

# Smart Access Control System for Industrial Machines and Vehicles based on RFID Technology

Davide Colaiuda<sup>1</sup><sup>a</sup>, Giuseppe Ferri<sup>1</sup><sup>b</sup>, Alfiero Leoni<sup>1</sup><sup>c</sup>, Andrea Pelliccione<sup>1</sup>, Piero Faraone<sup>2</sup>, Orlando Quaranta<sup>2</sup>, Valerio Arezzo<sup>2</sup> and Vincenzo Stornelli<sup>1</sup><sup>d</sup>

<sup>1</sup>Department of Industrial and Information Engineering, University of L'Aquila,

Località Campo di Pile, via Gronchi 18, L'Aquila 67100, Italy

<sup>2</sup>Faraone Industrie S.p.A., via S. Giovanni 20, Tortoreto 64018, Italy

**Keywords:** RFID, Radio-frequency Identification, Smart Card, NFC, Work-related Accidents, Access Control, Industrial Trucks, Smart Systems, Industry 4.0.

**Abstract:** In this paper a smart system for Access control of industrial machines and vehicles is presented. The development of the so-called Industry 4.0, together with the spread of contactless technology such as NFC Radio Frequency Identification, and the massive industrialization of working process, resulted in a significant integration of information technologies in smart industrial vehicles and forklifts. These are one of the main causes of work-related accidents, due to a frequent improper usage of this machines. The presented solution is a smart system that uses RFID reader and personal smart cards that interrupts machine ignition or movement, allowing just trained workers use them. Machines usage data are stored in system internal memory. A dedicated application makes new cards compatible and saves user data in them; a simple user interface is also implemented to add or remove employees permission or authorised cards and tags.

## 1 INTRODUCTION

In the last years, a significative part of tracking and tracing procedures is realized with wireless systems. Among them, Radio Frequency Identification (RFID) gained a significative popularity due to its simple structure, which may involve magnetic coupling or a proper RF wave transmission, according to the implemented antenna (Turcu, 2009). This technology permits a contact-less data transmission using tag or cards equipped by a built-in memory chip with a proper data interface and signal modulation circuits (Kuilin Chen, Dongyan Zhao, Haifeng Zhang, Yubo Wang & Liang Liu, 2013), based on the operating frequency. One of the most diffused RFID technologies is based on data transmission at a 13.56 MHz frequency. In the last years, different standards have been defined, such as the ISO/IEC 14443, for which several IC cards interfaces have been

developed, based on Near Field Communication (NFC) (Lu Chao & Li Yong-ming, Kuo et al., 2018).

Wireless and contactless data transmission is widely diffused today, and smart cards are suitable items to easily store personal data (Bejo, Winata & Kusumawardani, 2018, Mirza & Alghathbar, 2009). A “smart card” is a common plastic card that integrates an IC embedding a non-volatile memory where data can be stored, a demodulator and an antenna (Hendry, 1998, Domingo-Ferrer, 2000) that work passively, getting its energy supply from the magnetic field generated from a proper reader or writer interface. Memory blocks are usually protected by one or more authentication and control keys, that allows to read or write their content. This guarantees a certain degree of security, using proper encryption algorithms for data protection (Feng, Wang, Lu, Jin & Shu, 2021, He, Lin, Wang & Wang, 2020, Naija, Y., Beroulle, V., Hely, D., & Machhout, M., 2016).

<sup>a</sup> <https://orcid.org/0000-0002-8488-9606>

<sup>b</sup> <https://orcid.org/0000-0002-8060-9558>

<sup>c</sup> <https://orcid.org/0000-0002-0066-4216>

<sup>d</sup> <https://orcid.org/0000-0001-7082-9429>

Because of this, they are growing in popularity also in money-involving applications (Jesani, Gupta, Bhatt, Singh & Saxena, 2020). Every system based on this technology is very suitable for a lot of different applications: these usually associate data to tags (or cards, if using NFC) and elaborates them to find out sensors data (Turki et al., 2019, Trevisan & Costanzo, 2014), to track items position (Wang, Liu & Wang, 2010, Renuka, Ng Chin Nan & Ismail, 2013) or localizing them (Al-Saedi & Azim, 2017) and for other data measures (Chen, Peng & Yan, 2019, Bevacqua, Bellizzi & Merenda, 2019).

Nowadays there are a lot of available commercial solutions for NFC RFID communications that uses smart cards to store data and permissions, managing other systems with the information stored in them. Just a few of them, anyway, are aimed to reduce work-related risk and injuries; a lot of studies focused their attention on both fatal and non-fatal accidents involving heavy machinery on working places (Kazan & Usman, 2018, Jeong, 1998, Larsson & Rechnitzer, 1994, Stout-Wiegand, 1987, Pan et al., 2007). Recent data shows that every year there are over 3 million of work-related accidents ("Non-fatal accidents at work by NACE Rev. 2 activity and sex - Products Datasets - Eurostat", 2022), of which more than 3000 are fatal ("Fatal Accidents at work by NACE Rev. 2 activity - Products Datasets - Eurostat", 2022). This kind of injuries are mainly reported by manufacturing, construction and wholesale industries that make a great use of forklifts, aerial platforms, and other industrial trucks. These in fact can be driven only by trained and qualified operators, due to the heavy weights, the low stability and the altitudes involved, and a great part of accidents is due to operator inaccuracy and lack of training.

In this situation, research is going towards the "Industry 4.0", that is in the design of smart machines with autonomous control systems (Patil, Rajurkar, Salunke & Pljonkin, 2019, Kasahara & Mori, 2015), that can automatically abrupt certain operations if they detect a risk for workers. With this mind, this paper proposes a built-in access control system for industrial vehicles, that uses NFC passive smart cards to manage engine ignition and movement, depending on the user permissions and specific training.

## 2 SYSTEM OPERATION

A block diagram of RFID card (or tag) and reader is shown system in Fig.1. The proposed system (Fig.2) consists of two devices: one or more Access Tag Writer (ATW) with a dedicated software application

and several Access Tag Readers (ATR), one for each machine to control. The system is completed with a number of MIFARE Classic 1K (NXP, 2022) smart cards depending on the number of possible operators and workers in which are stored operator data.

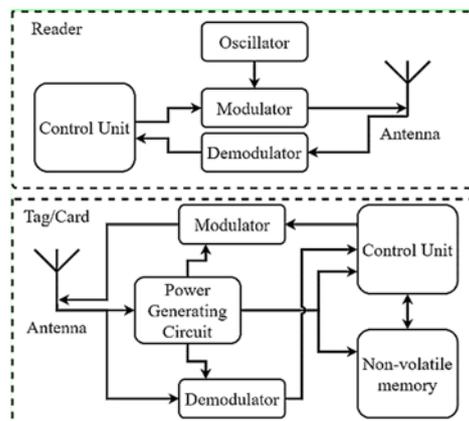


Figure 1: Block diagram of a RFID-based reader and a RFID passive smart card.

The data structure of 1K MIFARE Classic cards is that following: the whole memory storage is divided into 16 sectors, with 4 blocks of 16 bytes each. For every sector, the first three blocks are general purpose usable bytes, that can be written with user information and data; the last block of a sector (called "sector trailer") contains the protection bytes and access bits for the whole sector's block. The first and last six bytes contains two protection keys (key A and key B, respectively) that needs to be used (one or both, depending on Access bits) to read or write on the relative sector. The left 3 bytes are Access bytes (whose combination controls permissions to read, write or doing other operations) and a general purposes byte. Once correctly authenticated, the card content can be read or written by a compatible RFID reader. In the proposed system each worker has a personal smart card containing information and guidance permissions for heavy trucks and machines utilisation.



Figure 2: Proposed system operation.

The ATW writes users data on their personal smart card, making them compatible with the ATR.

This process is realized through the dedicated application (see Fig. 3) where information is entered, and cards (or tags) are written or deleted. The ATR is installed on a machine and divides truck engines

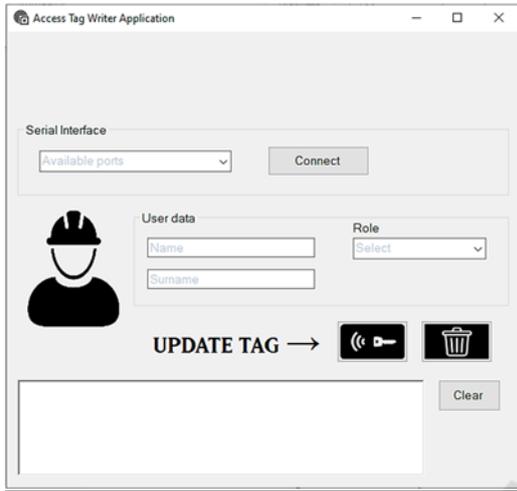


Figure 3: Access Tag Writer (ATW) application interface.

with their power supply, using normally opened relays. Since permissions can be temporary, a specific role for adding and remove permissions has been implemented. In this way, a department head can use his own smart card to give driving permission to a specific user without the need of using the ATW, but just passing his card close to the ATR and right before passing the worker one, so to authorise to drive the vehicle (the same principle is used to remove that permission). This device is the effective machines access control and is designed to work only with specific cards written by the ATW. Also, to keep trace of vehicle usage, user data are stored in a local memory every time the machine is enabled by an operator.

### 3 INTERNAL ARCHITECTURE

The presented ATW consists of a microcontroller that communicates with a commercial RFID reader IC, reading data from a serial port (transmitted by the application in the correct format) and writing the detected tag immediately after. To associate a card with his owner, the designed ATW is used: this is a device with an RFID tag reader and writer (compatible with Standard ISO/IEC 14443 smart IC cards), that works on empty cards. Through the dedicated application, user data are entered in the app and transmitted to the ATW through a serial port; these data concern in identity and role (that includes

permissions). Once entered, an empty smart card must be approached to the ATW in order to write them and protect the used sectors with secret keys: this is both for security and with the aim to make new cards compatible with the ATR.

The ATR also consists of a microcontroller and the same RFID reader, but it also embeds relays for engines, a non-volatile memory chip, an RTC and some status led. When the machine is powered on, the RFID reader of the ATR starts scanning for MIFARE cards in his close field and tries to authenticate them with the same keys written by the ATW. When it detects a valid smart card, the role written in the relative blocks is checked. At this point, machine engines will be powered on only if the user have the permission to drive it, and time and data of the user activity will be registered on an internal memory to keep trace of machine usage. In Fig. 4 is shown a simplified algorithm run by the ATR installed on machines. When powered up, the device starts

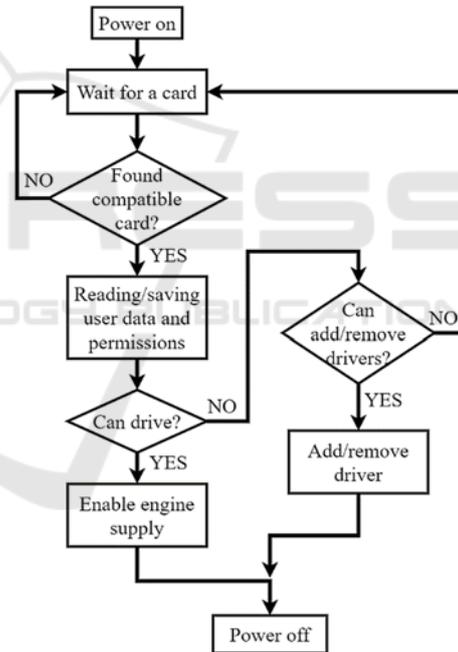


Figure 4: Simplified algorithm executed by the Access Tag Reader.

scanning his field close looking for a card; if a compatible one is detected, the system saves user data and check its authorization to drive or to change other users permissions. In this way, the Access Tag Writer is required only to make cards compatible as first instance or to newly hired employees; the truck driving permission can be managed just on the truck themselves. In this way, the proposed system guarantees a safe usage of industrial trucks letting

only trained people drive them, then identity information is collected to avoid card disposal among workers.

To better evaluate system functionality, a prototype version of the full system has been implemented to ensure its functionality. It has been mounted on the machine Elevah® 5 ("Elevah E5 - Aerial platform", 2022), that is an aerial lift designed



Figure 5: Elevah® 5 aerial platform by Faraone Industrie S.p.A.

by Faraone Industrie S.p.A. (see Fig. 5): this has two engines that control movement and elevation, respectively. The ATR interrupted their power supply, enabling them just if an allowed smart card was detected, confirming the overall functionality.

## 4 CONCLUSIONS

This work proposed a RFID-based system, composed of an Access Tag Writer to write user data in their personal smart card, and a device (the Access Tag Reader, specific for each machine) that manages engines power supply according to the operator permission, to avoid accidents and physical damage due to improper use of vehicles from unqualified users. Data read from cards are stored every time engines are enabled from an operator with their card, which contains identity and licenses of the owner. Though cards data can be written only with the relative application, permission managing is easily implemented with proper tags, that when read from the ATR make the following-read card allowed or not-allowed to drive the truck. As a future development, different sensors, such as distance sensors or accelerometer, can be embedded to the system, so to control differently machine movements, enabling just the ones for which the operator is

trained. Also, a proper remote interface can be implemented embedding a WiFi or GSM module, reading usage data from a remote software application for data consultation.

## REFERENCES

- Turcu, C. (2009). *Development and implementation of RFID technology*. IN-TECH.
- Kuilin Chen, Dongyan Zhao, Haifeng Zhang, Yubo Wang, & Liang Liu. (2013). 13.56 MHz passive electron tag for smart card application with high-security. *2013 IEEE International Conference On RFID-Technologies And Applications (RFID-TA)*.
- Lu Chao, & Li Yong-ming. The RF interface circuits design of contactless IC cards. *ASICON 2001. 2001 4Th International Conference On ASIC Proceedings*.
- Kuo, Y., Grosso, A., Galimberti, F., Tantera, J., Mallo, J., & Verrastro, S. (2018). Analog front-end design of contactless RFID smart card ISO/IEC14443A standard — Compliant. *2018 IEEE 9Th Latin American Symposium On Circuits & Systems (LASCAS)*.
- Bejo, A., Winata, R., & Kusumawardani, S. (2018). Prototyping of Class-Attendance System Using Mifare 1K Smart Card and Raspberry Pi 3. *2018 International Symposium On Electronics And Smart Devices (ISESD)*.
- Mirza, A., & Alghathbar, K. (2009). Acceptance and Applications of Smart Cards Technology in University Settings. *2009 Eighth IEEE International Conference On Dependable, Autonomic And Secure Computing*.
- Hendry, M. (1998). Smart Card Security and Applications. *EDPACS*, 25(11), 18-18.
- Domingo-Ferrer, J. (2000). *Smart card research and advanced applications*. Boston: KLUWER ACADEMIC PUBLISHERS.
- Feng, Y., Wang, H., Lu, H., Jin, W., & Shu, N. (2021). Security Analysis and Optimization Methods of LSFR Generating Function for MIFARE Classic CARD. *2021 IEEE 4Th International Conference On Computer And Communication Engineering Technology (CCET)*.
- He, H., Lin, H., Wang, R., & Wang, H. (2020). Research on RFID technology security. *2020 IEEE 3Rd International Conference On Automation, Electronics And Electrical Engineering (AUTEEE)*.
- Naija, Y., Berouille, V., Hely, D., & Machhout, M. (2016). Implementation of a secured digital ultralight 14443-type A RFID tag with an FPGA platform. *2016 International Conference On Design And Technology Of Integrated Systems In Nanoscale Era (DTIS)*.
- Jesani, N., Gupta, N., Bhatt, S., Singh, P., & Saxena, A. (2020). Smart Card For Various Application In Institution. *2020 IEEE International Students' Conference On Electrical, Electronics And Computer Science (SCEECS)*.
- Turki, B., Ali Ziai, M., Hillier, A., Belsey, K., Parry, A., & Yeates, S. et al. (2019). Chemical Vapor Detecting Passive RFID Tag. *2019 IEEE International*

- Conference On RFID Technology And Applications (RFID-TA).*
- Trevisan, R., & Costanzo, A. (2014). Exploitation of passive RFID technology for wireless read-out of temperature sensors. *2014 IEEE RFID Technology And Applications Conference (RFID-TA).*
- Wang, W., Liu, Y., & Wang, S. (2010). A RFID-enabled Tracking System in Wire Bond Station of an IC packaging assemble line. *2010 IEEE International Conference On RFID-Technology And Applications.*
- Renuka, N., Ng Chin Nan, & Ismail, W. (2013). Embedded RFID tracking system for hospital application using WSN platform. *2013 IEEE International Conference On RFID-Technologies And Applications (RFID-TA).*
- Al-Saedi, S., & Azim, M. (2017). Radio Frequency Near Communication (RFNC) Technology: An Integrated RFID-NFC System for Objects' Localization. *2017 9Th IEEE-GCC Conference And Exhibition (GCCCE).*
- Chen, L., Peng, C., & Yan, Z. (2019). A simple NFC parameters measurement method based on ISO/IEC 14443 standard. *2019 IEEE International Conference On RFID Technology And Applications (RFID-TA).*
- Bevacqua, M., Bellizzi, G., & Merenda, M. (2019). Field Focusing for Energy Harvesting Applications in Smart RFID Tag. *2019 IEEE International Conference On RFID Technology And Applications (RFID-TA).*
- Kazan, E., & Usmen, M. (2018). Worker safety and injury severity analysis of earthmoving equipment accidents. *Journal Of Safety Research, 65*, 73-81.
- Jeong, B. (1998). Occupational deaths and injuries in the construction industry. *Applied Ergonomics, 29*(5), 355-360.
- Larsson, T., & Rehnitzner, G. (1994). Forklift trucks—analysis of severe and fatal occupational injuries, critical incidents and priorities for prevention. *Safety Science, 17*(4), 275-289.
- Stout-Wiegand, N. (1987). Characteristics of work-related injuries involving forklift trucks. *Journal Of Safety Research, 18*(4), 179-190.
- Pan, C., Hoskin, A., McCann, M., Lin, M., Fearn, K., & Keane, P. (2007). Aerial lift fall injuries: A surveillance and evaluation approach for targeting prevention activities. *Journal Of Safety Research, 38*(6), 617-625.
- Non-fatal accidents at work by NACE Rev. 2 activity and sex - Products Datasets - Eurostat. (2022). Retrieved 4 March 2022, from [https://ec.europa.eu/eurostat/web/products-datasets/-/hsw\\_n2\\_01](https://ec.europa.eu/eurostat/web/products-datasets/-/hsw_n2_01)
- Fatal Accidents at work by NACE Rev. 2 activity - Products Datasets - Eurostat. (2022). Retrieved 4 March 2022, from [https://ec.europa.eu/eurostat/web/products-datasets/-/hsw\\_n2\\_02](https://ec.europa.eu/eurostat/web/products-datasets/-/hsw_n2_02)
- Patil, P., Rajurkar, V., Salunke, A., & Pljonkin, A. (2019). Smart Forklift to Reduce Accidents. *2019 2Nd International Conference On Intelligent Communication And Computational Techniques (ICCT).*
- Kasahara, M., & Mori, Y. (2015). The proposal of the forklift fall accidents prevention method using sliding mode control. *2015 54Th Annual Conference Of The Society Of Instrument And Control Engineers Of Japan (SICE).*
- NXP (2022). Retrieved 4 March 2022, from [https://www.nxp.com/docs/en/data-sheet/MF1S50YYX\\_V1.pdf](https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf)
- Elevah E5 - Aerial platform. (2022). Retrieved 4 March 2022, from <https://www.elevah.com/en/products/elevah-5>.