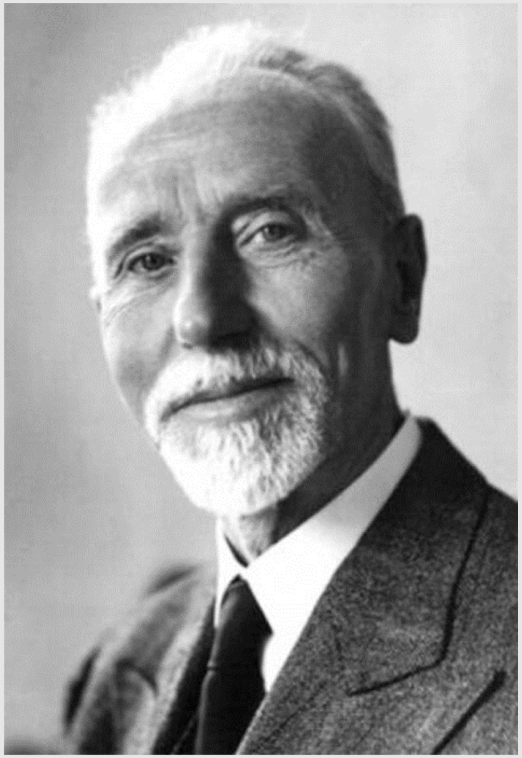
Farpointe Data®
Readers • Credentials

Wiegand?

August 2018

Stephen 'Shep' Sheppard
Key Accounts Sales Manager
Farpointe Data, Inc.



John R. Wiegand

Wiegand: An Introduction

Wiegand (pronounced *wee-gand*) is a standardized interface protocol commonly utilized to communicate data between a credential and a reader, as well as between a reader and a door controller, within the electronic access control (EAC) system environment.

In addition to being a term used to describe the above EAC interfaces, Wiegand has also been used to describe…

- Card data formats
- Reader interface wiring
- Electronic signals
- Physical card technology
- Electromagnetic effects
- And more!

Wiegand: An SIA Standard

Many Farpointe readers can follow the Wiegand standard specified in the Security Industry Association's (SIA) Access Control Standard Protocol for the 26-Bit Wiegand Interface Standard.

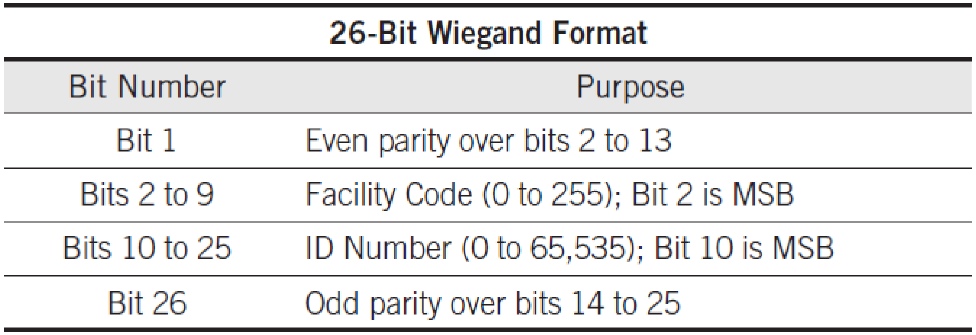
EAC system manufacturers have adopted the SIA's 26-bit Wiegand standard to establish a common device interface.

A benefit of this cost-effective common device interface is that it provides a level of compatibility and interoperability that can be used throughout the channel – EAC system manufacturers, distributors, integrators, dealers, consultants, specifiers and end users – when setting system design, installation and use criteria.

Model P-300-H 125-kHz Proximity Reader
- Can communicate via the SIA's Wiegand Device Interface -

Wiegand: The 26-Bit Wiegand Format

- The composition of the SIA’s Access Control Protocol for the 26-Bit Wiegand Interface Standard, known commonly as the 26-Bit Wiegand Format, contains two bits for parity, eight bits for the facility code and 16 bits for the ID number, for a total of 26 bits.
  - Bit is an abbreviation for ‘binary digit’, which are used in a number system composed of just two parts (zero and one).
- The table below, known as a Bit Map, provides a summary the standard 26-Bit Wiegand format:



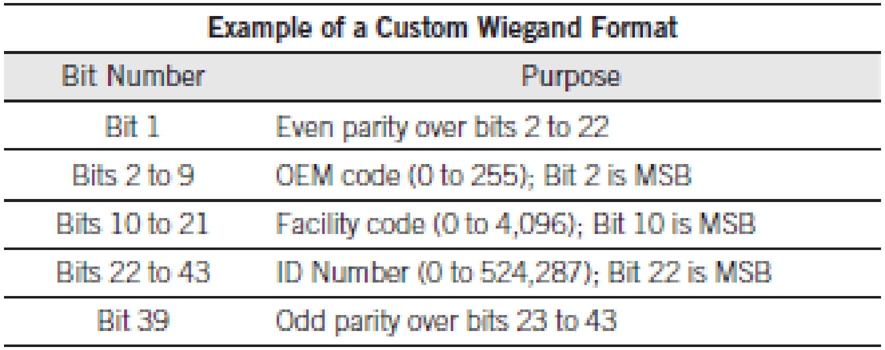
26-Bit Wiegand Format

Bit Number	Purpose
Bit 1	Even parity over bits 2 to 13
Bits 2 to 9	Facility Code (0 to 255); Bit 2 is MSB
Bits 10 to 25	ID Number (0 to 65,535); Bit 10 is MSB
Bit 26	Odd parity over bits 14 to 25

- The first and last bits are utilized as parity bits.
  - Parity bits are a method of error detection in data transmissions.
- The eight facility code bits allow for a total of 256 facility codes (2^8), ranging from 0 to 255.
  - A facility code, also known as a site code, may be utilized to numerically identify a distinct customer, or location, of an EAC system.
- The 16 ID number bits allow for a total of only 65,536 individual ID numbers (2^{16}), within each individual facility code. An ID number can range in value from 0 to 65,535.
  - An ID number recognizes a person as unique from all others.
- Both the facility code and ID number utilize MSB (Most Significant Bit).
  - MSB is the bit in a binary number that is of the greatest numerical value.

Wiegand: Custom Format

- To address the limitations of the SIA’s standard 26-Bit Wiegand Format, an common option is to create a custom Wiegand format.
- With a custom Wiegand format, the system manufacturing partner controls the format.
  - Tracking of card coding optionally available and may provide for additional security.
  - Typically, up to 64 bits are available for creating a custom Wiegand format.
- The Bit Map below provides an example of a 39-bit custom Wiegand format:



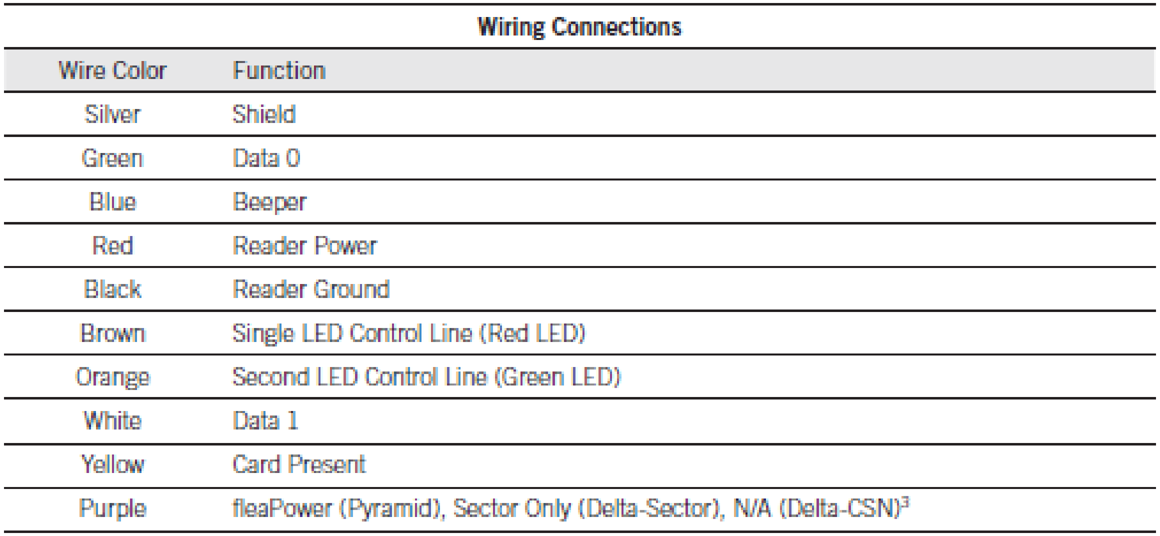
Example of a Custom Wiegand Format

Bit Number	Purpose
Bit 1	Even parity over bits 2 to 22
Bits 2 to 9	OEM code (0 to 255); Bit 2 is MSB
Bits 10 to 21	Facility code (0 to 4,096); Bit 10 is MSB
Bits 22 to 43	ID Number (0 to 524,287); Bit 22 is MSB
Bit 39	Odd parity over bits 23 to 43

- A custom Wiegand format can be a viable alternative to the 26-Bit Wiegand Format.
  - Proprietary to the system manufacturing partner, i,e, the partner is the entity controlling the format.
    - Helps insure credential re-orders are pulled through the partner.
  - Typically many more unique code combinations are available.
  - More fields can create greater client control.
    - An example is the OEM (Original Equipment Manufacturer – a company who resells another company's product under their own name and branding) code in the Bit Map above. In this example the each OEM code represents a unique number assigned to an individual OEM. Typically, if that OEM code is not communicated to the EAC system as assigned and required, then access will not be granted.

Wiegand: Reader Interface Wiring

- The Wiring Connections table to the right illustrates in detail the typical connections between a reader and an EAC system’s door controller that conforms to the SIA’s Access Control Protocol for the 26-Bit Wiegand Interface Standard.
- All connections between the reader and EAC system’s door controller are made through the reader cable, an example of which is also shown on the right.
- Other connections with additional function may be made. An example is a tamper wire, which may be employed by an EAC system to indicate a reader’s operational status.



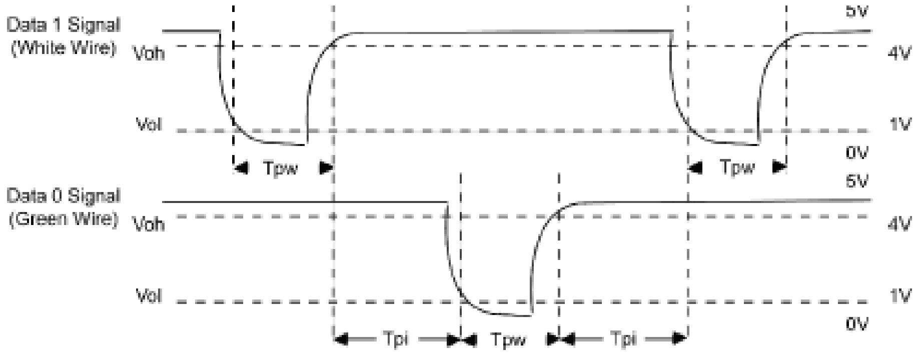
Wiring Connections

Wire Color	Function
Silver	Shield
Green	Data 0
Blue	Beeper
Red	Reader Power
Black	Reader Ground
Brown	Single LED Control Line (Red LED)
Orange	Second LED Control Line (Green LED)
White	Data 1
Yellow	Card Present
Purple	fleaPower (Pyramid), Sector Only (Delta-Sector), N/A (Delta-CSN)[3]

Reader Cable

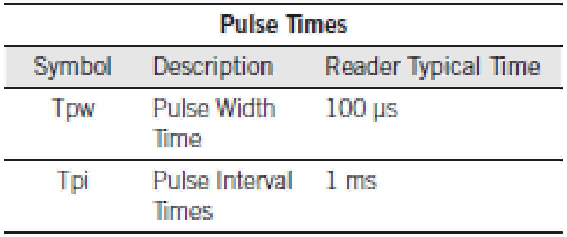
Wiegand: Electronic Data Signals

- The figure below displays the timing pattern for data bits sent by the reader to the EAC system’s door controller.
  - This timing pattern falls within the Wiegand guidelines as proscribed by the SIA’s Access Control Protocol for the 26-Bit Wiegand Interface Standard (a Pulse Width time between 20 uS and 100 uS, and a Pulse Interval time between 200 uS and 20 mS).



  - The Data 1 and Data 0 signals are held at a logic high level (above the Voh level) until the reader is ready to transmit data. The reader places data as asynchronous low-going pulses (below the Vol level) on the Data 1 or Data 0 lines to transmit the data stream to the access control panel (the “saw-teeth” in Figure 1). The Data 1 and Data 0 pulses will not overlap or occur simultaneously.

- The figure below provides the minimum and maximum allowable pulse width times (the duration of a pulse) and pulse interval times (the time between pulses) as proscribed by the SIA’s Access Control Protocol for the 26-Bit Wiegand Interface Standard.



Pulse Times

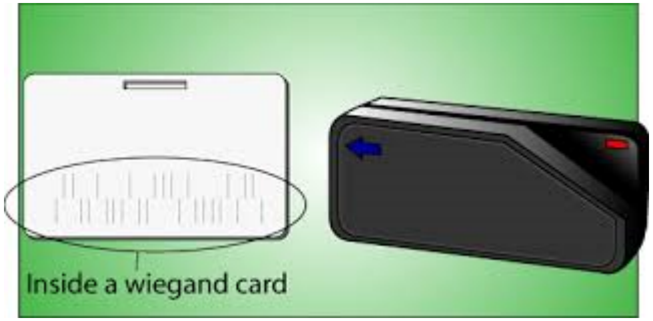
Symbol	Description	Reader Typical Time
Tpw	Pulse Width Time	100 µs
Tpi	Pulse Interval Times	1 ms

Wiegand: Card Technologies

- The original Wiegand card, was a swipe-type card with embedded Wiegand wires, that when pulled across an electromagnetic field, produced pulses that could be converted to binary data, 0s and 1s.

- Today's proximity and contactless smart cards utilize an embedded radio frequency integrated circuit (RFIC). When these cards are presented to a reader they are powered via resonant energy transfer. This energy causes the card's RFIC to transmit its data. The reader receives this data, processes it, and then outputs it the EAC system's door controller. This output is an emulation of the Wiegand format.

- Proximity and contactless smart cards are not Wiegand swipe cards. However, since they are involved in emulating the Wiegand format, they are sometimes categorized as Wiegand or Wiegand-based credentials.



Examples of Proximity and Contactless Smart Cards

Wiegand: Disadvantages and Alternatives

- The Wiegand is not without its disadvantages.
  - 26-Bit Wiegand Format and its potential for code duplication.
    - The fact that 26-Bit Wiegand Format is the SIA's Access Control Standard Protocol speaks to its ubiquitous nature and wide adoption.
    - Codes are limited to just 16,777,216 unique combinations (256 facility codes X 65,636 ID numbers = 16,777,216 unique combinations).
  - Custom Wiegand formats are often unique to individual EAC system manufacturers.
    - Format may be proprietary to a single manufacturer, and neither available from or supported by other manufacturers.
  - Wiegand is a unidirectional protocol.
    - May leave the protocol, and the EAC system utilizing it, vulnerable to numerous exploits, such as man-in-the-middle and relay attacks.
- There are alternatives to the Wiegand protocol.
  - Chief among these is Open Supervised Device Protocol, commonly referred to as 'OSDP'.
    - Is a serial protocol standardized by the SIA that supports bi-directional communications among devices, as well as encryption.
    - Two disadvantages of OSDP are (1) the use of symmetric key, and not public key, for secure channel communications, and (2) system latency, i.e. slow reader response.
  - Another alternative is the legacy ABA Track II protocol, an emulation of the magnetic stripe protocol.
    - Is also a unidirectional protocol, with many of the same disadvantages as Wiegand.

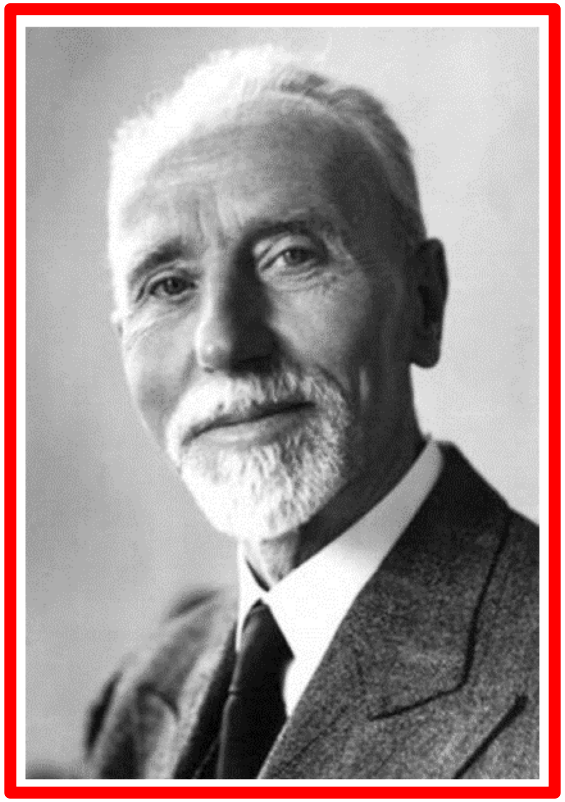
Wiegand: The Discoverer

John Richard Wiegand, born 1912 in Germany, discovered the Wiegand effect.

The Wiegand effect is a physical phenomenon in which a special wire, called a "Wiegand wire", produces small magnetic fields. An accompanying Wiegand reader can be used to detect magnetic pulses produced by the two-domain wire embedded within, typically, plastic cards.

The Wiegand effect was first thought to be a commercially viable solution to better ignition systems for internal combustion engines. This is the reason Echlin Corporation, an automotive parts manufacturer acquired Sensor Engineering, a manufacturer of Wiegand swipe cards and readers, in the 1970s. Note the ignition solution was eventually displaced by the electronic ignition system.

-Wikipedia



John Richard Wiegand

Additional Information

For additional information on Wiegand, please make a point to visit the sites listed below:

- http://www.cs.tufts.edu/comp/116/archive/fall2017/bchung.pdf
- https://www.kerisys.com/pages/blog/2017/07/27/what-wiegand-brief-history/
- http://www.machinedesign.com/engineering-essentials/brushing-wiegand-man-effect-and-wire-changed-engineering
- https://en.wikipedia.org/wiki/Wiegand_interface
- https://www.hidglobal.com/sites/default/files/hid-understanding_card_data_formats-wp-en.pdf
- https://code.tutsplus.com/articles/number-systems-an-introduction-to-binary-hexadecimal-and-more--active-10848
- https://en.wikipedia.org/wiki/John_R._Wiegand
- http://www.farpointedata.com/downloads/forms/Credential_OrderForm.pdf
- http://www.farpointedata.com/downloads/qsg_and_ref/CustomCredentials.pdf

Thank You!

Contact Details:

Stephen ‘Shep’ Sheppard;
Key Accounts Sales Manager

Farpointe Data, Inc.
1376 Borregas Avenue
Sunnyvale, CA 94089 USA
Tel: +1-408-731-0468
Email: Stephen.Sheppard@FarpointeData.com
Web: www.FarpointeData.com

Farpointe Data, the OEM for RFID Readers and Credentials

Farpointe Data's mission is to provide extremely reliable RFID products and options that let our electronic access control channel partners supply value-added solutions at highly competitive prices. Since 2003, we've offered these security professionals a selection of premium OEM contactless identification solutions, both standard and custom, based upon our own 125-kHz proximity, 13.56-MHz smartcard, 433-MHz long-range and now 2.4-GHz mobile smartphone technologies. Our vision is to remain the preferred supplier of RFID products and options for electronic access control to a growing community of global specifiers, dealers, integrators, VARs, distributors and system manufacturers.