UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

WAVELYNX TECHNOLOGIES CORP.
Petitioner,

v.

ASSA ABLOY AB
Patent Owner.

Case No. IPR2023-01018
Patent No. 8,943,562

# DECLARATION OF EMMANOUIL TENTZERIS, PH.D.

**TABLE OF CONTENTS**

I, Emmanouil Tentzeris, declare:

## I. INTRODUCTION AND SUMMARY OF OPINIONS

1. I have been retained by WaveLynx Technologies Corporation ("Petitioner"), to provide analysis and expert opinions on various topics, including: (1) an overview of the art related to U.S. Patent No. 8,943,562 ("the '562 patent"), the patent challenged in this proceeding; (2) the level of ordinary skill in the art; and (3) the patentability of claims 1-14 (the "Challenged Claims") of the '562 patent. In particular, for the purposes of this declaration, I have been asked to provide an analysis of the scope and content of the '562 patent relative to the prior art at the time of the '562 patent's priority date (which I have been asked to assume is August 11, 2008 (hereinafter, the "priority date"), and to provide my opinions from the perspective of a person having ordinary skill in this art (which I will refer to as a "POSITA").

2. This declaration summarizes the opinions that I have formed to date and is based on personal knowledge, skill, experience, and review of materials read and considered in connection with this opinion. I may modify my opinions if necessary, based on further review and analysis of information provided to me at a later date. If asked to give my sworn testimony in a deposition regarding the contents of this declaration, I will do so.

3. Based on the level of ordinary skill in the art, which I describe in more detail below, it is my opinion that the challenged claims of the ’562 patent are un-patentable based on at least the following separate bases:

| Basis | Claims | Statutory Basis | Reference(s) |
|---|---|---|---|
| 1. | 1-4, 6-9, and 11-13 | §102 | U.S. Patent No. 6,988,203 (“Davis”) (EX1006) |
| 2. | 5, 10, 14 | §103 | Davis |
| 3 | 5, 10, 14 | §103 | Davis in view of U.S. Patent No. 7,030,731 (“Lastinger”) (EX1022) |

4. I reserve the right to supplement this declaration as permitted to address any issues raised by expert(s) engaged by Patent Owner or resulting from further discovery. Additionally, I reserve my right to supplement this section if new information that would affect the Priority Date becomes available to me.

5. I am being compensated for my time at my standard rate of $795.00 per hour, plus actual expenses. My compensation is not dependent in any way upon the outcome of the *inter partes* review of the ’562 patent.

## II. PROFESSIONAL BACKGROUND AND QUALIFICATIONS

6. My complete qualifications and professional experience are described in my curriculum vitae, a copy of which is provided as Exhibit 1005. The following is a brief summary of my relevant qualifications and professional experience.

7. I am currently a Professor with tenure in the School of Electrical and Computer Engineering at the Georgia Institute of Technology. I received my Bachelor of Science degree in Electrical Engineering from the National Technical University of Athens in Greece in 1992. I received my Master's degree and Ph.D from the University of Michigan at Ann Arbor in 1994 and 1998, respectively. A complete list of my academic positions, activities, and publications is set out in my CV, attached. (EX1005).

8. Between 1991 and 1992, I was a research assistant in the Microwave Lab at the National Technical University of Athens, Greece. From 1992 to 1998, I was a research assistant in the Radiation Laboratory at the University of Michigan, Ann Arbor. I became an assistant professor at the School of Electrical and Computer Engineering at Georgia Technical Institute in 1998, lasting until I became an Associate Professor in the same School in 2004. I then served as Associate Professor until my promotion to Professor in 2016, a title I have held since then. Also in 2016, I was appointed as the Ken Byers Professor in Flexible Electronics.

9. As described in my CV, I have more than 30 years of industry and academic experience. I have experience with radio frequency identification ("RFID") and circuit design for these systems. As a professor of Electrical and Computer Engineering, I have taught courses relating to RFID technologies. A

complete list of my teaching positions, honors, and classes taught is set out in my CV, EX1005. As a professor, I collaborated with over 130 Undergraduate, Masters and Doctoral students, as well as visiting students, post-doctoral fellows, and other researchers, including on topics such as "Hybrid EM and Circuit Optimization of RF Devices Built on Si, GaAs and Multilayer Ceramic (LTCC) and Organic Substrates," "Vertical Integration of Inkjet-Printed RF Circuits and Systems," and "3D-Printed RF Circuits."

10. Throughout my career, I have received a variety of awards. I am a Fellow of IEEE, a member of the MTT-15 Committee, an Associate Member of European Microwave Association (EuMA), a Fellow of the Electromagnetics Academy, and a member of Commission D, URSI and of the Technical Chamber of Greece. In recognition of my world-leading achievements in the area of RFIDs, I served as an IEEE C-RFID (Committee on RFID technologies) Distinguished Lecturer from 2016-2022 and I served as an IEEE MTT Distinguished Microwave Lecturer (DML) from 2010-2012. I have won awards for my contributions in developing various technologies, including RFID systems operating at different frequencies and RFID applications with different power constraints. My achievements include the following:

- IEEE fellow — a distinction reserved for select IEEE members whose extraordinary accomplishments in any of the IEEE fields of interest are deemed fitting of this prestigious grade elevation. IEEE, About the IEEE Fellow Program, http://www.ieee.org/membership/fellows/.

- 2021 IEEE Antennas and Propagation Symposium (APS) Best Student Paper Award (co-authored)
- 2019 Humboldt Research Prize
- 2019 IEEE APS Conference Co-Chair
- 2018 Intel IEEE ECTC 2018 Best Student Paper Award
- 2015-present IEEE CRFID Distinguished Lecturer
- 2010-2012 IEEE MTT-S Distinguished Microwave Lecturer
- 2017 Georgia Tech Outstanding Achievement in Research Program Development Award
- 2017 Archimedes IP Salon Gold Medal
- 2016 Bell Labs Prize Third Award
- 2015 IET Microwaves, Antennas and Propagation Premium Award
- 2014 Georgia Tech ECE Distinguished Faculty Achievement Award
- 2014 IEEE RFID-TA Best Student Paper Award
- 2013 IET Microwaves, Antennas and Propagation Premium Award
- 2012 Finland Distinguished Professor (Fi.Di.Pro.) Award
- 2012 Architecture Award of Excellence, Architecture World Summit

- 2010 IEEE Antennas and Propagation Society Piergiorgio L. E. Uslenghi Letters Prize Paper Award
- 2010 Georgia Tech Senior Faculty Outstanding Undergraduate Research Mentor Award
- 2009 IEEE Transactions on Components and Packaging Technologies Best Paper Award
- 2009 IEEE Antennas and Propagation Symposium (APS) Second Best Student Paper Award
- 2009 E.T.S. Walton Award from Science Foundation Ireland
- 2007 IEEE Antennas and Propagation Symposium (APS) Best Student Paper Award
- 2007 IEEE International Microwave Symposium (IMS) Third Best Student Paper Award
- 2007 IEEE International Symposium on Antennas and Propagation (ISAP) Poster Presentation Award
- 2006 Asian-Pacific Microwave Conference (APMC) Award
- 2006 IEEE-MTT Outstanding Young Engineer Award
- 2004 IEEE Transactions on Advanced Packaging Commendable Paper Award

- 2003 NASA Godfrey "Art" Anzic Collaborative Distinguished Publication Award
- 2003 IBC International Educator of the Year Award
- 2003 IEEE-CPMT Outstanding Young Engineer Award
- 2002 International Conference on Microwave and Millimeter-Wave Technology Best Paper Award (Beijing, China)
- 2002 Georgia Tech-ECE Outstanding Junior Faculty Award
- 2001 ACES Conference Best Student Paper Award
- 2000 NSF CAREER Award
- 1999 Technical Program Co-Chair of the 54th ARFTG Conference, Atlanta, GA
- 1997 Best Paper Award, International Hybrid Microelectronics and Packaging Society
- 1989 Papastavridios Greek Mathematics Excellence Fellowship
- 1988-1992 Greek Government Academic Excellence Fellowships

11. In Google scholar, there are over 25,924 citations to my work and my work has an h-index of 80. An h-index represents the number of papers with the same number of citations, meaning I have over 80 papers with 80 citations.

12. I have authored or contributed to over 30 books and 835 refereed journal and conference papers; spoke in over 140 presentations, many of which

relate to antenna arrays, RFID systems, and other modes of wireless communication and electronics design. A complete list of my publications and conference presentations is included in my curriculum vitae (EX1005).

13. I am a named inventor on 20 patents in the US and in Europe. In particular, I am a named inventor on patents relating to antenna design, RF systems, and means of reducing signal interference in RF applications. A complete list of my patents and published applications is included in my curriculum vitae (EX1005).

14. In addition to gaining expertise via my academic training, professional experiences, and research accomplishments described above, I have kept abreast of various sub-disciplines within the RFID space, such as locating technologies, by reading technical literature, attending and presenting at conferences, and attending and presenting at symposia. I have served as an editor for various journals and participated in the peer review process for various technical journals and conferences, and have reviewed manuscripts submitted by other scholars relating to RFID. I have contributed further to the profession by chairing conference committees and planning conferences and panels. Furthermore, I have collaborated with or have communicated with many of the scholars and engineers in the field of RFID systems.

15. I am not an attorney and offer no legal opinions, but in the course of my work, I have had experience studying and analyzing patents and patent claims from the perspective of a POSITA.

## III. MATERIALS REVIEWED AND CONSIDERED

16. My findings, as explained below, are based on my years of education, research, experience, and background in the field of RFID systems and circuit design, as well as my investigation and study of relevant materials for this declaration. When developing the opinions set forth in this declaration, I assumed the perspective of a POSITA, as set forth in Section IX below. In forming my opinions, I have also reviewed and considered all of the exhibits and prior art references I discuss in this declaration.

## IV. MY UNDERSTANDING OF LEGAL STANDARDS

17. I have not been asked to offer an opinion on the law; however, as an expert assisting the Board in determining patentability, I understand that I am obliged to follow existing law. I have therefore been asked to apply the following legal principles to my analysis.

18. I understand that "*inter partes* review" (IPR) is a proceeding before the United States Patent & Trademark Office for evaluating the patentability of an issued patent's claims based on prior-art patents and printed publications.

19. I understand that, in this proceeding, Petitioner has the burden of proving that the challenged claims of the ’562 patent are unpatentable by a preponderance of the evidence. I understand that “preponderance of the evidence” means that a fact or conclusion is more likely true than not true.

20. I understand that determining whether a particular patent or printed publication constitutes prior art to a challenged patent claim can require determining the priority date to which the challenged claim is entitled. I understand that for a patent claim to be entitled to the benefit of the filing date of an earlier application to which the patent claims priority, the earlier application must have described the claimed invention in sufficient detail to convey with reasonable clarity to the POSITA that the inventor had possession of the claimed invention as of the earlier application’s filing date. I understand that a disclosure that merely renders the claimed invention obvious is not sufficient written description for the claim to be entitled to the benefit of the filing date of the application containing that disclosure.

21. I understand that for an invention claimed in a patent to be patentable, it must be, among other things, new (novel—*i.e.*, not anticipated) and not obvious from the prior art. My understanding of these two legal standards is set forth below.

### A. Anticipation

22. I understand that, for a patent claim to be "anticipated" by the prior art (and therefore not novel), each and every limitation of the claim must be found, expressly or inherently, in a single prior-art reference. I understand that a claim limitation is disclosed for the purpose of anticipation if a POSITA would have understood the reference to disclose the limitation based on inferences that a POSITA would reasonably be expected to draw from the explicit teachings in the reference when read in light of the POSITA's knowledge and experience.

23. I understand that a claim limitation is inherent in a prior art reference if that limitation is necessarily present when practicing the teachings of the reference, regardless of whether a POSITA recognized the presence of that limitation in the prior art.

### B. Obviousness

24. I understand that a patent claim may be unpatentable if it would have been obvious in view of a single prior-art reference or a combination of prior-art references.

25. I understand that a patent claim is obvious if the differences between the subject matter of the claim and the prior art are such that the subject matter as a whole would have been obvious to a POSITA at the time the invention was made.

Specifically, I understand that the obviousness question involves a consideration of:

- the scope and content of the prior art;
- the differences between the prior art and the claims at issue;
- the knowledge of a person of ordinary skill in the pertinent art; and
- if present, objective factors indicative of non-obviousness, sometimes referred to as "secondary considerations." (To my knowledge, the Patent Owner has not asserted any such secondary considerations with respect to the '562 patent.)

26. I understand that in order for a claimed invention to be considered obvious, a POSITA must have had a reason for combining teachings from multiple prior-art references (or for altering a single prior-art reference, in the case of obviousness in view of a single reference) in the fashion proposed.

27. I further understand that in determining whether a prior-art reference would have been combined with other prior art or with other information within the knowledge of a POSITA, the following are examples of approaches and rationales that may be considered:

- combining prior-art elements according to known methods to yield predictable results;

- simple substitution of one known element for another to obtain predictable results;
- use of a known technique to improve similar devices in the same way;
- applying a known technique to a known device ready for improvement to yield predictable results;
- applying a technique or approach that would have been "obvious to try," *i.e.*, choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success.
- known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art;
- some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior-art reference or to combine prior-art reference teachings to arrive at the claimed invention. I understand that this teaching, suggestion or motivation may come from a prior-art reference or from the knowledge or common sense of one of ordinary skill in the art.

28. I understand that for a single reference or a combination of references to render the claimed invention obvious, a POSITA must have been able to arrive at the claimed invention by altering or combining the applied references.

## V. PERSON OF ORDINARY SKILL IN THE ART

29. I have been informed and understand that for purposes of assessing whether prior-art references disclose every element of a patent claim (thus "anticipating" the claim) and/or would have rendered the claim obvious, the patent and the prior-art references must be assessed from the perspective of a POSITA, based on the understanding of that person at the time of the patent claim's priority date. I have been informed and understand that a POSITA is presumed to be aware of all pertinent prior art and the conventional wisdom in the art, and is a person of ordinary creativity. I have applied this standard throughout my declaration.

30. The '562 patent involves technology in the field of RFID reader data transfer. I have been asked to provide my opinions as to the state of the art in this field by August 2008. I use this timeframe because the face of the '562 patent indicates an earliest claimed priority date of the August 11, 2008 filing date of a provisional application. EX1001, Title Page, (60). I am unaware of any claim by Patent Owner to an earlier date of invention or of any evidence that Patent Owner could provide to establish any earlier conception date. Therefore, whenever I offer an opinion in this declaration about the knowledge of a POSITA, the manner in

which a POSITA would have understood the claims of the ’562 patent or its description, the manner in which a POSITA would have understood the prior art, or what a POSITA would have been led to do based on the prior art, I am referencing the August 2008 timeframe, even if I do not say so specifically in each case.

31. In my opinion, a POSITA at the time of the alleged invention would have had at least an undergraduate degree in electrical engineering, or equivalent education, and at least two years of work experience in the field of access control.

32. By August, 2008, I held a Ph.D and I had 10+ years of experience with RFID systems and radio frequency communication. Therefore, I was a person of more than ordinary skill in the art during the relevant timeframe. However, I am familiar with the ordinary level of skill in the art as described above, including by having worked with many people who fit the characteristics of a POSITA. When developing the opinions set forth in this declaration, I assumed the perspective of a person having ordinary skill in the art, as set forth above.

## VI. BACKGROUND AND STATE OF THE ART

### A. Access Control Systems

33. Prior art access control systems in use by the mid-2000s generally comprised of cards, card readers, control panels, and host computers. As

recognized by Davis, the typical arrangement of an access control system was as follows:

> Typically, a device such as a card reader is positioned near a doorway of a secure area such as a computer room. A person desiring to enter the secure area must present to the reader a card having user data that can be read by the reader. The reader will transmit the user data via a hardwired bus to a control system typically consisting of numerous control panels ultimately connected back to a host computer, which will decide based on certain rules if that person should be allowed to enter the premises at that door. . . . If the host computer determines that access should be allowed, it will send a command that will, for example, activate a relay that will open a door strike mechanism, thusly allowing entry by the user that presented the card.

EX1006, at 1:13-32; *see also* EX1001, 1:22-25; EX1010, ¶[0004] ("In access control systems, Radio Frequency Identification Devices (RFIDs) or other security credentials are typically used to store data that uniquely identify a holder of the RFID device or the holder's access authorizations. In order to gain access to an asset, such as a building, room, safe, computer, files, information, etc., a holder presents the RFID device to a reader that reads the data and subsequently transmits the data to a panel, processor, or a host system where a decision is made to either grant access to the subject asset or not."); EX1014, ¶[004] ("Usually, the Wiegand reader is located to be accessible to the user (Wiegand card holder) while the control panel, which after a positive evaluation of the data, performs a security relevant operation (e.g. unlocking a door) is located in an area which is not accessible to the user, e.g. in a secure room, to guarantee a certain level of security."); *see also* EX1025, ¶[0002] ("Typically, an RFID system includes one or more RFID cards (also known as contactless IC cards), which are provided to system users. An RFID reader (also known as an RFID interrogator) receives RF (radio frequency) signals from proximate RFID cards, decodes identification information from the received RF signals and forwards it to a remote access controller. The access controller, which typically includes a computer system located in a secure area [], authenticates an RFID card holder based on the provided identification information to determine whether to grant the card holder access to the restricted area or service.")

34. Before the priority date, the communication between card readers and panels typically utilized the Wiegand interface, as described further below. *See* EX1007.

### B. Wiegand Wiring and Communication Protocols

35. The Wiegand *interface* refers to a wiring standard used in the art to power RFID readers and connect them to control panels. EX1007, at 5-13; EX1006, 1:33-52; EX1014, ¶[026], Fig. 1; EX1020, 3:38-40. The Wiegand *protocol* refers generally to the communications protocol that is used over the

Wiegand interface. EX1020, 3:45-49. Both the Wiegand interface, which has been used since the 1980s in card-reading systems, and the Wiegand protocol, which was also well known before the priority date, were formally defined by the 1996 publication of the Security Industry Association's "Access Control Standard Protocol for the 26-Bit Wiegand Reader Interface," which is attached as EX1007 (the "SIA Standard"). EX1020, 3:36-38; *see also* EX1006, 1:37-46; EX1007, at 8-10.

36. The Wiegand interface is a five-wire interface that connects the reader to the panel and provide power to the reader. EX1006, 1:34-36 ("One technology in prevalent use for many years is the wiegand protocol, which utilizes five wires to communicate data and provide power to a dedicated card reader as well known in the art."); *see also* EX1007, at 8-9 (defining the use of each wire). As Davis and the SIA Standard explain, "[t]he five wires are for power, ground, DATA0, DATAl, and LEDCTL." EX1006, at 1:36-37; EX1007, at 8-9; *see also* EX1014, ¶[026], Fig. 1; EX1020, 3:42-67. It was well known before the priority date that the DATA1 and DATA0 respectively deliver binary ones and zeros to the panel from the reader through electrical pulses sent along each line. EX1006, 1:36-39 ("The DATAl line is a reader output that delivers pulses [to a control panel] that are interpreted as binary ones. The DATA0 line is a reader output that delivers pulses [to the control panel] that are interpreted as binary zeros."); *see also*

EX1007, at 8; *infra* §VI.C.1. Likewise, it was well understood before the priority date that on the LEDCTL line, the panel controls the voltage level to determine the state (*i.e.*, color and duration of illumination) of the LED on the reader. *See* EX1006, 1:39-42. ("The LEDCTL line is the panel output that determines the state of the LED contained on the reader (off, red, green, or amber)."); EX1007, at 8 ("The LED signal is provided by the panel to control the reader LED state."). As the SIA Standard explains, "[t]he meaning of the various LED states … defined by the panel manufacturer." EX1007, at 12; *see also id.* at 7; EX1006, at 4:37-43.

37. Thus, it was well understood before the priority date that the standard Wiegand protocol is a one-way data-transfer protocol. EX1006, 1:53-57; *see* EX1007, at 5, 9, 11, 12; EX1012, ¶[0009] ("The Wiegand protocol is essentially a unidirectional protocol that only provides for data transmission from a reader to an upstream device (e.g., a control panel, host, or processor)."). For example, as explained by Davis, "the Wiegand protocol is a one-way protocol, since the reader can send data to the panel but the panel cannot send any data to the reader except to control the door mechanism and a status LED." EX1006, 1:53-57; *see* EX1007, at 5, 9, 11, 12; EX1012, ¶[0009]. And as U.S. Patent Pub. No. 2007/0046424 explains, "[a]lthough there is a signal sent back from the upstream device to the reader, this signal is essentially a logic signal used to convey status to a cardholder by controlling a reader's LED. A superset of the Wiegand protocol adds additional

logic signals to control an audible device in the reader and provides for additional reader LED colors. These are not bi-directional protocols because substantive data is still sent in only one direction. The host cannot give the reader a command. Only simple signals are sent from the host to the reader." EX1012, ¶[0009]; *see also* EX1007, at 7, 9, 12; EX1006, at 4:37-43.

38. However, it was known before the priority date that the LED line could be used to send commands or data back to the reader, for example, in order to instruct the reader to change the content of the data communicated to the panel, or to enable security measures in the data communication. EX1006, 2:29-43 ("A second major improvement is that the LEDCTL line controlled by the panel is now used to transmit data back to the reader As a result of this invention, described herein, no additional wires are required to be connected between the panel and the reader, thus preserving the existing Wiegand infrastructure while providing increased functionality. The panel computer will require no changes to its interface (or other) hardware; only the firmware needs to be modified in accordance with the invention. Messages can be customized by users in accordance with the extended protocol set forth herein."), 5:18-63; EX1010, ¶[0045] ("The control panel 104 could inform the reader 112 to change how it is working through the list with a prompting signal sen[t] via an LED control signal, or may do so through an interruption to the power supply of the reader 112."); *see also infra* §IX.

39. The SIA Standard sets out the "minimum set of features a reader or panel must provide to be in compliance. Manufacturers may have additional features as long as they do not conflict with features specified herein." EX1007, at 5. Some known additional features before the priority date include hardware tamper and temperature sensors. EX1006, 3:22-31, 4:15-24, Fig. 3. It was also known before the priority date to add additional data onto the Wiegand reader-to-panel data streams. EX1006, 2:55-64, 3:1-34, 4:48-5:17, Fig. 2.

### C. Wiegand Data Communication

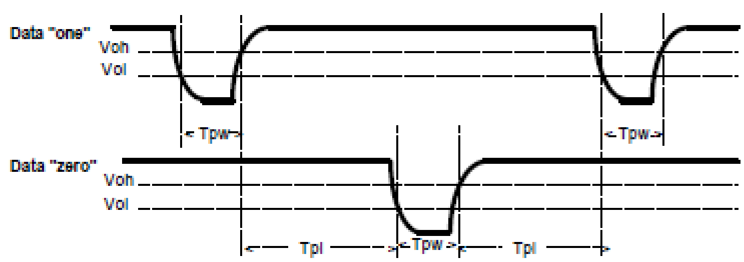
40. As the '562 patent recognizes, it was known in the prior art that data may be communicated in packets and that additional security mechanisms may be implemented on the Wiegand interface. *See* EX1001, 1:32-47, 2:30-3:22, 18:63-21:58.

#### 1. Data Packets

41. The transfer of data over the Wiegand interface takes place by the reader sending packets of data to the panel. *See* EX1007, at 13. A "packet" of data refers to "[a] short section of data of fixed length that is transmitted as a unit," that is, "[t]he basic unit of [data] encapsulation" for transmission. EX1021, at 5 (McGraw-Hill, Fifth Edition (1994) definition of "packet" for communications); EX1018, at 5; *see also* EX1016, at 13 ("The term packet is used generically here to mean the data of one transaction between a host and its network. The format of

data blocks exchanged within the [] network will generally not be of concern to us."); EX1015, at 2 ("The term LOCAL PACKET is used generically here to mean the formatted bit string exchanged between a host and a packet switch. The format of bit strings exchanged between the packet switches in a PSN will generally not be of concern to us.").

42. In addition to the wiring, the aforementioned SIA Standard, published on October 17, 1996, discloses the method of data transfer in the Wiegand protocol. This includes the use of non-overlapping data pulses for the Data One and Data Zero lines, and the transmission of data signals by holding the signals "at a high logic level until the reader is ready to send a data stream":




EX1007, at 12. Each pulse of data has a "Pulse Width Time," or TPW, and the gap between pulses is defined as the "Pulse Interval time," or TPI. The SIA Standard instructs that "[t]he following timing parameters shall be observed":

| SYMBOL | DESCRIPTION | MIN | MAX |
|---|---|---|---|
| TPW | Pulse Width Time | 20 µs | 100 µs |
| TPI | Pulse Interval Time | 200 µs | 20 mS |

EX1007, at 12. The units "ms" and "µs" (or usecs, see infra §IX.C) respectively refer to milliseconds and microseconds.

43. Using these data transfer conventions, the SIA Standard defines a packet data format. *See* EX1007, 13. The data packet according to the SIA standard includes 26 bits. *Id.*; *id.* at 1. Of the 26 bits, only the middle 24 contain data. *See* EX1007, at 13 ("The 26 bits of transmission from the reader to the panel consists of two parity bits and 24 code bits"). The first transmitted bit is a parity bit for the first 12 data bits, and the last transmitted bit is a parity bit for the second 12 data-carrying bits. *Id.* ("The first bit transmitted is the first parity bit, P1, it is even parity calculated over the first 12 code bits. The last bit transmitted is the second parity bit, P2, it is odd parity calculated over the last 12 code bits."). Parity bits were well understood before the priority date to be "[a]n additional nondata bit that is attached to a set of data bits to check their validity," which enables error detection. *See* EX1021, 6 (McGraw-Hill, Fifth Edition (1994) definition of "parity bit"); *see also* EX1007, at 13.

44. The following image from the SIA Standard shows its packet structure. *See* EX1007, at 13. The SIA Standard states that "[t]he bits are transmitted in the order described," where the top two rows under "CODE FORMAT" and "PARITY FORMAT" provide the number (*i.e.*, 1 through 26) of the 26 transmitted bits (where each column is read top-down). *See* EX1007, 13.

CODE FORMAT

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| P1 | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | C | P2 |

PARITY FORMAT

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| P1 | E | E | E | E | E | E | E | E | E | E | E | E | | | | | | | | | | | | | |
| | | | | | | | | | | | | | O | O | O | O | O | O | O | O | O | O | O | O | P2 |

| | |
|---|---|
| P1: | First, or even parity bit. |
| C: | Code bits. |
| P2: | Second, or odd parity bit. |
| E: | Bits for calculation of even parity. |
| O: | Bits for calculation of odd parity. |

EX1007, 13.

45. Outside of Wiegand communication, packet communication of digital data has been well understood since the 1970s. For example, the Network Working Group's Request for Comment (RFC) 675, published in December, 1974, described a "Specification of Internet Transmission Control Program" and a 128 bit packet format for sending over the "internetwork." EX1015, at 1, 17-42.

46. As another example, RFC 1055, which is discussed in the '562 patent, was published in 1988 and describes a packet framing standard for "Serial Line IP," or SLIP. EX1017, at 1. "SLIP has its origins in . . . the early 1980's. It is

merely a packet framing protocol: SLIP defines a sequence of characters that frame IP packets on a serial line, and nothing more." EX1017, at 1.

47. RFC 1055 discloses C coding to send and receive SLIP packets, which the '562 patent also lists:

```
 /* SLIP special character codes
  */
#define END             0300    /* indicates end of packet */
#define ESC             0333    /* indicates byte stuffing */
#define ESC_END    0334    /* ESC ESC_END means END data byte */
#define ESC_ESC     0335    /* ESC ESC_ESC means ESC data byte */
/* SEND PACKET: sends a packet of length "len", starting at
 * location "p".
 */
void send_packet(p, len)
            char *p;
            int len; {
   /* send an initial END character to flush out any data that may
    * have accumulated in the receiver due to line noise
    */
      send_char(END);
   /* for each byte in the packet, send the appropriate character
    * sequence
    */
            while(len--) {
                  switch(*p) {
                  /* if it's the same code as an END character, we send a
                   * special two character code so as not to make the
                   * receiver think we sent an END
                   */
                  case END:
                        send_char(ESC);
                        send_char(ESC_END);
                        break;
                  /* if it's the same code as an ESC character,
                   * we send a special two character code so as not
                   * to make the receiver think we sent an ESC
                   */
                  case ESC:
                        send_char(ESC);
                        send_char(ESC_ESC);
                        break;
                  /* otherwise, we just send the character
                   */
                  default:
                        send_char(*p);
                        }
                  p++;
                  }
            /* tell the receiver that we're done sending the packet
             */
            send_char(END);
            }
/* RECV_PACKET: receives a packet into the buffer located at "p".
 *          If more than len bytes are received, the packet will
 *          be truncated.
 *          Returns the number of bytes stored in the buffer.
 */
int recv_packet(p, len)
            char *p;
            int len; {
            char c;
            int received = 0;
/* sit in a loop reading bytes until we put together
 * a whole packet.
 * Make sure not to copy them into the packet if we
```

```
 * run out of room.
 */
while(1) {
        /* get a character to process
         */
        c = recv_char( );
        /* handle bytestuffing if necessary
         */
        switch(c) {
        /* if it's an END character then we're done with
         * the packet
         */
        case END:
                /* a minor optimization: if there is no
                 * data in the packet, ignore it. This is
                 * meant to avoid bothering IP with all
                 * the empty packets generated by the
                 * duplicate END characters which are in
                 * turn sent to try to detect line noise.
                 */
                if(received)
                        return received;
                else
                        break;
        /* if it's the same code as an ESC character, wait
         * and get another character and then figure out
         * what to store in the packet based on that.
         */
        case ESC:
                c = recv_char( );
                /* if "c" is not one of these two, then we
                 * have a protocol violation. The best bet
                 * seems to be to leave the byte alone and
                 * just stuff it into the packet
                 */
                switch(c) {
                case ESC_END:
                        c = END;
                        break;
                case ESC_ESC:
                        c = ESC;
                        break;
                        }
        /* here we fall into the default handler and let
         * it store the character for us
         */
        default:
                if(received < len)
                        p[received++] = c;
                }
        }
}
```

EX1001, 20:16-21:45; *compare id. with* EX1017, at 4-6.

48. Likewise, RFC 1661, published in July of 1994 and also mentioned in the '562 patent (EX1001, 19:65-20:3), describes point-to-point protocol (PPP) packet encapsulation as generally including "a protocol field" then an "information

field" and finally "padding," which are transmitted in that order. EX1018, at 6. This RFC also discloses multiple formats for "Link Control Protocol" packets, each of which contains an octet (8 bits) of "Code" data; an "Identifier" octet; two octets of a "Length" field, which "indicates the length of the LCP packet"; and then finally the substantive data of the transmission. *Id.* at 28-31. Each of these data fields is transmitted in the serial order described. *Id.*

### 2. Security of Wiegand Transmissions

49. Before the priority date, there were several ways known in the art to add security to Wiegand packet transmissions, as the '562 patent recognizes. For example, it was known before the priority date that "by using a tamper sensor [connected to a reader 10], an alarm may be sent to the control panel in the event that someone attempts to alter or destroy the reader 10, and such activity is sensed by the tamper sensor." EX1006, at 4:20-23; *see also* EX1001, 3:67-4:31 (citing EX1006). The reader may append additional data bits from the tamper-detection device to the Wiegand transmission to the panel in order to inform the panel of any tamper-related security threats. EX1006, 3:9-31, 4:15-24.

50. Likewise, other encryption techniques that shroud the actual data communication from a reader to a panel were known in the art before the priority date. These techniques were known to protect against "a rogue device" being "connected to monitor communications between the reader and control panel" and

used to "replay" messages that successfully opened a door "whenever illicit entry is desired." EX1012, ¶¶[0011]-[0014], [0054]; EX1014, ¶[049]. One way that was known before the priority date was to prevent this type of replay attack was to add a time-stamp to the data transmission, such that any recorded messages played back on the Wiegand wires to gain access would not be successful because the time-stamp on the message would be out-of-date. EX1014, ¶[049].

51. Another protective technique that was known before the priority date to be used against a replay attack was to include a code in addition to the credential information in the data stream from the reader to the panel. EX1012, ¶¶[0019], [0038], [0047] [0050]-[0055], [0059]-[0067]. In this "rolling code" set up, the code in each message "'rolls' or changes whenever a particular event occurs," for example, when a message is sent or after the passage of a certain amount of time. *See* EX1019, ¶¶[0023], [0032], [0039], [0050]; *see also* EX1012, ¶¶[0038], [0047] [0050]-[0055]. The code included in the transmission may change by the reader rolling through a predetermined list of codes, by the reader generating a new code, or by waiting for a predetermined period of time to pass for the reader to advance to the next code. EX1012, ¶¶[0038], [0047] [0050]-[0055]; *see also id.* ¶¶[0059]-[0067]. This would prevent a replay attack using an expired code from being granted access. *See id.* ¶¶[0018], [0020], [0048], [0058]. And as the '562 patent admits, "many rolling code generators" were known in the art before the priority

date. EX1001, 14:9; *see, e.g.*, EX1012, ¶¶[0005], [0006], [0054]-[0057]; EX1019, ¶¶[0023]-[0024], [0031], [0037]-[0055], [0061]-[0063], Figs. 2-6, 9. Similarly, the use of digital signatures on messages, which allowed the source of the transmission to be verified, was also known before the priority date to be used individually or in conjunction with rolling codes or other forms of encryption before the priority date. EX1014, ¶¶[037]-[046].

52. It was also known in the art before the priority date that the reader-panel transmissions may be encrypted so as to protect against any data harvesting on the data lines. *See, e.g.*, EX1012, ¶¶[0005], [0006], [0054]-[0057], FIG. 4; EX1014, ¶[036]; EX1025, ¶¶[0006]-[0007], [0028]-[0035], FIGS. 1-5. In systems using an encryption and key, the communication is encrypted before being sent from the reader. *See* EX1012, ¶¶[0054]-[0057], FIG. 4; EX1025, ¶¶[0006], [0028]-[0034], FIGS. 1-5. Upon receipt at the panel, the panel applies a decryption key to the message received in order to decrypt the credential information contained in the transmission to determine whether to grant access. EX1012, ¶¶[0054], [0057], FIG. 4; EX1025, ¶¶[0007], [0031]-[0032], [0035], FIGS. 1-5. In these systems, "[e]ven if someone is harvesting signals sent from the reader 112 to the control panel 104, they must know the encryption/decryption key and decrypt the message before any substantive information about the message can be determined. Essentially, the encryption of the message makes it more difficult for an attacker to

steal a valid rolling code and valid credential data" included with the message. EX1012, ¶[0054].

# VII. THE '562 PATENT

## A. Overview

53. The '562 patent is purportedly directed towards a method and system "that enhances the security of unidirectional communication protocols used in access control systems, such as the Wiegand protocol." EX1001, Abstract; *see also id.*, 1:14-16 ("The present invention is generally directed to authentication of a reader and the security, privacy and efficiency of messaging in a secure access control system."); *id.*, 1:16-18 ("More specifically, the present invention provides extensions to unidirectional security protocols, such as the Wiegand protocol.").

54. The '562 patent states that prior art "Wiegand wires provide only a one-way channel for the communication of digital data, namely from the card reader to the upstream device." *Id.*, 11:1-4. But, according to the '562 patent, a "number of advanced features of physical access control systems can be realized if communication in the other direction, namely from the upstream device to the card reader, can be achieved." *Id.*, 11:5-8. One example given by the '562 patent is that "without true bi-directional data communication, there is no way that a reader can receive new configuration data, keys, or firmware without human intervention such as, for example, presenting a special configuration card to the reader or removing

the reader from the wall to connect to a serial communication port reserved for this purpose." *Id.*, 11:48-54; *see also id.*, 12:50-65.

55. The '562 patent thus purports to add bidirectional communication to the Wiegand system as follows:

> In accordance with at least one embodiment of the present invention, systems and methods are provided that allow existing physical access control systems using Wiegand wires for communication between readers and upstream system components such as control panels to be modified to also support data communication from the upstream components back to the readers. This may be affected by making modifications solely to the software and firmware contained in the readers and upstream devices and thus without making any changes to existing hardware. As an immediate consequence of the application of these inventive means, methods and systems, two-way, communication may be realized between card readers and upstream devices.

EX1001, 9:57-10:59. Specifically, the '562 patent states that "[t]his is accomplished by utilizing one or more of the Wiegand wires currently defined to carry only a high-low indicator signal with pre-defined semantics to carry packets of digital data." *Id.*, 11:27-30; *see also id.*, 12:9-11 ("packets of digital data can be sent from the upstream components including control panels back to the reader"); *id.*, 12:38-44 ("The data transmission of packets of data from an upstream device back to a reader via the Wiegand LEDCTL line or any of the other Wiegand control signal is described. . . ."); *id.*, 18:66-67 ("packet format such as the datagrams of the Internet Protocol (IP)").

56. Figure 5, for example, shows an embodiment of the '562 patent "depicting a full-duplex configuration of a reader and host" wherein the host can transmit data to the reader over existing wiring (EX1001, 13:52-54):

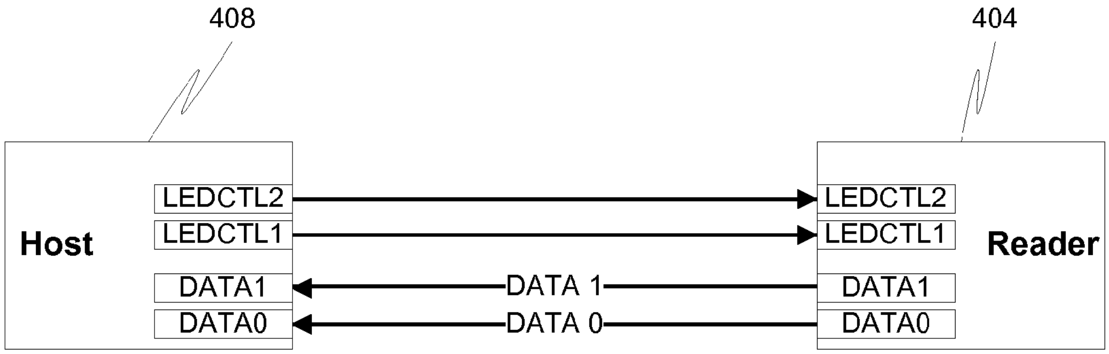



***Fig. 5***

57. The '562 patent describes that "[o]ne mode is the communication of the current art according to the SIA Standard." EX1001, 17:9-10. The other mode can be either "the advanced two-way packet-mode of communication described herein" or "the secure Wiegand mode." *Id.*, 17:10-14. Thus, the '562 patent states that:

> Modal communication necessitates a method of changing from one mode to the other and then optionally back to the original mode. In the teachings of the current disclosure, either the card reader or the upstream device can initiate mode change from Wiegand-format mode

> to packet-mode or from legacy Wiegand mode to secure Wiegand mode.

*Id.*, 17:15-22. The ’562 patent further states:

> By describing the communication of digital data in the other direction, from the upstream device to the reader, and by defining communication between the card reader and the upstream device while maintaining conformance to the SIA standard and on existing hardware, embodiments of the present invention connect the end nodes of physical access control systems to the Internet and thereby drastically decrease their maintenance and administration costs and greatly increase their security.

EX1001, 22:25-33. The ’562 patent further notes that “[b]i-directional communications enables the ability to utilize mutual authentication, a well established mechanism commonly used to authenticate communication devices.” *Id.*, 13:20-22. Further, the ’562 patent discusses multiple prior art methods to add security to Wiegand communications, such as the use of a tamper sensor attached to the reader, optionally in conjunction with adding additional data bits from the tamper-detecting device in the messages from the reader to the panel to alert the panel of any tampering. *Id.*, 3:37-4:24. Another example is a rolling code, or a code that changes regularly to prevent a prior recording of a reader-panel transmission from being replayed to gain access. *Id.*, 5:19-67. Finally, the ’562 patent states that the reader-panel data stream may be encrypted, such that even if the message is intercepted, the credential information will not be available without the deciphering key. *Id.*, 4:32-5:18.

### B. The Challenged Claims

58. Independent claim 1 recites a communication method taking place between a credential reader, including a memory and a processor, and an "upstream device," such as a control panel. The reader of claim 1 is capable of operating in a first mode—a "non-secure Wiegand mode" and in a second mode. The second mode comprises "at least one of a secure Wiegand mode and a packet-mode." The communication method of claim 1 requires that the reader: receive a message from the upstream device, determine that the message came from the upstream device, and then based on the determination, transition the credential reader from the first mode to the second mode. The other independent claims (claims 6 and 11) require the same features, but recite a non-transitory computer readable medium comprising processor-executable instructions, or a credential reader, respectively.

59. The dependent claims either specify that the communication protocol that the reader uses to communicate with the upstream device is a unidirectional protocol, such as the Wiegand protocol, or specify that the length of the message

from the upstream device to the reader that initiates the transition between modes lasts for "a predetermined amount of time," such as 10 ms.

### C. Prosecution History

60. The application that became the '562 patent was filed on November 29, 2012. EX1002. It is a divisional of another application filed on August 11, 2009, which later because U.S. Patent No. 8,358,783 ("the '783 patent"), and is related to a provisional application filed on August 11, 2008. *See id.*

#### 1. Prosecution of the '783 Patent

61. During prosecution of the '783 patent, on February 27, 2012, the applicant responded to a restriction rejection and elected "the claims in Group I (Claims 1-29), identified by the Office Action as being drawn to obfuscating data using a rolling code, for immediate prosecution on the merits." EX1003, at 1475-76.

62. Thereafter on April 13, 2012, the examiner issued a non-final office action rejecting all pending claims. EX1003, at 1479-90. The primary reference used in the rejections was U.S. Pub. No. 2009/0128392 ("Hardacker") (EX1019). *Id.* at 1482-89. Secondary references used in certain obviousness rejections with Hardacker included U.S. Pub. No. 2007/0046424 ("Davis '424"), U.S. Pub. No. 2006/0123466 ("Davis '466") (EX1009), U.S. Pub. No. 2008/0037466 ("Ngo"), and U.S. Pub. No. 2006/0210081 ("Zhu"). EX1003, at 1482-1489.

63. The applicant responded by amending the pending claims and providing remarks on August 13, 2012. EX1003, at 1513-21. The pending independent method claim, as amended, read as follows:

> 1. (Currently Amended) A communication method, comprising:
>
> obfuscating data transmitted in a first message from a first communication device to a second communication device, wherein the first and second communication devices communicate using a unidirectional communication protocol and wherein the obfuscation of the data is effected with a predetermined code wherein the first communication device is upstream of the second communication device, the method further comprising:
>
> determining that the message received at the first communication device was transmitted by the second communication device, wherein determining is performed by one or more of (i) analyzing an out-of-band communication received at the first communication device from the second communication device and (ii) analyzing a special code that identifies the second communication device is an advanced communication device in an advanced communication mode; and
>
> based on determining that the message was transmitted by the second communication device, transitioning the first communication device from a first mode of operation to a second mode of operation, wherein the first mode comprises a Wiegand-format mode and the second mode comprises a packet-mode.

*Id.*, at 1514.

64. The applicant argued in support of the patentability of the amended claims that Davis '466 "only discloses the concept of a 'Wiegand Extension' where extension bits are transmitted between a reader and panel" and that "there is absolutely no disclosure in Davis '466 of causing a reader to transition from a first mode of operation to a second mode of operation where the first mode comprises a Wiegand-format mode and the second mode comprises a packet-mode." EX1003,

at 1520. The applicant further stated that "[t]he advantages of having a reader configured to transition into a packet-mode of operation are described in detail in the originally-filed application at, for example, pages 29-33 and pages 38-40." *Id*.

65. The applicant made two other arguments concerning Davis '466: (1) that the table between paragraphs [0032] and [0033] of Davis '466 "only discloses bit values for commands sent by the panel," and (2) that "[t]here is no disclosure of causing a reader to perform [a transitioning function] by transmitting messages of [*sic*] a Wiegand wire, namely the LEDCTL line of the Wiegand wire."[1] EX1003, at 1521.

66. A first notice of allowance next issued on August 31, 2012, but a subsequent amendment was made to one of the claims via an examiner's amendment on October 17, 2012, following an examiner interview. EX1003, at 1530, 1550-51. In this amended form, another notice of allowability was issued on October 17, 2012, and U.S. Patent No. 8,358,783 issued on January 22, 2013. *Id.* at

[1] As discussed below, the applicant's statement that Davis '466 does not disclose "causing a reader to perform [a transitioning function] by transmitting messages of [*sic*] a Wiegand wire, namely the LEDCTL line of the Wiegand wire" is incorrect. *See infra* §IX.A.2.e, EX1006, 5:47-64.

1548-52; EX1011, (45). The primary examiner during prosecution of the ’783 patent was Cordelia Zecher.

### 2. Prosecution of the ’562 Patent

67. Claims that eventually issued in the ’562 patent were submitted on November 29, 2012, and were examined by a different examiner (Samson Lemma) than the examiner of the application that issued as the ’783 patent. EX1002, at 7-63, 171-182. On January 17, 2014, the examiner issued a non-final office action, rejecting all pending claims (1-20) as being unpatentable under the doctrine of obviousness-type double patenting over claims 1-27 of the ’783 patent. *Id.* at 171-175. Further, claims 1-5, 8-12, and 15-18 were rejected as being anticipated by International Publication No. EP1760985 (EX1010).[2] EX1002, at 179-81. The examiner found that the claimed mode-switching capabilities were taught by the ’985 publication’s disclosure that “the control panel could inform the reader to change how it is working…with a prompting signal send via an LED control signal.” EX1002, 180 (quoting EX1010, ¶[0045]). I note that this quotation does not appear to describe another mode of operation. Rather the ’985 publication appears to only describe changing which rolling code is used. *See* EX1010,

[2] Other claims were rejected under 35 U.S.C. 112, second paragraph and and/or 35 U.S.C. § 101. EX1002, at 175-78.

¶[0045] ("The control panel 104, at any random time, may change the order in which the code generator 148 goes through the list. The control panel 104 could inform the reader 112 to change how it is working through the list with a prompting signal send via an LED control signal, or may do so through an interruption to the power supply of the reader 112. This ensures that the code generator 148 does not necessarily have to go through a finite list of valid rolling codes in the same order until a new list of codes is provided to the code generator 148. Rather, the same list may be used for a relatively longer amount of time and a higher level of security can be maintained.").

68. The examiner rejected claims directed to the alteration of a control line signal for a predetermined amount of time over the following disclosure of WO 02/082367 (EX1008):[3]

> The panel system in the preferred embodiment is able to switch a Wiegand generator [(a reader)] from the basic protocol to the extended protocol as follows. Note that this procedure will typically be run when the panel is initialized. The panel will drop the LEDCTL signal low three times within a one-second interval. The Wiegand generator starts an interval timer when the first pulse is received, and then checks to see if it receives two additional

[3] WO 02/082367 (EX1008) is the international equivalent publication of Davis (EX1006). Davis (EX1006) is incorporated into EP1760985 by reference. (EX1010, ¶[0013].)

pulses within the one-second period from the first pulse. If it receives exactly three pulses as described, then it sends the Wiegand extension message "Capable of Using the Wiegand Extension" in message group 0. The panel then will send out the "Use Wiegand Extension" command to the Wiegand generator, and the Wiegand generator sends the "Command received and executed" message in group 0 and sets a flag in non-volatile memory to use the Wiegand extension (even if power is lost and subsequently restored)

EX1002, at 180-81 (citing EX1008, at 13).

69. The applicant responded on April 21, 2014, amending the pending independent method claim as follows:

> 1. (Currently Amended) A communication method, comprising:
>
> operating a credential reader in a first mode of operation<u>, the credential reader comprising at least one of a microprocessor and firmware that enable the credential reader to operate in the first mode of operation</u>;
>
> receiving, at <u>a communication interface of</u> the credential reader, a message from an upstream device;
>
> determining, by the credential reader, that the message was transmitted by the upstream device; and
>
> based on determining that the message was transmitted by the upstream device, transitioning the credential reader from the first mode of operation to a second mode of operation<u>, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode</u>.

EX1002, at 320. The applicant argued that the addition of the first mode and second mode definitions (underlined above), which the examiner had indicated were allowable, rendered the pending claims patentable. EX1002, at 320-323, 325,

181. The applicant did not provide any arguments regarding the disclosure of WO 02/082367 noted above. *See* EX1002, at 324-26.

70. After the applicant submitted a terminal disclaimer following a final rejection on May 22, 2014 for double patenting, a notice of allowance issued on September 16, 2014. EX1002, at 335-40, 372, 382. The ’562 patent issued on January 27, 2015. EX1001, (45).

### D. Priority

71. The earliest possible effective filing date of the ’562 patent is August 11, 2008, which I have been asked to assume is the priority date.

## VIII. CLAIM INTERPRETATION

72. I understand that determining whether a claimed invention is novel and non-obvious requires comparing the prior art to the claim. I understand that claim terms are typically given their ordinary and customary meaning, as would have been understood by a POSITA. I understand that one must consider the language of the claims, the specification, and the prosecution history of record when construing claim terms.

73. I understand that, in IPR proceedings, claim terms in a patent are given their ordinary and customary meaning as understood by a person of ordinary skill in the art (“POSITA”). I understand that claim terms are to be construed in the context of the entire patent, including the specification, and that the specification is

the best guide to the meaning of a disputed claim term. I understand that the patent's prosecution history should also be considered in construing the claims. It is also my understanding that evidence such as expert testimony, technical treatises, and dictionaries may be consulted to determine the meaning of claim language. However, if the specification provides a special definition for a claim term that differs from the meaning the term would otherwise possess, the specification's special definition controls. If a claim element is expressed as a "means" for performing a specified function, I understand that it covers the corresponding structure described in the specification and equivalents of the described structure. I have applied these standards in preparing the opinions in this declaration. For any claim term not addressed below, I adopted the ordinary and customary meaning of the same as it would have been understood by a POSITA as of August, 2008.

### A. "non-secure Wiegand mode"/ "secure Wiegand mode"

74. In my opinion, a POSITA would have understood "non-secure Wiegand mode" and "secure Wiegand mode," which are recited in claims 1, 6, and 11, to respectively refer to the "legacy Wiegand communication protocol with no added security features," as described in the 1996 SIA standard, and the "legacy Wiegand communication protocol with one or more added security features."

75. First, the claims compel this understanding. By contrasting "non-secure Wiegand mode" with "secure Wiegand mode," the claims inform that the difference between the two modes is that the "secure Wiegand mode" is *secure*, whereas the "non-secure Wiegand mode" is not.

76. The specification provides consistent meaning for "non-secure Wiegand mode." For example, the '562 patent teaches two embodiments where, in one embodiment, "**[o]ne mode is the communication of the current art according to the SIA standard**. The other mode is the advanced two-way packet-mode of communication described herein. In another embodiment, **one mode is the standard Wiegand communication mode** and the other mode is the secure Wiegand mode." [4] *See* EX1001, 17:9-14. In my opinion, the descriptions that one mode is "the communication of the current art according to the SIA standard" or "the standard Wiegand communication mode" directly inform that "non-secure Wiegand mode" refers to "legacy Wiegand communication protocol." *See also id.* 1:22-24 ("The Wiegand protocol is the predominant method by which physical access control card readers communicate with upstream devices. . . .).

[4] All emphasis added unless otherwise noted.

77. Likewise, the specification describes transitioning "from **legacy Wiegand mode to secure Wiegand mode,**" showing that "non-secure Wiegand mode" refers to the "legacy Wiegand communication protocol." *Id.* 17:17-22.

78. Likewise, the specification also instructs the meaning of the phrase: "secure Wiegand mode." *See* EX1001, 17:12-22 ("In another embodiment, **one mode is the standard Wiegand communication mode and the other mode is the secure Wiegand mode**. . . . In the teachings of the current disclosure, either the card reader or the upstream device can initiate mode change from Wiegand-format mode to packet-mode **or from legacy Wiegand mode to secure Wiegand mode.**").

79. Despite the specification using "i.e." to describe secure Wiegand mode as both "i.e., the secure use of rolling codes in accordance with the Wiegand mode" (*id.* 17:20-22), and as "i.e., a packet transmission mode or any other secure Wiegand mode discussed herein," (*id.* 18:46-47), it is my opinion that these statements contradict each other and do not act to narrowly define "secure Wiegand mode." For example, by equating the secure Wiegand mode as "i.e., a packet transmission mode" does not make sense in light of the separate claim terms, and thereby separate terms and meanings of "packet-mode" and "secure Wiegand mode." *See* §§VIII.B, A [packet mode CC section, secure Wiegand mode section]; *see also* Ground 1, Claim 1[D] *infra* §IX.A.2.e. Further, to limit the

definition of secure Wiegand mode" to the narrow security measure of the "secure use of rolling codes in accordance with the Wiegand mode" would negate the '562 patent's statement that the secure Wiegand mode can be "any **other** secure Wiegand mode discussed herein," when indeed, the specification includes substantial description of mechanisms to add security to the Wiegand protocol. *See* EX1002, 6:10-14 ("**In accordance with still further embodiments of the present invention, two devices may be enabled to use a synchronized pseudo-random number generator (PRNG) to secure the communication between them**, for example."), 22:43-46 ("In accordance with at least some embodiments of the present invention, two devices may be using a synchronized PRNG to, for example, secure the communication between them."), 3:43-9:55 (describing prior art methods to add security to Wiegand communications, including appending additional bits to the reader-panel data transmissions, use of time stamps in messages, encryption, and the use of rolling codes), 13:59-17:22 (the Detailed Description describing a security mechanism for "obscuring Wiegand Data" and then "Two-Way Packet-Mode Communication"), Title ("Secure Wiegand Communications"), Abstract ("The present invention is directed toward secure access systems."). Indeed, it is my opinion that in the complete context of the '562 patent, including by titling the '562 patent as "Secure Wiegand Communication" and including material spanning over ten columns (columns 3 through 9 and 13 through 15) that is directed to security in Wiegand communications, that the secure Wiegand mode refers to the "legacy Wiegand communication protocol with added security features."

80. In my opinion, the prosecution history does not add further illumination to the meaning of "non-secure Wiegand mode" or "secure Wiegand mode."

81. Further, my own experience and understanding of the Wiegand interface support these constructions. Indeed, as described above, the standard Wiegand protocol was subject to known security threats, and security measures have been devised which may be added to the standard Weigand protocol. *See supra* §VI.C.2. Therefore, it would have been consistent with the prior art and the POSITA's understanding of the art to construe "non-secure Wiegand mode" as the "legacy Wiegand communication protocol," as described in the 1996 SIA standard because such standard is subject to known security risks, and to construe "secure Wiegand mode" as the "legacy Wiegand communication protocol with added security features" because there are known security features that may be implemented to secure the Wiegand interface and its communications.

82. Thus, in my opinion, a POSITA would have understood "non-secure Wiegand mode" to refer to the "legacy Wiegand communication protocol," as described in the 1996 SIA standard. Likewise, in my opinion, a POSITA would

have understood "secure Wiegand mode" to refer to the "legacy Wiegand communication protocol with added security features."

83. Moreover, the construction of "non-secure Wiegand mode" as the "legacy Wiegand communication protocol," as described in the 1996 SIA standard is consistent with Patent Owner's infringement contentions for the '562 patent in related litigation. *See* EX1013, at 10-13 (asserting that Petitioner's products "switch from a defaulted Weigand mode" to meet the "non-secure Wiegand mode" limitation, and quoting installation guide's statement that "[b]y default, the reader will transmit credential and keypad data in Weigand communication mode").

**B. "packet-mode"**

84. I understand that the phrase "packet-mode," as recited in claims 1, 6, and 11 to mean "a mode wherein a Wiegand control signal is used to transfer packets of digital data to the reader."

85. Although the '562 patent does not define what a "packet" is, the term was well understood in the art before the priority date to refer to "[a] short section of data of fixed length that is transmitted as a unit," that is, "[t]he basic unit of [data] encapsulation" for transmission. EX1021, at 5 (McGraw-Hill definition of "packet" for communications); *see* EX1001, 11:30 ("packets of digital data"), 19:45-46 ("Imputing meaning to the bytes in a frame is called packet framing and results in a packet of data."); EX1018, at 5; *see also supra* §VI.C.1.

86. Moreover, the ’562 patent’s specification instructs that “packet-mode,” refers to a “mode wherein packets of digital data are transferred on the Wiegand LEDCTL wire.” For example, the specification states that:

> Elements of this particular aspect include electrical and logical digital encoding techniques that enable the transmission of digital data to card readers in access control systems from upstream devices such as control panels. **This is accomplished by utilizing one or more of the Wiegand wires currently defined to carry only a high-low indicator signal with pre-defined semantics to carry packets of digital data.** The existing methods of communication on Wiegand wires as described by the SIA standard only provide for the transmission of a single high-low indicator to be sent from an upstream device to the reader, **in particular on the LEDCTL wire**. . . . In accordance with at least some embodiments of the present invention, additional meaning is given to both the [voltage] levels and transitions of the LEDCTL signal. By programming these additional meanings into the software of the reader, **packets of digital data can be sent from the upstream components including control panels back to the reader.**

EX1001, at 11:23-12:11; *see also id.* at 12:38-44 (The data transmission of packets of data from **an upstream device back to a reader via the Wiegand LEDCTL line or any of the other Wiegand control signal** is described in the following in three aspects. 1. mode change protocol 2. data encoding 3. packet structure); 18:33-40 (“A reader implementing the teachings of the current disclosure having detected a voltage level duration on the LEDCTL wire of less than 10 ms sends an acknowledgement message, which may be obfuscated with a rolling code, on the DATA0 and DATA1 wires indicating that it has detected the request to **change to packet-mode communication on the LEDCTL wire and has switched to this mode of reception on the LEDCTL wire**."), 19:43-21:44 (describing data transmission on the LEDCTL wire); 21:59-61 ("The intent of the current disclosure is to cover all methods for the serial communication of digital data on the LEDCTL line…."), FIGS. 4, 5.

87. Further, as noted above, the '562 patent states that "[i]mputing meaning to the bytes in a frame is called packet framing and results in a packet of data" (*Id.*, 19:45-46), and the '562 patent likewise describes transmission of frames (packets of data given meaning) on the LEDCTL line. *See id.*, 19:13-19 ("There are in the current art methods of encoding sequences of 0's and 1's or digital data bits on a single wire such as LEDCTL. There are also in the current art methods of forming these streams into finite-length blocks of 8-bit elements called bytes. **The blocks of digital data received on the LEDCTL** wire are called frames").

88. In my opinion, the prosecution history does not add further illumination to the meaning of "packet-mode."

89. Thus, the phrase "packet-mode," refers to a "mode wherein packets of digital data are transferred on the Wiegand LEDCTL wire."

### C. "at least one of a secure Wiegand mode and a packet-mode"

90. In my opinion, in view of the '562 patent's specification and file history, the claim language of "**at least one of** a secure Wiegand mode **and** a packet-mode" of Claims 1, 6, and 11 only requires only **one of** the packet-mode **or** the secure Wiegand mode need to be present for the limitation to be met. Put another way, "and" should be read disjunctively, such that the claim language is met if at least one of secure Wiegand mode OR a packet mode are present.

91. The specification confirms this understanding. The specification states that:

> In the teachings of the current disclosure, communications between the reader and upstream systems is modal. Embodiments of the present invention contemplate **at least** two modes of communication. One mode is the communication of the current art according to the SIA standard. The other mode is the advanced two-way packet-mode of communication described herein. **In another embodiment**, one mode is the standard Wiegand communication mode and the other mode is the secure Wiegand mode."

EX1001, 17:6-14. To require both the secure Wiegand mode and a packet-mode in claim 1[D] would collapse these two embodiments into one, providing **only** two modes of operation: non-secure Wiegand mode, on one hand, and the packet-mode and the secure-Weigand mode on the other hand. This contrasts with the cited disclosures above, which provide for **three** modes of operation: (1) non-secure

Wiegand mode and (2) packet-mode, or (1) non-secure Wiegand mode and (3) secure Wiegand mode. Thus, reading the claims to require only one of the packet-mode or the secure Wiegand mode maintains the embodiments of the specification.

# IX. THE CHALLENGED CLAIMS ARE UNPATENTABLE IN LIGHT OF THE PRIOR ART IDENTIFIED IN THE PETITION

## A. Ground 1: Claims 1-4, 6-9, and 11-13 Are Anticipated by Davis

### 1. Davis (EX1006)

92. Davis issued on January 17, 2006, from an application that was filed on April 6, 2001. EX1006.

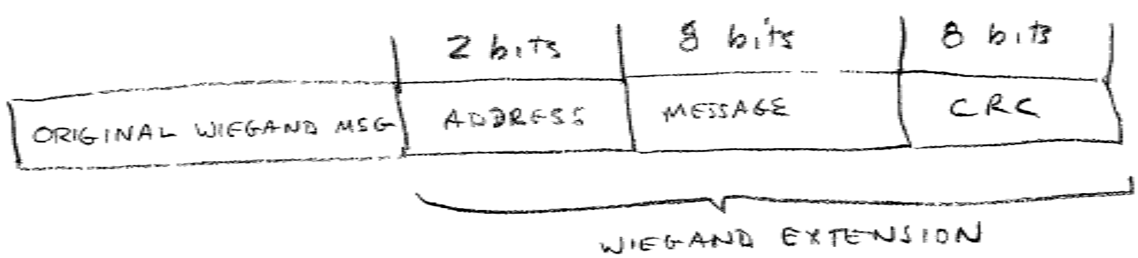
93. Just like the ’562 patent, Davis discloses a system and method of extending the “industry standard Wiegand protocol for enabling two way extended communication, enhanced error detection, encryption, . . . and enhanced information regarding the embedded data stream between a Wiegand device[,] such as a card reader[,] and a control panel on the existing 5-wire bus structure without requiring the modification to the existing infrastructure.” *Id.*, Abstract, Title.

94. Davis recognizes that the “Wiegand standard protocol [was] well known in the art” and was “in prevalent use for many years.” EX1006, 1:33-43. Davis further recognizes “problems” that “exist[ed] with the Wiegand protocol.” *Id.*, 1:53. “For example, the Wiegand protocol is a one-way protocol, since the

reader can send data to the panel but the panel cannot send any data to the reader except to control the door mechanism and a status LED." *Id.*, 1:54-57.

95. As such, Davis discloses, *inter alia,* a "major improvement" in "that the LEDCTL line controlled by the panel is now used to transmit data back to the reader." EX1006, 2:29-31. Davis's so-called "Wiegand extension" was able to "be turned on or off, so that if a panel does not support the extension, it is not used and the reader behaves as an existing prior art device." *Id.*, 2:41-43. To enable the panel to send data to the reader, "[d]ata transfers are made by the control panel using the electrical characteristics of the Wiegand protocol via the LEDCTL input signal as a serial protocol." *Id.*, 2:64-67; *see also id.*, 5:18-45 (description of preferred embodiment under heading, "Data Transfer from Panel to Reader").

96. An illustration of Davis's "extended Wiegand protocol" is shown at Figure 2:




EX1006, FIG. 2. The Wiegand extension uses additional fields, including those for address, message, and cyclic redundancy check (CRC). *See id.*; *see also id.* 2:23-29, 7:43-44. "The panel system in the preferred embodiment is able to switch a Wiegand generator from the basic protocol to the extended protocol. . . ." *Id.*, 5:47-49.

97. The "Wiegand extension" may be turned on or off through transmissions over the LEDCTL line. *Id.*, 2:41-43; *see also id.,* 2:64-67*,* 5:18-6:44. The panel system turns the Wiegand extension on by dropping "the LEDCTL signal low three times within a one-second interval." *Id.*, 5:50-52. As noted, "[t]he panel system in the preferred embodiment is able to switch a Wiegand generator from the basic protocol to the extended protocol. . . ." *Id.*, 5:47-49. If the Wiegand extension is turned off, for example "if a panel does not support the extension, it is not used and the reader behaves as an existing prior art device," and only one-way communication is possible. *Id.*, 2:41-43, *see also id.*, 1:54-57. Thus, Davis's reader can operate in two modes: as "an existing prior art device," or in the "Wiegand extension," where data may be transmitted back to the reader from the panel through the LEDCTL line and the messages from the reader to the panel may include additional data bits, such as data bits from a tamper sensor connected to the reader. *Id.*, 2:29-31, 2:41-43, 3:9-31, 4:15-24, 5:47-49.

98. Davis is in the same field as the '562 patent because Davis relates to the electronics and communication protocols used in access control systems. EX1006 at Abstract, 2:23-3:34. Davis is pertinent to the problems the '562 patent purportedly addresses because Davis is directed to an access control system having

the ability to switch between the legacy Weigand mode and a secure Weigand mode or packet-mode. *Id.* Davis is therefore analogous art to the ’562 patent.

### 2. Claim 1

#### a. 1[pre]: “A communication method, comprising”

99. I understand that “[a] communication method, comprising” is the preamble of claim 1. I have been asked to assume that the preamble is limiting. In my opinion, Davis discloses the preamble. Specifically, Davis discloses a “System and **Method of Extending Communications with the Wiegand Protocol**.” EX1006, Title. Davis’s communication method provides “[a]n extension of the industry standard Wiegand protocol for enabling two way extended communication . . . between a Wiegand device such as a card reader and a control panel on the existing 5-wire bus structure without requiring the modification to the existing infrastructure.” EX1006, Abstract. An object of Davis is “to provide a methodology and system for extending the functionality of the Wiegand protocol such that improved readers and panels may be implemented, without requiring rewiring of the existing Wiegand infrastructure in use today.” EX1006, 2:4-8. The following communication method steps are disclosed by Davis.

**b. 1[A]: "operating a credential reader in a first mode of operation, the credential reader comprising at least one of a microprocessor and firmware that enable the credential reader to operate in the first mode of operation"**

100. Davis discloses this limitation. Davis also teaches that the reader may operate in a first mode of operation: "The Wiegand extension can be turned on or off, so that if a panel does not support the extension, it is not used and the reader behaves as an existing prior art device." EX1006, 2:41-43. By teaching a reader that "behaves as an existing prior art device," Davis teaches "operating a credential reader in a first mode of operation." Indeed, a POSITA would have understood the reader behaving "as an existing prior art device" to describe a first *mode* because it describes a mode of operation. A POSITA would have understood that "an existing prior art device" is a different mode of operation than the "Wiegand extension" Davis teaches may be "turned on or off." *See* §§IX.A.1, VI.B. A POSITA also would have understood the Wiegand extension mode to comprise the second mode of operation, as described below. *See infra* §IX.2.e.

101. As shown below in Figure 3, Davis discloses a credential reader 10 with processing/logic 24. The reader 10 includes "an RF transmitter/receiver 26, which is known in the art and which is used for reading an access control card when presented thereto." EX1006, 4:12-14. Davis further discloses that the 5-wire Wiegand interface is implemented in the reader, with "[t]he transmitter 12 and

receiver 14 … connected to the DATA1, DATA0, and LEDCTL wires of the standard Wiegand interface as known in the art" (*id.* 4:9-12), and the power (PWR) and ground (GND) connected to power supply circuit 16 (*id.* 4:6-9).

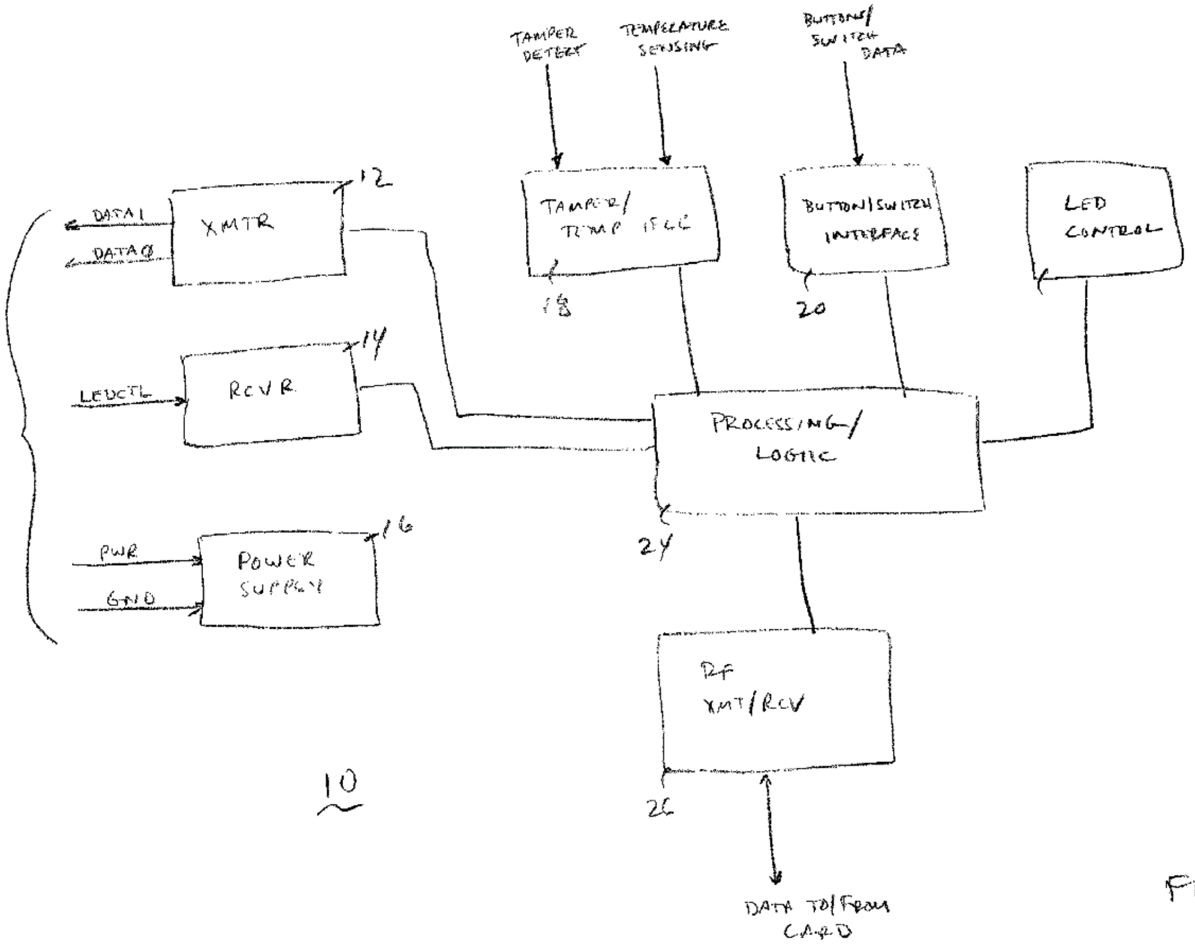



FIG. 3

EX1006, FIG. 3.

102. Davis teaches that "Processor 24 is used to read data from the external sources, formulate data to be transferred over the 5-wire interface, and run all other functions that may be required by the reader 10 of the present invention." EX1006, 4:45-48. A PHOSITA would have understood processing/logic to comprise a

microprocessor. Indeed, processing of commands and executing programming logic was well understood to take place on a microprocessor.

103. Davis teaches that its reader has firmware. EX1006, 2:35-38 ("As a result of this invention, described herein, no additional wires are required to be connected between the panel and the reader, thus preserving the existing Wiegand infra-structure while providing increased functionality. The panel computer will require no changes to its interface (or other) hardware; only **the firmware** needs to be modified in accordance with the invention. Messages can be customized by users in accordance with the extended protocol set forth herein."). A POSITA would have understood that this firmware interacts with the aforementioned hardware to "enable the credential reader to operate in the first mode of operation." Indeed, it is inherent or strongly suggested that there is firmware that enable the processor in Davis's reader to interact with its hardware in order to enable the physical functions, including sending data transmissions to the panel, described with respect to the Wiegand Extension or to enable the reader to behave "an existing prior art device" (*Id.* 2:41-43). Further, if there were no firmware, Davis's reader would not function because the processor's commands could not be executed on the hardware.

104. As such, a POSITA would have readily understood Davis to disclose at least one of a microprocessor and firmware as recited in claim 1 of the ’562 patent.

#### c. 1[B]: “receiving, at a communication interface of the credential reader, a message from an upstream device;”

105. Davis discloses these limitation. Specifically, Davis discloses a reader (“also referred to as a Wiegand generator,” EX1006, 4:52-57) operating in a first mode (“the basic protocol”) receiving a communication from a panel (an upstream device):

> The panel system in the preferred embodiment is able to switch a Wiegand generator from the basic protocol to the extended protocol as follows. Note that this procedure will typically be run when the panel is initialized. **The panel will drop the LEDCTL signal low three times within a one-second interval. The Wiegand generator starts an interval timer when the first pulse is received, and then checks to see if it receives two additional pulses within the one-second period from the first pulse. If [the Wiegand generator] receives exactly three pulses as described, then it sends the Wiegand extension message “Capable of Using the Wiegand Extension”** in message group 0.[5] **The panel then will send out the “Use Wiegand Extension” command to the Wiegand generator**….

[5] Davis explains that “there are seven groups of messages; each is used for different Wiegand generators. … Group zero is reserved for messages common to all group[s].” *Id.* at 5:12-17.

EX1006, 5:47-63. As shown in Figure 3, below, the signal over the LEDCTL wire is received at the receiver (14), which a POSITA would understand is a communication interface. *Id.*, FIG 3. Indeed, Davis explains that the receiver 14 receives and sends messages over the LEDCTL wire and DATA1 and DATA0 wires, thus providing an interface through which data communications may be sent or received. *See* EX1004, 4:5-14.

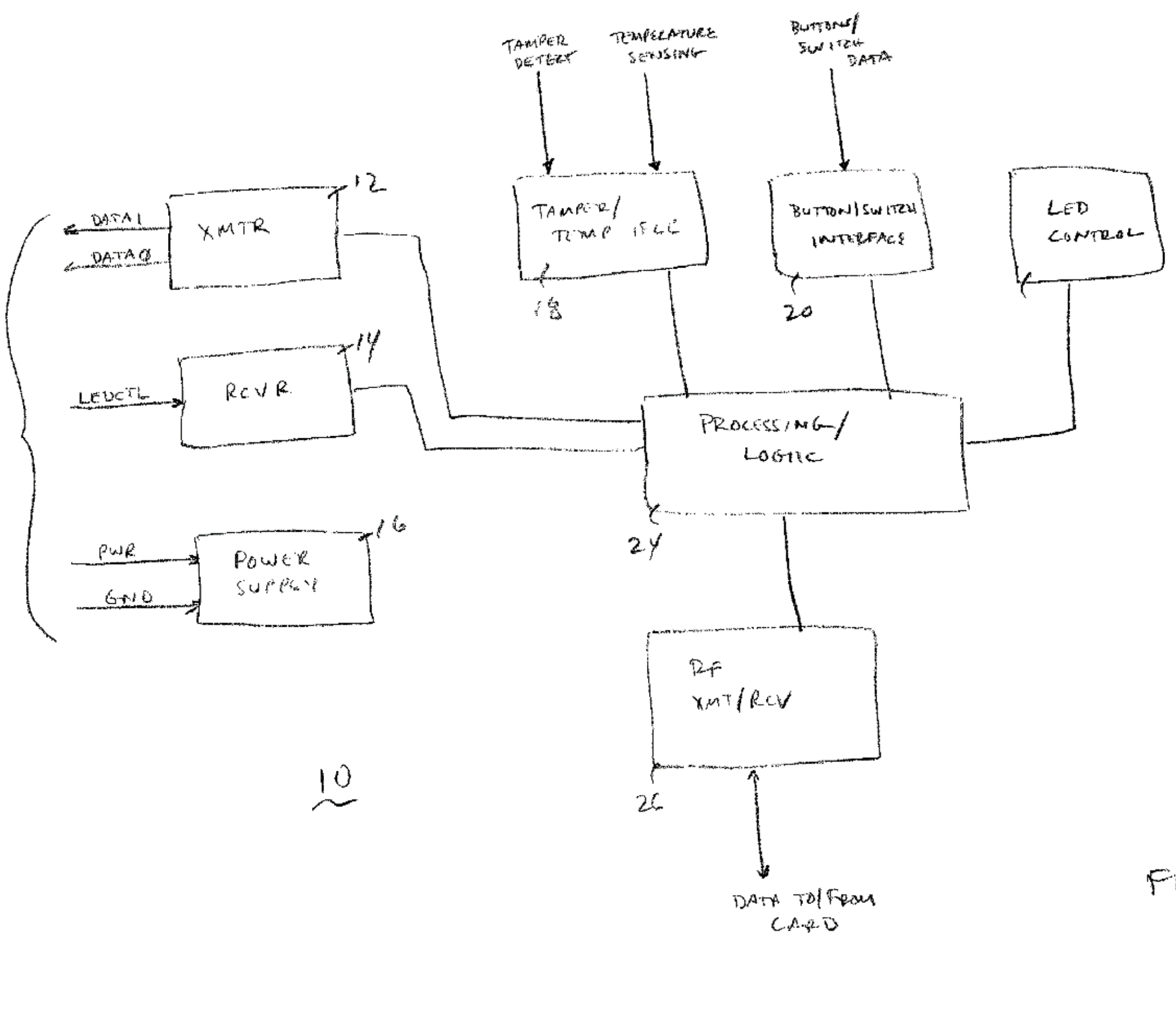



FIG. 3

### d. 1[C]: "determining, by the credential reader, that the message was transmitted by the upstream device; and"

106. The specification of the '562 patent does not appear to support or otherwise describe the "determining" step by the credential reader. But to the extent the claim language of "determining, by the credential reader, that the message was transmitted by the upstream device," requires an additional step, Davis also discloses it. For example, to the extent the "determining" step is met if the reader merely "listens" for a message from an upstream device, as Patent Owner contended in related litigation, Davis teaches this interpretation. EX1013, at 9-10. A POSITA would have understood the reader "check[ing] to see if it receives two additional pulses within the one-second period form the first pulse" to describe a reader listening for messages from the upstream device because checking is generally synonymous with listening. EX1006, at 5:52-55.

107. Further, Davis discloses that the Wiegand generator (reader) will send the "Capable of Using the Wiegand Extension" message **"[i]f [the Wiegand generator] receives exactly three pulses as described."** *Id.* at 5:55-58; *see also id.* at 5:52-55 ("The Wiegand generator starts an interval timer when the first pulse is received, and **then checks to see if it receives two additional pulses** within the one-second period from the first pulse."). A POSITA would have understood this to teach the "determining" step because Davis describes a determination by the

Wiegand generator that three pulses are received from the panel (*i.e.*, the upstream device) before the Wiegand generator changes modes.

108. Moreover, as Davis explains, panel sends the reader the command to change modes over the LEDCTL line. EX1006, 5:47-63. The signals coming over this line necessarily come from an upstream device, as Davis discloses (and legacy Wiegand requires) that any signal to the reader over the LEDCTL line is from an upstream device. *See* EX1006, 1:40-42, 1:53-57, 2:29-43, 4:37-44; EX1007, at 5, 9, 11, 12; EX1012, ¶[0009]; *see supra* §VI.B, the signals coming down this line to the reader necessarily come from an upstream device. Thereby, because there is no other line on which the reader of Davis could receive a message from an upstream device, the reader would determine that the message on the LEDCTL line came from an upstream device.

**e. 1[D]: "based on determining that the message was transmitted by the upstream device, transitioning the credential reader from the first mode of operation to a second mode of operation, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode."**

109. Davis discloses this limitation. In response to the determination that "that the message was transmitted by the upstream device" noted in Claim 1[C], *supra* §IX.2.e, Davis teaches that the "panel system in the preferred embodiment is

able to switch a Wiegand generator from the basic protocol to the extended protocol" by:

> The panel [] drop[ping] the LEDCTL signal low three times within a one-second interval. The Wiegand generator starts an interval timer when the first pulse is received, and then checks to see if it receives two additional pulses within the one-second period from the first pulse. If [the Wiegand generator] receives exactly three pulses as described, then it sends the Wiegand extension message "Capable of Using the Wiegand Extension" …. **The panel then will send out the "Use Wiegand Extension" command to the Wiegand generator, and the Wiegand generator sends the "Command received and executed" … and sets a flag in non-volatile memory to use the Wiegand extension (even if power is lost and subsequently restored).**

EX1006, 5:47-63. As explained in Ground 2, Claim 5; and Ground 3, Claim 5 *infra* §§IX.B.1, IX.C.2, a POSITA would have understood the three pulses within the one-second interval to be a form of a start signal.

110. A POSITA would have understood that the "basic protocol" and the "extended protocol" to comprise the first and second modes, respectively, because each protocol describes a different mode of operation. The '562 patent discloses that the first mode ("an existing prior art device," *see* Claim 1[A], *supra* §IX.A.2.b is "a non-secure Wiegand mode," or as properly construed, the "legacy Wiegand communication protocol with no added security features." *See* §VIII.A, *supra*.

111. The standard Wiegand protocol—the first mode—was very well understood in the art before the priority date. *See* §§VI.B-C, *supra.* For example, Davis states in its background section:

> One technology in prevalent use for many years is the [W]iegand protocol, which utilizes five wires to communicate data and provide power to a dedicated card reader as well known in the art. The five wires are for power, ground, DATA0, DATA1, and LEDCTL. The DATA1 line is a reader output that delivers pulses that are interpreted as binary ones. The DATA0 line is a reader output that delivers pulses that are interpreted as binary zeros. The LEDCTL line is the panel output that determines the state of the LED contained on the reader (off, red, green, or amber). The Wiegand standard protocol [is] well known in the art and is described in detail in "Access Control Standard Protocol for the 26-Bit Wiegand Reader Interface," by the Security Industry Association.

EX1006, 1:32-46. Indeed, the Wiegand interface described by the SIA standard was discussed in multiple exhibits attached to this filing. *See e.g.*, EX1001, 1:33-39; EX1006, 1:42-48; EX1008, at 4; EX1011, 1:32-38; EX1012, ¶[0008]; EX1014, ¶[065]. Thus, Davis teaches the first mode.

112. The second mode disclosed by Davis (extended protocol, or Wiegand extension) also teaches both the "packet-mode" and the "secure Wiegand mode," even though the claim language of "at least one of a secure Wiegand mode and a

packet-mode" only requires one of the two, when properly construed. *See supra* §VIII.C.

113. Relating to the packet-mode, Davis teaches this limitation, properly construed as "a mode wherein a Wiegand control signal is used to transfer packets of digital data to the reader." *See supra* §VIII.B. Davis further teaches that a "major improvement is that the LEDCTL line controlled by the panel is **now used to transmit data back to the reader**." EX1006, 2:29-31. "Data transfers are made by the control panel using the electrical characteristics of the Wiegand protocol **via the LEDCTL input signal** as a serial protocol." *Id.* 2:64-67; *see also id.* 4:39-43. A POSITA would have understood "LEDCTL" within the context of Davis to refer to the LED control line. Indeed, the '562 patent describes Davis as teaching "transmitting data back to the reader from the upstream device **via an LED control line**." EX1001, 4:21-31. A POSITA would have understood that Davis's transmissions on the LEDCTL line are Wiegand control signals because the signals are sent on a control line. *See, e.g.*, EX1001, 11:55-12:41, 15:45-51, 17:38-18:57; EX1006, 5:19-27, 5:50-52. Further, the voltage on the LED wire is altered to send a signal. *See* EX1001, 17:38-18:57, EX1006, 5:19-27, 5:50-52.

114. Davis describes "Data Transfer from Panel to Reader" as follows:

> In accordance with the invention, the panel may send data to a reader using an asynchronous serial data stream via the LEDCTL wire at 1200 baud, 8 data bits, 1 stop bit, no parity. All fields in this instance are one

byte long. The first byte of a command is divided into two sub-fields. The first two bits are the address field (00-11), and the last six bits contain the command code (000000-111111). The following commands are available in the preferred embodiment:

| COMMAND SENT BY PANEL | | WIEGAND GENERATOR RESPONSE |
|---|---|---|
| 00h <CRC> | 0 = retransmit last Wiegand data transmission <CRC> = 8-bit CRC | Retransmits last Wiegand data message |
| 01h <address> <CRC> | 1 = Return value of selected parameter address <address> = 00 thru FF <CRC> = 8-bit CRC | Parameter value of desired address is transmitted back via the Wiegand extension |
| 02h <address> <data> <CRC> | 2 = set value of selected parameter address <address> = 00 thru FF <data> = 00 thru FF <CRC> = 8-bit CRC | Acknowledgement that data was written is transmitted via the Wiegand extension |
| 03h <LEDCTL> <seconds> <CRC> | 3 = Turn on LED <LEDCTL> = simulation of LED control signals <# of seconds to keep LED on> <CRC> = 8-bit CRC | Acknowledgement is transmitted via the Wiegand extension |

EX1006, 5:19-46.

115. A POSITA would have understood that the disclosure of an "8 data bits, 1 stop bit, no parity" data stream that the "the panel may send [] to a reader . . . via the LEDCTL wire" teach packet-mode, construed as "a mode wherein a Wiegand control signal is used to transfer packets of digital data to the reader." *See supra* §VIII.B. In addition to being sent on the Wiegand LEDCTL wire (a Wiegand control signal wire, *see* EX1001, 12:38-41 ("the Wiegand LEDCTL line or any [] other Wiegand control signal…")), the "8 data bits, 1 stop bit, no parity" comprises a packet of data because it is "[a] short section of data of fixed length

that is transmitted as a unit." EX1021, at 5 (McGraw-Hill definition of "packet" for communications). These communications enable, for example, panel-reader communication where "[i]f the panel determines that there is an error in the received Wiegand data (i.e., due to a CRC error), then it can request the reader to retransmit as described herein." EX1006, 4:60-63. Because the panel may transition the reader from the standard Wiegand protocol, where the no data is transmitted over the LEDCTL wire, to a mode in which the panel may send these packets of data to the reader over the LEDCTL line, Davis teaches a packet-mode, when properly construed as "a mode wherein a Wiegand control signal is used to transfer packets of digital data to the reader." *See supra* §VIII.B.

116. Further, the '562 patent does not purport to have invented the communication of data in packets, as recited in the claims. *See* EX1001, at 19:65-20:3 ("**There are in the art other packet framing protocols that would be appropriate for use on two-way, packet-mode serial communication means for Wiegand wires described in the current disclosure** such as the serial line internet protocol (SLIP) described in RFC 1055 and the point-to-point protocol (PPP) described in RFC 1661."); 22:7-14 ("By adding hardware to either the card reader or the upstream device or by inserting additional hardware components such as gateways and translators into the physical access control system, there are alternative methods of achieving the communication of packet data from upstream

devices to card readers using Wiegand wires. **Indeed there are such devices in the art**."); *see also id.* at 1:33-47 (describing prior art packets), 4:21-31 (describing the extended Wiegand format of Davis), 5:19-29 (describing the use of rolling codes of U.S. Patent App. No. 11/464,912 (EX1012)), 23:35-45 (describing the packet framing of the SIA standard). The SLIP and PPP protocols of RFC 1055 and 1661, respectively, are discussed *supra*, §VI.C.1, along with the packet framing of the SIA Standard. As explained above, both of these protocols and the SIA Standard concern and disclose packet-mode communication. *Id.*

117. Moreover, Davis also teaches the "secure Wiegand mode" aspect of the second mode, when properly construed as the "legacy Wiegand communication protocol with one or more added security features." *See supra* §VIII.A.

118. As an initial note, the '562 patent does not purport to have invented anything relating to the use of rolling codes or other security mechanisms. *See* EX1001, at 14:9 ("There are in the art many rolling code generators."); 15:4-6 ("There are in the art many ways of performing this combination [of providing encrypted messages and a decryption key]. Many of these means are known in the art as stream ciphers."); *see also id.* 4:10-5:29 (describing prior art security mechanisms for Wiegand readers); 4:32-48 (describing EX1014 to Merket as teaching time-stamping messages sent over the Wiegand wires for added security).

119. Davis teaches this element by disclosing that the Wiegand extension enables "enhanced error detection, **encryption**, . . . **and enhanced information regarding the embedded data stream**." EX1006, Abstract.

120. For example, Davis teaches the use of an "extended data field" on the messages from the reader (also described as "an access interface unit," *see* EX1006, at 4:52-57), to the panel. EX1006, 3:9-13. The extended data field can include information relating to whether any physical tampering with the access interface unit has been detected by an external device:

> The access interface unit may also include external status input means for accepting external status data from an external device coupled thereto, and the status information field of the extended data field then will include the external status data. . . . The external device may . . . be adapted to detect physical tampering with the access interface unit.

EX1006, 3:22-31; *see also id.* 4:15-24 ("A tamper and temperature sensing interface 18 is shown in FIG. 3, which allows connection of the reader 10 to external tamper and temperature sensing devices. By using a temperature sensor, temperature data may be transmitted back to the control panel 4 with the extended data field. **Likewise, by using a tamper sensor, an alarm may be sent to the control panel in the event that someone attempts to alter or destroy the reader 10, and such activity is sensed by the tamper sensor. These types of sensors are well known in the art and need not be described in detail herein.**")

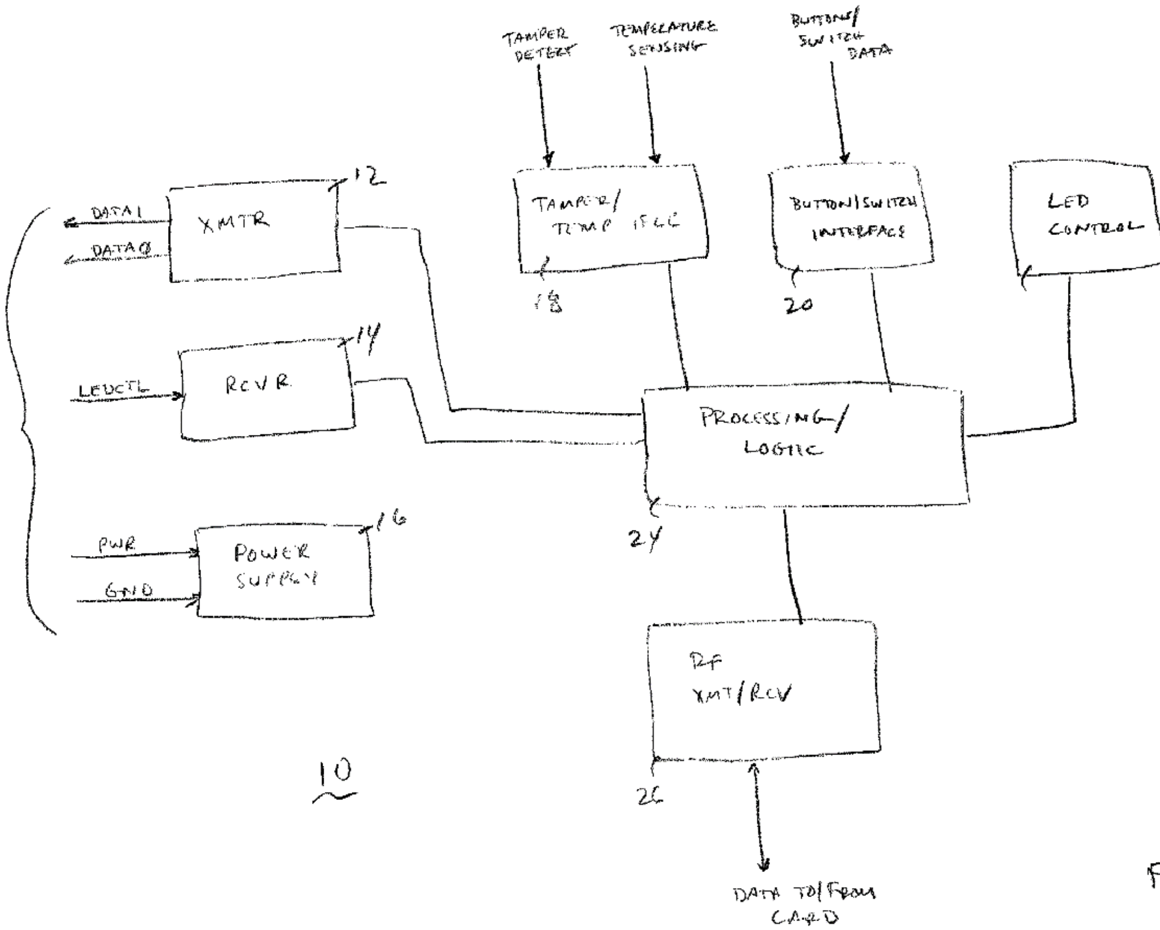



FIG. 3

121. A POSITA would have understood this to be a *secure* Wiegand mode (*i.e.*, the "legacy Wiegand communication protocol with one or more added security features," *see supra* §VIII.A) because Davis teaches the inclusion of data relating to reader security (*i.e.*, physical tampering) in the transmissions from the reader to the panel, thereby enabling more secure Wiegand communication.

**3. Claim 2: "The method of claim 1, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol."**

**4. Claim 3: "The method of claim 2, wherein the unidirectional communication protocol is the Wiegand protocol."**

122. Davis discloses these claims. Specifically, Davis discloses that the reader may communicate with an upstream device utilizing the Wiegand protocol, which is a unidirectional communication protocol. EX1006, 1:32-37 ("One technology in prevalent use for many years is the **[W]iegand** protocol, which utilizes five wires to communicate data and provide power to a dedicated card reader as well known in the art. The five wires are for power, ground, DATA0, DATAl, and LEDCTL."); 1:54-57 ("[T]he **Wiegand** protocol is a **one-way protocol**, since **the reader** can send data to **the panel** but the panel cannot send any data to the reader except to control the door mechanism and a status LED."). And, as noted, Davis's "**Wiegand extension can be turned on or off**, so that if a **panel** does not support the extension, it is not used and **the reader** behaves as an existing prior art device." *Id.* 2:41-43.

**5. Claim 4: "The method of claim 1, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and the upstream device for a predetermined amount of time."**

123. Davis discloses this limitation. As an initial note, the '562 patent does not purport to have invented the use of a limited-duration signal to initiate a

process or command. In fact, the ’562 patent states that the use of a START signal was known in the art before the priority date: “In telecommunications art, the 10 ms signal is called a START signal.” EX1001, 18:31-32. Indeed, START signals were known in the art before the priority date. *See, e.g.*, EX1022, 8:37-40; EX1023, ¶¶[00054], [0063]-[0065], [0076]; EX1024, ¶[0038].

124. The ’562 patent describes altering the control wire by sending “LEDCTL signals, **[adjusted voltage] levels**, and/or communication data” along the LEDCTL wire. EX1001, 18:11. Davis similarly discloses altering the control line signal between the upstream device (panel) and the reader by dropping the signal voltage level low, *i.e.*, adjusting the voltage level of the control line, for a predetermined amount of time. Specifically, Davis teaches altering the control line signal three times within a one second interval, a predetermined amount of time:

> The panel system in the preferred embodiment is able to switch a Wiegand generator from the basic protocol to the extended protocol as follows. Note that this procedure will typically be run when the panel is initialized. **The panel will drop the LEDCTL signal low three times within a one second interval. The Wiegand generator starts an interval timer when the first pulse is received, and then checks to see if it receives two additional pulses within the one-second period from the first pulse.** If it receives exactly three pulses as described, then it sends the Wiegand extension message “Capable of Using the Wiegand Extension”….

EX1006, 5:47-59. Davis discloses that this alteration is for a predetermined amount of time—1 second or less. *Id.*

### 6. Claim 6

#### a. 6[pre]: "A non-transitory computer-readable medium comprising processor-executable instructions, the processor-executable instructions comprising"

125. I understand that "[a] non-transitory computer-readable medium comprising processor-executable instructions, the processor-executable instructions comprising" is the preamble of claim 6. I have been asked to assume that the preamble is limiting. In my opinion, Davis discloses the preamble.

126. Davis discloses the use of non-volatile memory in readers. EX1006, 5:58-63 ("The panel then will send out the 'Use Wiegand Extension' command to the Wiegand generator, and the Wiegand generator sends the 'Command received and executed' message … and sets a flag in **non-volatile memory** to use the Wiegand extension (even if power is lost and subsequently restored)."). A POSITA would have understood a non-volatile memory to be a "non-transitory computer readable medium." Indeed, non-volatile memory was well-understood as being able to store commands for more than a transitory period of time. For example, if a computer shut down, data or instructions in volatile memory would not be preserved, but data or instructions in non-volatile memory would be preserved when the computer powered back up.

127. Davis also discloses processor-executable instructions. As shown in Figure 3 below, Davis discloses a credential reader 10 with processing/logic 24:

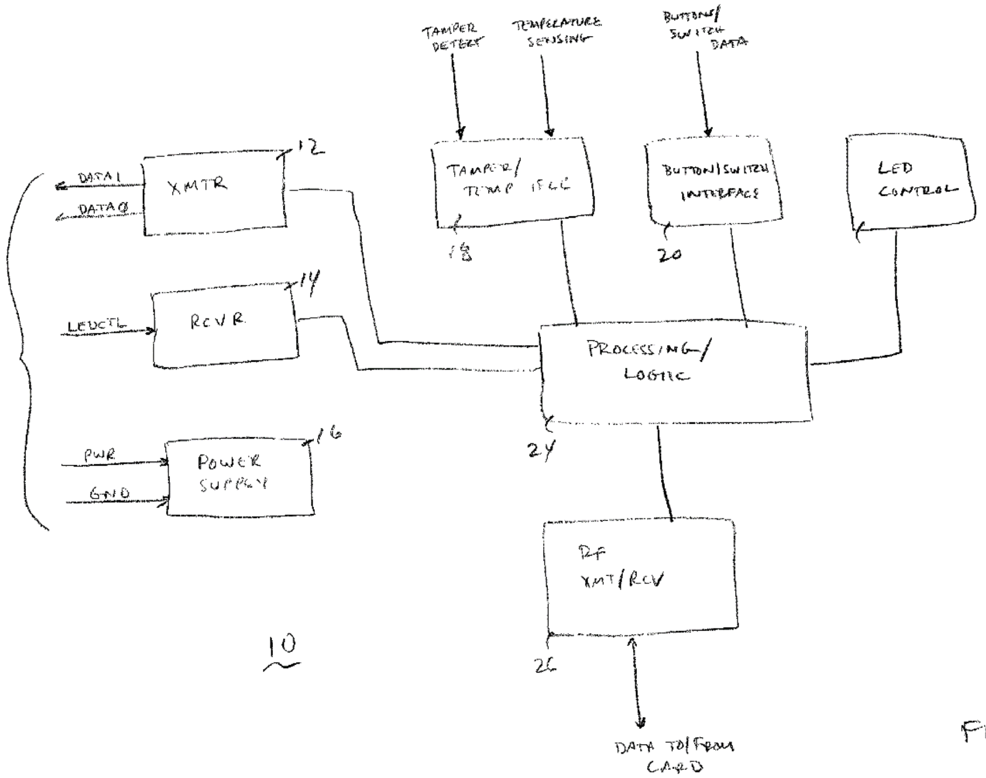



FIG. 3

Davis discloses that the "[p]rocessor 24 is used to read data from the external sources, formulate data to be transferred over the 5-wire interface, and **run all other functions that may be required by the reader 10 of the present invention**. EX1006, 4:45-48.

128. As described below, a POSITA would have understood Davis to disclose the following processor-executable instructions to be housed in the non-volatile memory of Davis's reader.

### b. 6[A]: "instructions configured to cause a credential reader to operated [*sic*] in a first mode of operation;"

129. As described in Claim 1[A], *supra* §IX.A.2.b, Davis discloses operating in a first mode of operation. And as described in Claim 1[A], Davis discloses that "the DATA1, DATA0, and LEDCTL," are connected to "[t]he transmitter 12 and receiver 14," which are in turn connected to processing/logic 24, as shown in Figure 3:

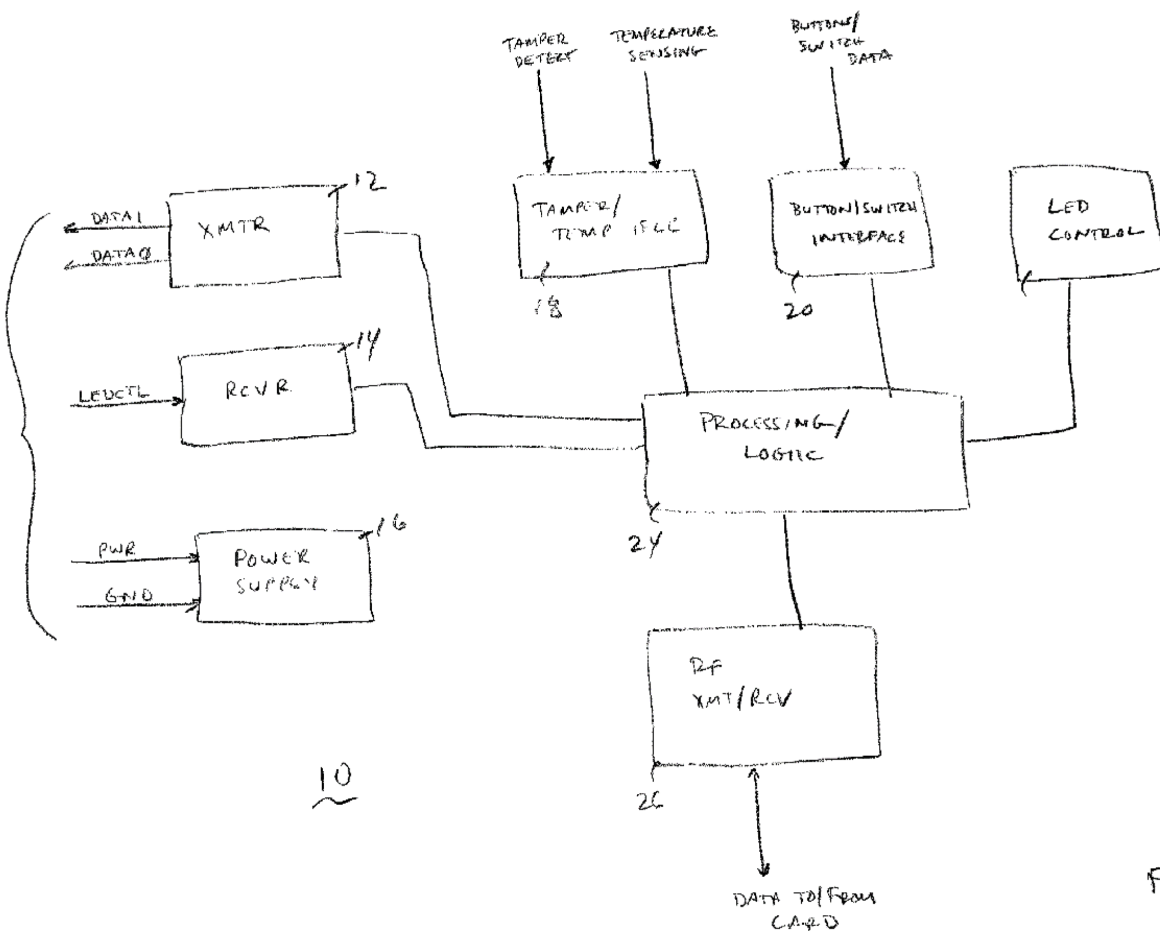


FIG. 3

*See id.*; EX1006, 4:9-14, FIG. 3. The "[p]rocessor 24 is used to read data from the external sources, formulate data to be transferred over the 5-wire interface, and run all other functions that may be required by the reader 10 of the present invention."

EX1006, 4:45-48. Indeed, in order for the processor "to read data from the external sources, formulate data to be transferred over the 5-wire interface, and run all other functions that may be required by the reader 10 of the present invention" (EX1006, 4:45-48), the processor must run instructions on how to read data from external sources, format data to be transferred, and run other functions.

130. Davis teaches that "[t]he Wiegand extension can be turned on or off, so that if a panel does not support the extension, it is not used and the reader behaves as an existing prior art device." EX1006, 2:41-43. A POSITA would have understood that the reader "behav[ing] as an existing prior art device" describes the reader having processor-executable instructions stored in the non-volatile memory that enable the reader to operate as a prior art device. Indeed, there is no other way for the reader to behave as a prior art device except through processor-executable instructions stored in the non-volatile memory of the reader. For example, Davis describes the indication as to which mode to use (the standard Wiegand protocol or the Wiegand extension) as being controlled by "a flag in non-volatile memory." EX1006, 5:58-64. A POSITA would have understood that Davis thus teaches that the processor-implemented instructions required to operate in either mode are located in the non-volatile memory.

131. Moreover, in order for the processor to operate in the first mode (the standard Wiegand mode), the processor would have to be connected to the non-

volatile memory that contains instructions as to how to perform the functions necessary to operate in the first mode. Davis further discloses that the reader's non-volatile memory allows instructions to continue to be stored "even if power is lost and subsequently restored," thus indicating that the instructions are stored in a non-transitory computer-readable medium. *See* 5:58-64.

132. Moreover, the operation of the prior art Wiegand reader was well known in the prior art before the priority date. *See supra* §§VI.B-C.

#### c. 6[B]: "instructions configured to receive a message at the reader, the message being received from an upstream device;"

133. Davis discloses this limitation. As noted, Davis teaches that:

> The panel will drop the LEDCTL signal low three times within a one-second interval. The Wiegand generator starts an interval timer when the first pulse is received, and then checks to see if it receives two additional pulses within the one-second period from the first pulse. If [the Wiegand generator] receives exactly three pulses as described, then it sends the Wiegand extension message "Capable of Using the Wiegand Extension" …. The panel then will send out the "Use Wiegand Extension" command to the Wiegand generator, and the Wiegand generator sends the "Command received and executed" … and sets a flag in non-volatile memory to use the Wiegand extension.

EX1006, 5:50-62.

134. By teaching that the Wiegand generator "receives" and executes commands sent by the panel, a POSITA would have understood this to teach "instructions configured to receive a message at the reader, the message being received from an upstream device" which are implemented on a processor. A POSITA would have understood the term "command" to refer to a processor-implemented instruction. *See* EX1021, at 4 (McGraw-Hill Definition of "command" as "A signal that initiates a predetermined type of computer operation that is defined by an instruction."). Moreover, Davis teaches that the processor is used "to read data from the external sources, formulate data to be transferred over the 5-wire interface, and run all other functions that may be required by the reader 10 of the present invention" (EX1006, 4:45-48), which would include the receipt and interpretation of commands.

135. A POSITA would have understood from this disclosure that these processor-implemented commands would have been stored in Davis's non-volatile memory, which is a type of non-transitory memory (*see* Claim 6[pre], §IX.A.6.a, *supra*). For example, as noted above, Davis teaches the changing of modes through the setting of "a flag in non-volatile memory to use the Wiegand extension (even if power is lost and subsequently restored)." EX1006, 5:58-64. A POSITA would have understood that at a non-volatile memory is thus involved in the mode-changing process Davis describes at 5:47-64, and further, that the commands that

permit Davis's reader to receive and execute messages and commands from the panel (that teach this limitation) are stored in Davis's non-volatile memory. Indeed, it was well-understood in the art that commands may be stored in a non-volatile memory.

136. Moreover, if the commands were not stored in the non-volatile memory, Davis's reader would not be able to operate as described. Indeed, it would have been well understood by the POSITA that if the instructions to receive a message from the panel were only stored transiently, then the Wiegand generator (reader) would not be able to interpret any messages it receives from the panel because the reader would not be able to pull up the instructions as to how to interpret each message or command from the panel, if a message arrives after the transient storage of the instruction has passed. Further, in the event that "power is lost and subsequently restored" (*id.* 5:58-64) to the reader, the reader would not be able to subsequently turn the Wiegand extension on or off, as described at *id.* 2:41-43, through the mode-change protocol described at 5:47-64 if the instructions were only stored transiently. This is because the processor-implemented instructions that enable the reader to interpret the signal received from the panel would have been lost with the loss of power. Thus, a POSITA would have readily understood that Davis's teaches this limitation, and that the "instructions configured to receive a

message at the reader, the message being received from an upstream device" are stored in Davis's non-volatile (*i.e.*, non-transitory) memory.

#### d. 6[C]: "instructions configured to determine that the message was transmitted by the upstream device; and"

137. Likewise, as described above, the reader of Davis determines that the message was sent by an upstream device. *See* Claim 1[C], *supra* §IX.2.d. A POSITA would have understood Davis's disclosures that teach claim 1[C] to be performed by instructions executed by the processor. *See id.*; EX1006, 4:45-48 ("Processor 24 is used to read data from the external sources, formulate data to be transferred over the 5-wire interface, and **run all other functions that may be required by the reader 10 of the present invention**.").

138. Moreover, in order for the processor to perform the determining function of this limitation, it would have to be connected to a memory that contains instructions as to how to perform this functions. Indeed, in order for the processor 24 "to read data from the external sources, formulate data to be transferred over the 5-wire interface, and run all other functions that may be required by the reader 10 of the present invention" (EX1006, 4:45-48), such as receive messages and determine their origin, the processor must be connected to a memory, which stores instructions on how to analyze messages from the panel.

139. A POSITA would have understood from this disclosure that these processor-implemented commands would have been stored in Davis's non-volatile memory, which is a type of non-transitory memory (*see* Claim 6[pre] §IX.A.6.a, *supra*). For example, Davis discloses that its reader contains a non-volatile memory, or a memory that does not erase its commands if power to the device is lost. *See* 5:58-64 ("The panel then will send out the 'Use Wiegand Extension' command to the Wiegand generator, and the Wiegand generator sends the 'Command received and executed' [message to a group of readers] and sets a flag in **non-volatile memory** to use the Wiegand extension (even if power is lost and subsequently restored)."). A POSITA would have understood that Davis's non-volatile memory would store commands related to operation in legacy Wiegand mode or the Wiegand extension, including instructions to determine the origin of any message received by a reader. Indeed, it was well-understood in the art that commands related to operating modes and receiving messages may be stored in a non-volatile memory so that such commands are not lost if power is lost.

140. Indeed, if the commands were not stored in the non-volatile memory, Davis's reader would not be able to operate as described. It was well understood by the POSITA that if the instructions to determine whether the message was transmitted by the panel were only stored transiently, then the Wiegand generator (reader) would not be able to interpret any messages it receives from the panel

because the reader would not be able to pull up the instructions as to how to determine that a message came from the panel, if a message arrives after the transient storage of the instruction is lost. Further, in the event that "power is lost and subsequently restored" (*id.* 5:58-64) to the reader, the reader would not be able to subsequently turn the Wiegand extension on or off, as described at *id.* 2:41-43, through the mode-change protocol described at 5:47-64 if the instructions were only stored transiently. This is because the processor-implemented instructions that enable the reader to determine that the message received came from a panel and that the message from the panel was instructing the reader to change modes would have been lost with the loss of power. Thus, a POSITA would have readily understood that Davis's teaches this limitation, and that the "instructions configured to determine that the message was transmitted by the upstream device" are stored in Davis's non-volatile (*i.e.*, non-transitory) memory.

**e. 6[D]: "instructions configured to transition the credential reader from the first mode of operation to a second mode of operation, wherein the transition from the first mode of operation to the second mode of operation occurs based on determining that the message was transmitted by the upstream device, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode."**

141. Davis discloses this limitation. As described above in Claim 1[D], *supra* §IX.A.2.e, Davis discloses "transition[ing] the credential reader from the

first mode of operation to a second mode of operation" by the following process: (1) "[t]he panel will drop the LEDCTL signal low three times within a one-second interval"; (2) the reader sends "the Wiegand extension message 'Capable of Using the Wiegand Extension'"; (3) the panel "will send out the 'Use Wiegand Extension' command to the Wiegand generator; (4) the Wiegand generator sends the "Command received and executed" message; and (5) the Wiegand generator "sets a flag in non-volatile memory to use the Wiegand extension." EX1006, 5:47-62. A POSITA would have understood this transition to have been achieved through appropriately configured instructions. Indeed, in the context of programming, a command refers to "[a] signal that initiates a predetermined type of computer operation that is defined by an instruction" (EX1021, at 4)—an instruction that would be carried out by the processor of Davis. *See* EX1006, 4:45-48.

142. A POSITA would have understood that these processor-implemented instructions for transitioning modes are stored in the non-volatile memory of Davis. As noted, Davis explicitly teaches setting a "flag in non-volatile memory" relating to which mode to use in response to a command from the panel. EX1006, 5:58-64. EX1006, 5:58-62. A POSITA would have understood that at a non-volatile memory is thus involved in the mode-changing process Davis describes at 5:47-64, and further, that the instructions that permit Davis's reader to "to

transition the credential reader from the first mode of operation to a second mode of operation" are stored in Davis's non-volatile memory. Indeed, it was well-understood that commands may be stored in a non-volatile memory.

143. Indeed, the reader of Davis changing to the Wiegand extension mode by setting "a flag in non-volatile memory" describes the same mode change operation as that which is described in the '562 patent. The '562 patent also states that the mode is set by "set[ing] a flag that indicates the change to the secure Wiegand mode has been executed." EX1001, 18:45-49. The purpose of setting a flag is also the same. By setting a flag, if the reader loses power and powers back up, the flag directing the reader to use the second mode will remain set. *Compare* EX1001, 18:49-57 ("In accordance with at least some embodiments of the present invention, when the reader powers up, the reader stays in this mode so that a power cycle, for example, cannot be used to attack the reader and send it back to an unsecured mode of operation. While there may be some secure way of causing a reader to go back to its initial mode of operation (i.e., resetting the flag), it should not be due to a power down of the reader, which could be easily exploited by an attacker to compromise the system.") *with* EX1006, 5:58-64 ("The panel then will send out the 'Use Wiegand Extension' command to the Wiegand generator, and the Wiegand generator sends the 'Command received and executed' message … and **sets a flag in non-volatile memory to use the Wiegand extension (even if power**

**is lost and subsequently restored**.)"). Because of this purpose—maintaining the mode if power is lost—a POSITA would have understood that just as with the '562 patent, the flag of Davis is also stored in a non-transitory memory because the Davis's non-volatile memory, by definition, does not lose the information and settings saved therein if power to the memory is lost.

144. Moreover, in order for the processor to operate and to transition modes, it would have to be connected to a memory that contains instructions as to how to perform this function. Indeed, in order for the processor 24 "to read data from the external sources, formulate data to be transferred over the 5-wire interface, and run all other functions that may be required by the reader 10 of the present invention" (EX1006, 4:45-48), such as transition between modes, the processor must be connected to a memory, which stores instructions on how to read data from external sources, format data to be transferred, and run other functions. If the commands were not stored in the non-volatile memory, Davis's reader would not be able to operate as described. Indeed, it would have been well understood by the POSITA that if the instructions "to transition the credential reader from the first mode of operation to a second mode of operation" were only stored transiently, then the Wiegand generator (reader) would not be able to transition modes because the reader would not be able to recall the instructions as to how to "to transition the credential reader from the first mode of operation to a

second mode of operation," if a message arrives after the transient storage of the instruction has passed. Thus, a POSITA would have readily understood that Davis's teaches this limitation, and that the "instructions configured to receive a message at the reader, the message being received from an upstream device" are stored in Davis's non-volatile (*i.e.*, non-transitory) memory.

145. And as described above, Davis also teaches transitioning modes "based on determining that the message was transmitted by the upstream device." *See* Claims 1[C], [D] and 6[C], *supra* §§IX.A.2.d, e, IX.A.6.d.

146. As described in Claim 1[D], *supra* §IX.A.2.e, Davis discloses that "the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode."

**7. Claim 7: "The non-transitory computer-readable medium of claim 6, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol."**

**8. Claim 8: "The non-transitory computer-readable medium of claim 7, wherein the unidirectional communication protocol is the Wiegand protocol."**

147. As explained above with respect to claims 2 and 3, Davis discloses that "the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol" and that "the unidirectional communication protocol is the Wiegand protocol." *See supra* §§IX.A.3-4.

### 9. Claim 9: "The non-transitory computer-readable medium of claim 6, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time."

148. As explained above with respect to claim 4, Davis discloses that "the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and the upstream device for a predetermined amount of time." *See supra* §IX.A.5.

### 10. Claim 11

#### a. 11[pre]: "A credential reader comprising:"

149. I understand that "[a] credential reader comprising" is the preamble of claim 11. I have been asked to assume that the preamble is limiting. In my opinion, Davis discloses the preamble.

150. Davis discloses the preamble. Davis discloses an "access control group 6" that "contains up to three access interface units (card readers)." EX1006, 3:58-60. Each reader maybe configured to read "an access control card, a data transponder, [or] a data-carrying key fob" (*id.* 3:2-5)—all well understood and conventional types of credentials. *See* EX1028, 1:21-35. The credential reader of Davis comprises the following claimed features.

#### b. 11[A]: "at least one of a microprocessor and firmware that enable the reader to operate in a first mode of operation,"

151. As explained above with respect to Claim 1[A], Davis discloses "operating a credential reader in a first mode of operation, the credential reader comprising at least one of a microprocessor and firmware that enable the credential reader to operate in the first mode of operation." *See supra* §IX.A.2.b.

#### c. 11[B]: "receive a message from an upstream device,"

152. As explained above with respect to Claim 1[B], Davis discloses "receiving, at a communication interface of the credential reader, a message from an upstream device." *See supra* §IX.A.2.c.

#### d. 11[C]: "determine that the message was transmitted by the upstream device, and"

153. As explained above with respect to Claim 1[C], Davis discloses "determining, by the credential reader, that the message was transmitted by the upstream device." *See supra* §IX.A.2.d.

**e. 11[D]: "in response thereto, transition the credential reader from the first mode of operation to a second mode of operation, wherein the transition from the first mode of operation to the second mode of operation occurs based on determining that the message was transmitted by the upstream device, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode."**

154. As explained above with respect to Claim 1[D], Davis discloses "based on determining that the message was transmitted by the upstream device, transitioning the credential reader from the first mode of operation to a second mode of operation, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode." *See supra* §IX.A.2.e.

**11. Claim 12: "The credential reader of claim 11, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol, and wherein the unidirectional communication protocol is the Wiegand protocol."**

155. As explained above with respect to claims 2 and 3, Davis discloses that "the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol" and that "the unidirectional communication protocol is the Wiegand protocol." *See supra* §§IX.A.3-4.

### 12. Claim 13: "The credential reader of claim 11, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time."

156. As explained above with respect to claim 4, Davis discloses that "the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and the upstream device for a predetermined amount of time." *See supra* §IX.A.5. The method step described with respect to Claim 4, teaches this limitation because it is implemented on a credential reader. *See id.*

## B. Ground 2: Claims 5, 10, and 14 Are Obvious over Davis

### 1. Claim 5: "The method of claim 4, wherein the predetermined amount of time is less than 10 ms."

157. As described above in Ground 1, Davis discloses the limitations of claim 4. *Supra*, §IX.A. Davis also renders this claim obvious. The use of a 10 ms or less predetermined amount of time as an alteration of the control line signal between the reader and upstream device, such as a panel, would have been an obvious design choice for at least the reasons outlined below.

158. As noted, the '562 patent does not purport to have invented the use of a limited-duration start signal to initiate a process or command. *See* EX1001, 18:31-32 ("In telecommunications art, the 10 ms signal is called a START signal."); Claim 4, *supra* §IX.A.5. Indeed, START signals were known in the art before the priority date. *See, e.g.*, EX1022, 8:37-40; EX1023, ¶¶[00054], [0063]-[0065], [0076]; EX1024, ¶[0038].

159. Davis also teaches a form of a start signal:

> The panel system in the preferred embodiment is able to switch a Wiegand generator from the basic protocol to the extended protocol as follows…. The panel will drop the LEDCTL signal low three times within a one-second interval. The Wiegand generator starts an interval timer when the first pulse is received, and then checks to see if it receives two additional pulses within the one-second period from the first pulse. If [the Wiegand generator] receives exactly three pulses as described, then it sends the Wiegand extension message "Capable of Using the Wiegand Extension."

EX1006, 5:47-57. In response to this signal, the reader "sets a flag in non-volatile memory to use the Wiegand extension." *Id.* at 5:58-63. A POSITA would have recognized the three-pulses within the one-second interval to be a form of a start signal. This is because the three signals initiate the start of another procedure—the use of the Wiegand extension on the reader of Davis.

160. Davis also teaches that a panel may transmit 8-bit signals to the reader. In particular, Davis teaches that "the panel may send data to a reader using an asynchronous serial data stream via the LEDCTL wire at 1200 baud, 8 data bits, 1 stop bit, no parity. All fields in this instance are one byte long. The first byte of a command is divided into two sub-fields. The first two bits are the address field (00-11), and the last six bits contain the command code (000000-111111)." EX1006, 5:19-25.

161. There are multiple commands the panel of Davis may send to the reader in these 8-bit signals. *See* EX1006, 5:18-64. For example, Davis teaches at least 4 commands from the panel to the reader "are available in the preferred embodiment":

| COMMAND SENT BY PANEL | | WIEGAND GENERATOR RESPONSE |
|---|---|---|
| 00h<br><CRC> | 0 = retransmit last Wiegand data transmission<br><CRC> = 8-bit CRC | Retransmits last Wiegand data message |
| 01h<br><address><br><CRC> | 1 = Return value of selected parameter address<br><address> = 00 thru FF<br><CRC> = 8-bit CRC | Parameter value of desired address is transmitted back via the Wiegand extension |
| 02h<br><address><br><data><br><CRC> | 2 = set value of selected parameter address<br><address> = 00 thru FF<br><data> = 00 thru FF<br><CRC> = 8-bit CRC | Acknowledgement that data was written is transmitted via the Wiegand extension |
| 03h<br><LEDCTL><br><seconds><br><CRC> | 3 = Turn on LED<br><LEDCTL> = simulation of LED control signals<br><# of seconds to keep LED on> <CRC> = 8-bit CRC | Acknowledgement is transmitted via the Wiegand extension |

EX1006, 5:30-46.

162. Davis's teachings of a "1200 baud, 8 data bits, 1 stop bit, no parity" signal describes a 7.5 ms signal, which is obtained by dividing nine bits, the total number of bits in the data stream ("8 data bits, 1 stop bit"), by the baud, which is disclosed by Davis to be 1200. This calculation yields the total length of the data transmission: 6.67 ms of data transmission, 7.5 ms for transmitting the entire

message, including the stop bit. The baud or baud rate is well understood to be the data transfer rate, and describes the number of signal alternations (*e.g.*, pulses or bits of digital information shared) per second. EX1021, at 3 (Definition of "Baud"); *see also* EX1001, 2:30-67.

163. Although Davis teaches that the mode change may be initiated by the panel sending three pulses within one second on the LEDCTL signal line, as described in Claims 1[D] and 4, *supra* §§IX.A.2.e, IX.A.5, it would have been obvious to also use Davis's 8-bit 6.67 ms data signal to effectuate a mode change, as described below.[6] Indeed, as described 8-bit start signals were known in the art. See EX1022, 8:37-40. Additionally, although the following is discussed with reference to the 8-data bit transmission, which is sent in 6.67 ms, including the stop bit Davis describes is at the end of the 8 data bits would have been an obvious design choice and the resulting 9-bit, 7.5 ms transmission would also teach this claim.

---

[6] Furthermore, as the '562 patent recognizes, the prior art literature agreed that a 10 ms activation of an LED would have been subliminal. EX1001, 17:38-18:2 ("[T]he psychophysical literature generally agrees that presentation times below 10 ms may be subliminal or not perceived at all."). This thus provides another reason to use a duration of less than 10 ms.

164. To the extent this modified 6.67 ms signal of Davis contains data, this does not detract from its ability to be used to effectuate a mode change, and indeed this is permissible in the ’562 patent. EX1001, 17:59-61 (“Additionally, data may be sent to the reader in a secure fashion (i.e., through obfuscation with a rolling code) within the 10 ms window”).

165. Using Davis’s 8-bit signal to transition modes would have been a simple design alternative to the one-second mode changing START signal of Davis. Substituting one for the other would be a simple design choice. Indeed, START signals and signals that initiate electronic processes were conventional in the art, as the ’562 patent admits and as multiple attached references confirm. EX1001, 18:31-32 (“In telecommunications art, the 10 ms signal is called a START signal.”); *see* EX1022, 8:37-40; EX1023, ¶¶[00054], [0063]-[0065], [0076]; EX1024, ¶[0038] (“the host computer 202 first transmits a start signal . . . .”).

166. Further, because Davis teaches the use of an 8-bit signal in connection with the sending of commands from the panel to the reader on the LEDCTL wire, as described above, it would have been an obvious extension of this disclosure to also use the 8-bit signal as a START signal through which the panel commands the reader to change modes.

167. A POSITA would have known that it was known to be advantageous to use a shorter-duration signal as a start signal. In particular, by enabling a faster mode change in Davis's reader enables more rapidly changing to the Wiegand extension, which would permit the benefits of the Wiegand extension (bi-directional commands, extended data field that includes external status data from a tamper sensor, and improved error correction) to be enabled more quickly (6.67 ms verses 1 second). Enabling the Wiegand extension and these benefits faster would be advantageous in high-use systems so as to minimize the likelihood that reader-panel transmissions that would benefit from the Wiegand extension are transmitted without the Wiegand extension. Likewise, it would narrow the window during which the tamper sensor is not sending data to the panel. Additionally, changing modes in 6.67 ms, as opposed to 1 second, would minimize any perceived lag in the transition of modes perceived by the user, providing a more optimal user experience.

168. Further, it would also have been advantageous to use Davis's 8 bit start signal to initiate Davis's mode change because doing so would simplify the programming within the reader and the panel. By basing all transmissions to turn on the Wiegand extension on the 8-bit signal, this would eliminate the need for processor-executable instructions to generate the three-pulse-within-a-second (by the panel) and instructions to receive and determine that three pulses were received

within a second (by the reader). Moreover, it would have been obvious to try to implement the mode-changing START signal as an 8-bit signal among the 8-bit signals Davis's panel sends to its reader.

169. It would have been well within the skill of the POSITA to implement an 8-bit command (the two address bits and six-bit command code between 000000 and 111111) to change modes. In order to initiate a change to packet-mode using the 8-bit signals from the upstream device, a POSITA would have been motivated, as a matter of obvious known design choice, to designate a particular string of bits (for example, a string of only 1s or 0s) sent by the panel to the reader to correspond to a start signal. The range of 000000 to 111111 (Davis's 8-bit panel-to-reader transmission, less the leading two address bits) provides 63 discrete possibly commands, only 4 of which are directly described by Davis. *See* EX1006, 5:30-46. Thus, there are 59 possible combinations of 1s and 0s for the POSITA to designate as a mode-change command. A POSITA would also have been able to associate the 8-bit START signal with a processor-executable command in a non-transitory memory, such as Davis's non-volatile memory, such that the reader would transition the mode of the reader in response to the designated START signal. A POSITA would have understood how to program the reader and panel of Davis's system, as programming was well-understood, and the change in Davis's panel and reader's programming would have led to predictable results. *See*

EX1006, 4:64-5:64; EX1022, 8:37-40; EX1007, 12-13; EX1010, ¶¶[0004], [0009]-[0025], [0032], [0045]; EX1012, ¶¶[0040], [0050]-[0057]; EX1017, at 1-6; EX1019, ¶¶[0053]-[0077]; EX1023, ¶¶[00054], [0063]-[0065], [0076]; EX1024, ¶[0038]; EX1025; ¶¶[0019], [0023]-[0039]. Thus, a POSITA would have been able to implement a 10 ms or less start signal.

#### 2. Claim 10: "The non-transitory computer-readable medium of claim 9, wherein the predetermined amount of time is less than 10 ms."

170. As explained above with respect to Claim 5, Davis discloses that "the predetermined amount of time is less than 10 ms." *See supra* §IX.B.1.

#### 3. Claim 14: "The credential reader of claim 13, wherein the predetermined amount of time is less than 10 ms."

171. As explained above with respect to Claim 5, Davis discloses that "the predetermined amount of time is less than 10 ms." *See supra* §IX.B.1.

### C. Ground 3: Claims 5, 10, and 14 Are Obvious over Davis in view of Lastinger

#### 1. Lastinger (EX1022)

172. Lastinger issued on April 18, 2006, from an application that was filed on June 14, 2002. EX1022. Lastinger claims priority to a provisional application filed June 14, 2001. *Id.*

173. Lastinger relates to locational monitoring systems, for example, that "track the location and movement of objects, animals or personnel for maintaining inventory status, providing access to portions of a facility (e.g., unlocking doors for

a particular personnel), directing materials handling equipment, and assisting in discovering the location of objects, animals and personnel." *Id.* at 2:63-3:3.

174. Lastinger teaches that this tracking may be achieved in a "warehouse or other facility housing a large number of articles," *Id*. at 2:63-3:3, 3:24-40. The warehouse or facility "may have a plurality of fixed low frequency transmitters or 'locators' positioned at various locations around the warehouse, each transmitter having a specified zone of transmission. A grid or matrix of such fixed locators may be arranged to have overlapping zones of transmission to increase the accuracy of locating of tagged items. When each locator broadcasts location information (e.g. Locator ID, geographical coordinates), any tags in the respective zone of transmission respond by broad casting their own transmissions. Such tag broadcasts include the location identification information received from the one or more locators that initiated the tag broadcast." *Id.* at 3:24-40.

175. For example, as shown in Figure 1A, "[m]onitor 140 may be any device or combination of devices for receiving location identification broadcast by tag 130. For example, monitor 140 may be an RF receiver receiving wireless transmissions from tag 130 and/or locators 110, 120. Moreover, monitor 140 may also include, or be connected to, a respective processing unit 150 for determining locations based on the received location information." *Id.* at 5:8-14.

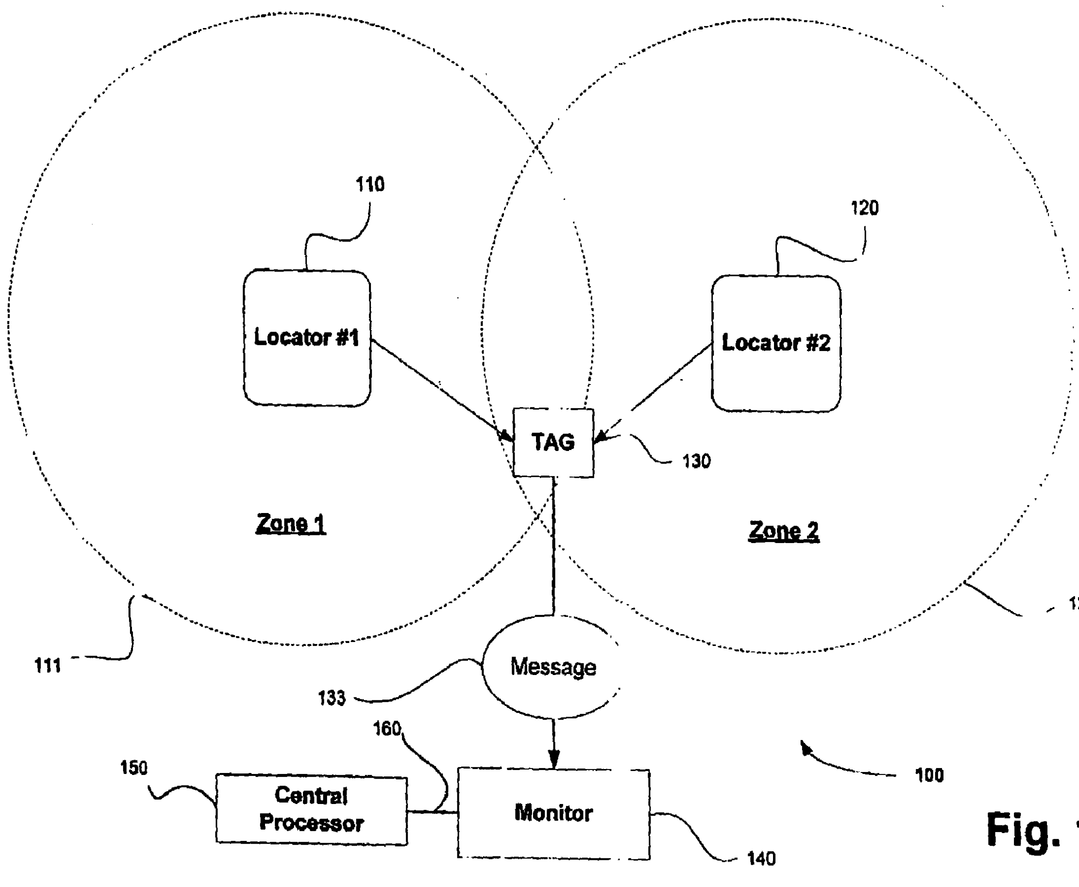



Fig. 1A

*Id.* at Fig. 1A.

176. Figure 3 shows a "functional block diagram of a tag according to various aspects of the present invention."

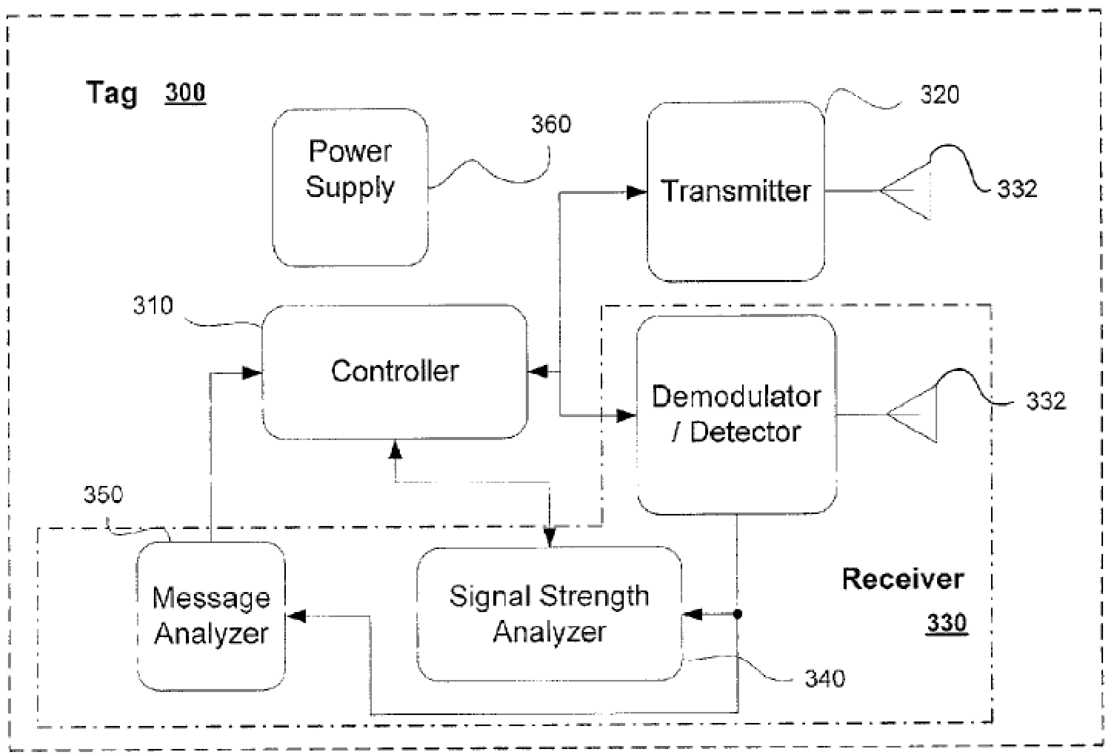



**Fig. 3**

*Id.*, 2:43-44, FIG. 3. Each "[t]ag 300 functions to receive signals having location identification information through receiver 330, optionally, analyze strengths of received signals if more than one signal is received, and broadcast signals including received location identification information, such as a Locator ID or navigational coordinates or the like." *Id.* at 7:4-9.

177. The "[r]eceiver unit 330 [of the tag 300] may be any device or combination of devices for receiving and/or decoding a signal from a tag (e.g., tag 130; FIG. 1). Receiver 330 is preferably capable of receiving a carrier signal in the range of 100 KHZ to 13.56 MHZ (depending on optional chip selection) from a setup unit or a locator unit. The locator unit(s) can operate independently or synchronously under the control of a centralized control unit. Receiver 330 preferably receives a wakeup or start signal of eight bits or more followed by a twenty-four bit word individually or in groups of up to eight words. Receiver 330 optionally operate in sampling mode where receiver 330 turns on and off intermittently. For example, it turns on for 100 usecs every 80 msecs (i.e., 800 to 1). This corresponds to a broadcast from a locator unit having a start pulse length of 100 usecs and a repetition rate of 250 msecs or less." *Id.* at 8:30-45.

178. Lastinger teaches that the transmission mode of each tag may be "changed automatically or initiated by, for example, a received transmission commanding the tag to change." *Id.* at 10:18-22. The modes include a beacon-only output mode or a fast interrogation output mode. *See id.* at 7:28-30, 10:7-12:41.

179. Lastinger is in the same field as the '562 patent because relates to access control RFID systems and communication protocols used in those systems. *Id.* at 1:12-24, 2:63-3:23 ("Systems according to various aspects of the present invention . . . provid[e] access to portions of a facility (e.g., unlocking doors for a

particular personnel….”). Lastinger is pertinent to the problems the ’562 patent purportedly addresses because Lastinger is directed to the start signals known to be used in RFID systems. *Id.* at 8:30-45. Lastinger is therefore analogous art to the ’562 patent.

#### 2. Claim 5: “The method of claim 4, wherein the predetermined amount of time is less than 10 ms.”

180. As described above in Ground 1, Davis discloses the limitations of claim 4. *Supra*, §IX.A.5. To the extent Davis alone does not render this claim obvious in Ground 2, Lastinger provides additional motivation to modify Davis such that Davis in view of Lastinger teaches this claim.

181. Lastinger teaches the use of an 8-bit start signal. Lastinger teaches that a radio frequency receiver on a location monitoring tag “preferably receives a wakeup or **start signal of eight bits or more** followed by a twenty-four bit word individually or in groups of up to eight words.” EX1022, 6:65-7:3; 8:37-40. The 8-bit start signal of Lastinger is transmitted in 100 usecs (microseconds), or 0.1 ms (milliseconds). *Id.* 8:43-45.

182. As noted in Ground 2, claim 5, Davis also teaches a start signal to change modes that comprises the panel sending the reader three pulses within one second. *See supra* §IX.B.1. Also as noted, Davis teaches that a panel may transmit 8-data bit signals to the reader within 6.67 seconds. *See id.*; EX1006, 5:19-25. Thus, Lastinger provides additional motivation, on top of that described in Ground

2 (*supra* §IX.B.1) for Davis to use its 8-bit panel-to-reader message in order to transition modes because Lastinger explicitly recognizes that 8-bit signals may be used as START signals.

183. Furthermore, although Davis teaches that the mode change may be initiated by the panel sending three pulses within one second on the LEDCTL signal line, as described in Claims 1[D] and 4, *supra* §§IX.A.2.e, IX.A.5, it would have been obvious to also combine Davis's 8-bit data signal with Lastinger's 8-bit 100 usec signal to effectuate a mode change by transmitting Davis's 8-bit signal in 100 usec. This obvious modification to Davis would thereby teach this claim.

184. In addition to providing the advantages of a shorter start signal discussed in in §IX.B.1, *supra*, this combination would provide for even faster mode change, thereby providing even faster activation of the Wiegand extension, narrowing the window in which the tamper sensor is not transmitting to the reader, and further minimizing any perceived system lag.

185. A POSITA would have been inclined to consider the transmission protocol of Lastinger in conjunction with the transmission protocol of Davis in contemplating the design of data packets to use over the Wiegand interface because both Lastinger and Davis relate to transmission of data in RFID systems. Indeed, as explained above, both Lastinger and Davis teach design choices for start signals, and the use of either to initiate a procedure in a credential reader would

have been obvious. The 8-bit START signal of Lastinger is a simple design alternative to the three-pulses-within-a-second START signal of Davis. Substituting one for the other would be a simple design choice. Indeed, START signals and signals that initiate electronic processes were conventional in the art, as the ’562 patent admits and as multiple attached references confirm. EX1001, 18:31-32 (“In telecommunications art, the 10 ms signal is called a START signal.”); *see* EX1022, 8:37-40; EX1023, ¶¶[00054], [0063]-[0065], [0076]; EX1024, ¶[0038] (“the host computer [] first transmits a start signal . . . .”).

186. A POSITA would have been motivated to look to Lastinger to improve Davis’s functionality. I note that both Davis and Lastinger relate to radio frequency identification systems and data transmission protocols and are both classified under “H04.”

187. A POSITA would have been motivated to combine Davis with Lastinger. For example, both Davis and Lastinger relate to sending commands in radio frequency identification systems, so a POSITA considering the data transmission protocol described in Davis would have been motivated to consider the solutions described in Lastinger for details as to methods for implementing 8-bit START signal commands in RFID systems.

188. It would have been within the skill of a POSITA to implement this change. As described above, the designation of the 8-bit command to implement a

mode change would have been trivial. *See supra*, §IX.B.1. Furthermore, a POSITA would have been able to adjust the baud rate so as to transmit Davis's 8-bit start signal within the 100 usec of Lastinger through a processor-implemented instruction.

189. Thus, Lastinger would have been a natural place for a POSITA to look when searching for further details on how to design or improve data transmission protocols in a radio frequency identification system.

#### 3. Claim 10: "The non-transitory computer-readable medium of claim 9, wherein the predetermined amount of time is less than 10 ms."

190. As explained above with respect to Claim 5, Davis in view of Lastinger teach that "the predetermined amount of time is less than 10 ms." *See supra* §IX.C.2.

#### 4. Claim 14: "The credential reader of claim 13, wherein the predetermined amount of time is less than 10 ms."

191. As explained above with respect to Claim 5, Davis in view of Lastinger teach that "the predetermined amount of time is less than 10 ms." *See supra* §IX.C.2.

* * *

192. I declare that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

193. I declare under penalty of perjury that the foregoing is true and correct.

Dated: June 9, 2023

Emmanouil M. Tentzeris, Ph.D.

## X. CLAIM LISTING

The following claim listing assigns element labels (*e.g.*, 1[A], 1[B], etc.) to certain claims for clarity.

| Claim 1 |
| --- |
| **1[pre]** A communication method, comprising: |
| **1[A]** operating a credential reader in a first mode of operation, the credential reader comprising at least one of a microprocessor and firmware that enable the credential reader to operate in the first mode of operation; |
| **1[B]** receiving, at a communication interface of the credential reader, a message from an upstream device; |
| **1[C]** determining, by the credential reader, that the message was transmitted by the upstream device; and |
| **1[D]** based on determining that the message was transmitted by the upstream device, transitioning the credential reader from the first mode of operation to a second mode of operation, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode. |
| **Claim 2** |
| **2.** The method of claim 1, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol. |
| **Claim 3** |
| **3.** The method of claim 2, wherein the unidirectional communication protocol is the Wiegand protocol. |
| **Claim 4** |
| **4.** The method of claim 1, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and the upstream device for a predetermined amount of time. |
| **Claim 5** |
| **5.** The method of claim 4, wherein the predetermined amount of time is less than 10 ms. |
| **Claim 6** |
| **6[pre]** A non-transitory computer-readable medium comprising processor-executable instructions, the processor-executable instructions comprising: |
| **6[A]** instructions configured to cause a credential reader to operated [*sic*] in a first mode of operation; |

| |
|---|
| **6[B]** instructions configured to receive a message at the reader, the message being received from an upstream device; |
| **6[C]** instructions configured to determine that the message was transmitted by the upstream device; and |
| **6[D]** instructions configured to transition the credential reader from the first mode of operation to a second mode of operation, wherein the transition from the first mode of operation to the second mode of operation occurs based on determining that the message was transmitted by the upstream device, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode. |
| **Claim 7** |
| **7.** The non-transitory computer-readable medium of claim 6, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol. |
| **Claim 8** |
| **8.** The non-transitory computer-readable medium of claim 7, wherein the unidirectional communication protocol is the Wiegand protocol. |
| **Claim 9** |
| **9.** The non-transitory computer-readable medium of claim 6, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time. |
| **Claim 10** |
| **10.** The non-transitory computer-readable medium of claim 9, wherein the predetermined amount of time is less than 10 ms. |
| **Claim 11** |
| **11[pre]** A credential reader comprising: |
| **11[A]** at least one of a microprocessor and firmware that enable the reader to operate in a first mode of operation, |
| **11[B]** receive a message from an upstream device, |
| **11[C]** determine that the message was transmitted by the upstream device, and |
| **11[D]** in response thereto, transition the credential reader from the first mode of operation to a second mode of operation, wherein the transition from the first mode of operation to the second mode of operation occurs based on determining that the message was transmitted by the upstream device, wherein the first mode comprises a non-secure Wiegand mode and wherein the second mode comprises at least one of a secure Wiegand mode and a packet-mode. |
| **Claim 12** |

| |
|---|
| **12.** The credential reader of claim 11, wherein the credential reader is in communication with an upstream device utilizing a unidirectional communication protocol, and wherein the unidirectional communication protocol is the Wiegand protocol. |
| **Claim 13** |
| **13.** The credential reader of claim 11, wherein the message transmitted by the upstream device comprises an alteration of a control line signal between the reader and upstream device for a predetermined amount of time. |
| **Claim 14** |
| **14.** The credential reader of claim 13, wherein the predetermined amount of time is less than 10 ms |