Setup and User's Guide

RFID Door Simulator
Portable Learning Environment

Current Revision as of 2022/05/08

Document v1.3.0

Hardware v1.1.0

Firmware v1.2.0

RFID Door Simulator v1.2

Table of Contents

Introduction

What is the RFID Door Simulator?

The RFID Door Simulator is a portable hardware package intended to simulate basic authentication operations performed by a paired RFID credential reader and upstream door controller. Designed primarily as a classroom tool and research learning aid, the simulator consists of a custom card reader and an Arduino-compatible microcontroller for performing authentication of hard-coded demo credentials. The simulator also allows for custom enrolled credentials for demonstration purposes with credentials not supplied in this hardware package. The simulator can also be switched into a "Decode" mode. In "Decode" mode the door simulator will attempt to decode common 26-bit and 35-bit formats into their respective Facility Code and Card Number. The simulator also features a fully functional reader tamper mechanism to demonstrate environments where the reader tamper is connected to an upstream alarm monitoring device.

Features

- Multi-Technology RFID Credential Reader with Custom Migration Configuration
  - 13.56MHz Credential Support
    - MIFARE DESFire EV1 / EV2 (SIO / CSN)
    - MIFARE Classic (SIO / Legacy / CSN)
    - iCLASS Seos (SIO)
    - iCLASS SE (SIO)
    - iCLASS SR (SIO / Legacy)
    - iCLASS Standard (Legacy)
  - 125KHz Credential Support
    - HID Prox
    - Motorola / HID Indala (Standard 26-Bit Format)
    - AWID
    - EM4102
- Arduino-compatible Microcontroller
- Supports Standard 5V Wiegand Signaling Protocol
- Support for enrolling custom credentials to EEPROM
- Decode Facility Code and Card number for 26 and 35-bit formats
- Configurable Tamper detection mechanism
- 128 x 64 OLED Display
- Input Voltage Must Be Between 9VDC and 12VDC – DO NOT EXCEED 12VDC

Using the RFID Door Simulator

Included Hardware

The RFID Door simulator is comprised of three primary components:

- USB-C PD 2.0 12VDC Trigger Cable (2.1mm x 5.5mm, Center Pin Positive)
- RFID Door Simulator Box
- Student Credential Kit (Not Pictured)
- Control Card Pack v 1.1 (Not Pictured)

Hardware Introduction

Before class, it is advised that the student to familiarize themselves with the RFID Door Simulator's layout. The design is intended to be straight-forward and easy to understand.

Power Requirements

The Door Simulator requires a minimum of 5VDC to operate and supports up to 12VDC input.

The kit includes a USB-C PD 2.0 Trigger Cable set for use with the Door Simulator.

This cable will work with any USB-C PD 2.0 power supply supporting 12VDC output. When 12VDC is not supported by the connected PSU, the cable will attempt to downgrade to 9VDC. If 9VDC is also unavailable, it will failsafe to 5VDC.

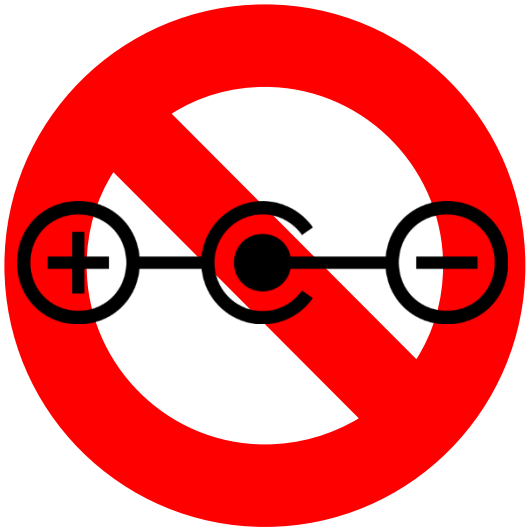
Although the RFID reader will work down to 5VDC, it will exhibit reduced read range and performance at voltages below 12VDC. The behavior is most noticeable when reading 125KHz Low Frequency RFID cards, and will result in reduced read range and increased latency.

In the unexpected event that the power adapter fails, or if a different one needs to be used, the following considerations should be kept in mind:

- The DC input voltage of the Door Simulator should be between 9VDC and 12VDC. Although the input voltage may be as low as 5VDC, read performance will drop considerably at lower voltages.
- The DC barrel jack used is common 2.1mm x 5.5mm type.
- The power supply should be a regulated power supply. Unregulated power supplies may provide too high of a voltage under the minimal load that the Door Simulator applies and would likely result in damage of the microcontroller and/or credential reader.
- The polarity of the DC jack is CENTER POSITIVE. If an alternate power supply is used, it must bear the following marking:

IT IS RECOMMENDED THAT REGULATED POWER SUPPLIES BE USED IN CONJUNCTION WITH DOOR SIMULATOR.

CONNECTION OF AN INCOMPATIBLE POWER SUPPLY WILL DAMAGE THE READER AND THE MICROCONTROLLER.



Testing the Door Simulator

Once the Door Simulator is connected to power, the credential reader and microcontroller will power up automatically. An LED at the top of the credential reader will turn magenta for 5-30 seconds, and eventually settle on red. The OLED display at the bottom of the Door Simulator will show “SECURED”.

To test the Door Simulator, retrieve the “El Pass” test credential from the student learning kit and present it to the reader.

Upon presentation of the credential the following behaviors are expected:

- The credential reader will beep once.
- The reader's LED will be held green by the microcontroller.
- The OLED Display will display a "SUCCESS" or "GRANTED" message.

The RFID Door Simulator testing is now complete and ready for class.

Enrolling Custom Credentials

The Door Simulator also supports enrolling your own credential data as an accepted credential.

To enroll your own credential, you will need two things:

- The "Enroll" Control Card
- The Credential to be Enrolled

The credential must be of a technology supported by the RFID reader.

To complete enrollment complete the following steps:

1. Present the control card labeled "Enroll". The unit will shift to Enroll mode, as indicated by the yellow title text at the top of the OLED display. The status message should read "Present New Card" (fig. 1), the door simulator is now ready to read the credential to be enrolled.

Figure 1

2. Present the credential to be enrolled to the reader.

3. When the door simulator detects a credential, the OLED display will ask the user to “Present Card Again” (fig. 2) indicating that a second presentation is necessary for confirmation.

Figure 2

Upon confirmation a “Card Confirmed” (fig. 3) message should appear. The Wiegand card data sent by the RFID reader will be stored in EEPROM as an authorized credential.

Figure 3

4. If the Wiegand data received between two subsequent reads does not, a “Card Mis-match” (fig. 4) message will appear.

Figure 4

Clear EEPROM

Enrolled credentials are stored in microcontroller's on-board EEPROM.

To erase enrolled credentials from EEPROM, you will need the following:

- The "Clear" Control Card

1. Present the "Clear" control card to the RFID reader to erase all stored credential data from the door simulator. The OLED display will display the header "CLEAR" (fig. 5). All credentials enrolled by the user will be erased from EEPROM. Default student credentials programmed at production will remain.

Figure 5

Decode Mode

As of firmware revision 1.2 the Door Simulator supports decoding of Facility Code and Card Number for the common 26-bit "H10301" and 35-bit "Corporate 1000" bit formats.

To enable "Decode" mode, you will need the following:

- The "Decode" Control Card

Note: Once "Decode" mode is enabled, the setting will be saved in EEPROM as the default boot mode until the mode is changed again.

Decode mode is indicated by the yellow "DECODE" header on the OLED display (Fig. 6).

Figure 6

To use decode mode, simply present a credential. If the credential contains PACS data in a supported bit format, the decoded Facility Code and Card Number will be displayed. (Fig. 7 & 8).

Figure 7

Figure 8

To exit "Decode" mode and switch back to the default "Door Simulator" mode, present the "Door Sim" Control Card.

Tamper

The Door Simulator also contains a functional tamper detection mechanism. This function is provided by the Credential Reader and indicates to a door controller or alarm monitoring system that a reader may be tampered with. Tamper functionality is disabled by default in the door simulator.

To enable tamper detection, you will need the following:

- The "Tamper" Control Card

Once tamper detection is enabled, the setting will be saved in EEPROM and will be persistent across power cycles.

Tamper mode is indicated upon presentation of the Tamper control card. The OLED display will indicate if Tamper detection is enabled (Fig. 9) or disabled (Fig. 10).

Figure 9

Figure 10

With Tamper detection enabled, upon removal of the reader you the door simulator will trigger the reader to beep and display the tamper indicator on the OLED display (Fig. 11).

Figure 11

Troubleshooting and Support

Issue:	The credential reader powers on but the LED is magenta instead of red.
Resolution:	This is expected behavior during initial power-up. Wait 30 seconds for the LED to reset to default.
Issue:	The credential reader and OLED display do not power on.
Resolution:	Plug the power adapter into a different outlet and re-test. Make sure the outlet is not switched off.
Resolution:	If an alternate 9VDC or 12VDC power supply is available, it may be used. See above section regarding "Power Requirements" for more information.
Issue:	OLED display shows "GRANTED / SUCCESS" and the same Wiegand data regardless of credential presented.
Resolution:	If the credentials presented are from the student kit, this is expected behavior that will be explained in class.
Issue:	The OLED display shows "DENIED / FAILURE" regardless of what credential is presented, even if the credential is known-good.
Resolution:	Power-cycle the RFID Door Simulator.
Issue:	In decode mode the OLED display shows a "Bit Format Not Implemented" message.
Resolution:	This bit format is not implemented. 26-bit H10301 and 35-bit Corporate 1000 are the currently supported bit formats for decoding.

Additional Support

Please contact training@redteamalliance.com with any additional questions.

Historical Background

What is Wiegand?

In the world of Physical Access Control Systems (PACS), "Wiegand" is a term that is used with extreme regularity, but with great inconsistency. In fact, Wiegand can refer to a physical credential type, a signaling protocol, a bit format, or even its namesake inventor. To fully understand modern PACS, it is necessary to fully understand these differences.

Wiegand, the Man

John R. Wiegand, the inventor of his namesake signaling technology, didn't start his career as an engineer. Born in Germany in 1912, he immigrated to the United States sometime in the 1930's to study piano and choral conducting at The Juilliard School of Music in New York City. Early on, Wiegand became interested in audio amplifiers, and in 1944 started working for a government contractor designing tape recorders. By the mid 1960's his focus turned to research to the effects of magnetic fields, resulting in his landmark patent in 1974 for his bistable ferromagnetic wire, now commonly referred to as "Wiegand Wire".

Wiegand, the Wire, and Wiegand the Effect

To understand the Wiegand effect, it is important to note one of its key components, the Barkhausen effect. In 1919 Heinrich Barkhausen discovered that when a smoothly and steadily increasing magnetic field was applied to a piece of ferromagnetic material, the material became magnetized in "steps" rather than a continuous change. This unusual phenomenon has been harnessed in various practical applications such as the detection of defects in materials.

John Wiegand harnessed this curious quality in a different way. First, he took Vicalloy wire 1 mil (0.001 inches) in diameter and cold-worked by twisting it and untwisting it under tension. The cold working process resulted in a wire that had a relatively hard shell, and a relatively soft center, as the center of the wire was subject to less work-hardening. The structure was then given permanence through age-hardening, and thus, the Wiegand wire was born.

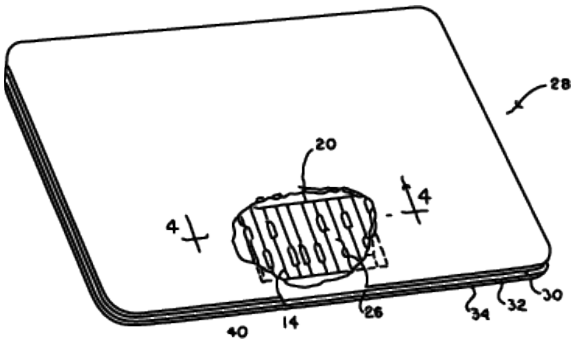
The wire's softer core exhibited lower coercivity, while the hardened surface shell exhibited higher coercivity. When subjected to a magnetic field, the inner core is saturated first, followed by the outer shell. Once fully saturated a magnetic field of the opposite polarity is applied, causing the inner core polarity to instantly flip. This rapid change in the magnetic field causes a current to be induced on the pickup coil. A pulse width of approximately 10 μs and 5-6V is common for most configurations.

Wigand's discovery is doubly fascinating because he discovered the peculiar effects of these wires even before he had access to an oscilloscope. His lab setup used a series of magnets, coils, and speakers that allowed him to listen to the wires, which he often referred to with "she" and "her" pronouns. Endearingly, Wiegand would say that his wires "sung" to him.

Over the next four decades, his peculiar discovery would find its way into nearly every facet of modern life. Since the wires themselves never degraded, and the pickup sensors could be used at a distance from the wires themselves, they never wore down or were subject to mechanical stress. This made them ideal for numerous industrial applications, and were used in a wide variety of linear and rotary encoders, including utility meters, anti-lock braking systems, speed sensors, positional indicators, casino chips, and countless other applications including Physical Access Control Systems.

Wiegand, the Credential

As the utility of Wiegand wires became clearer, it was not long before they were used for access control purposes. While magnetic stripe credentials were subject to mechanical wear, abrasion, and corruption by external magnetic fields, Wiegand wires were not subject to any of the same stressors. Taking advantage of this, Wiegand sandwiched a series of wires between plastic and the Wiegand swipe credential was born.



Wiegand wires were physically embedded in different positions in the credential. The position of each wire corresponded to the value of the bit that it represented. When the credential was swiped through the card reader, two different pickup coils would detect 0 or 1 bits depending on the positions of the wires in the card. Thus, the 26 wires present on a traditional Wiegand swipe credential represented 26 bits of credential data to be used by the door controller for access control.

Wiegand, the Signaling Protocol

Wiegand readers use a simple two-wire signaling protocol consisting of two 5V data lines, one for carrying 0 bits, and another for carrying 1 bits, commonly referred to as D0 and D1, respectively. D0 and D1 are both held high at 5V by default when there are no bits in transit, and when credential data is transmitted the corresponding D0 and D1 lines are pulsed low to 0V with a pulse width between 20 μs and 200 μs. The time between pulses can vary significantly between different readers, and the specification allows anywhere between 200 μS and 20,000 μS between pulses.

In 1996 the Wiegand specification was formally adopted by the Security Industry Association (SIA) as thus, what started first as a proprietary protocol for a new and revolutionary product became the de facto standard for modern access control.

Wiegand, the Data Format

Complicating Wiegand matters further is the Wiegand *data format* or *bit format*. The data format refers to how credential data is presented on the wire. Specifically, it may refer to how many bits are used, and how those bits are encoded, and how parity is calculated.

The most common format in use is the standard 26-bit format defined in the 1996 SIA specification, referred to by HID under ordering code H10301, but not all data formats are standardized. Hundreds of proprietary and non-standard bit formats exist today, and a "37-bit format" or "XX-bit format" from one vendor may use a different encoding from another vendor, even if the bit lengths are the same.

It is important to note that the RFID Door Simulator's operation is format-agnostic, meaning the data format used by the reader or the credential does not impact the operation of the Door Simulator. The binary bitstream is captured in its original form and compared or displayed exactly as it appears on the wire.

Revision History and Changelog

RFID Door Simulator Documentation

2022-05-08
Version 1.3.0 Added info about new USB-C PD power cable.

2021-03-21
Version 1.2.0 Updated documentation to reflect new firmware functionality.

2020-12-08
Version 1.1.0 Updated photos to reflect new enclosure.

2020-07-21
Version 1.0.1 Fixed typos.

2020-07-10
Version 1.0.0 Initial public release.

RFID Door Simulator Hardware Changelog

2020-12-08
Version 1.1.0 Redesigned enclosure.

2020-07-10
Version 1.0.0 Initial public release.

RFID Door Simulator Firmware Changelog

2021-03-15
Version 1.2.0 Complete re-write, add EEPROM enroll functionality, add decode functionality, add tamper functionality.

2020-07-10
Version 1.0.0 Pre-production Release.