FERROMOBILE and Security for Low Moment of Traffic Level Crossing

Rim Brahim, Simon Collart-Dutilleul, Philippe Bon, Pierre-Antoine Laharotte, Nour-Eddin El Faouzi

FERROMOBILE and Security for Low Moment of Traffic Level Crossing

Rim Brahim[1], Simon Collart-Dutilleul[2], Philippe Bon[3], Pierre-Antoine Laharotte[4], and Nour-eddin El Faouzi[5]

[1] rim.brahim@univ-eiffel.fr
[2] simon.collart-dutilleul@univ-eiffel.fr
[3] philippe.bon@univ-eiffel.fr
Univ Gustave Eiffel, COSYS-ESTAS, F-59650 Villeneuve d'Ascq, France
[4] pierre-antoine.laharotte@univ-eiffel.fr
[5] nour-eddin.elfaouzi@univ-eiffel.fr
Univ Lyon, Univ Gustave Eiffel, ENTPE, LICIT-Eco7, F-69675 Lyon, France

Abstract. Level crossings (LCs) are critical components of railway networks and their safety is always at the centre of debate. Several accidents have occurred at level crossings due to non-compliance with road regulations, lack of visibility, behaviour of road users and many others. An innovative project called "Ferromobile" proposes a multi-modal, flexible, and electric vehicle capable of operating on both roads and rails. The main objectives of this project are to ensure flexibility, reconnect territories, promote carbon emission reduction, and maintain affordable costs.

In this paper, the Wireless Access in Vehicular Environments (WAVE) system is proposed as a solution to enhance safety at the LC. WAVE ensures connectivity through dedicated short-range communications (DSRC) between the "Ferromobile" and the infrastructure collecting data about the environment. To ensure the integrity, confidentiality, and authenticity of the exchanged information, the methodology may include encryption mechanisms to protect the data against intrusions that have already happened, inducing an accident involving tramways.

Keywords: Level Crossing · Ferromobile · WAVE · Encryption.

1 INTRODUCTION

At the beginning stands the observation that even in rural areas, some roads were regularly congested, while the railway tracks remained surprisingly deserted. This led to the emergence of the "Ferromobile" project, which aims to use abandoned railway tracks to reduce road congestion and improve the quality of life for rural residents, offering them the convenience of comfortable travel."Ferromobile" is a flexible electric vehicle capable of starting its journey on the road, transitioning onto the railway tracks, and then returning to the

road. It operates at a speed of 70 km/h[6]. It is a shared and collective public transport service.

When the "Ferromobile" operates on railway tracks, it is autonomous. The question that arises is how to improve the safety of both road users and "Ferromobile" passengers at the LC?

Level crossings are places where railways and roads intersect at the same level. They are classified into 4 categories according to the ministerial decree of March 18, 1991 amended by decree no. 2019-525 of May 27, 2019 [7]: Public LCs which are open to all road users are classified in the 1^{st} category. They are equipped with barriers or half-barriers. They can be automated when the maximum speed of the trains is less or equal to 160 km/h, or else be monitored by agents authorized by the rail operator. In the 2^{nd} category, there are public LCs which are crossed under the full responsibility of road users without the presence of barriers or half-barriers and without special surveillance by an agent authorized by the rail operator on lines at speed less or equal to 140 km/h. In the 3^{rd} category we find the public LCs which can only be used by pedestrians and in the 4^{th} category we find the private LCs, for private vehicles, pedestrians and/or shepherds.

The required safety equipment and surveillance measures for each LC depend on the intended use and characteristics of the railways and roads involved. On usual critical parameter is the moment of traffic which is demonstrated to be statistically linked with the number of accidents at LC [20]. The definition of the traffic moment is the multiplication of the number of cars per day and the number of trains per day at a given intersection.

The case we are dealing with is level crossings in the countryside, which are generally low-traffic and sometimes private. To manage the interaction between road users and the rail vehicle, it is necessary to study simple and economical solutions and above all to reduce the additional equipment at the LC.

To improve safety, Intelligent Transportation Systems (ITS) use both short-range communication networks and long-range cellular technologies. These technologies are valuable as they provide crucial safety information, such as alerts in case of nearby anomalies like construction, obstacles, locks, accidents, and others.

In this article, the WAVE protocol is selected as a data transmission solution for LCs in the countryside, which are sometimes private, that offers security and convenience in an ITS. In the considered use case, the ITS covers: the "Ferromobile" that ride on the railway track, as well as, depending on the category of LC, alternative users crossing the track, like shepherds, pedestrian, or agricultural vehicles. WAVE is a wireless communication system to enhance road user safety by facilitating information sharing among them through Dedicated Short-Range Communications (DSRC) [15]. The requirements of DSRC include

[6] https://ferromobile.fr/actualites/insolite-un-vehicule-qui-roule-sur-la-route-mais-aussi-sur-les-rails-inaugure-pres-de-perpignan/

[7] https://securite-ferroviaire.fr/reglementations/arrete-relatif-au-classement-la-reglementation-et-lequipement-des-passages-niveau

maintaining real-time communication with low latency and high reliability [13]. Furthermore, it enables the deployment of decentralized traffic controllers, when the Roadside Units (RSU) supporting the communication are connected to local sensors and equipped with embedded computational abilities to interpret data and automatically generate messages (hazard warnings, etc) [2].

Indeed, a communication failure between a rail vehicle and the infrastructure can lead to serious risks. Without reliable information about the arrival of a rail vehicle, the LC may react inappropriately, thereby increasing the risk of severe accidents. Additionally, without critical information regarding the LC, the "Ferromobile" cannot respond appropriately. It is therefore essential to encrypt the messages exchanged between the rail vehicle and the LC to ensure the integrity and security of the wireless communication system.

To take an example, in 2008 [1], a 14-year-old boy who is an electronics enthusiast and an exemplary student, created a device similar to a TV remote control and used it to take control of the switching systems of public streetcars in the city of Lodz, Poland. As a result, four streetcars derailed and others applied emergency brakes, injuring passengers. Twelve people were injured.Although this attack was a prank as the teenager had told police [8], it is particularly significant as it represents the first cyber attack to have directly caused the injury. In many aspects, the "Ferromobile" system is similar to a tram system: it is a public transport where the infrastructure is not protected like the subway system. For this reason, it seems reasonable to implement protection against hacking even when it comes to level crossings in the countryside where the risks of accidents and collisions are lower compared to urban areas, but the risk of impact remains significant.. This protection remains at a very small cost in terms of money and computing time (being assimilated in the parameter "thinking time"). The country side low traffic lines are not a terrorist target like metro lines of Paris, as they have a little symbolic value.. However, since a prank has already led to serious consequences, this scenario should be reasonably considered. Message encryption is also considered in the following. To ensure the confidentiality of data generated by these connected objects, most Internet of Things (IoT) protocols incorporate cryptographic primitives into their specifications.

The evolution of classical encryption has given rise to a new type of encryption called lightweight encryption, specifically designed for IoT. This type of encryption is suitable for resource-constrained applications, meeting all the constraints of low-power computing applications, including energy consumption, data size, execution time, and more.

In the present paper, we further explore the feasibility and requirements to implement such a solution on the field through a deep analysis of feedback from the literature. The main specificity of the developed solution lies in the countryside requirements and constraints, *i.e.* restricted use of high-technologies and sensors (low-tech), compatibility between needs and resources, etc. We offer to consider a solution with an on-demand service request taking advantage only of communication technologies embedded into the "Ferromobile" vehicles. Some

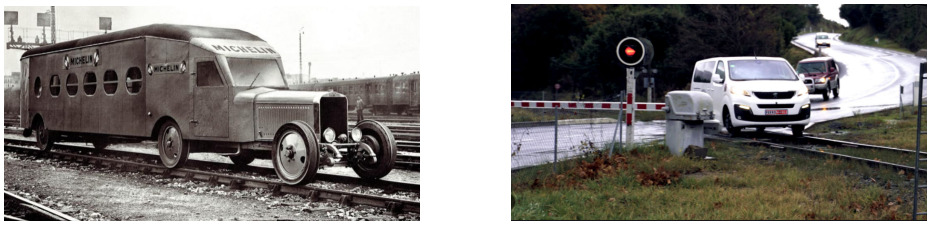
[8] `https://www.theregister.com/2008/01/11/tram_hack/`

efforts are made in the feasibility analysis to ensure safe crossings and fit the requirements with the specificities of "Ferromobiles", which are lighter than usual trains and with specific braking distances.

The remainder of the paper is organized as follow. The second section introduces a description of the "Ferromobile" project. Then, the safe crossing solution for "Ferromobiles" designed for the countryside is developed, and a deep analysis of the feasibility is performed. The feasibility analysis explores the multiple dimensions: (i) the WAVE protocol technology that can be used for communication between the "Ferromobile" and the LC, (ii) the existing literature on braking distance calculation, and (iii) the cryptographic methodology for securing the information shared between the "Ferromobile" and the LC.

2 Objectives of the "Ferromobile" project

In the 1930s, André Michelin developed a lightweight rail-car called the "Micheline" ("Fig. 1a")[9] that ran on rails and was designed to provide maximum comfort to its passengers. In revisiting this concept, an innovative project called "Ferromobile" ("Fig. 1b) has been proposed. The "Ferromobile" is an electric production vehicle from Peugeot that is capable of traveling on both roads and rails simultaneously. This car operates autonomously when on the railway tracks, allowing passengers to travel with ease without the need to drive.



(a) Micheline (b) Ferromobile

Fig. 1: The Mechline of 1930 and the new project "Ferromobile" .

To develop the entire system around the Railmobile, in 2021 the Society of Engineering Construction and Operation of the Ferromobile (SICEF) set up a collaboration between AKKODIS Technologies, Systra, Alstom, Gustave Eiffel University, Entropy, and the Occitanie region.

This project aims to reuse abandoned railroad tracks, which has several advantages. A de-carbonized mobility service will be available 24/7 in the territories, minimizing traffic and providing residents with safe and flexible travel options. It represents a cost-effective economic model suitable for low-traffic on

[9] `https://ferromobile.fr/en/ferromobile/`

small railway lines.The challenge is to bring back service where trains have disappeared.

The "Ferromobile" combines the best of the automobile and railway worlds. It has all the elements of passive safety (seat belts, airbags, etc.) and active safety (Anti-lock Braking System (ABS), Emergency Brake Assistance (AFU), etc.). These systems ensure a safe journey from the first to the last mile.

This "Ferromobile" is a Peugeot series vehicle, an 8-seater public transport, traveling at 70km/h. Thanks to this speed and its mass, its stopping distance is more than 10 times shorter than that of trains. For a train traveling at 90 km/h, it takes 800 meters to stop [17].

3 A solution to ensure safe crossing for "Ferromobiles"

This section details the global architecture and the technologies at stake to support our solution introduced to ensure safer crossing for "Ferromobiles".
In the subsequent sections, we provide an overview of the global architecture of the introduced system. Then, we explore the potential and feasibility of the described methodology according to two components: the use of the WAVE technologies to support data exchanges and the requirements

3.1 Overview of the global architecture

As mentioned earlier, our interest is the Level Crossings in the countryside, which receive low traffic and sometimes private flows. It is essential to monitor the crossing surface to identify potential hazards and improve the safety of road users(cars, pedestrians, and animals) as well as "Ferromobile" passengers.

However, in the countryside, alternative users crossing the "Ferromobile" tracks are expected to be sparse and epiphenomenon, which implies a high-level of risk *i.e.* even if the probability of risk is lower in rural areas due to lower occurrence compared to urban areas, the impact-risk remains significant. A careful attention need to be paid to monitor and manage the intersection during a short time period. To meet the requirements and as illustrated in Fig. 2, a pushbutton switch is used by alternative users to draw attention and trigger the safety system based on communication between the RoadSide Unit (connected to the pushbutton) and the "Ferromobile". Then, a secured communication protocols is applied. The system used to equip the LC can integrate the WAVE protocol as a solution for transmitting LC information to the "Ferromobile". This protocol enables efficient, reliable and interoperable transmission of information. This network enables the transfer of information for LC conditions, so that the "Ferromobile" can be warned immediately in the event of an obstacle on the track through broadcasted warning messages.

This message will be encrypted, broadcast through the Wave radio device and consulted by the "Ferromobile" (decryption and act accordingly). The warning message will continues to be broadcast until the shepherd presses an exit button to signal that the track is clear. This manual button has a light for feedback,

when the ferromobile receive the message. See Fig. 2.
In summary, for this proposed system, the communication mode is divided into

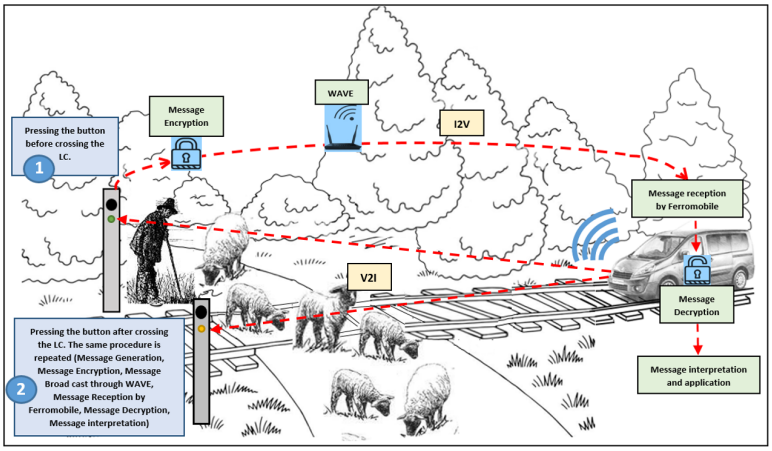


Fig. 2: Communication between infrastructure and "Ferromobile" through the WAVE protocol for LCs in the countryside.

two types, demonstrating the effective integration of ITS

- **Infrastructure-to-Vehicle (I2V) communication:** an alert message on the status of the LCs is provided from the level crossing to the autonomous vehicle (Ferromobile), making travel safer and more comfortable.
- **Vehicle-to-Infrastructure (V2I) communication:** this communication is visually confirmed by the lighting up of a light emitting diode to ensure effective reception of informations by the "Ferromobile".

Thus, V2V communication can take place when several "Ferromobiles" move one behind the other. When an alert message is triggered, the "Ferromobile" receives this message and acts accordingly, while the other railmobiles follow by slowing down or stopping. These "Ferromobiles" can communicate with each other through a local network.

An extended version could be considered for LCs on low-traffic urban areas, a communication system with a longer range than the Wave protocol is required. LC information can be detected by cameras, radars or other sensors. the use of two cameras can be envisaged: one to measure the upstream flow (flow priority level) and one to monitor the LC and detect dangerous situations. This enables the "Ferromobile" to react appropriately by adapting its speed or stopping to avoid a collision Fig. 3.

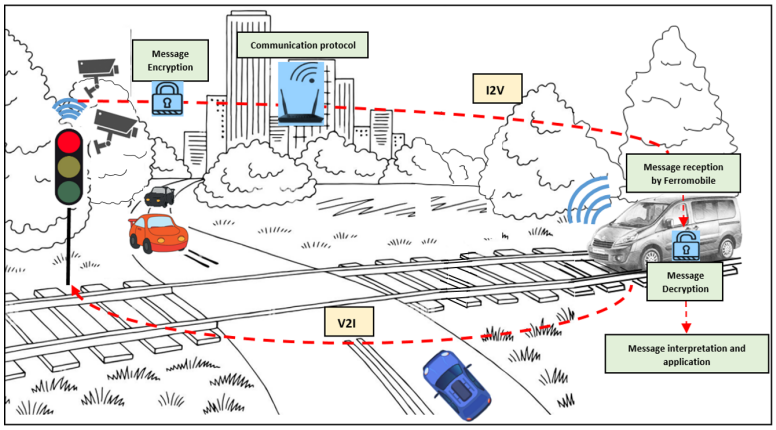


Fig. 3: LCs on the outskirts of urban areas with low traffic levels.

3.2 Wireless communication abilities and contributions

WAVE Standardization protocol: To interconnect machines, you need network cards, different types of cable (twisted pair, fiber optic, etc.), switches, and so on. This is a wired technology, i.e. cabling is required. In this type of communication, there are problems when stations are mobile, so wireless technologies are considered for data transmission with the critical agents that play a role in a potential LC scenario of an accident [24]. Using a methodology proposed in the SELcat European project leads to a focus on the communication between the LC and the "Ferromobile". This methodology is not detailed in the current paper.

The IEEE 802.11p standard, also known as WAVE, is an amendment by the DSRC working group of the IEEE , focusing on wireless access in intelligent transportation systems. Based on the IEEE 802.11 standard, it can be considered as a mobile adaptation of Wi-Fi. Investigating the use of the WAVE protocol correspond to a strategy giving priority to the use of car industry technologies as there is no business model for dedicated technologies for LC for sheep crossing for example [8].

The primary objective of this technology is to enable wireless communication among vehicles and infrastructure, utilising the frequency band allocated to DSRC. For wireless communications in Intelligent Transportation Systems (ITS), a frequency band of 5.850 to 5.925 GHz has been allocated to the DSRC by the Federal Communications Commission (FCC) in the United States, and 5.875 to 5.905 GHz by the European Union [23]. Furthermore, this technology provides a transmission range of up to 1km, allowing efficient communication over longer distances between vehicles [7].

In April 2012 [2], a project called "PANsfer" was tested in collaboration with the French Institute of Science and Technology for Transport, Development,

and Networks (IFSTTAR), the University of Technology of Belfort-Montbéliard (UTBM), École Centrale de Lille, and others[10].

Based on a statistical analysis of a database of accidents/incidents, in this article, the author developed three potential scenarios corresponding to the main causes of accidents (zigzagging, blockage due to congestion at the LC exit and obstruction on LC).

To improve safety, this project used a surveillance camera and the wireless communication system WAVE. The tests were conducted at a LC located in Mouzon, Ardennes. The objective of this project was to prevent collisions by informing vehicles of the presence of the LC and alerting them in case of abnormal behaviours observed on it.

Communication-Assisted Stopping Distance: The term "Stopping Distance" refers to the distance that a vehicle travels until it comes to a complete stop. This distance includes the time it takes for the driver or the vehicle's automated system to react to a problem and for the vehicle to decelerate fully after the brakes are applied. Stopping Distance can be divided into three categories that contribute to the total distance as described in "Fig. 4". The categories of

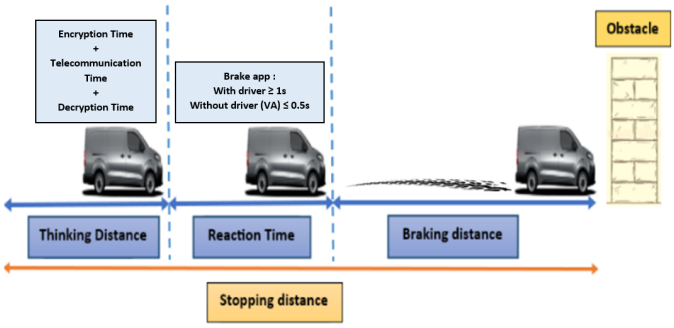


Fig. 4: Stopping Distance.

stopping distance are defined as follow:

- **Thinking Distance:** This refers to the distance a vehicle travels before the driver becomes aware of a problem. This concept of the state of the art is used to localize, in the functional architecture, the time used by the onboard computer to process information produced by the vehicle sensors or received through the network (for example from the LC). This elapsed time, includes the encryption , the telecommunication and the decryption delays. This duration finishes, when the system can take a decision.
- **Reaction Time:** This describes the time it takes for the driver to initiate a response to the encountered problem, such as applying the brakes. In the

[10] https://www.youtube.com/watch?v=MiV41lW8kdk

case of low-traffic LC with "Ferromobile", there is no Human Driver, but an automated one controlled by a computer. Obviously, the computer's reaction time is expected to be shorter than the human driver's one.
– **Braking Distance:** This is the distance the vehicle travels after the driver has responded, such as engaging the brakes, before the vehicle comes to a full stop.

On July 1, 2018 [11], [12], the measure number 5 of the Interministerial Committee for Road Safety (CISR) came into effect. This measure reduces the speed limit from 90 to 80 km/h on two-way roads without a central separator. The objective of this measure was to save lives by reducing the number of severe accidents on these roads.

To highlight the importance of this measure, Road Safety produced a film titled "13 Meters." This experiment was conducted by engineers from UTAC CERAM, experts, and specialists in testing and evaluations. It details an emergency braking situation and demonstrates that a reduction of just 10 km/h can result in gaining 13 meters during braking, which makes a significant difference in terms of stopping distance and accident consequences.

In this experiment, they showed that in the case of emergency braking:

– For a car traveling at 80 km/h, it would have covered 57 meters before coming to a complete stop.
– For a car traveling at 90 km/h, it would cover 70 meters before coming to a stop.

Since our "Ferromobile" travels at a speed of 70 km/h, we can conclude that its stopping distance in case of an emergency is approximately "43 meters".

Furthermore, in [13], the author discussed two equations for calculating the stopping distance. The two equations yield the same result when the car travels below 113 km/h. Using the simplest equation.

The stopping distance is formulated in equation 1:

$$D_S(m) = D_R + D_B \tag{1}$$

With:

– D_R : The thinking distance:

$$D_R(m) = V * T_R \tag{2}$$

V: Velocity / T_R: reaction time

[11] https://www.interieur.gouv.fr/Archives/Archives-des-communiques-de-presse/2018-Communiques/Mise-en-aeuvre-des-decisions-du-CISR-du-9-janvier-2018-concernant-les-pietons-et-l-alcool

[12] https://www.securite-routiere.gouv.fr/les-medias/nos-campagnes-de-communication/13-metres

In our case the thinking distance is:

$$D_R(m) = V * (T_R + T_E + T_T + T_D) \tag{3}$$

T_E : Encryption time / T_T : Telecommunication time / T_D : Decryption time

– D_B : The braking distance. For a vehicle traveling at speeds below 113 km/h, the braking distance is as follows:

$$D_B(m) = \frac{V^2}{2g\mu} \tag{4}$$

g: Gravity (9.81 m/s^2) / μ: coefficient of friction (usually around 0.8)

Generally, the reaction time T_R is about 1 second. However, this delay can be extended due to challenging traffic conditions such as night, fog, or rain, as well as the physical condition of the driver, such as fatigue, illness, or alcohol consumption.

All these issues do not have to be faced in the context of the "Ferromobile" project, as the vehicle is driverless. All the direct safety consequences must be eliminated from the safety analysis.

In terms of safety, autonomous vehicles (AVs) should outperform human drivers, since they adopt a more predictable and responsible driving system, and also have a shorter reaction time than humans (less than or equal to 0.5s [19]).

Regarding the thinking time and reaction time in the context of automated vehicles, they are expected to remain short and at minimal values with respect to the ones observed for Human Drivers.They will be much faster due to the automated system.

Before investigating deeper the selected technology performances, a big upper approximation corresponding to a thinking time and reaction time of 1 second is used. Please note that the telecommunication time reach a few tens of milliseconds plus the encryption and decryption time of a few micro or nanoseconds plus the reaction time less than or equal to 0.5s.

The Fig. 5 illustrates the relationship between stopping distance and velocity. As shown in Fig. 5, the stopping distance for a car travelling at 70 km/h is approximately "43.25 meters".

It is necessary to take into consideration that the friction between the tires and the rails is different from the friction between the tires and the road surface. On the rails, the tires have to adapt to a smooth metal surface. Therefore, the sliding of tires on the rails is generally higher than on the road, resulting in a longer braking distance on the rails than on the road. There is a working team focusing of this particular aspects, but at the moment the road braking distance are used as a reference, assuming that they are an underestimated approximation.

In addition, it is necessary to take into consideration that the alert message can be sent and the "Ferromobile" is not yet within the scope of the Wave protocol (range of 1km). As already mentioned, the message will be repeated until the railroad track becomes clear (until a button is pressed at the exit). The

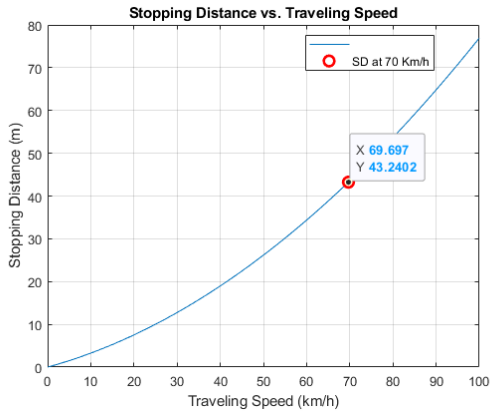


Fig. 5: stopping distance as a function of speed

frequency of the periodic alert message sending produce a time which must be added to the thinking time and the reaction time in order to be able to stop.

Actually, assuming all the preliminary approximations that we have made, the stopping distance including thinking time, reaction time and stopping distance is equal to 43.25 meters. This is more than 20 times less than the WAVE telecommunication distance of 1 km. Since the WAVE protocol allows for signal transmission at a distance of 1 km, we can conclude that the "Ferromobile" has enough time to come to a complete stop before a collision occurs at the LC.

3.3 Cryptography

Given that a 14-year-old was able to control the switching systems of public streetcars, it is likely that the basic Wave short-range communication system would be vulnerable to attack. Based on cryptographic algorithms available in the literature and simulation results for Brahim's master's thesis [6], the execution time for the encryption and decryption process of some micro or nanoseconds [22] is acceptable with the previously mentioned assumption (1 second for: thinking time and reaction time).

Nowadays, in the context of vehicular environments, security requirements such as confidentiality, integrity, non-repudiation, availability, authenticity, reliability, and many others, are of paramount importance due to the recent increase in cyber-attacks.

In the realm of the IoT, the extensive inter-connectivity of devices and the abundance of data being transmitted wirelessly, creates a susceptibility to various forms of attacks. To counteract this, cryptographic algorithms are used to provide the confidentiality of information and maintain its integrity.

"Cryptography" consists of transforming clear information into unintelligible information so that it can only be read by authorised individuals using a key, as described in Fig. 6.

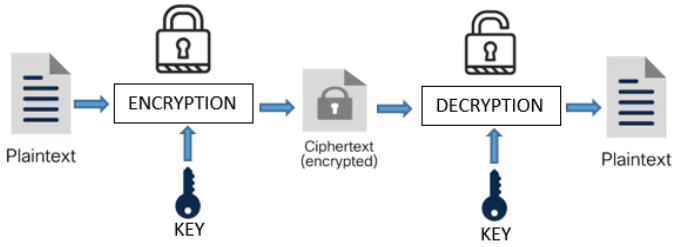


Fig. 6: Principle of cryptography.

The small size, constrained computational capacity, limited memory, and power resources of devices, make it challenging to employ resource-intensive traditional cryptographic algorithms for ensuring data security .

Unfortunately, traditional cryptographic techniques can cause problems in the context of embedded applications as they can be too slow, bulky, and energy-consuming. The Advanced Encryption Standard algorithm (AES) for example, is an excellent and preferred choice for almost all block cipher applications. However, it was not designed to be particularly efficient on low-power platforms such as those dedicated to IoT devices [5] [18].

Recently, research has mainly focused on improving cryptographic algorithms in order to achieve an optimal balance between security, speed, energy consumption, and cost. The development and implementation of lightweight block cipher (LWC) algorithms are very important in wireless sensor networks (WSN) [21].

Encryption algorithms are separated into two main categories, symmetric and asymmetric algorithms.

Asymmetric encryption is so called because two different keys are used each time. A public key to encrypt the message and a private key for the decryption process. Among these algorithms, we mention: Rivest Shamir Adleman (RSA), Diffie Hellman, Digital Signature Algorithm (DSA) and Elliptical Curve Cryptography (ECC) [9] .

In symmetric encryption, also known as secret key algorithms, the sender and receiver use the same secret key for both encryption and decryption processes. It includes hash functions, stream cipher and block cipher.

- **Hash functions**, example: The MD5 and SHA-1 algorithms.
- **Stream ciphers**: Among these algorithms, RC4 [3] is used as WIFI encryption algorithm, E0 algorithm [16] is used in Bluetooth protocol to secure communication and protect transmission, the A5/1 algorithm is used in most countries of the world to ensure confidentiality of conversations on GSM mobile phones and protect communications from eavesdropping [4] ...
- **Block ciphers**: There are different types of block ciphers based on their inner structure. Feistel networks, Substitution Permutation Networks (SPNs), AddRotate-XOR (ARX), NLFSR-based and hybrid. The algorithms based on Feistel network schemes and SPNs network schemes are the two most

widely-used families [11]. Example: PRESENT, PRINCE, LED, SIMON, PICOLO, RECTANGLE, TWINE...

To ensure IoT devices, Three lightweight cryptographic algorithms have been implemented in Brahim's thesis [6]: SIMECK, SIMON and LED in a monoprocessor architecture as three cryptographic instructions extension. The table in Fig. 7, extracted from Brahim's works [6], shows that the SIMECK and SIMON algorithms have an execution time of 440 ns, while the LED algorithm has an execution time of 1920 ns. These execution times are almost negligible compared to our total approximation of 1s time (thinking and reaction times).The same technology was used in [10], implementing the "PRESENT" and "PRINCE" algorithms as two instructions of lightweight cryptographic. These two proposed block cipher algorithms are characterized by high performance, They exhibit high throughputs, as well as good efficiency while maintaining moderate power consumption and dissipation. Consequently, such a technology could be used to ensure message security and respond to real-time and field requirements of our proposed system.

	FPGA	Data path/ bit	Key size/ bit	Slices numb-er	Flip Flops numb-er	LUTs numb-er	Exec-ution time (ns)	Maximu-m frequency (MHZ)	Throug-hput (Mbps)	Efficiency (Mbps/slices)
SIMECK	Spartan6 (Xc6s16 -3)	32	128	206	199	308	440	220.466	320.677	1.556
	Virtex7 (Xc7vx3 30t-3)			200	197	304		613.242	891.988	4.459
SIMON	Spartan6 (Xc6s16 -3)	32	128	206	199	346	440	236.867	344.534	1.672
	Virtex7 (Xc7vx3 30t-3)			202	199	309		576.777	838.948	4.153
LED	Spartan6 (Xc6s16 -3)	32	128	154	146	326	1920	251.27	83.921	0.544
	Virtex7 (Xc7vx3 30t-3)			144	144	323		564.685	250.971	1.742

Fig. 7: Table showing the results of implementing SIMECK, SIMON and LED architectures on two Spartan 6 and Virtex 7 platforms.

Moreover, chaos-based encryption has become popular among researchers due to its high efficiency in data protection. For data security, Jalolouli *et al.* [12] developed two lightweight chaos-based stream ciphers for devices with limited energy and time resources, such as those for IoT. Korba's thesis [14] aimed at designing new chaos maps (3D Cubic-Sine and 2D Cubic-Cat chaotic maps) for

the security of images transmitted over the physical layer of wireless multimedia sensor networks.

Such approaches could be used to refine the process and improve the communication efficiency between infrastructure and the "Ferromobiles".

4 Conclusion and perspectives

Level crossings are a particularly vulnerable link in the railway infrastructure. Numerous accidents occurred at this kind of intersection, resulting in life loss, serious injuries, major property damage, and more. Consequently, at LCs, it is essential to avoid collisions and ensure the safety of road users and rail vehicle passengers. For each type of LC, equipment and safety solutions differ. The "Ferromobile" project is designed to be deployed in rural areas and small towns, where there are LCs in the countryside that are sometimes private, as well as LCs in low-traffic urban peripheries. We, therefore, need simpler, less expensive, and above all, resource-parsimonious solutions to control LC. To sum it up, the LC technological package can be achieved without major investment in hardware and software development.

To improve safety, this article proposes the WAVE protocol as a communication solution between the infrastructure and the "Ferromobile" for LCs in the countryside. This wireless communication network offers significant safety benefits. It enables the transfer of information concerning LC status, thus warning the "Ferromobile" at an opportune moment. This enables it to react appropriately, adapting its speed or stopping to avoid a collision. The warning message can be broadcast up to a distance of 1 km, which is sufficient for a "Ferromobile" traveling at 70 km/h to brake in an emergency. A failure in communication between the LC and the vehicle can lead to dramatic or unacceptable consequences. To ensure the security of shared data, this paper proposes the use of LWC methodology and chaotic system-based encryption. These measures are designed to guarantee the confidentiality, integrity and authenticity of the information shared between the infrastructure and the "Ferromobile". Let us recall to mind that the execution times remain compliant with the global stopping distance of the current paper, even using the various considered technologies of encryption. Consequently, the main architectural assumptions are validated by the preliminary studies of the present paper:

- A low automation LC sending a safety message to the "Ferromobile" increase the safety.
- The use of the WAVE protocol is compatible with the stopping distance.
- The global safety assumptions are preserved by the use of an encrypted WAVE telecommunication mean, where encryption is used to protect the installation from a security point of view.

The aim of future work is to develop complete systems for each type of level crossing. For level crossings in the countryside, which are sometimes private, the combination of the WAVE protocol with the equipment on LCs, will open up

new prospects for more efficient management of LC, reducing the risk of collisions and improving the flow of rail traffic. For level crossings on the outskirts of low-traffic urban areas, a longer range communication system than the Wave protocol is required and security solutions differ. It exists a norm managing the links between security and operational safety. This was typically the case, when in 2008 a teenager corrupted the control of the interlocking of a tram in Poland. A systematic review of this normative context with regard to the targeted application on low-traffic LCs will be performed. In addition, providing the best safety services, taking into account the availability of different telecommunication services depending on the location of the LCs, will require an in-depth analysis of the system which has yet to be carried out.

5 Acknowledgment

The "Ferromobile" project is granted by ADEME in the "France 2030 program" (grant number 2282D0215-F).

References

1. Applegate, S.D.: The dawn of kinetic cyber. In: 2013 5th international conference on cyber conflict (CYCON 2013). pp. 1–15. IEEE (2013)
2. Bahloul, K., Defossez, F., Ghazel, M., Collart-Dutilleul, S.: Adding technological solutions for safety improvement at level crossings: a functional specification. Procedia-Social and Behavioral Sciences **48**, 1375–1384 (2012)
3. Berbain, C.: Analyse et conception d'algorithmes de chiffrement à flot. Ph.D. thesis, Paris 7 (2007)
4. Berzati, A.: Analyse cryptographique des altérations d'algorithmes. Ph.D. thesis, Université de Versailles-Saint Quentin en Yvelines (2010)
5. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J., Seurin, Y., Vikkelsoe, C.: Present: An ultra-lightweight block cipher. In: Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9. pp. 450–466. Springer (2007)
6. Brahim, R.: Implémentation d'un algorithme léger sur une architecture monoprocesseur pour l'internet des objets (iot). master thesis, Monastir scientific university (2021)
7. Dar, K., Bakhouya, M., Gaber, J., Wack, M., Lorenz, P.: Wireless communication technologies for its applications [topics in automotive networking]. IEEE Communications Magazine **48**(5), 156–162 (2010)
8. Dutilleul, S.C., Bon, P., Hamidi, H.: A railway norms application for small traffic railway lines autonomous vehicle. In: 2023 7th IEEE/IFAC International Conference on Control, Automation and Diagnosis (2023)
9. Dutta, I.K., Ghosh, B., Bayoumi, M.: Lightweight cryptography for internet of insecure things: A survey. In: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). pp. 0475–0481. IEEE (2019)
10. El Hadj Youssef, W., Abdelli, A., Dridi, F., Brahim, R., Machhout, M., et al.: An efficient lightweight cryptographic instructions set extension for iot device security. Security and Communication Networks **2022** (2022)

11. Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., Manifavas, C.: A review of lightweight block ciphers. Journal of cryptographic Engineering **8**, 141–184 (2018)
12. Jallouli, O., Chetto, M., El Assad, S.: Lightweight stream ciphers based on chaos for time and energy constrained iot applications. In: 2022 11th Mediterranean Conference on Embedded Computing (MECO). pp. 1–5. IEEE (2022)
13. Knowles Flanagan, S., Tang, Z., He, J., Yusoff, I.: Investigating and modeling of cooperative vehicle-to-vehicle safety stopping distance. Future Internet **13**(3), 68 (2021)
14. Korba, K.A.: La Sécurité des Réseaux de Capteurs sans fil Multimédia par des Systèmes Chaotiques. Ph.D. thesis, Université 08 mai 45 Guelma (Algérie) (2022)
15. Kumar, P., Ali, K.B.: Intelligent traffic system using vehicle to vehicle (v2v) & vehicle to infrastructure (v2i) communication based on wireless access in vehicular environments (wave) std. In: 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO). pp. 1–5. IEEE (2022)
16. Lu, Y., Vaudenay, S.: Faster correlation attack on bluetooth keystream generator e0. In: Advances in Cryptology–CRYPTO 2004: 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 2004. Proceedings 24. pp. 407–425. Springer (2004)
17. Mervent, P.: La question de la sécurité routière et de la sécurité ferroviaire aux passages à niveau. Les Notes du CREOGN **69** (2022)
18. Mohammad, H.M., Abdullah, A.A.: Enhancement process of aes: a lightweight cryptography algorithm-aes for constrained devices. TELKOMNIKA (Telecommunication Computing Electronics and Control) **20**(3), 551–560 (2022)
19. Patel, R., Levin, M.W., Boyles, S.D.: Effects of autonomous vehicle behavior on arterial and freeway networks. Transportation Research Record **2561**(1), 9–17 (2016)
20. Prosser, I.: Level crossings: A guide for managers, designers and operators. Tech. rep., Office of Rail and Road (ORR) (December 2011)
21. Radosavljević, N., Babić, D.: Power consumption analysis model in wireless sensor network for different topology protocols and lightweight cryptographic algorithms. Journal of Internet Technology **22**(1), 71–80 (2021)
22. Tawalbeh, L.A., Tawalbeh, H.: Lightweight crypto and security. Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications pp. 243–261 (2017)
23. Wong, R., White, J., Gill, S., Tayeb, S.: Virtual traffic light implementation on a roadside unit over 802.11 p wireless access in vehicular environments. Sensors **22**(20), 7699 (2022)
24. Öörni, R., Collart-Dutilleul, S., Khoudour, L., Heddebaut, M.: Use of fixed and wireless communication technologies in LC safety application in Proceeding of 2nd SELCAT Safer European Level Crossing Appraisal and Technology Workshop, pp. 161–162. Les collections de l'INRETS, INRETS (Nov 2007)