Tekhnê
January - June 2020, Vol. 17, No. 1, pp. 61 – 68


ISSN 1692-8407

# Password-based vehicle access control system for parking lots designed and simulated in Verilog

*Sistema de control de acceso de vehículos a estacionamientos con contraseña diseñado y simulado en Verilog*

Sergio A. Galindo G.[1] and Hernán D. Hernández G.[2]
[1]Facultad Tecnológica, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia
sagalindog@correo.udistrital.edu.co
[2]Facultad Tecnológica, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia
hdhernándezg@correo.udistrital.edu.co

This paper presents a low-cost embedded system for vehicle entry and exit control in conventional parking lots. Given the pandemic situation, the system seeks to ensure security and service optimization and reduce contact with security staff. The design of a sensor-activated control system that prompts the user for a password to enter or exit the parking lot is presented. In addition, the system incorporates a security alarm that is activated if the user enters the wrong password three times in a row. The simulation was performed by modules that refer to the data flow. The design of the digital components was done in Verilog. The results are successful; the system has a low implementation cost and does not require external components.

*Keywords:* Control system, digital system, parking lot, security

En este artículo se presenta un sistema embebido de control de ingreso y salida de vehículos en parqueaderos convencionales de bajo costo. El sistema busca garantizar seguridad y optimización del servicio, y además reducir el contacto con el personal de seguridad dada la situación de pandemia. Se presenta el diseño de un sistema de control activado por sensores que solicita al usuario una contraseña para poder entrar o salir del parqueadero. El sistema incorpora una alarma de seguridad que se activa en caso de que este ingrese la contraseña incorrecta tres veces seguidas. La simulación se realizó por módulos que hacen referencia al flujo de datos. El diseño de los componentes digitales se realizó en Verilog. Los resultados obtenidos son satisfactorios, el sistema tiene un bajo coste de implementación y no requiere de componentes externos.

*Palabras clave:* Parqueadero, seguridad, sistema digital, sistema de control

**Article typology:** Research

**Received:** April 1, 2020
**Accepted:** April 24, 2020

**Research funded by:** Universidad Distrital Francisco José de Caldas (Colombia).

**How to cite:** Galindo, S., Hernández, H. (2020). *Password-based vehicle access control system for parking lots designed and simulated in Verilog*. Tekhnê, 17(1), 61 -68.

## Introduction

Currently, many parking lot entry and exit control systems are carried out manually by security personnel. This results in a late and suboptimal parking lot management process, generating traffic at the entrances and exits. In addition, there is no control over the number of vehicles entering and exiting, which creates uncertainty regarding available space (Puranic et al., 2016; Widodo et al., 2020). The cost of an automated parking lot security system can be offset by productivity improvements and customer satisfaction resulting from a higher utilization rate for the parking lot.

Since automated systems have been implemented to solve the aforementioned problems, some of which are described below, there has been increased productivity and customer satisfaction. The parking lot security system is improved due to reduced road closures, automated toll collection in many locations, and the ability to control the number of cars allowed in and out of parking lots.

Biometric control systems are intended to restrict vehicle access according to the physical characteristics of the vehicle user, such as eye iris, eye retina, face geometry, hand vein pattern, fingerprint, hand geometry, voice, ear shape, etc. (Boriev et al., 2016; Buenano et al., 2009; Lourdes, 2017). Each of these characteristics is mapped to a unique code, which prevents access when the vehicle driver does not possess the corresponding code. Biometric systems have been deployed in numerous industries, including the U.S.

ALPR systems control vehicle access to restricted areas by applying artificial vision to recognize, fragment, and segment the characters of vehicle license plates based on images or videos taken by cameras (Martínez et al., 2018; Martınez et al., 2018; Montiel et al., 2018). Thus, only vehicles with specific license plates can access a particular area (Mohandes et al., 2016; Puranic et al., 2016). Local law enforcement agencies have been using ALPR to reduce crime and improve highway safety.

RFID systems are based on recognizing tags using radio frequency at a certain distance and frequency. The tags are devices consisting of a microchip and an antenna. These are incorporated into vehicles so that their recognition allows access to a specific area (Pala & Inanc, 2007; Zhou & Zhihua, 2016). Tags are affixed to the sides of license plates, fixed to a special paper that identifies the owner.

Other control systems include automatic vehicle barriers and electromechanical arms. However, the abovementioned strategies imply a high development complexity and an increased investment cost. That is why we are interested in designing a simple and efficient control system that does not generate high prices at the time of implementation in a parking lot.

This project aims to design a system for vehicle access to parking lots through the entry of a single password per user. The project is intended for a parking lot with two entrances and one exit. The system will be designed with the Verilog hardware description language; it will consist of the detection of vehicles from sensors and the activation of the access levers according to the password entered by the user. In addition, a security alarm will be provided in case of multiple errors when entering the password.

The system will allow the control of the vehicles in the parking lot for a better management of availability, and will perform the procedure of control of entry and exit of vehicles in a more optimal way. In addition, it will offer a secure and automated way to do so since it is implemented on a small embedded system (Galvis & Madrid, 2016).

## Problem Statement

Currently, some parking lots have antiquated systems for controlling the entry and exit of vehicles, such as the manual systems used by security personnel, which have security and service optimization problems (Boriev et al., 2016; Buenano et al., 2009).

Some of the problems highlighted in the conventional control systems are theft of vehicles or vehicle accessories, superficial vehicle damage, late management of the parking lot, traffic in the entrance areas, inconveniences with identity verification, etc. Added to this, with the current situation of COVID-19, continuous contact with security personnel becomes a problem.

In the market, some solutions propose the automation of control systems, but many have a high implementation cost that does not justify their installation in parking lots. That is why the need arises for a control system that is not very complex, economical, and easy to implement for conventional parking.

Most systems on the market require very complex integrated systems since they are based on particular characteristics of users, such as biometric systems or license plate recognition. This means that the technology is very sophisticated and requires external components such as high-level equipment, which is why its implementation is not justifiable in any parking lot.

Is it possible to design and simulate a simple, safe, and economically viable vehicle entry and exit control system for conventional parking lots?

The solution to the problem is to design a vehicle entry and exit control system based on a password, which is requested when a sensor detects the presence of a vehicle at the entrance or exit of the parking lot; the validation of the password will result in the opening of the entry lever; on the other hand, if it is entered three times incorrectly, a security alert will be triggered. The system described above will be designed with the Verilog hardware description language.

## Research Method

The modules shown in the flowchart in Fig. 1 are programmed using the Verilog hardware description language. In the following, we will briefly discuss how to develop each of the modules.

### Password entry in BCD

The first module consists of a numeric keypad where the user can enter the four characters of the password. There will also be an OK button to transmit the password information to the entire login control system.

A module with a single nine-bit input and a single 4-bit binary output will be used, its programming will be based on the always statement and the case function will be used to describe each of the input digit possibilities.

### Binary password entry

This module is in charge of making sure that the four characters of the password occupy an independent space each, so that the password can be entered completely. For this, the module will be sensitive to each keystroke made by the user, with each keystroke the position of the character will advance to the next, until completing the four positions of the password.

This module will be programmed with the always statement, it will have as input the binary output of the first module and as output the four positions of the password. The module will be based on a demultiplexer, which will have four output channels that represent the characters of the password. This with the difference that the switches that control the channel that is shown at the output will vary their position according to the keystrokes made by the user.

### Graphical interface

The password entered by the user can be displayed through a graphical interface consisting of four seven-segment LEDs.

For this, a module will be used in which each character position of the password in binary will have a respective value in the 7 segments. The 7 segments will show the numerical value in decimal of each password position.

The simulation will be based on a 7-segment common anode display.

### Password verification

This module receives the four password characters and compares them with the correct passwords, if the password is incorrect it sends the data to an error counter that goes up to number three, on the contrary, if it is correct it sends a logical one to the door status module,

The module uses the always statement and is based on a simple else if loop, which sends a single true and an error signal of up to three bits, which allows counting the number of errors. Once a success is detected in the password the error counter is reset.

### Door and alarm condition

This module is in charge of defining the status of the door based on several variables such as the correct password, the error counter, the sensor and the manual operation input. The gate states are defined as a two-bit bus, each combination representing one state as shown in Table 1.

**Table 1**

*Coding of door states*

| Entry Signal | Door Action |
|---|---|
| 00 | Maintain current status |
| 01 | Open the door |
| 10 | Close the door |
| 11 | Remove power for manual operation |

On the other hand, the alarm is activated only with a logic one, and remains off when it receives a logic zero.

Considering this, the module will have as output the state of the two-bit gate and the one-bit alarm. The module will work with an else if block, which contains all the conventional combinations of the different inputs and the combinations that are not there will have a gate status of 00 and alarm off.

Fig. 2 shows the block diagram by which the connection of the modules and therefore the control system is represented.

## Results and Discussion

All modules were simulated in the online software Playground, where different combinations of the layers of each module were injected.

### Password entry in BCD

Fig. 3 shows the component created in the PSoC Creator software corresponding to module 1. Fig. 3 shows the inputs and outputs of the module. All the number options that could be typed by the user on the numeric keypad were simulated, the results are shown in Fig. 4.

**Figure 1**

*Control system flowchart.*

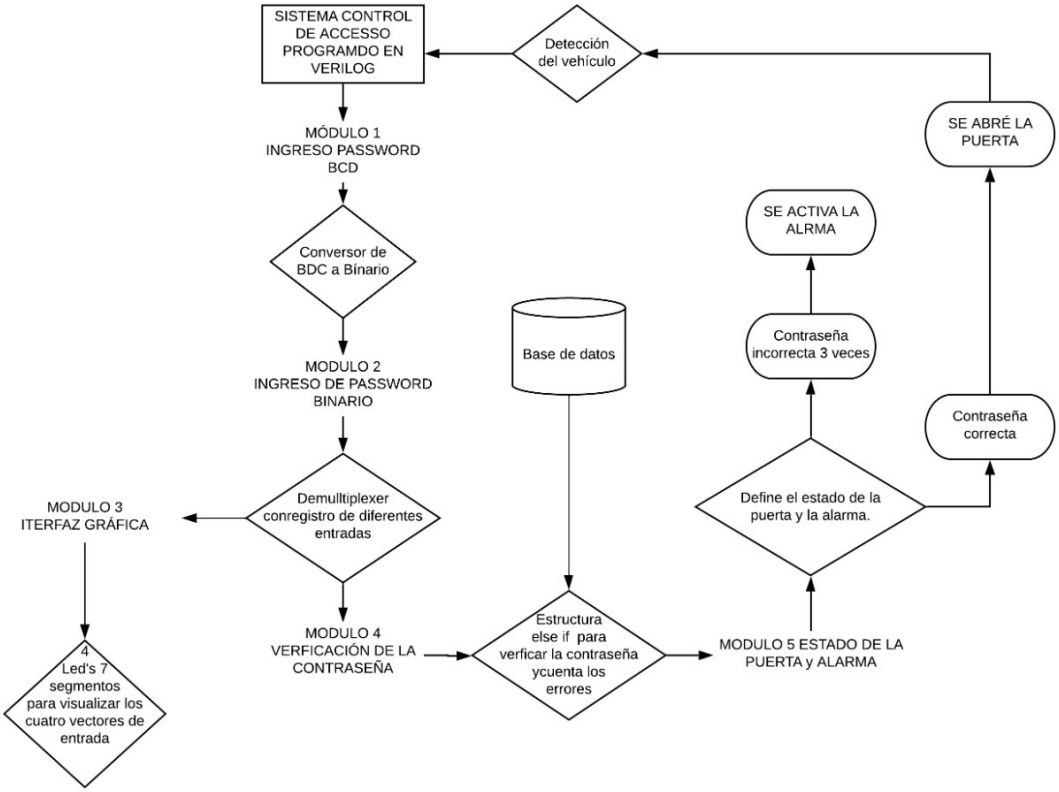



**Figure 2**

*Block diagram of the control system.*

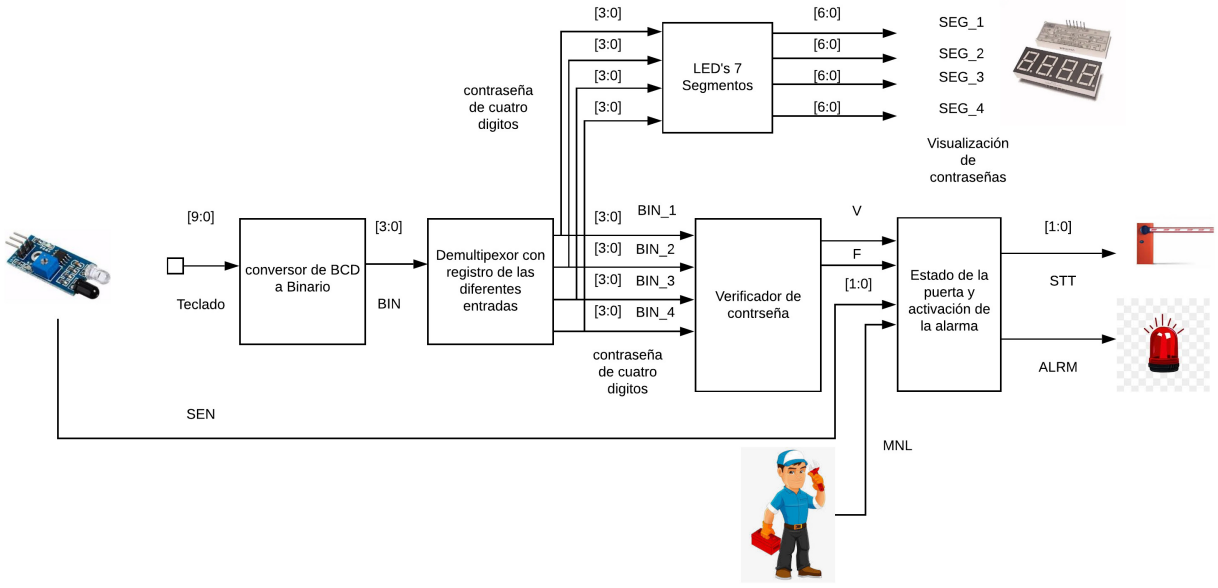
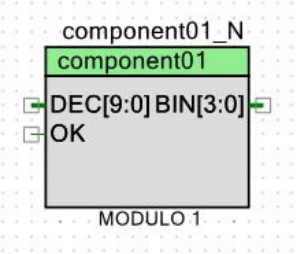


**Figure 3**

*Component module 1.*




As can be seen in Fig. 4, it shows the presses of a single button that has as representation a binary number in BCD.

### Binary password entry

For module 2, the four keystrokes of the user were simulated and how each one of them occupied an output position of the user in binary. Fig. 5 shows the image of the component created in PSoC Creator corresponding to module 2.

**Figure 5**

*Component module 2.*

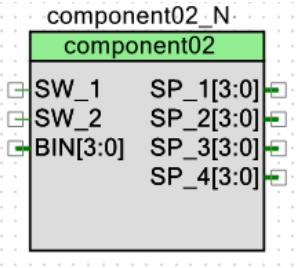


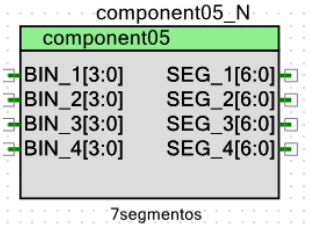

Fig. 6 shows how the user enters the password *1298* and how each of the characters is placed in an output position of the module. It can be affirmed then the correct operation of the same one.

### Graphical interface

For the graphic interface we used a single module that will show the representation of the digits selected by the user in four seven-segment LEDs of common anode, one seven-segment LED for each character of the password. Fig. 7 shows the component created in Verilog for this module.

**Figure 7**

*Component module 3.*



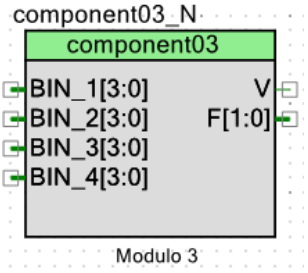

The simulation describes the behavior of a single seven-segment LED when pressed by the user and the others are ignored since the behavior is exactly the same for the other three. The simulation is shown in Fig. 8. All the digits that the 7-segment display represents are shown there.

### Password verification

In this module, the counting of errors and the signal corresponding to the success of the password was simulated, for this purpose, data buses corresponding to correct and incorrect passwords were injected in order to verify the proper functioning of this important module. Fig. 9 shows the component created in Verilog corresponding to this module.

**Figure 9**

*Component module 4.*




In the simulation, three correct passwords were entered, resulting in three correct password 'V' signals in one. Subsequently a wrong password was entered and it was observed that the error signal 'F' changed state to 1 and the 'V' signal changed to low. Following this, three wrong passwords were entered and it could be seen how the errors were counted in the output 'F'. The simulation can be seen in Fig. 10.

### Door and alarm condition

For the simulation of this module, all the door states were obtained according to the different inputs (V, F, Sensor, Manual intervention). The component created for this module is shown in Fig. 11.

**Figure 4**

*Simulation of module 1.*

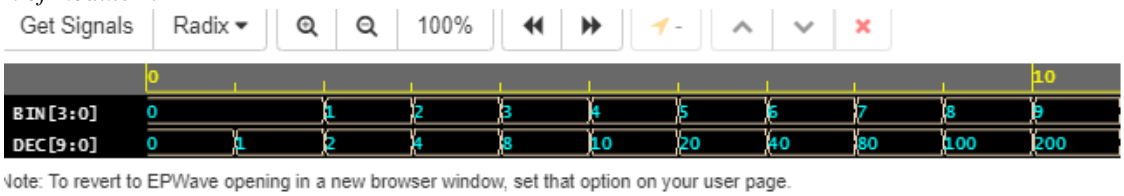



**Figure 6**

*Simulation of module 2.*

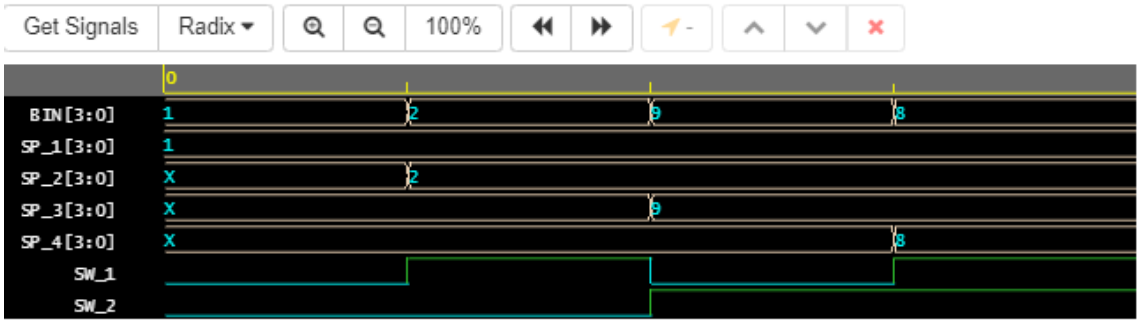



**Figure 8**

*Simulation of module 3.*

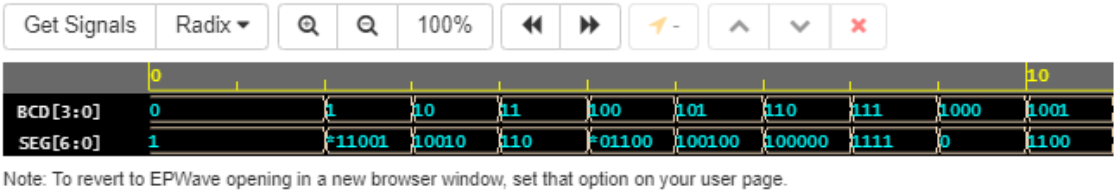



**Figure 10**

*Simulation of module 4.*

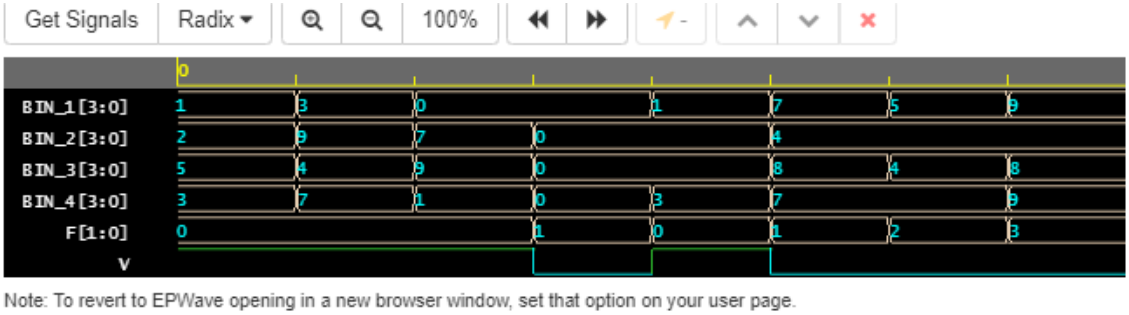
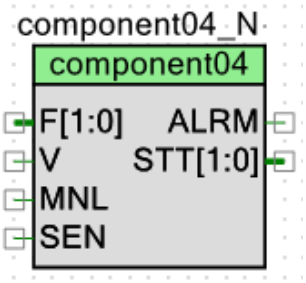


**Figure 11**

*Component module 5.*




The values given to the inputs in the simulation allowed us to check the positions of the 'STT' door according to the basic criteria, you can see a case in which three errors are received, therefore the door remains in its current state (closed) and the 'ALRM' alarm is activated, or how when the sensor is at zero the door is ordered to close since there is no vehicle present, which means that the vehicle has already entered. It can also be seen that when the password signal 'V' is high and the door opens and so on, until obtaining all the states of the door according to their inputs. The simulation can be seen in Fig. 12.

## Conclusion

It can be observed that the control system works satisfactorily according to the parameters indicated in the methodology; this is according to the effectiveness of the simulation of each of the proposed modules. This suggests that the control system will behave adequately in a future implementation in an actual parking lot.

Within the analysis presented above concerning a vehicle access control system, the results indicate that the implementation of a security system using a password to replace systems such as bioelectrical detectors, ALPR systems, RFID, and automatic barriers is reliable since our system makes use of free software, hardware with very low investment and high reliability.

The systems that allow us to increase security, in the case that concerns us, an access control system to parking lots using technology, using logical systems that limit human intervention and reduce the risk of danger.

Automatic and efficient systems such as the one described above allow us as a society a better way to interact in the current environment, which suggests a minimum social interaction to preserve our health and that of our loved ones.

The development of our article allowed us to acquire better handling of the hardware description language Verilog, to carry out an idea in a practical way with multiple forms of development, given the various tools that the PSoC Creator software has.

## References

Boriev, Z., Nyrkov, A., Sokolov, S., & Chernyi, S. (2016). Software and hardware user authentication methods in the information and control systems based on biometrics. *IOP Conference Series: Materials Science and Engineering*, *124*, 012006. https://doi.org/10.1088/1757-899x/124/1/012006

Buenano, G., Clavijo, S., Flores, H., & Galio, G. (2009). Desarrollo de un sistema biometrico de control de acceso de entrada y salida vehicular. *Artículos de tesis*.

Galvis, J., & Madrid, J. (2016). Fuzzy control system for brushless dc motor (bldc) on embedded hardware. *Tekhnê*, *13*(2), 43–48.

Lourdes, C. (2017). Sistemas de seguridad: La introducción de la tecnología biométrica como una solución inteligente. *15º Simposio Internacional IEEE 2017 sobre Sistemas Inteligentes e Informática (SISY)*.

Martínez, F., Montiel, F., & Martínez, F. (2018). Blueprints obtention by means of using digital image processing algorithms. *International Journal of Engineering and Technology*, *10*(4), 1129–1135.

Martınez, F., Penagos, C., & Pacheco, L. (2018). Deep regression models for local interaction in multi-agent robot tasks. *Lecture notes in computer science* (pp. 66–73). Springer International Publishing. https://doi.org/10.1007/978-3-319-93818-9_7

Mohandes, M., Deriche, M., Ahmadi, H., & Kousa, M. (2016). Un sistema inteligente para el control de acceso de vehículos utilizando tecnologías rfid y alpr. *Revista Árabe de Ciencia e Ingeniería*, *41*, 3521–3530.

Montiel, H., Jacinto, E., & Martínez, F. (2018). Driver for visualization of graphics on VGA screens using FPGA's. *International Journal of Applied Engineering Research*, *13*(20), 14728–14732.

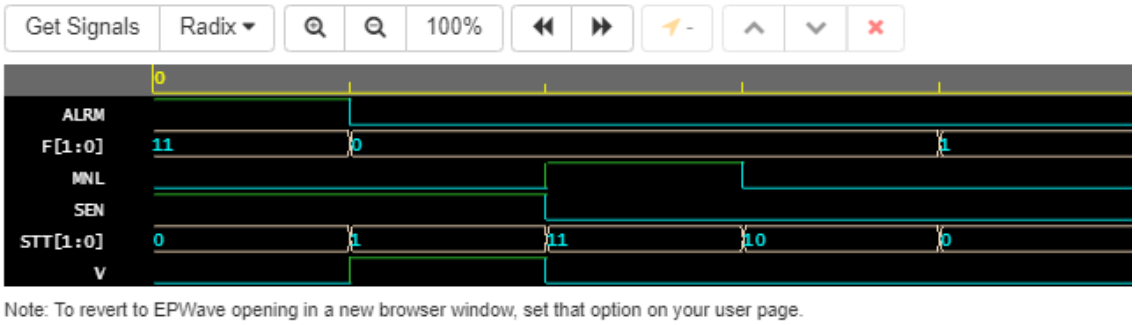
Pala, Z., & Inanc, N. (2007). Aplicaciones de estacionamiento inteligente con tecnología rfid. *2007 1st RFID Eurasia anual*.

Puranic, A., Deepak, K., & Umadevi, V. (2016). Vehicle number plate recognition system: A literaturereview and implementation using template matching. *International Journal of Computer Applications*, 0975–8887.

Widodo, S., Miftakhul, M., Sutrisman, A., Cofriyanti, E., & Maulani, R. (2020). Implementation of parking portal door security system using RFID and password based on microcontrollers in sriwijaya state polytechnic. *Journal of Physics: Conference Series*, *1500*, 012114. https://doi.org/10.1088/1742-6596/1500/1/012114

**Figure 12**

*Simulation of module 5.*




Zhou, H., & Zhihua, L. (2016). Un sistema inteligente de gestión de estacionamiento basado en rs485 y rfid. *Conferencia Internacional 2016 sobre Computación Distribuida Cibernética y Descubrimiento de Conocimiento (CyberC)*, 355–359.