I), Vehicle-to-Sensors (V2S), and Vehicle-to-Personal Devices (V2P) [12, 13]. With these designations, roadside infrastructure would include things like traffic lights or controllers, and network infrastructure would include cell towers, wireless hubs, or the cloud. **Error! Reference source not found.** summarizes the five communication modalities in IoV.

TABLE 1. SUMMARY OF COMMUNICATION BETWEEN IOV AND SMART CITIES

IoV Communication Modality	Connection Category	Examples
V2P	Personal devices	Phone, tablets, glasses, watches Also includes haptic feedback steering wheels
V2V	Inter-Vehicle	Detection of other cars, position of other objects through Wi-Fi/Bluetooth
V2R	Roadside device	Stop lights and intersections lights, cameras, potentially "smart" signs
V2I	Network infrastructure	Cell towers, Wi-Fi access points, signal boosters
V2S	Intra-vehicle Sensors	Gas pressure, chemical composition sensors, cameras/laser/radar

Industry experts expect technology adoption to change rapidly, and that within 3-5 years autonomous trucking may become common in the United States, and also abroad in affluent, technologically advanced hubs (e.g., Singapore, Dubai, or Seoul) [14]. There are many reasons for this, but in many regards the trucking industry is better suited for autonomous driving than commuter cars due to long stretches of roads through less populated areas [15]. It's unlikely that autonomous trucks, specifically trucks with multiple trailers, will see autonomous driving in populated areas due to difficulty traversing narrow roadways with many obstacles. Connected convoys of autonomous trucks, each connected through cellular or Wi-Fi, will allow aerodynamic improvements that reduce fuel consumption and save money [8]. Additionally, safety will be increased as once the first truck responds to a situation, such as breaking, all trucks in the line can respond instantly with no delay. While autonomous vehicles are not a focus of this assessment, the field is symbiotic with IoV. Developments in IoV have fed the progress of autonomous vehicle development, while simultaneously the anticipation of autonomous (or semi-autonomous) vehicles has driven many car manufactures to pre-emptively incorporate additional IoV sensors in current vehicle models. For example, Tesla has already shipped cars with their Autopilot semi-autonomous sensor arrays which is claimed to only require software upgrades to become fully autonomous.

Adoption of IoV technology is driven by the private market, which has raised over $1.4 billion for self-driving trucks between 2014-2017 alone [16]. Industry experts suggest, like many other transportation technologies, the role of the government is to help legislate its use. Municipalities more open to technological adoption will be the first to see it implemented. Therefore, it is expected to begin widespread use in, and between, Texas and California; then progress up-the-coast, and finally into the Midwest [16]. Pilot routes have already been conducted throughout the country, and proof-of-concept demonstrated. Such pilots include government entities, such as the United States Postal Service running autonomous mail trucks between Phoenix and Dallas [17].

Transportation security will soon need to consider the impacts of the vehicle technology developments of autonomous vehicles, the on-board sensor systems that support them, and the associated networks that are used by them not because nuclear or radioactive material will be transported by autonomous vehicles but because the cyber-physical systems created will be ubiquitous and may introduce avenues for adversary advantage (see CAN bus attacks.)

3.1. Sensors, Devices, and Applications in Freight

At the smallest scale, IoT in freight begins with sensors in and on the shipping container monitoring cargo. Depending on the application sensors, Global Navigation Satellite Systems (GNSS) receivers or other positioning devices are used to track individual shipment geo-spatial location, while temperature, moisture/humidity, light, shock, and smoke sensors are used to convey environmental conditions [18]. Until recently, tracking technologies such as GPS and cell-tower triangulation have been expensive, have limited battery life, and did not capture key environmental statuses [18]. Additionally, many implementations were company-centric (e.g., passive radio frequency identification (RFID) tags) identifying cargo contents and route information [15]) instead of logistics chain-centric. New paradigms in sensor technology, specifically in mesh networks, enable resilient networking

where information can be transmitted passively, just by being on a network [18]. In a mesh network, the device, like a cell phone, may pass through numerous networks, connecting to any number of them. Often, these networks may be solar powered, or be part of a Smart City architecture. This means cargo can be geospatially located at any point in the logistics chain, when moving or when at rest on a dock, cargo station, or airport.

Sensors are also prevalent throughout modern vehicles and are utilized for a variety of tasks. In 2018, the average number of sensors per consumer vehicle was 60-100, but the number is expected to rise to over 200 sensors per vehicle in the next two years [19]. **Error! Reference source not found.** summarizes several use categories, each with examples and applications [20]. Currently sensors may monitor stops, door openings, light exposure, temperature, pressure, or shock [21]. This data, if provided in real time, can be used to flag aberrant behaviour via trained artificial intelligence algorithms, providing an efficient additional safety and security layer. Importantly, it also provides methods for implementing monitoring that correspond with Enhanced Transport Security in the IAEA's graded security approach [22]. The IAEA has developed several cybersecurity nuclear series publications [23, 24], but transport cybersecurity has not been specifically addressed. The unique geospatial disparity and rapid change in technology landscape introduces multiple application-specific security considerations for transportation, as we discuss here. Additional training and education on cybersecurity specific to transportation is recommended.

TABLE 2. Summary of various categories of sensors used in-vehicles [20].

Category	Examples	Application
Safety	Oscillators, speed, haptic, radar/laser beams	Radar/laser identify obstacles, early stopping; haptic provides tactile steering wheels
Diagnostic	Position sensors, chemical/gas composition sensors, temperature, pressure sensors	Vehicle performance and health, predicting maintenance needs
Traffic	Cameras, radars, ultrasonic sensors	Monitor traffic conditions
Assistance	Humidity sensors, thermometers, torque sensors, rain sensors	Determining conditions inside the vehicle for both driver and cargo
Environmental	Pressure sensors, thermometer, cameras	Determining conditions outside the vehicle
User	Smart watches, cameras, heart rate sensors	User-worn sensors that might also interface with the vehicle

In newer vehicles these sensors may also influence vehicle behaviour, such as radar identifying obstacles and forcing an abrupt stop. These safety devices therefore provide an additional mechanism where vehicle control is exposed.

Starting in 2017, the United States Department of Transportation mandated all commercial trucking companies to install Electronic Logging Devices (ELDs) [25]. This rule required cargo carriers to electronically log their hours of service, in lieu of paper records. Devices must be integrally synchronized with a truck's engine and ensure drive routes are captured. Therefore, although cells phones could meet this mandate, with specialized hardware or with Bluetooth connection to sensors attached to the engine, dedicated devices are preferred. These devices also usually pass route data in near real-time to a fleet or safety manager, which can then be used to further optimize routes and monitor cargo location (see, for example, products like Geotab for fleet management [26]). Because of the mandate, trucking services in the US have near full adoption; international locales may not. However, even without a government mandate, many medium-to-large shipping fleets make use of ELDs to manage their fleet (see Section 4 for more discussion on logistics and management in shipping). Shipments of sensitive materials should ideally use ELDs to help facilitate monitoring and transparency.

Knowing a truck's geo-spatial location also allows for additional security measures to be put in place. For instance, sensitive cargo routes could be placed in a geo-fence. Geo-fences are virtual perimeters for a real-world geographic area. Any deviation from a planned route could set off an alarm, both for the driver and an outside monitoring group. This provides real-time detection that can be easily implemented, such as what is recommended

by the IAEA NSS 9-G [22]. Alternatively, checkpoints can be established, where managers can be alerted every time the cargo crosses another checkpoint or arrives at one late. Similar technology allows one to take the actual path traversed and reverse geo-locate to report crossing city/state boundaries. Such use-cases of geo-fencing truck shipments is commonplace in industry like oil and gas, where the shipment of products by third parties are billed according to both time and distance travelled, less any demurrage. However, in the case of nuclear and radioactive material transport, delays or late transfer of custody at known locations can provide indications of compromise from geospatial data alone, even if undetected by other tamper security measures. For example, an unusual delay along a segment of road that cannot be corroborated with a viable external reason (e.g., traffic) may indicate the altering of material in transport even if it ultimately appears to arrive intact at the destination. Additionally, how this information is stored and transmitted can present security vulnerabilities. These types of vulnerabilities are discussed later: transmission of cargo data in real-time is discussed in Section **Error! Reference source not found.** (**Error! Reference source not found.**); storage of route and security information are often held in emerging applications known as TMS and are the subject of Section **Error! Reference source not found.** (**Error! Reference source not found.**);

Above the sensor level, IoT and VANET combine to form IoV. Many of these developments are now common in the consumer environment, such as fully functional cameras and semi-autonomous vehicles (e.g., adaptive cruise control). These systems are also increasingly utilized in cargo transport as well, but at a larger scale. For example, large transport trucks might utilize a half-dozen cameras around the trailer to monitor traffic, assist in parking, and avoid collisions. In cutting-edge setups, the cameras are high-resolution, wide-angle lens with night vision options and a built-in microphone. These six cameras connect to a touchscreen monitor through Wi-Fi or Bluetooth. The video can either be saved locally or uploaded via the internet to a cloud server. Cameras may also face the driver, to identify drivers who are impaired, in distress or exhibiting erratic behaviour [27]. Lower tiered options might also only save video in the ten seconds before or after a qualifying event, such as an accident. Accidents would be detected by a vehicle sensor, such as a simple accelerometer identifying an impact. The use of camera and audio feeds in the cabin of vehicles to automatically identify impaired or distressed drivers is an active area of research [28]. Automatic identification of impaired or distressed drivers via algorithmic behaviour detection, would increase the efficacy, and thus adoption, of this type of technology. However, algorithmic and artificial intelligence (AI) implementations of these capabilities bring with them additional vulnerabilities, such as those discussed in this recent publication by the Office of International Nuclear Security [29].

Adoption of these technologies in freight is accelerating with the convergence of several paradigms. These paradigms include the recent recognition that delivery operations are strategic to core business models, such as with increased E-commerce for stay-at-home shopping during quarantine orders [30, 31]. Further, COVID-19 has exacerbated the need for rapid technological adoption as fleets must find ways to perform their duties while maintaining social distance. Many medical goods, like vaccines and certain therapeutics, must be kept at sub-zero temperatures during transit and storage, and therefore require constant monitoring to ensure safety [9]. While not directly related to nuclear or radioactive material transport, these recent world events have served to accelerate both the development and adoption of these technologies. Such adoption is unlikely to revert even as the triggering events subside.

The challenges presented by the COVID pandemic has also affected shipments. A significant decrease in commercial airline flights (~30%) has created complications for freight forwarders who use space on commercial flights. This decrease in commercial travel also has many providers considering retiring old wide-body aircraft, providing an additional reduction in future availability for cargo forwarding in the near term. Global routing is further complicated by travel restrictions. Limited capacity on many routes has resulted in high freight rates this past year, with projections expecting this trend to continue for the next 2-3 years [31]. All of this serves to force shippers to find or create operational efficiencies in order to maintain business viability in the current climate. The need for efficiencies will drive adoption of TransTech in general, including IoV.

3.2. IoV Cybersecurity Threats

As IoV technology permeates, numerous novel threats become viable at the individual truck level. This section will summarize these threats, while the threat implications of IoV within city-wide networks will be discussed in Section 4.2.

Smart transport has two primary openings for attacks: sensors (internal susceptibility) and network (external susceptibility). Sensors typically have a small form factor, with limited memory and computational power. This means that they lack sophisticated authentication schemes and other safety controls. For instance, most sensors cannot defend against denial-of-service (DOS) attacks. Similarly, if they require authentication, they may not be able to support methods that are robust in preventing brute force attacks. Bluetooth is infamous for these vulnerabilities, where limited password lengths enable a successful brute-force attack, where every possible password is submitted via trial and error until the correct one is found, in less than 10 seconds [32]. This attack vector played a part in how attendees of the DEF CON conference were able to hack multiple cars almost a decade ago [33]. Changes to Bluetooth standards in the intervening years, including higher safety levels requiring additional authentication protocols, have eliminated that opening, but Bluetooth is still a common threat vector [32, 34].

Systems comprised of numerous, interconnected sensors obviously provide a larger threat surface. IoV systems should require rigorous standards at every level, for every device, and every connection reflecting the graded approach to transportation security [22]. These standards should include keeping best practices for passwords and authentication. This is critical in order to maintain information security alongside physical security. This will help prevent low-level cyber-attacks. Additional considerations include strong standards for authentication procedures, suitable access controls including principles of least privileges between various parts of the network and devices, data verification, data availability, digital integrity checks and digital signatures, and real-time guarantees, as data processed out of time order may be dangerous.

With small form factors, low memory availability, and limited battery life, authentication procedures are non-trivial in IoV applications. Conventional cryptographic algorithms (e.g., Advanced Encryption Standard [AES], Rivest-Shamir-Adleman [RSA], Digital Signature Algorithm [DSA]) are not suitable for this environment. Therefore, there has been a great deal of interest in lightweight cryptographic algorithms suitable for vehicle deployment. At present, there is still no widely accepted solution, and this is an active research area. Current research includes RFID-based authentication, signcryption [35], and even distributed ledger (blockchain) approaches. Blockchain approaches would have a public key infrastructure where all devices inside a vehicle have a standard group key, and blockchain is used to communicate “externally” to the vehicle [36]. Because of the nascent state of solutions in this field, IAEA is well-positioned to assist in maintaining situational awareness as new methods and technology emerge.

Research by the Stimson Center’s Blockchain in Practice program in 2020 highlighted how successful blockchain applications in areas such as health and supply chain logistics could benefit the transport of nuclear and radioactive material. Based on Stimson’s initial studies, blockchain (distributed ledger) technology presents an opportunity to complement existing physical security measures by way of tracking information and conditions that give relevant security stakeholders confidence that processes are being followed in a secure manner. Unlike traditional databases, DLT encrypts, timestamps, replicates, and stores “hashed” data into an immutable ledger that are linked together in “blocks,” making it difficult to reverse-engineer. The information stored on the blockchain does not have to be sensitive information itself (i.e., location of nuclear material), but metadata or ancillary information that helps corroborate that it is in a secure environment (e.g., who / when accessed nuclear material; did the conditions of nuclear material change overtime).

Unlike public blockchains (e.g., Bitcoin), a blockchain suited for nuclear and radioactive material security would be permissioned and have protocols corresponding with the various security levels associated with each type of material in transport. If an insider threat attempted to manipulate data such as transport routes stop times, then all relevant participants within the network would be notified. Companies such as Maersk [37], Kuehne + Nagel [38], and IBM [39] have developed blockchain applications for transport processes.

The 2015 Euratom Supply Agency study identified the lack of harmonization and overregulation in transport authorization as a significant risk because of complex systems of national reporting and authorization in cross-border transport. Moreover, the IAEA observed that over half of IAEA-reported incidents involving radioactive material occurred during transport, which makes clear the persistent challenges with transport. For instance, a shipment of UF6 cylinders can travel almost 14,000km (about 9,000 mi) from Germany to the United States, or upwards of 13,000km (8,000 mi) for Co-60 shipments from the manufacturing facility in Canada to end-user facilities in East Africa [2]. Given differing country laws, regulations, and guidelines for different types of materials, transporters must grapple with differing security requirements that meet the material’s risk profile. Such a dynamic, multi-pronged endeavour could lead to misalignment of information.

Interestingly, quarantines and health restrictions imposed as a response to COVID-19 are compelling many organizations and companies to rely on technology (i.e., the Internet), as well as "no touch" systems [40] to communicate information beyond faxes and hardcopy. For example, Circulor, a blockchain developer that tracks the transit of critical minerals, is exploring ways to pair blockchain with artificial intelligence and the Internet of Things (IoT) to develop a "mesh" or web of sensors that would cover high-value materials during transport. If the material is disturbed in an unexpected way, this would register as an anomaly and would be logged on a blockchain platform so that this information cannot be erased or manipulated and can be immediately accessed by all the relevant parties that need to know its material conditions.

Many traditional cybersecurity problems are relevant to transportation, in particular Denial of Service (DOS) and Distributed Denial of Service (DDOS). These are particularly dangerous with regards to VANET and IoV applications simply because of the low-memory profile of the devices. In transport scenarios, these attacks can jam communication channels, both those channels internal to the VANET as well as external communication channels to the network. In each of these scenarios, the vehicle's safety systems are compromised, meaning an intruder could cause accidents or control the vehicle, as well as potentially access records of cargo being transported. To handle DOS attacks, and other typical cybersecurity threats, novel solutions must be considered for IoV. For DOS attacks, systems might be built to recognize an unreasonable increase in traffic, and then try to filter known traffic [41].

Additionally, as with any connected devices, problems can occur when manufacturers push patches and updates to their systems. At these moments all vehicle components are vulnerable, as a trusted external source, often a 3rd party, is connected. If this external source is compromised, the whole system can be jeopardized. As an example, last year the University of South Florida (USF) had a virus sweeping through campus cyclically. Every time the virus was contained and eliminated it would appear at another location infecting student devices with no clear connection between them. This occurred repeatedly, until it was identified the infecting agent was a campus smart bus. Transportation department employees ran a software update on the bus using a compromised USB thumb drive. As the bus drove around campus, its Wi-Fi signal would be picked up by students, who would then become infected (or re-infected) [32].

The most dangerous time for any freight remains when it is at rest [21]. Truck drivers spend an average of 2-3 hours waiting for their trucks to be unloaded or handed off to a subsequent carrier. Rest stops and taking even short walks or smoke breaks create huge security openings, where breaches become viable. The IAEA recognizes that even with nuclear material transport, stops can be unavoidable under common conditions [22]. It is at these times when cargo, the truck itself, or connected sensors can be most easily tampered with. Aside from direct hacking or physical attack, subtler attacks can be initiated. For example, the signature of the cargo's stock keeping unit (SKU) code could be switched with another, meaning materials could be shipped to different destinations and no one would realize until delivery. These types of attacks don't require physical contact, just a nearby Bluetooth or network connection, so malicious actors could potentially alter cargo's signature without physical contact.

External vulnerabilities include anything that can interface with the freights network, Wi-Fi, Bluetooth, or 5G access. These could come from many sources, such as a nearby vehicle with its own router and signal, or even from cell phones. Generally, attacks on IoV would rely on the concept of a pivot: accessing a low-functioning system (such as a camera or sensor) to get credentialed access to the internal network. This is identical to how hackers use cameras to infiltrate universities and commercial laboratories, where once the camera is accessed via its default password, access is gained to the wider network [32]. Once inside, a sniffer is installed (a software tool that monitors activity on devices, such as network packets or user behaviour) to monitor passwords and keystrokes. The increased cyber threat surface of material in transit thus necessitates a different approach to security practices that includes remote cyber-attacks which in turn directly compromise the physical security.

Like IoT, IoV will likely have third-party application developers which have access to certain subsystems. This presents yet another vulnerability in the IoV supply chain, where one has an authenticated application running in the background. Even if all the installed applications are benevolent, some of these applications might have openings. Therefore, best practices should limit installing any applications beyond those required.

Another potential opening to IoV internal networks is with a "Wi-Fi Pineapple." Pineapples enable a simple "man in the middle attack" where the device acts as a "hotspot honeypot." [32, 42] In other words, the Pineapple identifies local Wi-Fi hotspots and then copies their name and pretends to be an extension of that network. Nearby devices expecting to connect to a real network connect to it instead. Once connected, the Pineapple can re-route the user to malicious websites without the user knowing. Pineapples could conceivably be set up in a car traveling

next to the truck carrying the cargo of interest. The best way to prevent this is to limit the types of access trucks with sensitive cargo can interact with, or by requiring on communication through encrypted channels.

The vulnerabilities of this technology are common cybersecurity vulnerabilities, and therefore traditional cybersecurity best practices should be encouraged. Principles such as installing only necessary software, requiring secure passwords, multiple levels of authentication, secure authentication protocols where possible, and adopting the principle of least privilege are important. Like many cybersecurity environments, it is difficult to enforce these standards because of the complex organizations involved, and the large number of people interacting with the cargo and trucks. The same is true here, where mechanics, truck drivers, and dispatchers might each interact with various pieces of cargo in transit. Moreover, the rapid increase in vendors with limited industry-accepted approaches requires due diligence on the part of the purchasing organization to ensure the entire product, from hardware to embedded software, is secure.

Finally, it is also possible to create invasions through cell phones and GPS spoofers. Simple apps can be used to "spoof" a device's location, making it appear they are elsewhere. Beyond individual phones, simple thumb drive sized devices can be used to jam GNSS receivers of nearby vehicles and infrastructure [43]. This recently occurred in 2019 when a truck driver successfully jammed the GPS receiver of his truck – along with planes landing in the nearby Newark airport. Identifying the interference, originating in a nearby highway, required "considerable resources" according to United Airlines [44].

A significant threat to nuclear material transport would be someone "spoofing" the location of a conveyance, either stealing it and showing it as in its expected place, or showing it stolen when it hasn't been moved. This could provide opportunities to steal or alter it later. Building confidence in a cargo's true location is possible using a combination of various technologies, such as combining GNSS tracking, inertial measurements, and vehicle CAN bus data. Solutions like this are complicated and expensive to implement, requiring careful forethought.

3.3. Threats, Benefits and Recommendations

3.3.1. Benefits and Threats

The Internet of Vehicles (IoV) provides unprecedented telemetry into the location, system health and safety of cargo in transit. Freight vehicles are utilizing an ever-increasing number of sensors to monitor both vehicle safety (e.g., tire pressures, cameras, LIDAR) and cargo (e.g., temperature, pressure, and humidity sensors). This also includes Wi-Fi or cellular connection between trucks and other vehicles. Each of these sensors and connections provide opportunities for greater transparency into and monitoring of a conveyance. Specifically, this technology can facilitate compliance with the IAEA's enhanced transport security level providing immediate detection of compromise [22].

Conversely, IoV is vulnerable to traditional cybersecurity attacks but requires novel preventative measures. This is because attacks, such as DDOS attacks, are focused on sensors which have limited form factor, memory, and battery power in these applications. Specifically, new authentication and DOS defense methods are needed specifically for IoV because of limited memory availability. It is likely that these authentication routines will combine many technologies and paradigms, such as pseudo-random key generation and RFID tags.

3.3.2. Maturity and Urgency

Actual market penetration of this technology is already high domestically, indicating a high maturity level that is ready for use by even small shipping operations. This increases urgency for education and standards around use for nuclear material transport.

It is widely expected by industry Subject Matter Experts that in the next 3–5-year timeframe autonomous cargo trucks will become more commonplace in the United States along long-haul routes [15, 45]. Trucks will transition to autonomous mode once outside of densely populated cities and may travel in groups to improve fuel efficiency. This indicates the urgency of addressing the threat surface, or capitalizing on the benefits, is unlikely to subside in the near future.

3.3.3. Recommendations

Work should continue to interface with the international community and subject matter experts to identify continuing trends and predictions. Additionally, best practices can be recommended for auditing carriers and technology vendors for safety and adherence to security recommendations. The IAEA should be encouraged to address these emerging cyber-physical technologies and concerns in transportation safety and security by interacting with member states, training and workshop materials and publications.

4. SMART CITIES AND INFRASTRUCTURE

The proliferation of smart devices connected through IoT leads to a concept called the "Smart City," where all aspects of life have a digital imprint. Smart Cities originated to improve efficiency, reduce cost, and streamline traffic and economic gains, but the concept has expanded well beyond these examples. Similar to how IoT promotes physical objects to active participants in a network, Smart Cities tie together "smart" physical objects into one distributed network, promoting them into active business participants [11]. Smart cities use internet connected energy sources, buildings, transportation, health care, education, security, government, and environment. For instance: energy production can be predicted and optimized; buildings can self-diagnose HVAC faults, resulting in unsafe or environmentally uncomfortable situations; transportation and urban planning can include multi-functional systems to minimize traffic wait times and accidents; healthcare can better predict patient heath and effective treatment; safety systems can improve emergency prevention, alarm, and response [46].

Smart City planning, if widely realized, would be able to better distribute energy resources through "peak shaving" or "load smoothing," where during peak times energy production would decrease or increase, depending on need. Or for other resources, similar effects could be handled. For instance, vehicular accidents or emergencies could be identified more quickly, and the Smart City could respond with optimized, coordinated resources across departments and dynamic adjustment of traffic controls (e.g., traffic lights) to aid the flow of traffic around the accident.

The adoption of smart technology, from individual sensors to large multi-functional devices, creates a distributed, universal mesh network, where every object is connected seamlessly from geographic location to location. When a person crosses the street, they are detected and possibly connected by the traffic camera, the cell tower across the street, multiple building Wi-Fi points, and roadside assistance units (RSU's) used in traffic monitoring. That person's devices, such as smart watches and other wearable technology, also connect. These mesh networks allow for decentralized routing, such that any node in the network (e.g., the cell tower, RSU, or Wi-Fi point) route some traffic through it. This enables connections to chains of devices, all which might have different security measures in place.

The variety and shear number of sensors and network connections provides myriad openings for attack, and cities must consider a tradeoff: distributed networks are generally fault tolerant, which makes them obvious choices for high-risk environments such as nuclear power plants [6], but as in IoT and IoV, individual elements are often easy to hack, and reduce security for everyone connected. In this case, once an intruder is successful at accessing the system, he/she can turn the system against itself, by directly controlling the sensors and objects making up the Smart City. They could bring critical city infrastructure, such as traffic lights, or grid functions such as power distribution to a halt.

Smart Cities are also adopting Open Data Initiatives with increasing frequency. These are platforms where city governments make significant portions of their information public, from health inspections, school performances, crime statistics, agricultural production, and traffic data. These are often provided in standard, open-source formats for easy consumption. The United States requires localities to provide this data via statute, not policy [47]. Many other governments, including China, Russia, and the United Arab Emirates also participate in similar initiatives, as well as specific cities such as Kiev, Ukraine [48] and Baku, Azerbaijan [49]. These provide a wealth of information that municipalities use for analytics purposes and to train AI systems. This type of information may be leveraged by malicious actors, looking for information on traffic systems, patterns, or emergency services routes/timing [50]. This information could be used to identify likely travel routes, travel times, or detours of repeated shipments. It is conceivable that data on city traffic and planning could be leveraged in a coordinated attack in order to maximize the probability of success through well-informed selection of timing and location. For example, use traffic patterns discerned from Open Data may be used by an adversary to cause a

traffic incident at a pre-determined location in order to force the rerouting of a material shipment. By pinpointing the time and location of the staged traffic accident, the adversary can not only estimate their window of opportunity but maximize it based on common behaviour of city infrastructure. In effect, the adversaries can themselves become data driven. Member states with Open Data Initiatives are encourage to diligently review the available data, ensure it is properly anonymized and secure, and work to understand if it exposes any openings. Because the data is inherently intended to be accessed in an Open Data Initiative, the threat surface here is distinctly different than that of cybersecurity attacks or hacks. Some data sources should be excluded from the Open Data Initiative to reduce the risk from this threat surface. Training and workshops are needed to be prepared for an Open Data Initiative.

Conversely, the data collected by Smart City infrastructure can also improve the safety and security of nuclear material transport. Similar to how an adversary may make use of data for a coordinated attack, transportation safety and security professionals may make use of it to find the shipment time and route that minimizes risk. Especially where city data can be coupled with other intelligence, transportation professionals can receive not only better situational awareness, but real time updates on risk as events (related or unrelated to the shipment) unfold along a route.

Building and maintaining such smart infrastructure is costly, and therefore is more likely to be present in affluent countries. A recent report by McKinsey clearly showed that early adoption of smart technology is strongly dependent on GDP per capita, with stronger economies generally scoring higher for smart technology adoption. That said, even the most advanced cities scored modestly in adopting technology [51]. This survey, of only 50 cities, included cities from all six habited continents. Trends showed slightly stronger adoption in North America and Asia than other continents, and that the most active adoption has been in communication and mobility. This is unsurprising, as mobile technologies are ubiquitous, high impact, and have a large market. Larger cities in China (e.g., Beijing, Shanghai, Shenzhen), South Korea (Seoul), and the Middle East (e.g., Dubai) scored relatively high in the survey, on par with even more affluent cities in the United States such as New York, San Francisco, and Los Angeles. However, we note that less affluent countries adopting Open Data or Smart City initiatives may be those of greatest concern. With the rapidly decreasing cost of some Smart City devices (e.g., single-camera traffic light control systems) and public, cloud-based data sharing platforms [52] it is likely we will see adoption of this technology by countries who may not have the corresponding budgets to secure it properly.

4.1 Smart Communication and Networking in Transportation

In the transportation domain, Smart Cities provide much of the external infrastructure that IoV's use, such as Roadside Units (e.g., such as traffic control boxes, traffic lights) and much of the network infrastructure (e.g., cell towers, 5G access points). Both Smart Cities and IoV are naturally supported by similar network architecture. This architecture is divided into four layers, each layer interfacing with the adjacent one. First is an environmental layer, which takes data directly from sensors. This data must then be transported via the network to a remote monitoring hub for data analysis – the network access/transport layer and the coordinative computing layer. Finally, various applications can be run on this data to optimize traffic patterns or influence driving habits/conditions. **Error! Reference source not found.**, **Error! Reference source not found.**, shows a schematic of these layers and how they interconnect [12].

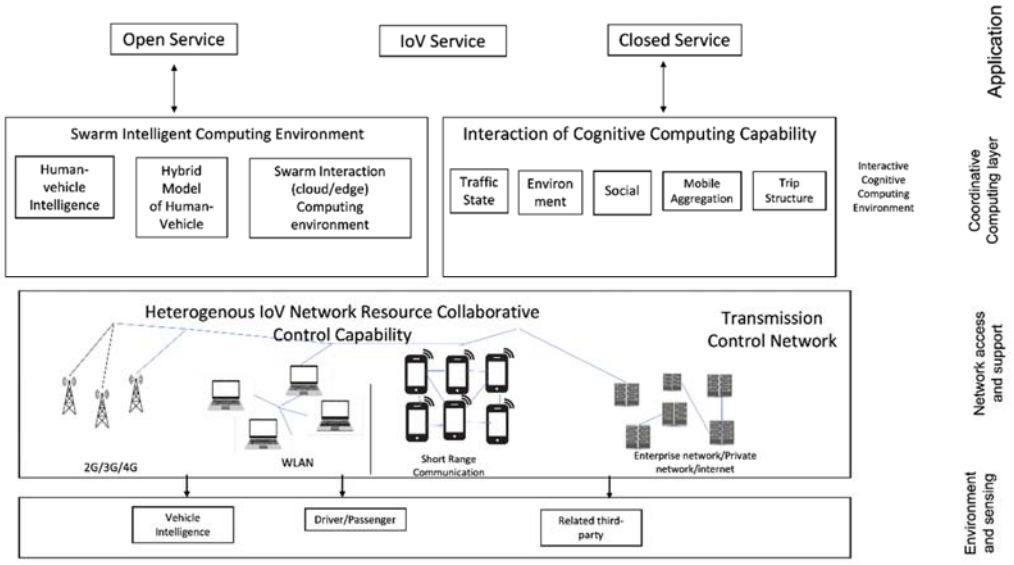

FIG. 1. Summary of IoV architecture layers.

These layers each require multiple types of technology, depending on the type of connection used. Typically, these can be divided into three types: vehicular communications, cellular/mobile communications, and short-range static communications [53]. Vehicular communications may include dedicated short-range communications (DSRC) or communications access for land mobiles (CALM). Short-range static methods might be Wi-Fi, ZigBee, or Bluetooth, while cellular and mobile networks include 4G/LTE/5G. Selection of systems depends on function, carrier, physical terrain and ultimately will depend on widespread acceptance.

Commercial and municipal acceptance is highly dependent on the feasibility of implementation as it translates to Return-On-Investment (ROI). For example, the type of cellular network chosen will depend on availability of power and networking infrastructure along the corridors of interest, as well as the radiofrequency propagation of the antenna across the terrain to be covered. For example, the limited range of 5G cellular coverage may be of little interest along a mountain corridor where new power lines will have to be installed. The lack of existing power and need for a large number of 5G antenna locations required to get meaningful corridor coverage can quickly reduce the ROI to a point that is not feasible for adoption. Network coverage can be simulated using readily available antenna specifications and topological maps, and installation costs estimated from regional data and subject matter experts. An assessment of 5G deployment feasibility based on cost and efficacy of the technology should be completed prior to embarking on a Smart City initiative.

These technologies all provide myriad vulnerabilities, but apart from specific issues discussed in Section **Error! Reference source not found.**, these are the subject of conventional cybersecurity research. Beyond direct hacking of systems, via sensors or networks, each of these layers provides new avenues for attacks. Once adversaries gain access to a smart system, they have ever increasing access to data and additional systems, where they can change access, alerts, and even machine learning/decision making algorithms and training data [29]. This means that developing and implementing secure systems with best practices, with multiple authentication and verification protocols, will become more important than ever.

4.2 Novel Threats and Cybersecurity in Smart Cities

With widespread distribution of technology along mesh networks, Smart Cities are particularly vulnerable to various threats. Due to the varied types of sensors and connections, understanding this threat landscape is an active area of research. Examples of threats include hacking of sensors, as discussed in Section **Error! Reference source not found.**: **Error! Reference source not found.**s, network infiltration, or algorithmic tampering (e.g., changing traffic light timing or emergency response routes). Threats can be either passive, where they monitor data traffic on machines, or active, where intruders make clear changes to systems or algorithms.

Attacks focusing on the environment and sensing layer typically focus on hacking individual sensors. As discussed above, sensors tend to have small form factors, meaning they have small memory and CPU resources. This typically makes sensors easy to hack through brute-force.

As sensor signals are read from vehicles or roadside units, these data can be aggregated throughout a smart city's wireless infrastructure, such as road-side towers or cameras [19]. In the future, it is possible that these devices won't just receive data but could also provide responses. For example, drivers could be alerted to dangerous conditions or even force vehicles to slow down or abruptly stop. Roadside Unit signals could be delayed, creating unsafe conditions, or "spoof" emergency vehicles to change traffic flow. These applications use both V2V and V2I layers and require layers of hardware and software implementation, both of which would create vulnerabilities.

As newer wireless infrastructure is installed, there will be a mix of new modern smart devices with legacy controllers and cameras. This mix of technology and legacy technology may remain isolated or may be piped in through the same controller. If they are combined, they likely run on the same fiber cable or VLAN as other systems [45]. This means that once one is infiltrated, others are vulnerable. These may include traffic signals and roadside devices, which are also connected to municipal and state IT systems.

Like IoV, the biggest vulnerabilities for Smart Cities are attacks on the networking and communication layer, typically through "pivoting." While typical cybersecurity best practices should always be in place, there are some novel threats to consider once a malicious actor gains access. Since many of the network nodes (e.g., roadside units, traffic control boxes) both receive and provide information, once an attacker is inside, they could implement a DDOS attack using the city itself, as a centralized hub of army bots, against a target [55, 56].

One industry expert cautioned that many of the devices used in the transportation side are not overly sophisticated ("legacy devices have the sophistication of pocket calculators") [45]. For instance, many devices may be kept with simple default passwords (e.g., "admin", "password", or "12345"), or are left on default ports. This provides clear means of access to tunnel into networking systems via these devices.

Once inside a network, the application layer can be targeted. It is hard to predict exactly what is vulnerable at this layer, as that is application specific. However, the use of 3rd party software or firmware only serves to increase this attack surface. At this point, the intruders have two choices: to passively watch data, such as with a sniffer or keystroke recorder, or to actively alter the applications and system. This could include spamming the system, installing malware worms, or more subtle attacks such as altering algorithms or poisoning data [29, 56]. One pertinent example would be to stop traffic, enabling theft or sabotage of cargo at one location, while rerouting the emergency services to the opposite end of town. If an individual vehicle is targeted, the vehicle could be turned off or remotely controlled, as has been demonstrated in practical studies [33].

One possible way to explore these networking and application scenarios is with variants of traditional Red Teaming. For instance, traditional Red Teaming may try to gain access to a network or sub-system. Because Smart Cities and Smart Vehicles have so many interconnected networking layers and access points, these Red Teaming exercises might require new approaches. For instance, attacks might be attempted from external to the network, via sensors or Wi-Fi, where they have no access to the system. In subsequent exercises the Red Team may be given access to certain subnetworks, symbolizing a successful penetration of a sensor or network component. The goal would be to probe vulnerabilities at each level to ensure accessing one level does not grant access to another. This could be used to test various V2V or V2I attacks in a safe controlled system, at multiple points of entry through a Smart City. If the Red Team succeeds, the effectiveness of intrusion detection software, can be tested. Critically, the geographically disperse network of Smart Cities, which often include both modern and legacy systems across varying networking protocols creates an additional consideration for cyber-physical Red Teaming. For example, rather than taking a purely cybersecurity penetration testing approach, Smart City Red Teams may drive around a city attempting to find legacy systems with lower barriers to compromise or find the ideal

combination of cyber vulnerability combined with minimal physical security to gain physical access to IT infrastructure. Regardless of whether Red Teaming is implemented, it is critical that simple computer security measures, such as repeated authentication and the principle of least privilege is enforced to reduce any potential adverse effects.

Over the next five years, it is expected that Smart City technology will gain a substantial foothold, starting in larger, well-funded cities. Many such cities (e.g., Chicago, Los Angeles, New York, Denver) already have Smart City plans, or are developing them to prepare for the arrival of this technology [45]. Important areas of emphasis include robust system security plans for each outside group that requires access to internal data, and proper data storage paradigms. Subject matter experts expect that each project and agency will tailor their data storage in accordance with their own responsibilities and needs [45]. This approach, where every individual city and agency builds their own data sources, pipelines, and security, presents the possibility of further vulnerabilities. These could be from lack of a viable cybersecurity strategy that adequately incorporates Smart City considerations (e.g., neglecting firewall configurations or monitoring appropriate for Smart City devices), or not following industry best-practices where those exist.

Industry experts view that until now, governments have largely reacted to the arrival of Smart City technology, instead of actively legislating for its arrival. One salient example is the arrival of motorized Scooters and ride sharing in large cities; these arrived without warning seemingly (and in the case of the City of Denver literally overnight [45]). In the future, it is hoped governments will actively work with private industry by contributing adoption standards, permit requirements, or negotiate infrastructure additions to increase market penetration. As another example, cities might grant permission or planning for autonomous ride sharing services, but not engineering support. This will provide some oversight and needed safety standards [45], especially as this technology becomes more widespread. As one SME observed regarding Smart City technology and security, “The government just doesn’t move that fast. You see accelerated innovation and adoption driven from the private sector [45].” The IAEA could provide a forum to facilitate communication across Smart City stakeholders and ensure a coherent approach to security that keeps up with the space of technology.

4.3 Threats, Benefits and Recommendations

4.3.1 Benefits and Threats

The benefits of Smart Cities are numerous, and include reliable, redundant wireless mesh networks. These networks allow for fast, widely available internet connectivity which is useful in tracking freight. Smart Cities also allow for opportunities to streamline traffic, reducing congestion and eliminating unnecessary delays. However, with the addition of technological components, the threat landscape also increases. Many Smart City components do not only passively receive data, but actively push data to users. This could be used to turn a city into a network of malicious devices. For instance, information about traffic or emergency services may be conveyed to vehicles. In extreme scenarios, vehicles may be stopped or redirected to routes intended to mislead. Or a compromised city could issue a DDOS attack using the Smart City sensors and mesh network of a city.

Like the Internet of Vehicles, Smart Cities are vulnerable to traditional cybersecurity attacks but often require novel preventative measures. Many traditional attacks, such as DDOS attacks, will still focus on components with limited form factor, memory, and battery power.

4.3.2 Maturity and Urgency

Adoption of Smart City Initiatives have already occurred, and it is expected that within 3-5 years many large cities throughout the world will continue to implement Smart City solutions [15, 45]. These include mesh-networking, and a wide array of sensors, and adaptive traffic systems with emergency response optimization.

Smart Cities often include commitments to Open Data Initiatives, where aggregated data is kept and shared openly in standard formats. This provides openings to understand inefficiencies in transportation in cities, as well as potential vulnerabilities depending on how the data is presented, and what data is presented. Such initiatives have been adopted both domestically and internationally. The sensitivity of data stored varies by city.

The maturity of the technology is at the point of commercialization and therefore this is considered an urgent topic as reduction in technology costs will only expand its adoption.

4.3.3 Recommendations

Awareness is the first step to educating Smart City planners and implementers. Training and workshops should be made available to highlight the benefits and also point out the vulnerabilities and recommend practices that can lower the risk of potential malicious monitoring. Various avenues exist that could be matched to country sophistication, from simple location tracking of cargo containers to geo-fencing of routes and using municipal traffic cameras to actively monitor from a command center.

An additional recommendation is training and education to implement robust security plans and periodic security audits for any group granted access to Smart City internal data. This will help discover potential vulnerabilities, and ensure the system remains uncompromised.

5. DIGITIZATION OF TRANSPORTATION MANAGEMENT

The transportation and logistics industry has undergone tremendous change over the last decade, not only in terms of technology attached to cargo and transport, but in the development and implementation of new transportation management techniques. Until recently, delivery operators were regarded as a necessary but non-core function; with the advent of data-driven processes, organizations have realized that their logistics chain was a strategic component [30]. By optimizing and streamlining transportation and management systems, time could be saved, delivery speed increased, and money saved. For instance, time spent preparing and sending invoices is a significant expense; switching to automated systems can reduce processing time by 40%, drastically reducing costs [9].

The basic functions performed by Transportation Management Systems (TMS) includes planning and decision making for given shipments and prioritization of shipments, transportation cost estimating and invoicing, carrier outsourcing, post-service evaluation, and determination of key performance indicators. Most of these systems have Fleet Management Systems directly embedded inside them, and those that don't are provide ways to connect with external sources. Previously, all this was done by hand and required substantial time to execute. Each step required knowledge of clients, their needs, available routes and drivers, and invoicing. It's no surprise that market acceptance of Transportation Management Systems has rapidly accelerated: In 2014, only 36% of shippers used one; by 2020, roughly 80% of large and mid-sized shipping companies used one [9]. These companies, those with 51 or more trucks, found increased productivity from the technical innovation. Only about half of smaller companies, those with 50 trucks or fewer, have adopted TMS's, likely due to decreased margins when competing with larger, better managed fleets. Adoption of TMS has also increased because of the 2017 ELD mandate requiring electronic logging of freight. Most TMS systems can directly process the ELD feed. Other important checks could be accomplished via geo-fencing the "final mile." While cargo theft is present at all points of the chain, trucking is by far still the least secure mode of transport, compared with air, ocean, or rail [21]. Monitoring the first and last mile provides quick identification at the most vulnerable points should anything go wrong [18, 21, 57].

Advanced TMS systems can also integrate seamlessly into a connected smart transport system. This means that connecting to trucks and cargo will enable additional monitoring and transparency in shipping, all from one interface or application. Many integrate directly with Warehouse Management Systems and Inventory Management Systems. Therefore, TMS oversees the entire shipping process, and coordinate with each external company or entity. This may include payroll and human resources, as this information may be needed to contract and schedule drivers. The inclusion of human resource data can constitute a tremendous risk. Compromised personnel credentials, or PII necessary to forge those credentials, is an ideal attack vector for malicious actors looking to impersonate shipping personnel. Effective impersonation will allow the adversary to gain direct control of material shipments and exfiltrate the cargo in ways that become more difficult to detect in a timely manner.

Aside from invoicing and personnel management, these TMS will be an integral part of the future Smart City landscape. These are the systems that are, and will be, powering traffic and shipping route optimization and scheduling. The data generated by truck routes will provide information for traffic control. Additionally, they are an interface between the truck and Smart City resources, such as identifying routine or emergency maintenance or part failure. TMS programs are then a viable vector into a Smart City ecosystem.

The market is dominated by four major TMS providers: Innovative Trimble, LoadMaster, TMW Suite, and TruckMate. For the carriers that use a TMS, these control around 80% of the US domestic market [58]. Similar

consolidation exists in the international market, although there are a growing number of vendors focusing specifically on the Asian market [59]. Currently, many of these TMS are located on-premises because many of the carriers want to maintain control of their data. However, some vendors are now offering a cloud-based TMS, utilizing the Software-as-a-Service (SaaS) business model. While adoption of cloud based TMS is presently low, the technology is commercially available and a shift towards such products is likely within the next 3-5 years [35]. These new TMS, however, expand threat surfaces to include cloud-based cybersecurity attacks. This shifts much of the security management and protocols from the shippers to the TMS vendor. In some cases, (e.g., small, unsophisticated carriers) this may mean better security than on their on-premises systems. However, a large TMS cloud provider is also a more attractive target with a complex risk profile that potentially impacts multiple carriers simultaneous. For example, a compromised cloud TMS system could result in malicious actors gaining access to a tremendous amount of data on cargo manifests, routes and shipping personnel.

Freight carriers also rely on telematics data. Like the TMS market, there are several popular companies which control a majority of the industry (e.g., OmniTracs, Deep Trucking) [58]. These companies individually control the data for logging, vehicle information, shipments, and drivers. They often don't have specific information on the exact commodity being transported but provide a nearly full picture of the entire route and transportation chain. Visibility tools are currently being developed to merge this data with TMS to help develop an end-to-end understanding of cargo in transit. These tools are extremely powerful for optimizing routes but increase the complexity of the cybersecurity threat landscape.

These markets are likely to see rapid change and increased adoption over the next 3-5 years, with cloud based TMS and telematics services gaining substantial adoption [35]. Traditional providers of these technology are already losing market share to newer carriers using lightweight, modular solutions in their transportation chain [58]. These solutions include easily commoditized hardware such as Bluetooth and cameras. As companies enter or exit the market, care must be taken to ensure that any data stored by one vendor's product is properly transferred and chain of custody maintained. For instance, how emerging vendors handle data should be verified and security protocols audited before being used. Similarly, if a vendor exits the market (e.g., going out of business or getting acquired as is likely in a rapidly evolving industry), any data that vendor has should be properly disposed of. Care should be taken when considering a TMS to understand what security and data usage aspect must be vetted, as well as what to require from a vendor.

In addition to TMS, electronic manifests (eManifests) have been introduced at border crossings, such as the U.S./Canada border. eManifests are usually government sponsored services which allow pre-arrival data transmission. These services include information on cargo, value, crossing location, and the inclusion of any sensitive information [60]. This includes the type and amount of any radionuclides or nuclear reactor equipment [61]. These records are stored in the destination country's system and are kept for several years. Therefore, data might be kept on insecure servers or be accessed later to identify routes or repeated shipments. These data are closely related to those stored by TMS, and likely generated from TMS, but will be stored by various governmental groups in different countries. This provides yet more opportunity for sensitive data to become compromised.

5.1 Cybersecurity Threat in Transportation Management

It is well known in the industry that cybersecurity in the trucking industry, including TMS providers, is "horrible, with very weak cybersecurity culture [58]." Although many of the small/mid-sized carriers are not attractive targets due to their small data records, larger carriers are excellent targets with rich data sources. TMS programs provide a direct vector for compromising this data, especially a cloud based TMS where a compromised system potentially gives access to the data of a large number of carriers. If one of the major TMS providers was penetrated, an intruder could then imbed viruses or ransomware directly into their clients, or alter shipping carriers, routes or employee records directly without any notice, making it easy to confiscate or alter the cargo.

Several newer TMS systems are moving into the Cloud, storing, and manipulating data there. This makes them extremely powerful and flexible, but also provides further security openings. Although it is possible for unintended users to gain access through vulnerabilities in sensors or network openings, more likely scenarios are directly through human manipulation. This is similar to traditional cybersecurity threats, such as phishing or social engineering. A recent Office of International Nuclear Security paper provided substantial detail on human-based cybersecurity threat vectors [29].

The transportation industry is ripe for these attacks. The transportation industry dominated by small, owner-operated fleets, with 95% of companies managing less than 20 trucks [62]. Small and mid-sized fleets are disproportionately at risk for having a non-diversified customer base, and many therefore focus on specialized loads that larger companies may not be interested in accommodating. This means small shifts in demand may quickly bankrupt some companies. In fact, over 1,000 truck companies went bankrupt in both 2018 and 2019; due to COVID the number was over 3,000 in 2020 [63]. With such small margins and such high turnover these companies are often looking to cut costs, and therefore look for local solutions to manage their data operations rather than verified and trustworthy vendors.

Before implementing a TMS, the transportation professional should consult a security professional regarding best practices and cybersecurity awareness training that focuses on the transport-specific considerations in defending against these attacks. This may include educating employees with privileged access about password creation and enforcing two-factor authentication. For instance, using PII for passwords or password hints allow a quick scan of Google results and Facebook posts to provide some access to private phones or e-mail accounts. There have been several cases brought to court from University of South Florida where individuals have guessed passwords and PINs to access one e-mail account, to then reset the password for related e-mail accounts and then used those accounts to commit theft and other crimes [32].

For carriers specializing in hazardous material transport, it is likely they have already considered many of these issues and selected appropriate technology for their business model. Some carriers may require their drivers to have special training, or only use certain technology (e.g., certain phones or phone carriers) [58]. They also might include additional cameras or sensors to monitor cargo in real time or use TMS specifically designed with additional protections. The problem is there is a huge diversity of business models in the trucking industry [58], and carriers need to be vetted and/or educated.

TMS systems have access to shipping manifests, banking information, shipping routes, and have access to individual truck sensors and connections to Smart City services. For these reasons granting external access to TMS systems is incredibly risky, and their development and implementation needs to be carefully considered. Therefore, systems should include machine-learning/deep-learning based passive monitoring systems, such as intrusion detection programs, in TMS cloud servers. This way any abnormal behaviour can be immediately flagged and investigated. These solutions are becoming popular, with widespread adoption expected in the coming years. The key to remember about TMS security incidents is that the root cause of incidents is rarely just about the technology, but rather the implementation of it and how it’s used.

5.2 Threats, Benefits and Recommendations

5.2.1 Benefits and Threats

Transportation Management Systems are prevalent in the shipping field now and can provide enhanced transparency and management for partners transporting sensitive material. This will help create proper records, shipment routes, and provide baseline key performance metrics to evaluate success and safety across both individual shipments and in aggregate.

However, currently available TMS programs do not provide shipment routes based on security considerations that may be critical to nuclear transportation. Naïve usage of TMS-provided routes may lead to transit corridors a nuclear transportation security professional may otherwise recommend. It is important that carriers making use of these systems be aware that no security or threat consideration is typically included in TMS routing. Furthermore, although there are benefits of efficiency to having a consolidated record and access point, the vulnerabilities must also be evaluated created by a central access point to shipping manifests, billing records, security information, and the PII of individual cargo handlers.

5.2.2 Maturity and Urgency

TMS programs are available as commercial-off-the-shelf products with high adoption for on-premises solutions. Cloud based TMS are commercially available as well, but currently experience lower adoption rates. However, the cloud based TMS are expected to have high adoption within the next 3-5 year. The maturity of the

technology is at the point of market penetration with rapid changes expected in the near-term. Therefore, we consider this an urgent topic due to its potential impact as a risk surface for transportation security.

5.2.3 Recommendations

Standards for what make an appropriate TMS should be considered. TMS services that are via Software-as-a-Service, and/or exist as Cloud-based software should involve different standards than other programs living on local servers. It is recommended that transportation security experts investigate specific cybersecurity best practices and recommendations for TMS programs, including a deep dive into large vendors in their region. This will help guide development of relevant standards and proper education for the transportation industry.

When a vendor produces a cloud based TMS capable of capturing substantial market share it will likely disrupt the market, leading to consolidation as well as new vendors entering the space. Transportation security experts should continue to monitor the situation, and work with the industry to identify appropriate TMS products that will ensure proper confidentiality, integrity and availability for their data.

Traditional cybersecurity attacks are the most viable threat vector for TMS systems, and once a system is penetrated, intruders have access to everything from shipping routes to client information, and possibly to personnel or contractor information. Training should be added to existing cybersecurity training that TMS vulnerabilities and limitations. This may include educating partners on proper vetting of local carriers to ensure they are using best practices and have proper software support by reputable vendors, as well as best practices in educating transportation personnel against social engineering attacks and the vulnerabilities of human resource data leading to impersonation attacks.

6. CONCLUSIONS

The adoption of smart technology is accelerating, and will become standard on new transportation vehicles, adopted by transportation carriers, and implemented in Smart Cities increasingly over the next 5 years. This assessment has intentionally focused on those technologies that have, or are highly likely to, experience substantial market penetration and adoption. Each of these systems, from sensors to networks and cloud-based management software provides multiple areas for improved transparency and cybersecurity vulnerabilities. This paper provides key insights to the benefits and emerging threats posed by this new technology. Subject matter experts in cybersecurity and transportation security should work together in a cross-functional manner to address this emerging cyber-physical technologies landscape.

Previously, sensitive cargo, such as hazardous material, was most vulnerable when stopped for inspection (e.g., customs) or when changing carriers. With smart technology and distributed mesh networks, cargo is increasingly vulnerable every step of the way where monitoring and threat detection becomes dependent on remote telemetry. Passing cars could jam or spoof GPS signals or connect with Bluetooth devices, or attackers could infiltrate transportation management software to gain access to sensitive shipping manifests and routes.

However, many of these threat vectors are not new and can be addressed through traditional cybersecurity, albeit with some transportation-specific situational awareness required. However, novel threats do exist, often because the infrastructure of IoT allows systems to push behaviour back to the equipment connecting to it. This creates a geo-spatial diverse cyber-physical system. For example, adversaries could change traffic signal timing, reroute emergency services, or take control over vehicles. They could use all the sensor in a Smart City to launch a coordinated DDOS attack on an adversary.

The IAEA is encouraged to address this emerging cyber-physical technology landscape and bring together member states key stakeholders in cybersecurity, networking security, and transportation management to develop training and workshop materials, as well as, publications that address sensor types, interface, and security, as well as communication protocols between devices, cars, and networks. Strict authentication and encryption standards should be addressed for Smart City infrastructure. For instance, external network access should require two factor authentication where possible, and customer/invoicing information should be on separate, isolated networks from shipping information within a TMS. Similarly, hardware devices, such as cameras, need to be on isolated networks as well, and all external media, such as thumb drives and hard disks, should be patched and inspected before connection to the network.

Additional approaches may include a combination of simulation and cyber-physical transportation Red Teaming. These exercises could simulate attacks on multiple level: cargo, truck, and network. These exercises will be critical to identify vulnerabilities at each level of a Smart City and Smart Vehicle. This is an active area of research, and further investigation on their feasibility, limitations, and use-cases is warranted.

The future of Smart Cities, including Transportation Technology, Open Data Initiatives, and cloud-based Transportation Management Systems will be more fully realized in the next 5 years. These advances will disrupt the shipping industry, including nuclear and radioactive material shippers, by cutting costs and increasing efficiencies. It is important to be proactive in understanding the technology and work with partner countries to identify, introduce, and maintain best practices for evolving transportation security. This is especially true where each of the technologies discussed here is already commercially viable with a meaningful level of adoption, indicating high maturity and an urgent need to address with member states.

ACKNOWLEDGEMENTS

The authors acknowledge the support of the United States Department of Energy National Nuclear Security Administration Office of International Nuclear Security and the team that evaluates emerging threats and technologies.

REFERENCES

[1] IAEA, "Transport Security: Nuclear safety and security," 2021. [Online]. Available: https://www.iaea.org/topics/transport-security.

[2] UNITED STATES NUCLEAR REGULATORY COMMISSION, "Materials Transportation," December 2020. [Online]. Available: https://www.nrc.gov/materials/transportation.html.

[3] UNITED STATES REGULATORY COMMISSION, "Revision 1 Advance Notification of Import Shipment," [Online]. [Accessed 11 June 2020].

[4] STIMSON CENTER, "Governing Uranium: From Pit to Port," May 2020. [Online]. Available: http://uranium.stimson.org/pit_to_port/.

[5] BATEMAN A., BONANNI L., "What Supply Chain Transparency Really Means," Harvard Business Review, August 2019.

[6] THIBAUD M., CHI H., ZHOU W., PIRAMUTHU S., "Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review," Decision Support Systems, vol. 108, pp. 79-95, 2018.

[7] FREIGHTWAVES INC., "2020 Freight Market Outlook," 2020.

[8] TRANSFIX, "Get Ahead of the Curve: Learning from the Past to Prepare for the Future," FreightWaves, 2020.

[9] VECTOR, FREIGHTWAVES, "2020 Tech Trends and Challenges in Trucking," FreightWaves, 2020.

[10] NUCLEAR TRANSPORT SOLUTIONS, "Nuclear Transport Solutions," May 2021. [Online]. Available: https://nucleartransportsolutions.com/.

[11] RAGHUVANSHI A., KUMAR SINGH U., "Internet of Things for Smart Cities- Security Issues and Challenges," in Materials Today: Proceedings, 2020.

[12] SHARMA S., KAUSHIK B., "A survey on internet of vehicles: Applications, security issues & solutions," Vehicular Communications, vol. 20, 2019.

[13] LIU Y., BI J., YANG J., "Research on Vehicular Ad Hoc Networks," in 2009 Chinese Control and Decision Conference, Guilin, China, 2009.

[14] OVERSTREET W., Interviewee, Vice President of Strategic Partnerships, Gridsmart Technologies. [Interview]. 2018.

[15] NICHOLS A., Interviewee, Professor of Transportation Engineering, Marshall University. [Interview]. 10 May 2021.

[16] DELOITTE INSIGHTS, "Autonomous trucks lead the way," 2021.

[17] SOMERVILLE H., "Self-driving trucks begin mail delivery test for U.S. Postal Service," Reuters, 21 May 2019.

[18] DESCARTES SYSTEMS GROUP, INC., "The Future of Pharmaceutical Shipment Tracking," 2020.

[19] GUERRERO-IBÁÑEZ J., ZEADALLY S., CONTRERAS-CASTILLO J., "Sensor Technologies for Intelligent Transportation Systems," Sensors, vol. 18, no. 4, p. 1212, 2018.

[20] ABDELHAMID S., HASSANEIN H.S., TAKAHARA G., "Vehicle as a Mobile Sensor," in Procedia Computer Science (FNC-2014), 2014.

[21] OVERHAUL, "Redefining Supply Chain Security," 2020.

[22] IAEA NSS 9-G (Rev. 1), Security of Radioactive Material in Transport 9-G, Vienna: International Atomic Energy Agency, 2020.

[23] IAEA NSS 17, Computer Security at Nuclear Facilities: Technical Guidance Reference Manual, Vienna: International Atomic Energy Agency, 2011.

[24] IAEA NSS 33-T, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, Vienna: International Atomic Energy Agency, 2018.

[25] DEPARTMENT OF TRANSPORTATION: FEDERAL MOTOR CARRIER SAFETY ADMINISTRATION, "Federal Register, Rules and Regulations," 2015. [Online]. Available: https://www.govinfo.gov/content/pkg/FR-2015-12-16/pdf/2015-31336.pdf. [Accessed 2020].

[26] GEOTAB, "Geotab + dash cams: a powerful combination," Geotab, [Online]. Available: https://www.geotab.com/. [Accessed May 2021].

[27] SAFETY VISION, [Online]. Available: http://www.safetyvision.com/sites/safetyvision.com/files/RearVision_Brochure_2020_Final_1.pdf. [Accessed January 2021].

[28] HENAO A., Interviewee, National Renewable Energy Laboratory. [Interview]. 2021.

[29] BERTOLLI M., BRAYFINDLEY E., DAYMAN K., EDMUNDS T., EGGERS S., HAGEN A., HITE J., LUTTMAN A., PHATHANAPIROM B., PRESTON J., SAMPLE C., STEWART S., "Artificial Intelligence and Machine Learning – Emerging Technologies and Applications in Nuclear Security," Pacific Northwest National Laboratory, PNNL-SA-162157, Artificial Intelligence and Machine Learning – Emerging Technologies and Applications in Nuclear Security, T, 2021.

[30] PARAGON SOFTWARE SYSTEMS, "Modern Delivery Route Management," 2020.

[31] FREIGHTWAVES, "Government & Aerospace Report," 2020.

[32] GUILLETTE D., Interviewee, Associate Director of Security Operations and Engineering, University of South Florida. [Interview]. 25 January 2021.

[33] GREENBERG A., "Hackers Remotely Kill a Jeep on the Highway - With Me in It," WIRED, 21 July 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Accessed 25 Jan. 2021].

[34] BICKNELL A., "Top 5 Bluetooth Security Vulnerabilities," Global Sign, April 2020. [Online]. Available: https://www.globalsign.com/en/blog/top-5-bluetooth-security-vulnerabilities. [Accessed April 2021].

[35] ELKHALIL A., ZHANG J., "n efficient signcryption of heterogeneous systems for Internet of Vehicles," Journal of Systems Architecture, 2020.

[36] ZHANG Q., LI Y., WANG R., LI J., GAN Y., ZHANG Y., YU X., "Blockchain-based asymmetric group key agreement protocol for internet of vehicles," Computers and Electrical Engineering, vol. 86, 2020.

[37] MAERSK, "TradeLens Blockchain-Enabled Digital Shipping Platform Continues Expansion with Addition of Major Ocean Carriers Hapag-Lloyd and Ocean Network Express," Maersk, July 2019. [Online]. Available: https://www.tradelens.com/.

[38] KUEHNE + NAGEL GROUP, "Kuehne + Nagel Deploys Blockchain Technology for VGM Portal," Nuehne + Nagel, 2018.

[39] IBM, "IBM Food Trust. A New Era for the World's Food Supply," IBM, May 2021. [Online]. Available: https://www.ibm.com/blockchain/solutions/food-trust.

[40] REDINI M., "COVID-19 and the New Normal in LTL Shipping," Echo Transportation, March 2020. [Online]. Available: https://www.echo.com/blog/covid-19-and-new-normal-ltl-shipping.

[41] BANSAL P., SHARMA S., PRAKASH A., "A Novel approach for Detection of Distributed Denial of Service attack in VANET," International Journal of Computer Applications, vol. 120, 2015.

[42] KREBS B., "Target Hackers Broke in Via HVAC Company," Krebs on Security, 14 Feb 2014. [Online]. Available: https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/. [Accessed 25 Jan 2021].

[43] JONES S., "Apps Make It Easy for Teens to Fake Their Location," NBC CT, 4 Sept. 2019.

[44] STRUNSKY S., "N.J. man fined $32K for illegal GPS device that disrupted Newark airport system," NJ.com, 30 March 2019. [Online]. Available: https://www.nj.com/news/2013/08/man_fined_32000_for_blocking_newark_airport_tracking_system.html. [Accessed 25 Jan. 2021].

[45] THOMAS S., Interviewee, Principal of Apex Design. [Interview].

[46] CHEN D., WAWRZYNSKI P., LV Z., "Cyber security in smart cities: A review of deep learning-based applications and case studies," Sustainable Cities and Society, vol. 66, 2021.

[47] UNITED STATES GOVERNMENT, "Data.gov Open Government," [Online]. Available: https://www.data.gov/. [Accessed April 2020].

[48] KYIV CITY COUNCIL, "KyivSmartCity," [Online]. Available: https://www.kyivsmartcity.com/en/projects/open-data-portal/. [Accessed May 2021].

[49] MINISTRY OF TRANSPORT, COMMUNICATIONS, AND HIGH TECHNOLOGIES OF THE REPUBLIC OF AZERBAIJAN, "Open Data Portal of the Republic of Azerbaijan," [Online]. Available: https://www.opendata.az/en. [Accessed May 2021].

[50] MCKINSEY GLOBAL INSTITUTE, "Open data: Unlocking innovation and performance with liquid information," McKinsey & Company, 2013.

[51] MCKINSEY GLOBAL INSTITUTE, "Smart Cities: Digital Solutions for a More Liveable Future," McKinsey & Company, 2018.
[52] SODA DEVELOPERS, "Building something using data?," Socrata, [Online]. Available: https://dev.socrata.com/. [Accessed May 2021].
[53] KAIWARTYA O., ABDULLAH A., CAO Y., ALTAMEEM A., PRASAD M., LIN C., LIU X., "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," IEEE Access, vol. 4, pp. 5356-5373, 2016.
[54] YANG F., LI J., LEI T., WANG S., "Architecture and key technologies for Internet of Vehicles: a survey," Journal of Communications and Information Networks, vol. 2, pp. 1-17, 2017.
[55] ILASCU I., "IoT botnets responsible for more powerful DDoS attacks," Bitdefender BOX, 2018. [Online]. Available: https://www.bitdefender.com/box/blog/iot-news/iot-botnets-responsible-powerful-ddos-attacks/.
[56] WATROBSKI P., KLOSTERMAN J., BARKER W., SOUPPAYA M., "Methodology for Characterizing Network Behavior of Internet of Things Devices," National Institute of Standards and Technology, 2020.
[57] OVERHAUL AND FREIGHTWAVES, "Command and Control for Pharmaceutical Logistics," 2020.
[58] APPLEFELD S., Interviewee, CTO of ASR Solutions. [Interview].
[59] DE MUYNCK B., JOHNS B., DURAN O., WEST C., "Magic Quadrant for Transportation Management Systems," Gardner, 2021.
[60] FLS TRANSPORT, "The Complete Guide to Cross-Border Freight," 2020.
[61] U.S. CUSTOMS AND BORDER CONTROL, "Importing into the United States: A Guide for Commercial Importers," 2006. [Online]. Available: https://www.cbp.gov/sites/default/files/documents/Importing%20into%20the%20U.S.pdf. [Accessed April 2021].
[62] OWNER OPERATED INDEPENDENT DRIVERS ASSOCIATION, "Owner Operated Industry Facts," December 2020. [Online]. Available: https://www.ooida.com/wp-content/uploads/2021/03/Trucking-Facts.pdf. [Accessed April 2021].
[63] SMITH J., " Trucking Failures Surged Last Year Under Pandemic," Wall Street Journal, 8 February 2021.
[64] MURPHY K., "America Has a GPS Problem," The New York Times, 23 Jan. 2021.
[65] MACAULAY T., "Chapter 6 - Safety Requirements in the Internet of Things," in RIoT Control: Understanding and Managing Risks and the Internet of Things, Elsevier Inc., 2017, pp. 113-123.
[66] LIU Y., BI J., YANG J., "Research on Vehicular Ad Hoc Networks," in 2009 Chinese Control and Decision Conference, Guilin, China, 2009.
[67] JENG. S., CHU L., "Vehicle Reidentification with the Inductive Loop Signature Technology," Journal of the Eastern Asia Society for Transportation Studies, vol. 10, 2013.
[68] HE Y., RAHMAN M., AKIN M., WANG Y., DEY K., SHI X., "Connected Vehicle Technology for Improved Multimodal Winter Travel: Agency Perspective and a Conceptual Exploration," Sustainability, vol. 12, 2020.
[69] GREENBERG A., "Hackers Remotely Kill a Jeep on the Highway—With Me in It," Wired, 21 July 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[70] DONGLIANG CHEN P., "Cyber security in smart cities: A review of deep learning-based applications and case studies," Sustainable Cities and Society, vol. 66, 2021.
[71] NETRADYNE (WITH FREIGHTWAVES), "Using Artifical Intelligence to Humanize Analytics for Maximum Efficiency".
[72] PROOFPOINT, INC., "Protecting People 2019: A Global Cybersecurity Analysis of Vulnerability, Attacks, and Privilege," 2019.
[73] WEJO, Optimizing traffic signal performance to enhance safety and reduce infrastructure cost, YouTube, 2020.
[74] ARTIFICIAL INTELLIGENCE MACHINE LEARNING (AIML) WORKING GROUP, EMERGING THREATS AND TECHNOLOGIES, "Artificial Intelligence – Applications to and Implications for Nuclear Security Emerging Threats and Technologies".
[75] AIML WORKING GROUP, EMERGING THREATS AND TECHNOLOGIES, "Artificial Intelligence for Social Engineering," 2020.
[76] PENSKE, "4 Ways Supply Chain Visibility Drives Results".