



**HAL**  
open science

# Cyber-Physical Application for the Safety and Security Enforcement in Oil and Gas Transportation

Nicola Zingirian

► **To cite this version:**

Nicola Zingirian. Cyber-Physical Application for the Safety and Security Enforcement in Oil and Gas Transportation. 4th IFIP International Internet of Things Conference (IFIPIoT), Nov 2021, Virtual, Netherlands. pp.180-196, 10.1007/978-3-030-96466-5\_12 . hal-04471545

**HAL Id: hal-04471545**

**<https://inria.hal.science/hal-04471545v1>**

Submitted on 21 Feb 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License



This document is the original author manuscript of a paper submitted to an IFIP conference proceedings or other IFIP publication by Springer Nature. As such, there may be some differences in the official published version of the paper. Such differences, if any, are usually due to reformatting during preparation for publication or minor corrections made by the author(s) during final proofreading of the publication manuscript.

# Cyber-Physical Application for the Safety and Security Enforcement in Oil & Gas Transportation

Nicola Zingirian <sup>1</sup>[0000-0003-3229-9361]

<sup>1</sup> DEI - University of Padova - 35131 Padova, Italy  
nicola.zingirian@unipd.it

**Abstract.** The paper presents an innovative mobile application enabling the security and safety inspectors of Oil & Gas Transportation to receive in their car all the real-time data necessary to drive them to the visual evidence of the truck driver's unsafe or dishonest activities. The application works on the top of an IoT platform managing a sensor network installed on over 3,000 tank trucks. The paper presents the application domain, the architecture, the implementation, and the experiments, also reporting a set of quantitative experimental results that validate the application effectiveness. The results also qualify the application as one of the first cases of real-time Cyber-Physical Systems for Logistics and Transportation Safety and Security validated for the measured impact on the operations, and not just in terms of scenarios or technology potentials.

**Keywords:** Road safety, Transportation Security, IoT, Real Application.

## 1 Introduction

The paper presents an innovative mobile application developed on top of an Oil & Gas Transportation Internet of Things (IoT) platform based on a sensor network installed on over 3,000 tank trucks [21]. The use case refers to detectives who receive in their car all the real-time data necessary i) to chase and approach a truck secretly, and ii) to wait for the right time to come out of hiding in such a way to get the eye witnessed evidence of the truck driver's incorrect or dishonest actions against the safety or the security.

To better understand the critical mission of this application, it deserves to analyze the application scenario. The Oil & Gas Transportation domain is a very critical process, as it handles massive amounts of highly flammable, explosive, and pollutant fuels, mostly delivered in urban areas, where the exposure to disasters is very high [11]. Moreover, fuels are unfortunately subject to theft, being an easily salable value in illegal markets [4]. Finally, public authorities keep the fuel supply chains under special surveillance, as a large part of the transported value is represented by taxes and excise duties, so that every product loss also corresponds to tax evasion.

Furthermore, Oil & Gas Logistics and Transportation, like any other large-scale supply chain, are characterized by continuous and capillary deliveries over nationwide retail networks. Considering that the stock levels are often kept low because of cash

shortages, the supply imposes frequent small deliveries to the same reservoirs. This context makes the surveillance also very time-critical, as it should not interfere with the trip efficiency.

Over time, this scenario has made it very convenient to centrally monitor the tankers transporting fuels in real-time, to supervise i) the proper safety procedure execution, ii) the efficient product transportation and delivery, and, above all, iii) the product integrity against the product theft. Our research group, following up an EU-funded project [10], established a University Spin-off company that, in tight connection with the Department of Information Engineering, has created and is managing the IoT platform that today is used by all the major Italian oil companies as well as other companies in other countries.

The new application presented in this paper has been designed and recently deployed on the top of this monitoring system, to support the enforcement of safety procedures and the safeguarding of the product that is currently under test at the Italiana Petroli, the second-largest Italian oil company, considering that driver's fraud is by far the most severe security problem.

This application addresses the oil company personnel who are referred to as the inspectors. The inspector's role has been traditionally to verify, on the spot, the tanker equipment compliance with the contractual obligations specified in the transportation tenders and the procedural conformity during product loading, driving, and delivering. In recent years, however, the inspector's task has become increasingly focused on the dishonest behavior of the drivers who transport the fuel, because the margin reductions in the oil business has made the product losses, amounting up to several million euros yearly, less and less sustainable. This task is critical, as the product accounting alone is not precise enough to discriminate the product stealing from the metrological system tolerance errors caused by the approximations of mechanical and fluid dynamics models, also including the calculation of thermal volume variations<sup>1</sup>.

The application presented in this paper provides the inspectors with clues of illegal driver's operations. After the identification of these drivers, the mobile application first supports the inspectors to chase any selected moving truck, then to approach it, to understand the best moment to come out of the hide, and to register, directly on the spot, every non-conformity found, applying penalties to the transporter and, in severe cases, imposing the removal of the driver.

The rest of the paper presents the state of the art, the architecture, the implementation, and a report of experimental results.

---

<sup>1</sup> Being 0.5% the tolerance accepted by the European Standard Measurement Instrument Directive (MID), the cumulated accepted errors of both the load and the unload measurements, corresponding to a 40,000-liters trip is 40 liters, i.e., a value of about 60 Euros per trip, including the taxes. For an average of 2 trips per day, that value is more than 2.700 Euro per month, for each truck. Considering a typical 200 trucks fleet working daily for a medium oil company the non-accountable product loss standing within the MID's tolerance corresponds to over 6 million euros per year.

## 2 State of the Art

The solution presented is in the state of the art of the field automation to support the security and the safety of dangerous good transportation, as well as the state of the art of the Cyber-Physical Systems.

### 2.1 State of the art of tank truck automation

During the last two decades the industrial practice has given rise to various electronic devices that today are part of the standard tank truck equipment to counteract operation errors or abuses in fuel delivery. Among these are the Sealed Parcel Delivery System [6] and the automation of the loading and unloading operations [5], embedded in the electronic registers connected to the Metrologic sensors that measure the quantities delivered, based on volume [12], levels [1], mass [16] or flow rate [17] transducers.

These systems, by limiting the user's freedom in the valve actuation to access the product, help to avoid errors and abuses (e.g., product contamination [9], overfill [2]), but unfortunately cannot ultimately solve the security issues. Several system manufacturers have also included a data logging system in their automation systems, also proposed as industrial standards (e.g. [7]) so that service workshops can access the data locally, after authentication, to analyze the operation and the actions performed by the driver.

### 2.2 Cyber-Physical Systems

The cost of retrieving the data by connecting locally to the tank truck automation systems, as well as the incompleteness of such data, could not keep the security level sufficiently high. During the last decade, such limitations pushed the major oil companies to adopt early IoT and Sensor Networks [21], to

- include further vehicle sensors,
- perform on-board signal processing,
- collect and process all the data in real-time in a cloud platform,
- correlate all the data through expansible and shared logic implemented in the platform,
- make available the information to all transport customers and all the main Oil & Gas haulers to trigger appropriate corrective actions.

This trend has been initially favored by the European regulation for the road transportation of dangerous goods (the ADR, “Accord Dangereux Routier”), as it started requiring, since 2009, the GPS tracking for all vehicles transporting the main dangerous goods categories, including fuels. Unfortunately, this regulation has not evolved further, so that the current ADR-2019 release, despite the IoT and sensor network evolution, is still requiring just a basic Automatic Vehicle Location.

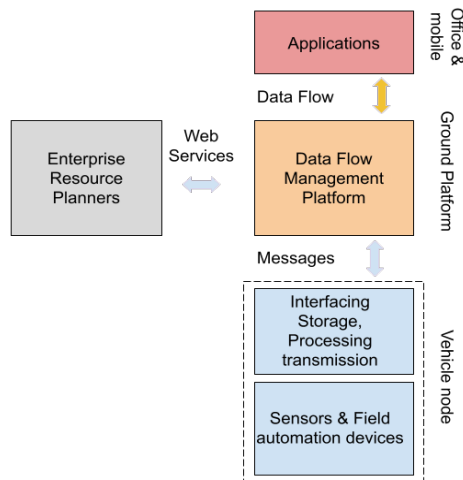
Nevertheless, during the last decade, such regulation limits have not prevented the Oil & Gas Logistics IoT platforms from deploying several new applications addressed

to a variety of stakeholders, e.g., Depots and Terminal Managers, Oil Company Managers, Haulers, Haulers' subcontractors, Authorities.

Among the recent applications, the one presented in this paper i) takes advantage, better than the others, of the real time sensor data potential, ii) includes human operators in a Cyber-Physical feedback loop [20] and iii) shows how critical logistics can be secured through Cyber-Physical Systems. We present this application as a contribution to extend the pool of Cyber-Physical System applications, (see e.g. [3] as well as the link [13] to the UC Berkeley Ptolemy project's taxonomy), as current taxonomies do not include the dangerous or critical transportation domain, limiting the main real application categories to Smart grids [14], Healthcare [15], and vehicle mobility [18] and a few others.

### 3 System Architecture

Figure 1 shows the overview of the System Architecture supporting the application described in this paper. The Vehicle Node manages the sensors installed on the tank trucks. The Data Flow Management Platform receives the messages from the Vehicle Nodes and dispatches data to the applications, adopting the management information received from external Enterprise Resource Planners (ERPs) as dispatching criteria. The applications consume, process and integrate data to provide the users with office and mobile services.



**Fig. 1.** System Architecture Overview

#### 3.1 Vehicle Node

The architecture of the sensor network installed on the tank trucks inherits some characteristics of the vehicle telematics, i.e., the Fleet Management Systems (FMS) and of the Automatic Vehicle Location/Management (AVL/M) systems. Such systems

periodically store and send the vehicle's GPS coordinates together with data sets including mileage, fuel consumption, working hours, driving, pauses, rests, etc.

Unlike the FMS and AVL/M black boxes, the Vehicle Node is equipped with an onboard remotely programmable microcontroller, capable of interfacing an ever-increasing number of sensors to monitor the transported goods and to support custom signal processing and filtering.

**Table 1.** Typical Tank Truck Sensor Network signal

Sensor	Information	Purpose
Wet leg	presence of product in the tanker trucks pipes.	Check whether pipes are empty after each delivery and filled before the first delivery
Valve	open or close foot valve state	Check whether the product is accessed not in correspondence with measured deliveries
Hatch open	open or close unloading station opened	Check whether the unloading station is accessed not in correspondence with measured deliveries
Level	Level of product in the tanker.	Check whether the level change not in correspondence with measured deliveries
Loaded product Temperature	Temperature of product in the tanker	Calculate the volume difference upon temperature changes between loading and unloading
Unload product temperature	Temperature of product during unloading	
Loading Couplers	Opening of the loading couplers	Check whether the couplers are opened not in terminals or depots.
EBS	Activation of the anti-roll system	Reports dangerous near miss
Digital Tachograph	Driver identity and Driver time	Check if the driver corresponds to the authorized person and bind any action to the driver
Electronic Measuring	Presets and unloaded volumes, total counters, flow rate, product, delivery ticket number	Bind any actions done on the unloading station to the delivery accounted

Sealing System (SPDSS)	State of the compartments: empty, sealed, broken seal.	Compare the information of the Sealing System with the detected driver's activities
Overfill	Overfill detection beyond the safety ullage for each tanker compartment.	Incident Near-miss
Electrical Grounding	Connection of the tanker chassis to the delivery point grounding system	Incident Near-miss
Density	measures the product density in each compartment	Allow precise calculation volume compensation and detects product crossovers.

The acquired data are analogic signals, digital inputs, and field device data interfaces such as RS232, RS485, CAN. Table 1 shows the typical sensor network signals interfaced.

Based on the data coming from the various sensors and field devices, the onboard unit generates periodic telemetries, as well as asynchronous events or alarms, each marked with timestamps, geo-coordinates, speed and direction values, plus other attributes such as the identifier of the main vehicle and of another vehicle possibly coupled, the driver identifier, etc. Each sensor connected to each Vehicle Node is accessible as a sensor network node.

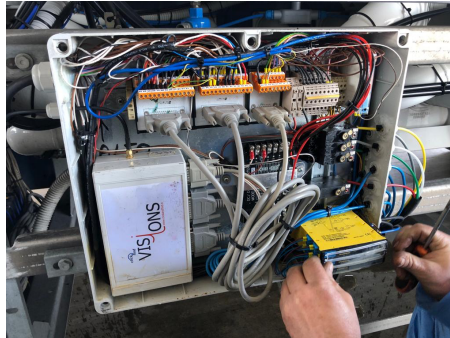
The collected signals never include any operator's data entries, except for the loading and unloading pre-sets, manually entered to activate the automated loading and unloading operations. The system, therefore, transparently collects all the information without requiring any manual input. This characteristic derives from security-by-design requirements. Similarly, the configuration of the Vehicle Node equipment itself does not depend on any on-site service operators, but on users authorized by the platform, through a command-based configuration interface.

The data transmission takes place via UDP/IP over GPRS or LTE. For each transmitted message a reply message acknowledges both data reception and information save, matching the sequence numbers. The message payload is AES256-encrypted, using a server-generated key that, at every daily or weekly key update, reconfigures the Vehicle Node through a specific key-change message encrypted by the old key to guarantee both authenticity and confidentiality. From the generation of the message to its availability to Remote applications, each asynchronous message constitutes the basic block of the whole architecture. The Data Flow is the sequence of messages dispatched to the proper modules, and each message is bound to one notification, at every data flow processing block.

The sensor equipment is defined by the contractual standards of the tank trucks that work for the major companies, including AGIP/ENI, Tamoil, Kuwait Petroleum (including Shell Network), Italiana Petroli (formerly Total Erg and API). These contractual standards have been constantly evolving for several years and constitute the driver for continuous system tuning and extension. Among the most recent innovations are the optical fiber-based sealing devices, the electrical continuity detection systems



between the vapor recovery lines and the grounding lines, and the availability of RFID seals.



**Fig. 2.** Vehicle Node Hardware mounted on a Tanker Semi-Trailer.

### 3.2 Data Flow Management Platform

This platform acts as a ground station receiving all the sensor data from all the Vehicle Nodes, works similarly to the FMS or AVL/M systems, as it generates reports, statistics, maps, tables, and dashboards.

However, unlike the FMS and AVL/M systems, it also manages the data as either real-time or deferred streams, called the Data Flow, addressed to various applications, making it possible to feed applications for transport customers, carriers, workshops, and public utility service centers.

This feature is managed by building a bidirectional data flow dispatching layer based on the vehicle attributes and of dynamic data (such as trip plans, geofence, truck operations), also supporting bidirectional communications.

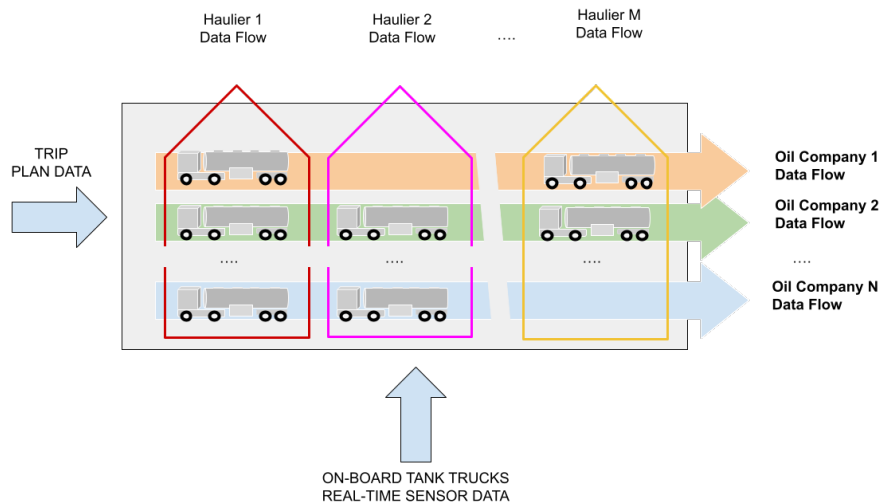
In particular, there are two Data Flow types:

- **Dynamic Data Flow** consists of messages that, according to appropriate dispatch rules, are directly routed to the destination as soon as the Vehicle Node generates and transmits them to the Data Flow Management Platform. These messages are dispatched in cut-through mode as real-time streams, instead of being stored, retrieved, and forwarded.
- **Static Data Flow** consists of pre-processed items derived from the Vehicle Node messages and prepared in advance by the Data Flow manager and dispatched upon the application request. The Static Data Flows appear like database query results, except for the fact the result sets, instead of being built on the fly from the Database fields, are pre-cooked streams that offer much more reactivity than multiple row selections on relational tables.

The main data flow is directly implemented as an incremental Unix file, where newly received and parsed messages are appended. The main data flow is dispatched in real-time to pre-cooked JSON files, after a cleansing filter, each organized by truck, day and

company to implement the static data flow. The dynamic dataflows are connected to the main data flow streams, using the Posix inotify services and in-line appropriate filters. This implementation on top of the Posix System calls, being strictly domain-oriented, delivers even more flexibility and performance than document-oriented DBMS, such as the MongoDB.

Figure 3 shows a basic scheme for forwarding Real-Time data flows, which depend on the ownership of the vehicle for directing flows to the haulers and on the trip plans, received from external ERPs for directing flows to the transport customers, i.e., the oil companies. Whereas the transporters are interested in obtaining the operational data of their vehicles, the transport customers, instead, are interested in obtaining real-time data related to the owned goods that are being transported, from the end of the product load up to the subsequent product load.



**Fig. 3.** Differentiated Data Flows dispatching rules to haulers (colored transparent vertical arrows) and to the oil logistic companies (solid horizontal-colored arrows)

Other criteria used for dispatching the Data Flows are, for example, the proximity of an authorized service operator or the entrance/exit in/out specific geo-fenced areas. The possibility to forward distinct Data Flows to distinct applications is the key platform feature. Such versatility has made the penetration of the solution extremely pervasive, thus creating a de facto standard in fuel transportation, so far, in Italy, Serbia and in some parts of South Africa.

### 3.3 Applications

The Applications developed on top of the Data Flow Management Platform cover different processes and include, for instance, travel tracking, electronic waybill

documentation, tank truck maintenance, just-in-time truck routing, terminal and depot surveillance.

The application presented in this paper represents a recent successful example of the application supported by dynamic Data Flows.

## 4 Application Logic

### 4.1 Office Operations

To analyze the behavior of the drivers, the route and the operations carried out by these drivers are examined in a dashboard showing all the information on a map that is studied by the inspectors (see Fig. 4). To facilitate the investigation, the system generates alarms in correspondence with suspicious situations, avoiding unnecessary human consultation of large data amounts. Table 2 shows a list of alarm logics in use. These logics derive from the human experience and retrospective analysis of the behavior of drivers who have been caught red-handed in their malicious operations. It is worth noticing that the employee's privacy law allows regarding the sensor data as equipment data, not as behavioral data. Therefore, such data can just provide behavior clues, but never as evidence of behaviors. The inspector's role is to understand the clues and to go on the spot and get visual evidence of misbehaviors. Thus, following the analysis of the alarms and of the traces displayed on the map, the inspectors decide to physically pursue the truck to catch the product stealing operation or the operation that does not comply with the regulation.

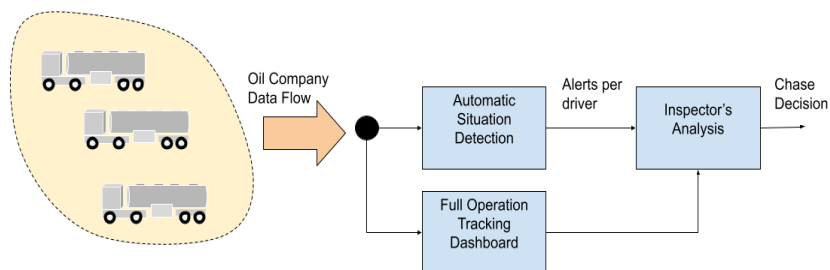
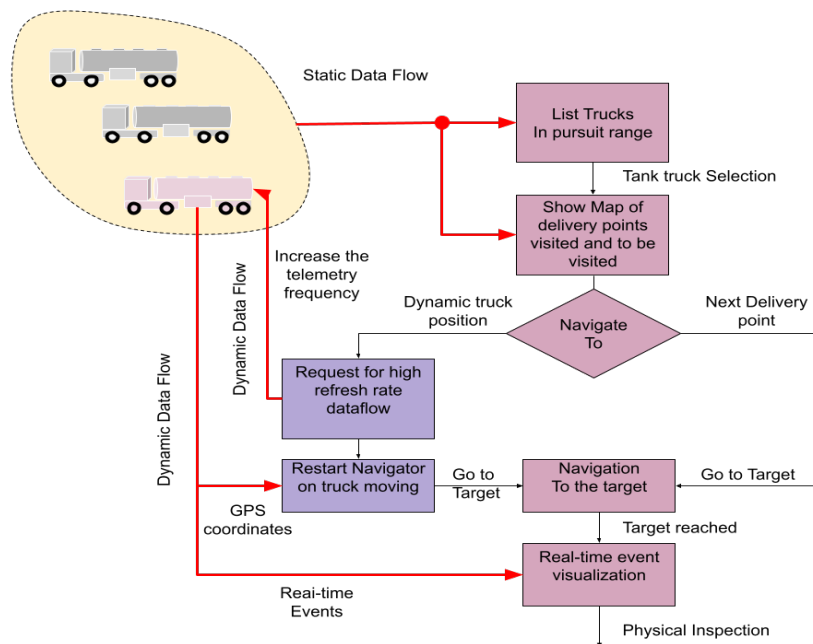


Fig. 4. Office Operations supported

**Table 2. Alerts**

Alert Name	Data
Opening of the hatch and or foot valves out of the delivery points	RFID-based opening sensor
Stop during residual product flush	Electronic Head Data
Opening of the hatch in hauler parking zones	RFID-based opening sensor
Stop in the parking zone before the end of the trip	Trip Plan, geo-coordinates, geo-fenced areas
Opening of the loading Coupler out of the loading zone	Namur proximity sensors in loading Coupler
Residual product detection after the last delivery	Wet Leg sensors
Delivered quantity discrepancy versus thermic variation	Temperature sensors in chambers, Metrologic delivery quantity



**Fig. 5. Diagram of the On-Field operations**

## 4.2 On-Field operations

The On-Field operations are organized as a sequence of steps, illustrated in Fig. 5, and detailed in this section.

- **Trucks Selection:** Before starting the chase, the inspector watches on his/her tablet the list of tank trucks that he/she is authorized to pursue, i.e., those that are currently operating for the oil company for which the investigation is taking place. This information is obtained by getting a filtered Data Flow of the trucks that are executing the trips planned for that customer (see the horizontal path of Figure 3). The list is sorted by the truck distance and filtered up to a maximum distance radius from the inspector's location and is also represented over a dynamic map in real-time.
- **Trip Progress Information** When a truck is selected, the current trip information appears on a map, showing the path so far covered, the delivery points already served and the planned delivery points to be reached.
- **Navigation** The inspector decides whether to follow at the proper distance the moving tank truck, or to wait for it at the next delivery place, according to some criteria including the trip progress information, the inspector location, and the place in which the misbehavior will likely take place, i.e., stopovers vs. delivery places. Following this selection, the navigation starts in static mode, if the target is the delivery place, otherwise, in dynamic mode if the target is the moving truck. If navigation is dynamic, the application continuously receives the geo coordinates and the events transmitted by the truck in dynamic Flow data. To always have fresh information, the application requires Data Flow Manager to reconfigure the onboard equipment of the tracked tanker, setting a 5 sec localization sampling period instead of the 60-sec default.
- **Real-Time Event Watching:** As noticed, the critical requirement of the inspector's activity is to appear on the spot at the exact moment when the non-conformity can be unequivocally documented. In this situation, the event messages (e.g., the start of the delivery, vapor recovery interconnection, hatch opening, electronic meter start, or valve opening, or end of the delivery) are the key information to decide when to physically catch the driver in the act of abusing or misusing the equipment.

## 5 Implementation Notes

The main implementation challenges relate to the on-field operations, as they represent the most critical part of the process.

### 5.1 Application Interfaces

The application is an Android App including the following control or data interfaces:

- **Data Flow Interfaces:** These data interfaces support the interaction with the Data Flow Management Platform. Both Static and Dynamic Data Flow are interfaced.

- *Static Data Flow*: The items are prepared as pre-cooked JSON records for the application's download. The client's requests can configure appropriate data filtering logic.
- *Dynamic Data Flow*: The application receives the messages as WebSocket data frames [8] that are handled asynchronously. The application interface allows configuring appropriate data filtering logic in the service subscription.
- **Navigation Interface**: This control interface opens the Navigation Software and refreshes the target. This interface takes advantage of the Android Intent mechanism. The Sygic navigator has been selected for the possibility of specifying the target in the intent link, also showing acceptable time overheads during the navigation target updates.
- **Location Service Interface**: This data interface allows retrieving the inspector's geo coordinates necessary to select the vehicle within a given distance radius from the inspector, both to limit the truck selection and to estimate the proper refresh navigation rate.

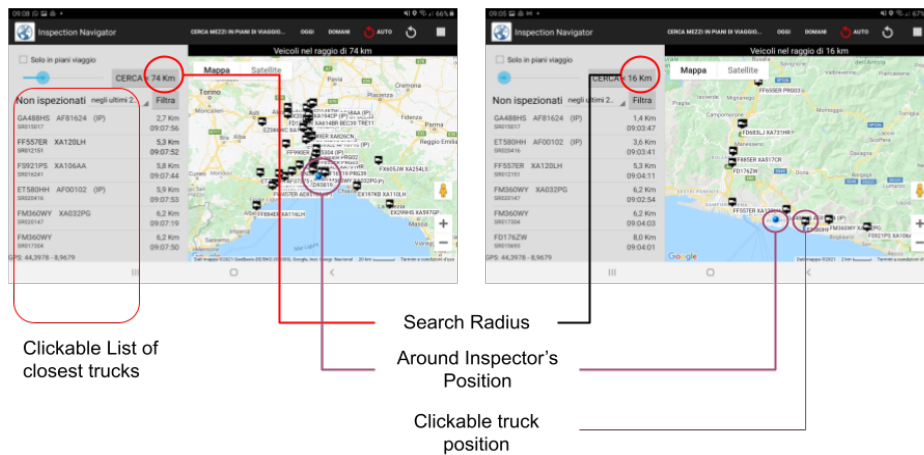


Fig. 6. User's interface for truck list visualization and truck selection

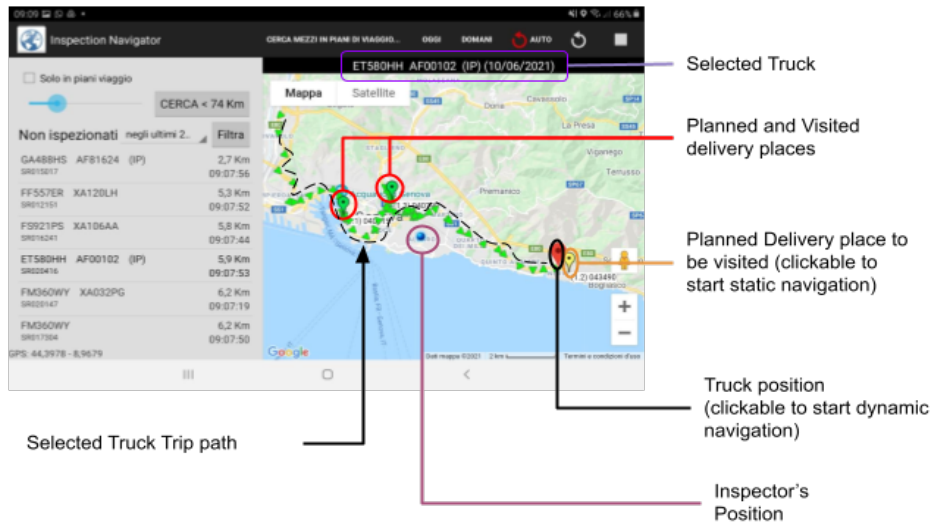


Fig. 7. User's interface for trip visualization and navigation selection

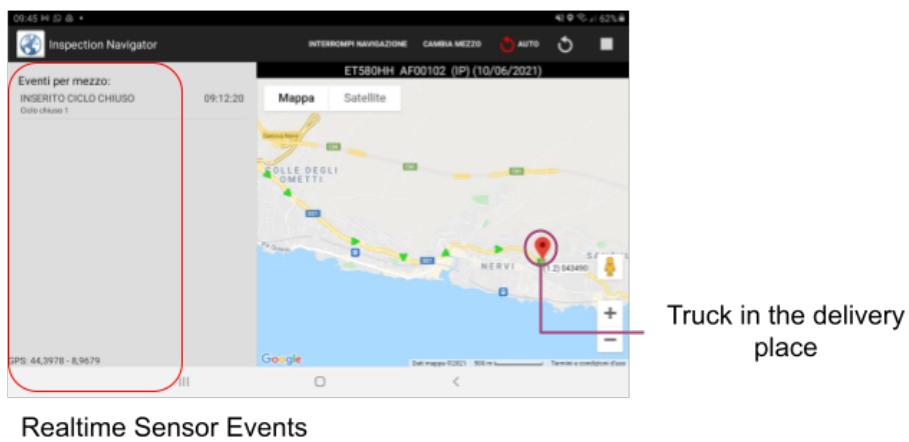


Fig. 8. User's interface for Real-Time Event check

## 5.2 Application Graphical User Interfaces

The GUIs are handled by Android Activities and Fragments. All the application GUIs, except for the navigation, which is directly managed by the third-party Sygic Software, consists of the following views:

- Clickable Map of the Pursuable trucks over the map: this is a Web View, connected to the static Data Flow (Figure 6)
- Clickable List of the pursuable trucks as ordered list and radius configuration cursor (Figure 6)
- Clickable Map view of the selected truck trip (Figure 7)
- Visualization for incoming dynamic events (Figure 8)
- Notifications over the Sygic maps implemented as Android Toast

## 5.3 Logic implementations

The implementation includes the following logic implementation

- **Selection of the truck according to their distance from the user's position.** This logic is implemented as a filter configuration in the Data Flow Manager, during the application request. Further filters apply to the inspector's identity to restrict the data visualization just to those trucks that are traveling at that moment for the inspector's company.
- **Trip stop coloring** This logic allows showing red pinpoints for the delivery places already visited, and yellow pinpoints for the places to be visited (See Figure 7). This logic is implemented in the Data Flow Manager. The Delivery point geo coordinates and status are maintained in the Data Flow Manager. It is worth noticing that the visit of the delivery point is confirmed only after the valve opening signal so that a simple stop in the delivery place does not correspond to a visit.
- **Navigation Updating Logic** This logic decides when the navigator target needs to be refreshed. Every asynchronous message coming from the Dynamic Data Flow interface wakes up the Navigation Updating logic, to verify whether the vehicle has changed position after the previous localization message, the distance between the user and the chased truck, and the time passed after the last target changes. The algorithm decides whether to trigger a new intent to the navigator or not, weighting the usefulness of the update and the time overhead caused the target change.

# 6 Experimental Results

## 6.1 Performance indicators

This section reports on the performance indicators derived from the analysis of the application logs related to the work of 4 inspectors, pursuing in total 68 tank trucks.

Table 3 reports the number of dynamic and static navigations activated. The balance between static and dynamic navigation changes from user to user, although in general

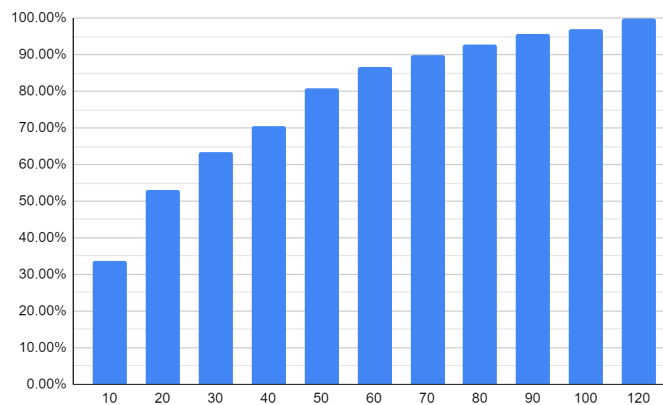


dynamic navigation is the preferred option. The dynamic navigation ran in total 76 times to follow 68 trucks as the chase of most selected trucks took place in one shot.

The average measured chase duration is 28 minutes, also including the waiting time between the truck approach and the physical intervention. More in detail, Figure 5 reports the distribution of the measured chase time, showing that 85% of the chases lasted less than one hour. This represents the main key performance index, considering that chasing a single truck without the application, typically took 4 hours in the past.

**Table 3.** Number of Navigations for each inspector (identified by Android ID) in Nov 2019

User (Android id)	Dynamic Navigation	Static Naviga- tion	<b>Total</b>
16321d9d4efb332a	10	7	17
2dc5b9f48de9422c	59	5	64
32b8b154976f7d26	0	25	25
46c91a52b1345bee	7	1	8
<b>Total</b>	<b>76</b>	<b>38</b>	<b>120</b>



**Fig. 9.** Chase duration distribution: the y-axis reports the percentage of chases lasting less than the duration reported in the x-axis (minutes).

## 6.2 Application impact

The performance has increased the inspector's efficiency. Before adopting this application, each inspector used to complete about 35 inspections per year on average. In 2019, using the application each inspector completed 146 inspections per year, thus increasing the performance by more than 4 times, allowing visiting all the trucks two times per year, on average. In 2019, the system allowed catching 23 cases of illegal

products found onboard. Table 4 reports further security and safety non-conformities detected, showing the categories and the relative occurrence of the bad practices.

**Table 4.** Top detected non-conformities (occurrence rate per inspection)

Checked item	Category	Severity	Non-conformities
Vapor Recovery	Safety	High	11.3%
Company physical sealing	Security	Medium	7.1%
Client's Livery	Quality	Low	7.0%
Explosion Proof Tools	Safety	High	6.9%
Correct Itinerary execution	Quality/Security	Medium	6.4%
Metrological Sealing	Security	High	5.9%
Illegal onboard	Security	High	5.2%
Couplers Opening	Security	High	4.5%
Electrical Grounding	Safety	High	3.0%

## 7 Privacy Issues

The compliance of the application to the privacy regulation (GDPR) is based on the following items.

- The transport companies declare their sensor data ownership to the National Privacy Authority, for the exact purposes of asset protection and people safety, appointing the data provider as the data manager.
- The data set is limited to the truck equipment, and does not extend to the driver, differently from the video surveillance.
- The driver identity is associated with the truck, using the tachograph identification card data, as the company has to guarantee to entrust the dangerous freights only to the drivers who are authorized to enter critical facilities are enabled to conduct the truck and are not blacklisted.
- The data related to product location, access, and delivery are exported in real-time to the oil company, which is the product owner. Each data item exported is specified in the contractual clauses.
- During the trip the driver, by his/her job description, has to carefully follow the routes and the schedules, for safety and security reasons, so that any discrepancy, including stops and over speeds, represents potential security or safety threats to be monitored.

- The data are maintained for 5 years, on-line or off-line, in a secure physical IT infrastructure, managed by a ISO 27001-certified provider, making the data remotely accessible to the staff entitled to view and analyse the data.
- The staff is not allowed to share such data to anyone who is not authorized.
- The physical authentication of the data sources is based on the serial numbers of the IoT device and the encryption key that can be changed only remotely by the provider, and on the cross check with serial number of other field devices, such as the electronic measuring system or the sealing system.
- No data processing is allowed to infer personal information of the driver.

## 8 Concluding Remarks

In addition to the application domain, the key innovative aspect of the application presented in this paper is to guide an organization towards the full reactivity in the anomaly management, by inserting the human operators in the physical process feedback, driving their actions and strategies through sensors' information in real time.

We believe that this type of application represents an emerging context of the Cyber-Physical Security Systems. In fact, while the Cyber-Physical Security is commonly understood as the security against cyber-attacks to the IT platforms managing or controlling physical systems[19], this application suggests extending the Cyber-Physical Security concept to the physical process security enhancement supported by the IT platforms, proving it in the full process, not only in the technologies.

## References

1. Boehm, A. "Device for discharging liquid from a tank and method for emptying the residue from a line section." U.S. Patent 8,196,904, issued June 12, 2012.
2. Cadman, G.R. and Thiara, J.S., Scully Signal Co, 1996., "Fluid overfill protection and product identification system", U.S. Patent 5,507,326.
3. Chen, Hong. "Applications of cyber-physical systems: a literature review.", *Journal of Industrial Integration and Management* 2, no. 03 (2017): 1750012.
4. Cottin B., "Black Gold, Black Market", *Risk Management*. 2009 Oct 1;56(8), Risk and Insurance Management Society, Inc
5. Dudley et al . Patent No .: US 10,787,358 B2 Sep. 29 , 2020 "Control Systems For Liquid Product Delivery Vehicles" Knappco , LLC , Kansas City , MO ( US )
6. EN 15208, Tanks for transport of dangerous goods - Sealed parcel delivery systems - Working principles and interface specifications
7. EN 15969:2018 Tanks for transport of dangerous goods - Digital interface for the data transfer between tank vehicle and with stationary facilities
8. Fette, I. and A. Melnikov, "The WebSocket Protocol", RFC 6455, IETF, DOI 10.17487/RFC6455, December 2011
9. FMC Technologies Measurement Solutions, Inc., Sening® Innovative Tank Truck Systems, "Sening® NoMix Cross-Over Prevention," Apr. 2009

10. Fornasa, M., et al., "VISIONS: A Service Oriented Architecture for Remote Vehicle Inspection," 2006 IEEE Intelligent Transportation Systems Conference, 2006, pp. 163-168, doi: 10.1109/ITSC.2006.1706736.
11. Ghaleh, S., et al., "Pattern of safety risk assessment in road fleet transportation of hazardous materials (oil materials)", *Safety Science*, Volume 116, 2019, Pages 1-12, ISSN 0925-7535, <https://doi.org/10.1016/j.ssci.2019.02.039>.
12. Haar, T., Haar Alfons Maschinenbau GmbH and Co, 1999. Method and apparatus for measuring the volume of flowing liquids. U.S. Patent 5,922,969.
13. <https://ptolemy.berkeley.edu/projects/cps/>
14. Jha, A.V., Appasani, B., Ghazali, A.N. et al. Smart grid cyber-physical systems: communication technologies, standards and challenges. *Wireless Netw* 27, 2595–2613 (2021). <https://doi.org/10.1007/s11276-021-02579-1>
15. Jimenez, J.I., Jahankhani, H. and Kendziarskyj, S., 2020. Health care in the Cyberspace: Medical cyber-physical system and digital twin challenges. In *Digital Twin Technologies and Smart Cities* (pp. 79-92). Springer, Cham.
16. O'Banion, T. "Coriolis: the direct approach to mass flow measurement." *Chemical Engineering Progress* 109, no. 3 (2013): 41-46.
17. Olivier, P.D., Shermer, W.P., and Nanaji, S.A. "Fuel dispenser fuel flow meter device, system and method." U.S. Patent 6,935,191, issued August 30, 2005.
18. Yanagihara, T. Nawa, K., Chandrasiri, N.P. and Oguchi, K., 2014. Cyber physical system for vehicle application. *Transactions of the Institute of Measurement and Control*, 36(7), pp.898-905.
19. Wells, L.J., Camelio, J.A., Williams, C.B. and White, J., 2014. Cyber-physical security challenges in manufacturing systems. *Manufacturing Letters*, 2(2), pp.74-77.
20. Zettsu, K., Sowe S.K., Simmon, E., De Vault, F. and I. Bojanova, "Cyber-Physical-Human Systems: Putting People in the Loop," in *IT Professional*, vol. 18, no. 1, pp. 10-13, Jan.-Feb. 2016, doi: 10.1109/MITP.2016.14.
21. Zingirian, N. and Valenti, C., "Sensor clouds for Intelligent Truck Monitoring," 2012 IEEE Intelligent Vehicles Symposium, 2012, pp. 999-1004, doi: 10.1109/IVS.2012.6232192. Author, F.: Article title. *Journal* 2(5), 99–110 (2016).