A Forensic-Ready Intelligent Transportation System

Abdellah Akilal[1(✉)] and M-Tahar Kechadi[2]

[1] Laboratoire d'informatique Medicale Limed, Faculte des Sciences Éxactes, Université A. Mira Bejaia, Bejaia, Algeria
abdellah.akilal@univ-bejaia.dz

[2] School of Computer Science and Informatics, University College Dublin, Dublin, Ireland
tahar.kechadi@ucd.ie

Abstract. The Intelligent transportation system (ITS) is a part of a smart city, and will for sure become a reality in the coming decades if not years. Viewed as a pivotal element in an economy, its market size is predicted to grow and governments are already investing in either development or deployment and maintenance. Researchers on the other hand have already investigated its feasibility and provided multiple architectures. Even if the predicted economic venues are interesting, several challenges related to security, privacy, resiliency are still concerning. New attack surfaces are emerging, incidents and cyber attacks are occurring. The omni-connectivity attribute of smart cities is inducing new risks where a digital vulnerability may be exploited to damage physical assets or endanger travellers' safety. If safety is a necessity, the preparedness to conduct a digital forensic investigation is also important. This paper focuses on the ITS Digital Forensic Readiness (DFR). More precisely, we aim to align the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) with the digital forensics readiness best practices in particular the ISO/IEC 27043:2015 standard.

Keywords: ITS · DFR · ARC-IT · ISO/IEC/27043/2015 · Cyber crime · Safety

1 Introduction

The Intelligent Transportation System (ITS) global market size is predicted to grow from $1643.8 million in 2018 to $8474.2 million by 2026 [13]. Multiple countries are already investing in the deployment and the maintenance of these critical infrastructures. For example, the U.S is already investing more than $25 billion in deployed ITS. The economic and societal usage of ITS by American travellers is exceeding $2.3 billion annually [3]. The critical nature of ITS, and the diversity of its ecosystem (components, technologies, stakeholders, etc.) have

S. Paiva et al. (Eds.): SmartCity360° 2021, LNICST 442, pp. 617–630, 2022.
https://doi.org/10.1007/978-3-031-06371-8_39

led several countries to deploy efforts towards the standardization and the development of associated architectures [22]. Therefore, there is abundant work issued from governmental agencies and researchers, such as the ARC-IT (USA) [4], the ITS architecture for Canada [2], and Europe [6,28].

Even if there is a significant advancement in ITS research, there are still several challenges and open questions. In fact, security, privacy, resiliency and safety are among the ITS concerning issues [7,19]. In regards to security, an ITS is exposed to at least three attack vectors (physical, network and wireless) [11]. Moreover, multiple ITS real-world attacks have taken place from 2016 to 2017 ranging from road sign hack [17] to ransomware attacks [11]. More recently, some major Metropolitan Transportation Authority's computer systems were the target of cyber crime [12,31].

Incidents and cyber crimes happen. In this paper, we aim to ensure the ITS due forensic readiness *(i.e., enhance the ITS with capabilities that ease the collection of digital evidence with a minimum disruption and less economic impact from a potential investigation)*. For this purpose, we investigate the opportunities of aligning the ISO/IEC 27043:2015 incident investigation principles and processes standard [15] with the ARC-IT architecture [4].

The rest of this paper is structured as follows: Sect. 2 presents some related works on ITS architectures, digital forensic readiness, forensic-by-design and forensic-ready systems. We then provide details on the ARC-IT and the ISO/IEC 27043:2015 in Sect. 3. In Sect. 4, we investigate the emerging opportunities and challenges from the integration of forensic requirements into an ITS architecture, and we conclude this paper in Sect. 5.

2 Literature Review

The economic impact of transportation is not be demonstrated. In fact, transportation is present in every single aspect of citizens daily life. From travelling to goods and merchandise delivery, the transport sector is a central nerve to a national economy. Thus, it is not astonishing to observe the symbiosis between this sector and the technological evolution in other domains. The ITS takes its origin from the USA in the 20th century [1,22], but it is gaining worldwide attention nowadays. Several projects and architectures have emerged from conjoint efforts of both government bodies and researchers [2,4,6]. The evolution of communication technologies, sensors and computation, in addition to customers needs has led to the emergence of a subset of ITS namely Cooperative Intelligent Transportation Systems (C-ITS) that takes advantage of the communication and cooperation between its participants [1].

Even though ITS benefit from consequent funds and technological advancement from other domains, there are still some challenging issues. In fact, security, privacy and resiliency are among the top concerning problems [7,19]. Moreover, incident and cyber attack are already taking place in ITS [11,12,17,31] and the worst scenario that may happen is the exploitation of a security vulnerability to endanger the travellers' safety [16,23]. Nonetheless, in case of an incident or

cyber crime, a forensic investigation is required and initiated. However, the first step in this process focuses on preparedness. The main motive of this study is to enhance the ability of an ITS to collect admissible digital evidence.

Digital Forensic Readiness (DFR) represents the *ability* of an organization or a system to collect admissible digital evidence, whilst minimizing the costs of an investigation. The necessity to enable a system with capabilities to ensure its' forensic readiness was first expressed by [29], later [27] formulated it as a ten step process. There is an abundant literature on DFR; While some researchers focused on the DFR context *(i.e., impact of DFR on domains, such as organization, networks* [5], *and the Cloud computing* [21], *etc.)*, others investigated the standardization aspect such as the work done by [32] that was later included in the ISO/IEC/27043:2015(E) standard [15] *(details on this standard will be provided in* Sect. 3). However, one of the most significant shifts in the DFR perspective is due to [26]. The Forensic-by-design strategy [26] aims towards the integration of forensic requirements during relevant phases of a system' design and development stages. This new vision impulsed the emergence of multiple studies arguing for the application of this new paradigm in several contexts, such as those proposed by [8,9,24,25].

In addition to Forensic-by-design, *"Forensic-ready"* is recently another emerging term. To the best of our knowledge, it was first associated to *"Systems"* by [8] in the context of employing the Forensic-by-design approach to engineer systems that possess the ability to collect admissible digital evidence, and in [24], the author associated this new concept with software systems, and explicitly stated it as the capability of supporting potential digital investigations.

We, in here, consider *"Forensic-ready"* as a system (or software) state that is associated with the system (or software) ability to collect digital evidence whilst minimizing the costs of an investigation and disruption of business, and which is related to a specific period of time along its life cycle. In fact a system (or software) may be engineered (designed and developed) to be forensically ready at the design and development stage by adopting the Forensic-by-design strategy, and continue to be *Forensic-ready* along its life cycle by allocating the required digital forensic readiness capabilities at the production, support and retirement stages. Thus, *"Forensic-ready"* is a temporal state (propriety) of a system (software).

The following section provides details on the selected ITS architecture, and the incident principles and processes standard.

3 Architecture and Standards

In this section, we introduce the ARC-IT architecture, provide details on its different stakeholder, viewpoints, views, and security capabilities, then present the incident investigation principles and processes standard [15].

3.1 Selected Architecture

Among the ITS architectures cited in Sect. 1, the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) (USA) [4] is the most advanced and maintained. In fact, the ARC-IT architecture was first initiated in 1996 and is still maintained and updated, even the ITS for Canada [2] is in a re-alignment process with it. Moreover, the U.S. Department of Transportation is licensing all the ARC-IT architecture documents and resources under in the public domain license. For the conjugate of the above arguments, we opted for this architecture.

The methodology behind the ARC-IT is encapsulated in the fact that: *"a system has an architecture, stakeholders have interests and concerns in a system. So, the architecture viewpoints frame the concerns and the architecture views address those concerns"* [4]. The distinction between viewpoints and views is of importance in the ARCT-IT. The group of stakeholders considered in this architecture is composed of: Federal government, state/local government, Non-profit/advisory, private sector and general public. Stakeholders' concerns and interests dictate the architecture viewpoints, therefore, as depicted in Fig. 1, the ARC-IT is composed of four views: (1) Enterprise, (2) Functional, (3) Physical, and (4) Communication.

The Enterprise viewpoint considers the policies, funding, agreements and jurisdictional structure; Provides a basis of ITS understanding for implementers and specifies their roles; Specifies the objectives and goals for the surface transportation system; Provides the policies and process to support transportation planning and project development. Additionally, it answers stakeholders potential concerns on roles and relationships. In fact, ITS involved groups may have roles that vary from installation, maintenance, providing applications or devices, providing transportation-related user services, etc. Therefore, creating an ecosystem of multiple providers and consumers, where relationships must be enumerated in a concise manner. In association with the Enterprise viewpoint, the Enterprise model provides details on concepts, such as Enterprise object, resource, role and relationship.

The Functional viewpoint provides an abstraction of the physical viewpoint to ease the task of potential application, device or service developers'. For this purpose, the Functional view comprises a set of abstract functional elements and their logical interactions, therefore answering potential developer questions on required data format and functionalities for a given service without bothering with the physical details at this layer. On the other hand, the ARC-IT Functional model is developed using a Structural Analysis methodology and use some structural analysis artefacts, such as process, process specification (p-spec), data flows, and terminators. Finally, the ARC-IT [4] specifies that: *"The Functional View defines Processes to control and manage system behaviour, such as monitoring, and other active control elements that are part of describing the functional behaviour of the system"*.

The physical viewpoint is an engineering viewpoint that describes physical elements and enables engineers to answer questions about involved physical

elements in a given delivered service, their interfaces, exchanged information, security consideration, etc. Therefore, it defines objects, such as physical objects (P-Object) (Center, Field, Support, Personal, Vehicle), Functional Object, Information flow, Triple, Subsystem, Terminator and Service Package Diagram.

The physical view comprises a set of physical objects (sub-systems and terminators), that are categorized in six different classes. A general ITS class that cover all of ITS, while five more specific classes (Center, Field, Support, Personal, vehicle) as shown in Fig. 2.

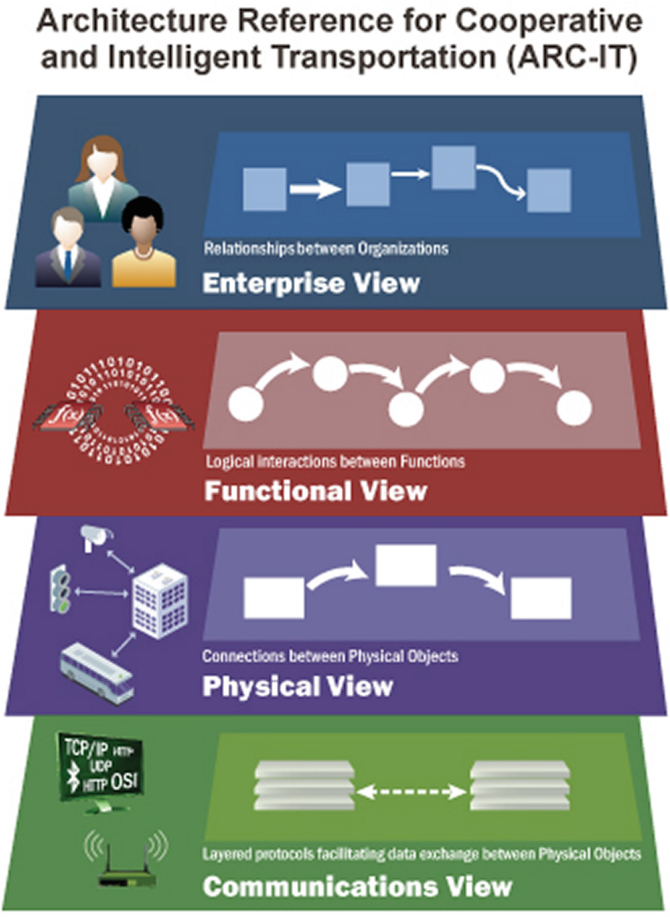

Fig. 1. Architecture reference for cooperative and intelligent transportation (ARC-IT) [4].

The ARC-IT specifies that: *"The general'ITS Object' includes core capabilities common to any class of object"*, thus making it an abstract object from which

all the objects of other classes derive. Therefore this object *"include the core capabilities and interfaces that may be included in any ITS system or device"*.

The communication viewpoint provides a set of protocols that enable the communication between physical objects. Thus, this viewpoint specifies a set of requirements, such as performance, interoperability, security, etc. Additionally, it comprises a set of environment and operational challenges associated with existent policies and regulations. Therefore, it aims to provide answers to potential engineers questions. The ARC-IT communication model comprises a set of layers; Access layer, TransNet layer, Facilities Layer, and ITS Application layer. Moreover, it also provides also a mapping with the OSI model, IETF IP Suite, NTCIP model, etc.

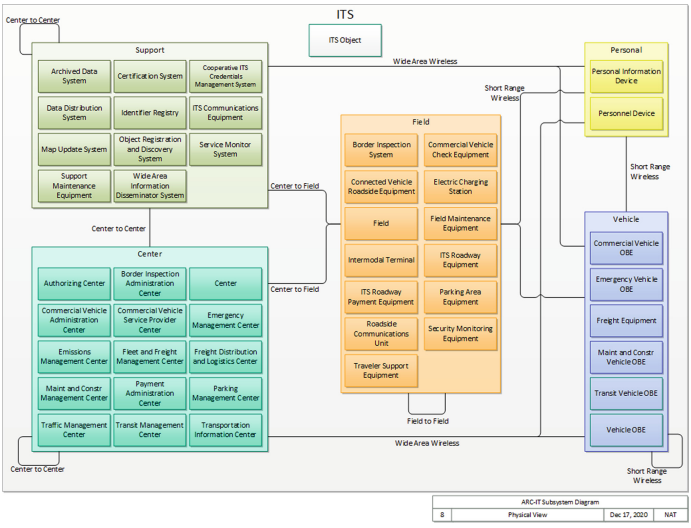

Fig. 2. The ARC-IT [4] physical view.

To prevent the disruption and the alteration of ITS operations, the ARC-IT comprise security measures that address some security aspects, such as information security, ITS personal security, Operational security and security management. The aforementioned security axes are enclosed in the *"Securing ITS"* capabilities, however, the ARC-IT defines eights areas for security appliance; Disaster Response and Evacuation; Freight and Commercial Vehicle Security; HAZWAT Security; ITS Wide Area Alert; Rail Security; Transit Security; Transportation Infrastructure Security; and Travellers Security.

While studying the ARC-IT, it seems that it does not offer any capability to address or support a potential digital forensic investigation. In the following section, we present a standard that aims to empower organization and systems with due capabilities to support potential digital forensic investigation.

3.2 Incident Investigation Principles and Processes

As stated in Sect. 2, incidents and cyber attacks are taking place in ITS. Moreover, some digital vulnerabilities may be exploited to endanger traveller's' safety. Beyond the emergency and the need for a prompt response to accidents, the investigation of incidents'—*physical or digital*—causes, liabilities and responsibilities is of importance. For this purpose, we investigate the emerging opportunities from applying the Incident Investigation principal and Process standard ISO/IEC 27043/2015 [15] to an ITS and more specifically those based on the ARC-IT architecture.

The ISO/IEC/27043/2015 standard [15] include 5 groups of processes; Readiness processes; Initialization processes; Acquisition processes; Investigative processes; and Concurrent processes. In the following, we provide details on the aforementioned processes groups, however, in the context of this study, the main focus will be set on the readiness processes group.

Readiness Processes. This group of processes aims to ensure the due preparedness before the proper investigation and contains 3 processes groups; Planning processes group; Implementation processes group; and Assessment processes group. The first group comprises activities, such as defining scenario where digital evidence is required, identification of potential digital evidence sources, pre-incident gathering, potential digital evidence handling and storage, system architecture definition, etc.

The implementation processes group aims to provide a system with the digital forensic readiness capabilities that were identified by the planning processes group, and which imply the need for the development/acquisition, installation of material, and software, and policies that will enforce the digital readiness across a system.

A continuous assessment of the system' readiness state is required. Thus, the last group aims to evaluate the implementation of the desired preparedness capabilities, in addition to a legal review of all the procedures, controls and architecture in order to ensure the admissibility of the produced digital evidence.

Initialization Processes. This group of processes are triggered at the initialization of an investigation in order to handle the first response to an incident, and to plan and prepare for the remainder of the investigation. Therefore, it comprises processes, such as incident detection, first response, planning and preparation.

Acquisition Processes. Even if an abnormal event is not escalated to a full digital investigation, there may be a requirement for digital evidence either to solidify the due preparedness or to comply with a potential law enforcement request. Therefore, this group comprises processes that ensure the identification, collection/acquisition, transport and storage of digital evidence.

Investigative Processes. In case of an escalation to a full digital forensic investigation, this group contains processes that permit the acquisition, examining, analysis of digital evidence, in addition to capabilities for reports generation and investigation closure.

Concurrent Processes. In addition to the aforementioned processes groups (i.e. readiness, initialisation, acquisition and investigation), this class of processes aims to assist during any phase of a DFI and contains processes, such as obtaining authorization, documentation, managing information flow, preserving chain of custody, preserving digital evidence, and interaction with physical investigation.

The ARC-IT is a reference architecture for building ITS that is system engineering based, and complies with the ISO standard for architecture definition [14]. The conjugate of this architecture and the incident investigation principles and processes is a promising venue for a Forensic-ready ITS. In the following section, we investigate the emerging opportunities from this perspective and potential challenges and issues.

4 Emerging Opportunities and Challenges

To the best of our knowledge, The ARC-IT does not contain any reference to the *"Digital Forensic"*. However, it addresses issues related to incident detection, first response, emergency situation handling, disaster response and recovery, etc. Additionally, it comprises aspects related to traffic management, especially violation enforcement and connection with law enforcement agencies. For the purpose of achieving a Forensic-ready ITS, we plan to adapt the ARC-IT to be aligned with the incident investigation principles and processes.

In the following, we first assess the opportunities to enhance the ARC-IT with capabilities that ensure the due DFR, secondly, we enumerate some of the challenging issues.

4.1 Opportunities

Enhancing an ARC-IT based ITS with the due forensic capabilities imply ultimately the update of the architecture itself. In fact, the ARC-IT is based on the ISO/IEC 42010 [14] architecture description standard.

Methodology. One of the major advantages of the ARC-IT is the fact that it is based on the [14] architecture description standard, which offers the flexibility to start from stakeholders' concerns and interests, establish different viewpoints, and provide associated views. Furthermore, it allows different scales of implementation, going from a local ITS to regional one. Moreover, it is also aligned with the systems and software engineering and adopts the "V" system engineering model [30].

Forensic-by-design. Similar to *"Security-by-Design"*, the *"Forensic-by-design"* [26] paradigm suggests the integrate the forensic requirements at the earliest phases of a system' design and development stages aiming for Forensic-ready system by essence. To the best of our knowledge, among the six key factors of the Forensic-by-design framework *(i.e. Risk management principles and practices, Laws and regulations, Forensic readiness principles and practices, CPCS hardware and software requirements, Industry-specific requirements, Incident handling principles and practices)* only the forensic readiness principles and best practices is missing in the ARC-IT architecture. However, there is an opportunity to integrate this key factor at the design and conception of an ITS by updating the ARC-IT architecture as explained in the following subsections.

Concerns. One of the major key elements in the ARC-IT methodology is the enumeration of stakeholders' *"concerns"*, such as performances, interfaces, security, risks, personal (safety, privacy), deployability, etc. Thus, conciliating the stakeholders' concerns and needs with the forensic requirements is a necessity. This may be achievable through the elevation of awareness about potential real world incidents that may be caused by digital incidents [23]. Once the level of awareness is attained, the integration of forensics requirements into the architecture will be feasible.

Readiness. In the ISO/IEC 27043:2015 standard, the readiness processes group contains indications on the proper methodology to prepare before an incident happens.

The *Scenario definition* process imposes the enumeration of all the scenarios in which digital evidence is required. For ITS scenarios, such as road signalization hack [17], remote car hacking [23], attacks on MTA [12,31], etc. are envisioned. More general scenarios may be derived from the analysis of potential ITS surface attacks. Thus, supposing the compromise of any ITS subsystems, terminator, object (physical, communication, functional) will lead to a scenario worth investigation.

Once the scenario is defined, the enumeration of digital evidence sources is next. For this purpose, the inventory of all potential sources within all the ITS sub-systems is required. In fact, potential evidence may lay inside physical and communication objects, and especially the ITS object which is considered as a template for other objects. Afterwards, the planning of evidence collection and storage will for sure induce changes in the physical, communication and functional objects, in addition to the emergence of new data flows related to evidence handling and storage. Finally the ARC-IT may be updated to contain a sub architecture related to the ITS forensic readiness. Even if there are promising opportunities to add forensic readiness to the ARC-It in order to obtain a Forensic-by-design ITS, there are still some concerning challenges that may undermine the feasibility or the implementation of such type of ITS, in the following some of these challenges.

4.2 Challenges

In the following some of the most important challenges that may impact the feasibility of a Forensic-Ready ITS.

Boundaries. An ITS is delimited by geographic and service boundaries. Therefore, the aggregation of services, data, and resources to investigate a potential incident that may occur outside the ITS borders is problematic. In fact, this challenge is more related to the multi-jurisdiction issues that may emerge. Additionally, the ARC-IT comprises *"Terminators"* (e.g. financial institution, weather service, and enforcement center) that are physical objects but peripheral to the ARC-IT environment and do not contain functional objects. Even if, *"the ARC-IT shows interfaces to and from these supporting or external physical objects but does not define functionality"*. Thus, in case of a cyber crime within the ITS boundaries (e.g. Remote vehicle hack [23] leading to a crash), the ARC-IT contains the capabilities to detect the incident, clear the way for the emergency services, transmit the related incident data to the associated Law Enforcement Agency, but still the conduct of a potential digital investigation on the perpetuated cyber crime is considered outside the scope of the ITS. The hypothesized scenario may become more complex if the remotely hijacked vehicle crash happens outside the geographic ITS' boundaries.

Digital vs Physical. Security is one of the ARC-IT stakeholders' concerns. However, incidents are viewed primarily from the perspective of physical and concrete assets rather than from the information perspective. In fact, incidents monitoring and detection in this architecture are related to traffic management, disaster response and evacuation, alert system, etc. So, securing the physical object and data flow by using devices to detect and monitor "real world" incidents derive from the analysis of scenarios were incidents are caused and initiated by attack on physical assets rather than those where the incident is caused by the exploitation of a digital vulnerability. For example, while investigating a multiple vehicle collision, investigator attention may be centred on conduct misbehaviour, traffic violation. However it may also be caused by light signalization hack. Therefore, the focus on the physical incident may mislead the investigator about the origin of the incident.

Requirements Elicitation. Even if the ARC-IT specifies stakeholders concerns, users needs, sub-systems and services packages requirements, to the best of our knowledge there is no mention of forensic requirements. As stated in potential opportunities, if the forensics concerns are considered then maybe there will be elicitation of its associated requirements.

Scale and Volumes. The implementation of an ITS induces a large scale deployment of sensors and actuators. In fact, the ARC-IT physical view contains

multiple objects (subsystems, terminators), and each system may require a set of sensors employing different technologies and allocated to different missions. For example, the Security Monitoring Equipment (class: field), contains a set of sensors dedicated to tasks, such as providing information on equipments security and fault indication, environment threats (e.g., chemical agent, toxic, biological, explosives and radiological), motion and intrusion detection, objects detection (metal), etc. In addition to sensors, there are also equipment and systems on vehicles, personal, centers and support physical classes. Therefore the aggregated data type is heterogeneous (text, images and videos), often in different formats, and voluminous. In addition to the aforementioned constraints, the nature of the ITS dictated a real time data processing, at least for traffic incident monitoring. These difficulties may urge the usage of paradigms such as cloud computing and fog computing. However, digital forensic readiness and investigation models in these two domains do not yet gain maturity and are still an ongoing research.

Standards and Practices. While studying the ARC-IT, it appears that there are no standards associated with multiple physical objects, such as security monitoring equipment, vehicle OBE, emergency telecommunications system, alerting and advisory system, etc. In addition to the lack of standards, vehicle forensic investigation is very challenging [18,20] in many aspects, such as vehicle constructors obfuscation of technical details, digital evidence collection issues, lack of vehicle digital evidence acquisition and analysis tools, and the need for a sound forensic investigation approach. Finally, one most important issue is related to the first responder and LE training [10], and their ability to recognize the necessity of digital forensic and to properly acquire, collect and handle digital forensic evidence on-scene, such ability is strongly required in case of a fatal vehicle crash.

5 Conclusion and Future Work

The Intelligent Transportation System (ITS) is part of a smart city and a pivotal element of an economy. The growth of ITS associated market size, the diversity of devices providers, government funding either in development, deployment are clear indicators of the effervescence it generates. Considered as a critical infrastructure, the ITS involves several stakeholders that have interests and concerns. Even if there are concrete advances in this field, there are still some concerns related to security, privacy, resiliency and safety. Incidents and cyber crime are no matter of speculation. In fact, Intelligent Transportation Systems are already targets of cyber attacks going from ransomware to road sign and remote car hack.

In this paper we investigate the feasibility of a Forensic-ready ITS, more precisely, we aim to analyse the opportunities and challenges that may arise from enhancing an existing ITS architecture with the due forensic readiness capabilities in order to ensure a designed forensic ready ITS. For this purpose, we provided details on the ARC-It which is an ITS reference architecture, and the investigation principle and process standard.

Even if there are some promising opportunities associated to the flexibility of the ARC-IT and the digital forensic readiness processes, there are still some challenges related to the ITS boundaries, the necessity to reconsider the balance between the digital vs physical aspects of an incident, the complexity of an ITS, the generated data volume, and finally the lack of standard and best practices.

Nonetheless, we believe that there are real opportunities to achieve a Forensic-ready ITS if only and only if there is a stakeholders' awareness on the possibility of exploiting a digital vulnerability to endanger traveller's safety.

In future works, we will aim to establish a digital forensic investigation model for ITS, aiming at first to enumerate some scenarios where digital evidence is required and then specify a sound and clear methodology to conduct a forensic investigation within an ITS.

References

1. Alam, M., Ferreira, J., Fonseca, J.: Introduction to intelligent transportation systems. In: Alam, M., Ferreira, J., Fonseca, J. (eds.) Intelligent Transportation Systems. SSDC, vol. 52, pp. 1–17. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-28183-4_1
2. Transport Canada: Its architecture for Canada (2021). https://www.itscanada.ca/about/architecture/index.html. Accessed June 08 2021
3. Chan-Edmiston, S., Fischer, S., Sloan, S., Wong, M.: Intelligent transportation systems (its) joint program office: strategic plan 2020–2025, Technical report, U.S. Department of Transportation (2020). https://www.its.dot.gov/stratplan2020/ITSJPO_StrategicPlan_2020-2025.pdf
4. DoT, U.: Architecture reference for cooperative and intelligent transportation (2021). https://local.iteris.com/arc-it/. Accessed June 08 2021
5. Endicott-Popovsky, B., Frincke, D.A., Taylor, C.A.: A theoretical framework for organizational network forensic readiness (2007). J. Comput. **2**(3), 1–11. https://doi.org/10.4304/jcp.2.3.1-11
6. ETSI: Its Europe (2021). Accessed June 08 2021. https://www.etsi.org/technologies/automotive-intelligent-transport
7. Ganin, A.A., et al.: Resilience in intelligent transportation systems (ITS). Transp. Res. Part C Emerg. Technol. **100**, 318–329 (2019). https://doi.org/10.1016/j.trc.2019.01.014
8. Grispos, G., Garcia-Galan, J., Pasquale, L., Nuseibeh, B.: Are you ready? Towards the engineering of forensic-ready systems. In: 2017 11th International Conference on Research Challenges in Information Science (RCIS). IEEE (2017). https://doi.org/10.1109/rcis.2017.7956555
9. Grispos, G., Glisson, W.B., Choo, K.-K.R.: Medical cyber-physical systems development: a forensics-driven approach. In: 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE). IEEE (2017). https://doi.org/10.1109/chase.2017.68
10. Holt, T., Dolliver, D.S.: Exploring digital evidence recognition among front-line law enforcement officers at fatal crash scenes. Forensic Sci. Int. Digit. Invest. **37**, 301167 (2021). https://doi.org/10.1016/j.fsidi.2021.301167
11. Huq, N., Vosseler, R., Swimmer, M.: Cyberattacks against intelligent transportation systems, TrendLabs Research Paper (2017)

12. The Philadelphia Inquirer: Septa was attacked by ransomware, sources say. It's still restoring operations stifled since august (2021). https://www.inquirer.com/transportation/septa-malware-attack-ransomware-fbi-employees-cybersecurity-20201007.html. Accessed 06 June 2021
13. Fortune Business Insights: Intelligent transportation system market size, share and global industry trend forecast till 2025 (2021). https://www.fortunebusinessinsights.com/enquiry/request-sample-pdf/intelligent-transportation-system-market-102065. Accessed 08 June 2021
14. ISO: Systems and software engineering—architecture description, Standard, International Organization for Standardization, Geneva, CH (2011)
15. ISO: Information technology—security techniques—incident investigation principles and processes, Standard, International Organization for Standardization, Geneva, CH (2015)
16. Jafarnejad, S., Codeca, L., Bronzi, W., Frank, R., Engel, T.: A car hacking experiment: when connectivity meets vulnerability. In: 2015 IEEE Globecom Workshops (GC Wkshps). IEEE (2015). https://doi.org/10.1109/glocomw.2015.7413993
17. Kelarestaghi, K.B., Heaslip, K., Khalilikhah, M., Fuentes, A., Fessmann, V.: Intelligent transportation system security: hacked message signs. SAE Int. J. Transp. Cybersecur. Priv. **1**(2), 75–90 (2018). https://doi.org/10.4271/11-01-02-0004
18. Kopencova, D., Rak, R.: Issues of vehicle digital forensics. In: 2020 XII International Science-Technical Conference Automotive Safety. IEEE (2020). https://doi.org/10.1109/automotivesafety47494.2020.9293516
19. Lamssaggad, A., Benamar, N., Hafid, A.S., Msahli, M.: A survey on the current security landscape of intelligent transportation systems. IEEE Access **9**, 9180–9208 (2021). https://doi.org/10.1109/access.2021.3050038
20. Le-Khac, N.-A., Jacobs, D., Nijhoff, J., Bertens, K., Choo, K.-K.R.: Smart vehicle forensics: challenges and case study. Future Gener. Comput. Syst. **109**, 500–510 (2020). https://doi.org/10.1016/j.future.2018.05.081
21. De Marco, L., Kechadi, M.-T., Ferrucci, F.: Cloud forensic readiness: foundations. In: Gladyshev, P., Marrington, A., Baggili, I. (eds.) ICDF2C 2013. LNICST, vol. 132, pp. 237–244. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-14289-0_16
22. Meneguette, R.I., De Grande, R.E., Loureiro, A.A.F.: Intelligent transportation systems. In: Intelligent Transport System in Smart Cities. UC, pp. 1–21. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-93332-0_1
23. Miller, C.: Lessons learned from hacking a car. IEEE Des. Test **36**(6), 7–9 (2019). https://doi.org/10.1109/mdat.2018.2863106
24. Pasquale, L., Alrajeh, D., Peersman, C., Tun, T., Nuseibeh, B., Rashid, A.: Towards forensic-ready software systems. In: Proceedings of the 40th International Conference on Software Engineering: New Ideas and Emerging Results. ACM (2018). https://doi.org/10.1145/3183399.3183426
25. Rahman, N.H.A., Cahyani, N.D.W., Choo, K.-K.R.: Cloud incident handling and forensic-by-design: cloud storage as a case study. Concurr. Comput. Pract. Exp. **29**(14), e3868 (2016). https://doi.org/10.1002/cpe.3868
26. Rahman, N.H.A., Glisson, W.B., Yang, Y., Choo, K.-K.R.: Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Comput. **3**(1), 50–59 (2016). https://doi.org/10.1109/mcc.2016.5
27. Rowlingson, R.: A ten step process for forensic readiness. Int. J. Digit. Evid. **2**(3), 1–28 (2004)

28. Sjoberg, K., Andres, P., Buburuzan, T., Brakemeier, A.: Cooperative intelligent transport systems in Europe: current deployment status and outlook. IEEE Veh. Technol. Mag. **12**(2), 89–97 (2017). https://doi.org/10.1109/mvt.2017.2670018
29. Tan, J.: Forensic readiness, Cambridge, MA:@ Stake, pp. 1–23 (2001)
30. National ITS Architecture Team: System engineering for intelligent transportation systems, Technical report, vol. 2007. Iteris, Inc., USA (2007)
31. The New York Times: The M.T.A. is breached by hackers as cyberattacks surge (2021). Accessed 08 June 2021. https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html
32. Valjarevic, A., Venter, H.: A harmonized process model for digital forensic investigation readiness. In: Peterson, G., Shenoi, S. (eds.) DigitalForensics 2013. IAICT, vol. 410, pp. 67–82. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41148-9_5