Biometrics in Physical Access Control

Issues, Status and Trends – White Paper

Authored and Presented by:
Bill Spence, Recognition Systems, Inc.
SIA Biometrics Industry Group Vice-Chair
&
SIA Biometrics Industry Group

Biometrics is a process of identifying a person by their unique and measurable human characteristics. A person's biometric characteristic can be the size and shape of a hand, the ridge and valley pattern of a fingerprint, the frequency of voice or iris characteristics of the eye. No longer are these devices found only in James Bond movies and Star Trek reruns. They are used on the front door of thousands of businesses around the world. Modern biometrics actually got their start in access control applications as far back as the mid 1970s. The early installations were typically very high security in nature, due primarily to the high cost of biometric devices. In recent years, the advent of inexpensive microprocessors and advanced imaging electronics have dramatically reduced the cost and increased the accuracy of biometric devices. More advanced technologies coupled with affordable components and the demand for high security have allowed biometrics to become a common component in the commercial access control landscape. Today, thousands of businesses use biometrics.

This paper will examine how biometrics are integrated into access control applications and the key issues to be considered when using a biometric device.

The Benefits of Biometrics in Access Control

The goal of any access control system is to grant access to authorized people into specific areas. Only with the use of a biometric can this goal be achieved. A card based access system will grant access to whoever is in possession of a registered card. Systems using PINs (personal identification numbers) require that an individual only know a specific number to gain entry. Who actually enters the code can not be determined. Biometric devices authenticate a person by their unique biometric characteristic, whether it is their hand, eye, fingerprint or voice.

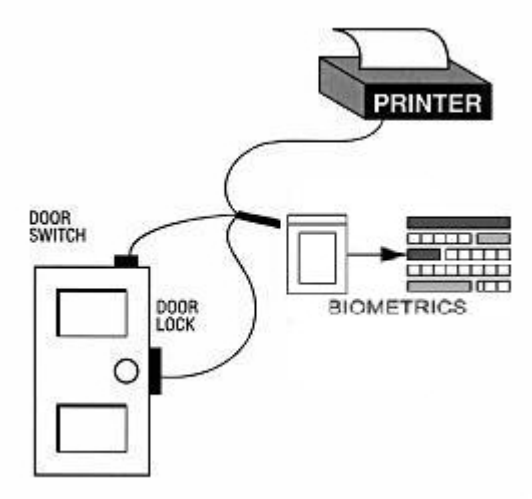
Biometrics can either eliminate the need for tokens or both can be layered to increase security. Cards, a popular token in access control, have dropped dramatically in price within recent years. The true benefit of eliminating them is realized through a reduced loss and increased accountability. The facility reduces loss in the cost of lost or stolen cards and in goods or information that is being protected. The accountability of every person authorized for access is also a very important factor. As card only systems are eliminated the accountability and activity of people in restricted areas is easier to pinpoint.

Integration

The primary function of a biometric device is to verify or identify registered people on a system. Access control requires the ability to authenticate a person and grant (or deny) access based on time restrictions. Door alarms are also monitored. There are several ways biometrics can accomplish these tasks.

Standalone Systems

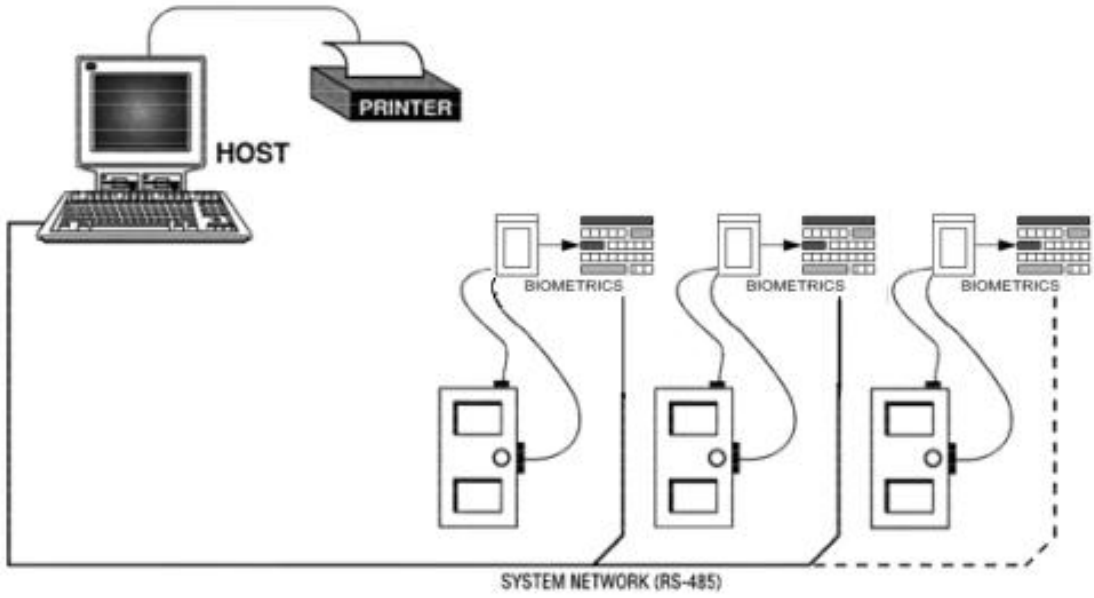
Standalone systems are able to authenticate and actuate a door locking mechanism without a need by external means, information about a registered user. Many biometric systems are available in a standalone type of configuration. These devices are not only a biometric, but also a complete door controller for a single door. Users are enrolled at the unit and their biometric template is stored locally for subsequent comparison. The actual comparison is accomplished within the unit and a lock output is energized depending on the outcome. Input points are available to monitor the door switch for "door open too long" and "door forced open" conditions. Outputs are provided to signal a bell or alarm panel if an alarm condition is detected by the system. An audit trail, if required, is available by connecting a printer to the unit or downloading the information to a personal computer (PC). All administration including enrollments, deletions and designating time restrictions are programmed through the integrated keypad. The number of users and audit trail entries is limited by the available memory and varies among each manufacturer.



Example of a Standalone Configuration

Networked Systems

Many access control applications have a need to control more than one door. While multiple standalone units could be deployed it would not be efficient. A network of biometric devices is more practical. By networking the systems and a computer together there are several advantages to the system administrator. The most obvious advantage is a centralized monitoring of the system. Alarm conditions and activity for all the doors in the system are reported back to the PC. All transactions are stored on the computer's disk drive and can be recalled for a variety of user customized reports. Networked systems also provide for a centralized template management. This process allows a user to enroll at a single location and have their template uploaded to other locations depending on access rights. A networked system can also provide authentication at the host PC where templates are extracted at any location and final authentication is performed at the PC to include access rights. Administration of a user record such as deletion of a user or changes in their access profile need only be entered at the PC. The user template and other information are sent to individual readers at each door. The connection between units is typically accomplished via RS485/422/232. Biometric systems today also have the capability to communicate by TCP/IP.



Example of a Network Configuration

Third Party System Integration

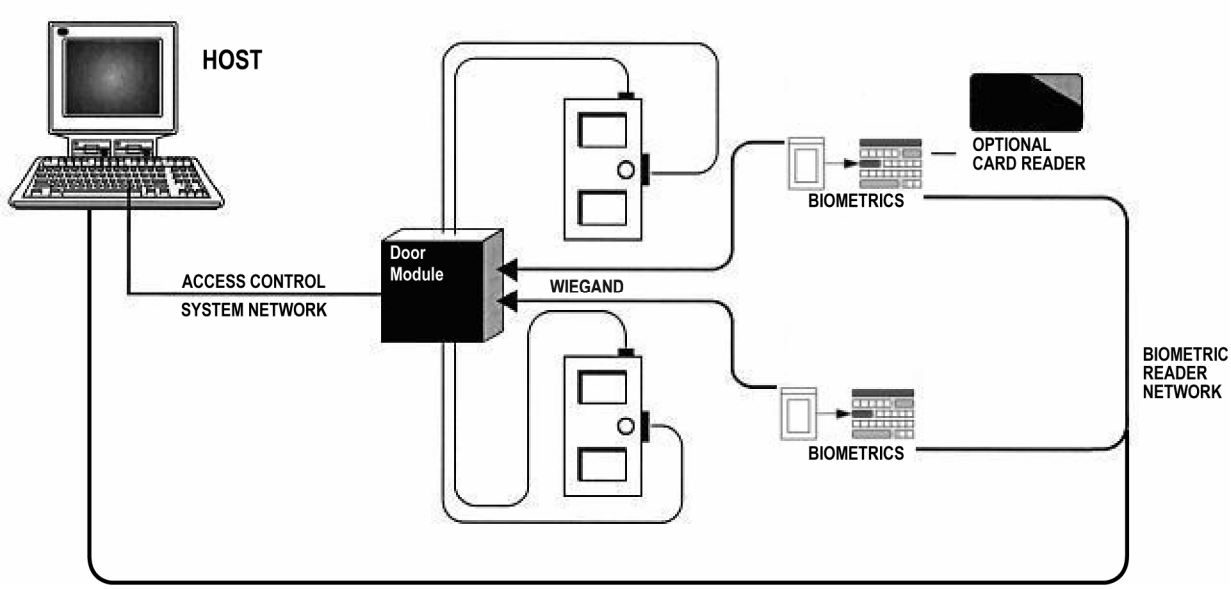
Wiegand Interface

Biometric manufacturers offer a variety of different methods to integrate into conventional access control systems. In the most common integration approach, the biometric device emulates a standard Wiegand card reader and simply outputs the the ID number of a biometrically *verified* user. The card reader output ports of the biometric device are connected to the panel's card reader input ports. This method is very effective when interfacing to existing Wiegand panel systems in the field. The wiring is identical to the card reader's wiring.

If and only if the person is authenticated by biometric, the biometric device outputs the ID number of the individual. If the user is not verified, no ID number is sent. The format and timing of the output is consistent with the card technology used by the Wiegand panel systems. Other formats may be emulated by the biometric system to operate with other type of access control panels. Once an ID number reaches the panel, it is handled as if it came from a card reader. The determination for granting access is made by the access control panel. Door control and monitoring are also handled by the access control panel.

As an alternative (or addition) to a keypad, biometrics have built in options for card readers or have an external input capability. At the biometric device, the user presents a card that contains an ID number. Upon recognizing a valid ID from the card, the biometric device will verify the user. If verified, the card data is passed to the panel for an access decision. Many different types of card technologies are supported by biometric manufacturers including proximity, magnetic stripe, bar code and, increasingly, smart cards.

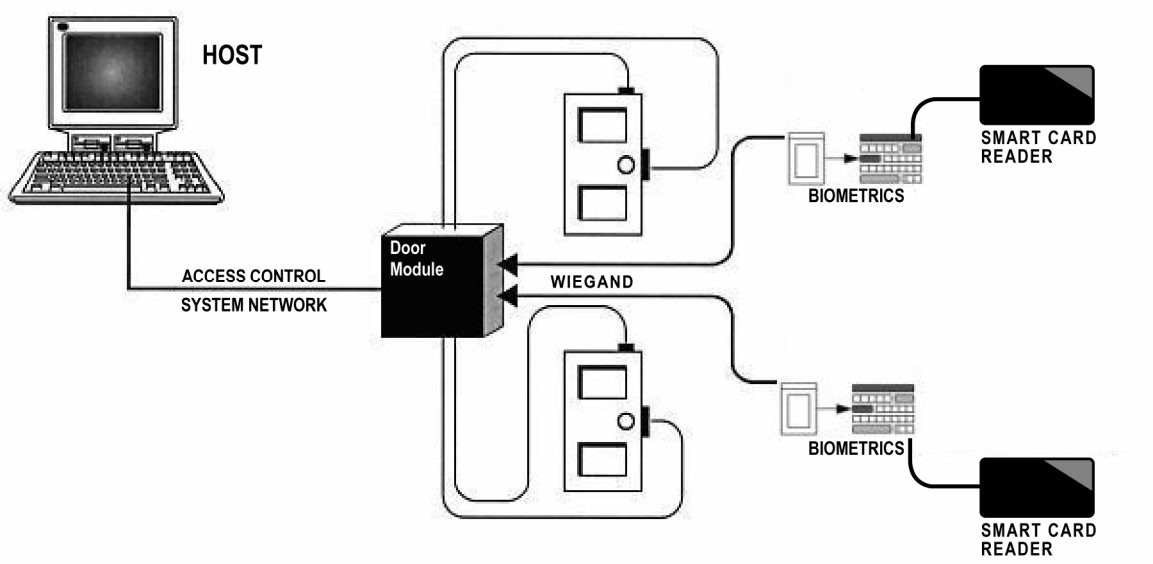
In most card reader emulation systems, template management is not handled by the access control panel. Template management can be an issue as the amount of biometric users and doors grows. In some biometrics, it is possible to link the biometric units together and let them handle the template management. This network is separate from the access control system but does allow users to enroll at a single location and have their template information distributed to other readers.



Example of Wiegand Integration

Smart Cards

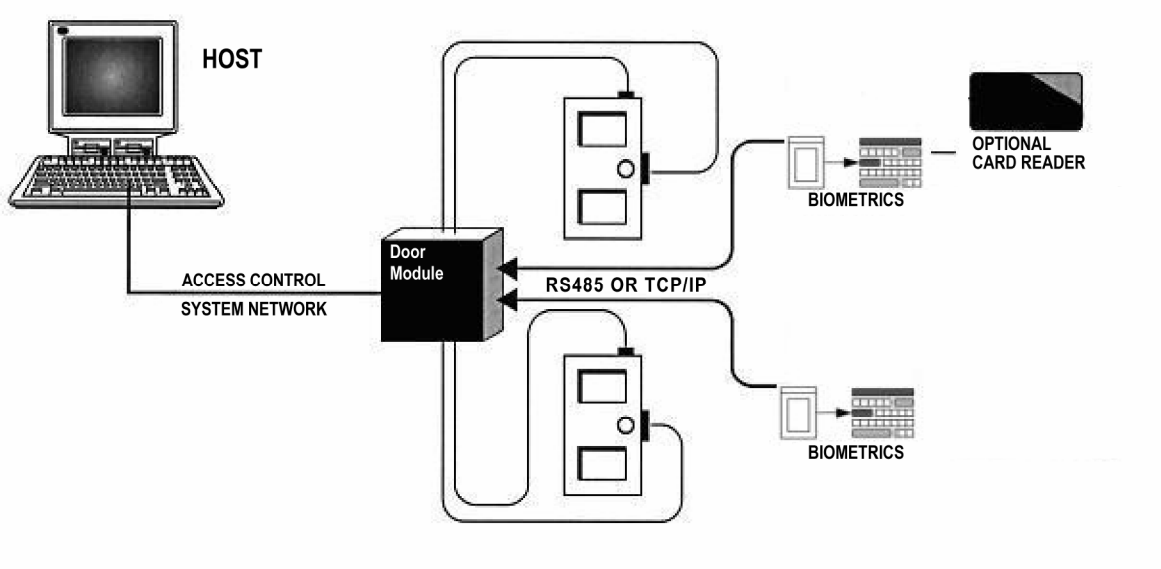
With the advent of lower cost smart card technologies, particularly proximity based cards, this media is beginning to take hold in the access control market. A strategy being used in conjunction with the read-write capabilities of these cards is to write the biometric template of the card holder into the smart card. The card holder's identity is simply read off the presented card and the user is then verified against it. Since the template is carried to the biometric reader by the card holder, this method of template distribution eliminates the need to link biometric devices together. Once the user is verified, the biometric sends the users ID number up to the panel for the ultimate access decision. The most common smart card technologies used in access control are based on ISO 14443 or ISO 15693 standards.



Example of Smart Card Integration

Full Biometric Integration

Some access control manufacturers have fully integrated biometrics into their access control systems. In this type of integration, the access control software handles the template management and communications to the biometric units. In this case, the biometric template data is handled just like any other piece of card holder information and is stored inside the user's data record at the head end. Template distribution happens through the access control system's network topography. Templates can be sent through the network and ultimately stored in the specific biometric unit at the door or concentrated in the access control panels.



Example of Full Biometric Integration

Issues to Consider

Acceptance
The most critical factor in the success of a biometric system is user acceptance of the biometric device. There are several factors which have an impact on acceptance. First, the device must cause no discomfort or generate concern by the user. This may be a subjective issue, but it is important to fully explain any concerns users may have. If people are afraid to use the device, they most likely will not use it properly and that may result in them not being granted access. Second, the biometric must be easy to use. People like things that are simple and intuitive. How many times have you been frustrated at a card reader that gives no indication of which way to swipe the card? Third, the biometric must work correctly. If a biometric is working properly, it does two things -- It keeps bad folks out and lets good folks in. Yet, no device is perfect and biometrics is no exception. The two errors a biometric can make are letting bad persons in and keeping GOOD persons out. The probability of one of these errors happening is characterized by the False Accept and False Reject error rates.

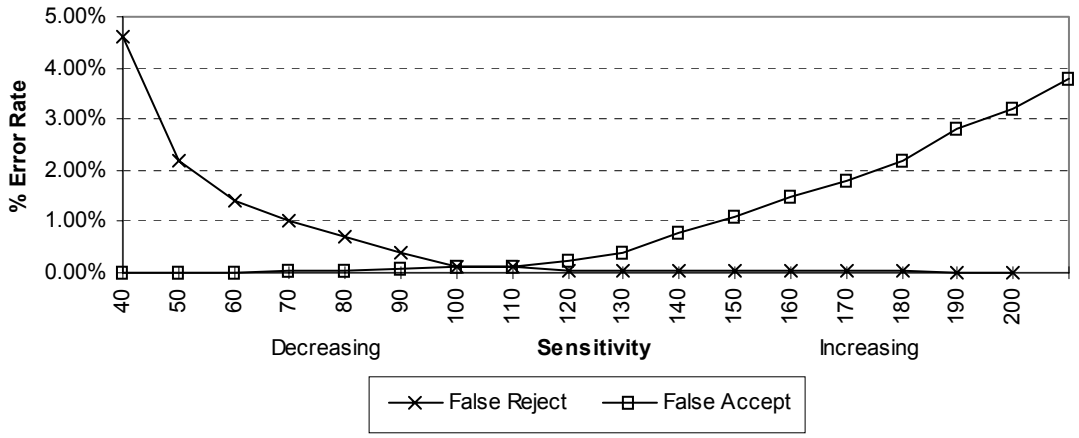
False Accept Rates
The probability of authenticating (verifying or identifying) any user registered or unregistered to another persons stored template is known as the False Accept Rate. This error rate must be low enough to present a real deterrent for a given application. False Accept Rates claimed in today's biometric access systems range from .0001% to 0.1%. It is important to keep in mind that the only way a false acceptance can occur is if someone tries. Therefore, the False Accept Rate should be multiplied only by the number of unauthorized attempts in order to determine the number of possible occurrences. To give some perspective to these numbers, the biometric used on the front entry area of 95 percent of U.S. nuclear power plants has a False Accept Rate of 0.1%.

False Reject Rates
False Accept Rates are certainly important in security applications. But, the False Reject Rate, which affects the good folks, is just as critical. The False Reject Rate or "Insult Rate" is the probability that the biometric does not recognize an authorized user and therefore denies them access. One can see the importance of a low False Reject Rate if you consider that an access control point that does not allow bad or good persons in, is commonly known as a wall. The False Reject Rates quoted for currently available systems vary from .00066% to 1.0%. A low False Reject Rate is so important because this type of error can occur with almost every use of the device. How many times will authorized people attempt to gain access in a given day? To illustrate this point, an example may be helpful. A company with 100 employees has a biometric device on the front door. On average, the front door is used by each employee four times per day. This would yield 400 transactions per day by the good folks. A False Reject Rate of 1.0% would predict that each day, four good persons (one percent of 400) would be denied access. Over the course of a five day week, that's 20 problems for the good folks. Reducing the False Reject Rate to 0.1% would result in only two problems for that same one week period. What is considered an acceptable level of false accepts and false rejects depends on the application. Understanding the impact to your application of these error rates can mean the difference between success and failure.

A low False Reject Rate will also have a significant impact on user acceptance. If someone is authorized to enter and the biometric recognizes them, then the system works. People like things that work. If the biometric mistakenly does not allow them access, frustration will set in quickly and the biometric may never be accepted.

Equal Error Rates

In a biometric device, the False Accept and False Reject Rates can be affected by increasing or decreasing the sensitivity of the device. The two rates are inversely proportional and can be likened to a car alarm. When your car alarm is very sensitive, the probability of the bad folks stealing your car (a false accept) is very low. Yet the chances of you accidentally setting off the alarm (a false reject) are higher. Reduce the sensitivity and the number of false alarms will go down, but then you increase the chances of someone being able to steal it. How much each error rate is affected by altering the sensitivity is a characteristic of each manufacturer's device. A device may offer an extremely low False Accept Rate at a given sensitivity, but the corresponding False Reject Rate may be totally unacceptable. The balance of the two error rates for a given application is critical to the success of a biometric installation. Error curves such as the one below give a graphical representation of the biometric device's personality, so to speak. The point at which the false accept and the false reject curves intersect is called the Equal Error Rate. This is the point where the two error rates equal one another. The corresponding sensitivity setting for the Equal Error Rate is found on the lower axis. The Equal Error Rate can be a good indication of the biometric's all around performance. The smaller the Equal Error Rate, the better.



Example of Error Rate Graphs

Failure to Enroll

A critical error rate to be considered is the failure to enroll rate. This describes the probability that a user cannot be enrolled into the biometric system. The reason they can not be enrolled usually has to do with damage to the characteristic required by that particular biometric device.

Failure to enroll rates varies dramatically from technology to technology. Also keep in mind that once an enrollment is completed, it does not guarantee that the person will verify reliably. While a facial system can easily enroll people, they typically have high false reject rates as compared to other technologies.

In access control, one must consider alternative forms of access for those people that cannot enroll into a system. Will they be given access by presenting only a card or PIN? How big an issue this error rate is depends on the size of the user population and the technology proposed. If the population is more than a couple of hundred people, it should be given very serious consideration

Validity of test data

In general, testing biometrics is a difficult task because of the extremely low error rates involved. In order to attain any statistical confidence in the results, thousands of transactions must be recorded from actual field use of the biometric device. Some quoted error rates are the result of theoretical calculations. Others are obtained by actual field testing of the devices. Field test data is usually more desirable since it is a real world test of the device. In the case of False Reject data, only field test results can be considered accurate. This is due to the fact that biometric devices rely on human interaction and require their unique biometric characteristics for verification. If the device is difficult for a person to use, false rejects will tend to go up. If the attribute used for verification varies for some reason, a false reject could also occur. None of these conditions can be accurately quantified and included in a theoretical calculation. On the other hand, False Accept Rates can be reasonably calculated for some biometrics by performing cross comparisons of templates in large template databases.

Currently, most field test error rate data for biometric devices have been generated by end users and various biometric manufacturers. In any case, it is important to remember that error rates are statistical in nature. They are derived from a series of transactions that were created by a population of users. In general, the larger the population and the greater the number of transactions studied, the greater the confidence level in the accuracy of the results. If the error rate is reported at 1 in a 100,000 and only 100 transactions were included in the study, the confidence level in the result would be very low. If the same error rate was reported and 1 million transactions were used, the confidence level would be much higher. The magnitude of the reported results will have an effect on the size of the sample needed for a reasonable confidence level. If the reported error rate is one in ten, then a sample of 100 transactions may provide a sufficient confidence level. Conversely, 100 transactions would be too small a sample if the error rate was reported as 1 in 100,000.

Throughput

A logistical issue that should be considered carefully when using a biometric is the throughput. Throughput of a biometric system is the time that it takes for a person to use the device until a result is provided by the biometric device. It is difficult for manufacturers to specify a throughput since it is application dependent. Most manufacturers specify the verification time for the reader, but that is only part of the equation. When a person uses a biometric reader, they typically enter an ID number on an integral keypad thus adding more time to using the system. The reader prompts them to position their hand, finger or eye where the device can scan physical details. The elapsed time from presentation to identity verification is the "verification time." Most biometric readers verify ID in less than two seconds. Those considering the use of biometrics for access control must look beyond the verification time and consider the total time it takes a person to use the biometric system. This includes the time it takes to enter the ID number, if required, and the time necessary to be in position to be scanned. If ID numbers must be entered, they should be kept as short as possible. If a long ID number must be used, some biometrics can obtain the number by reading a card, which contains the ID number in the card code. One must weigh faster throughput gained by using cards against the card administration costs. The total time required for a person to use the reader will vary between biometric devices depending on their ease of use and verification time.

Summary

As the use of biometrics grows, the need to understand the issues related to them becomes more critical. User acceptance will always be central to successfully utilizing a biometric. Unfortunately, there is no way that a biometric manufacturer can specify a device's user acceptance. Different classes of applications demand different biometric performance in order to achieve high user acceptance. The key quantifiable performance factors of a biometric are its various error rates. Therefore, understanding what these different error rates mean and how they can impact acceptance is extremely important.

Certainly, the future is bright for the biometric industry and their place in access control applications. The goal of access control is to restrict access to people in defined areas, making facilities more secure. Only a biometric device truly provides this capability to the end user. This technology is no longer science fiction. It has been used successfully for years by large and small companies alike. There are biometric systems available today which can economically meet the needs of almost any commercial access control application. And, as costs come down, justifying the use of a biometric will become a reality for more and more people.

For more information, please contact SIA Manager of Industry Groups, Doug Wright, at dwright@siaonline.org or 703/647-8494 (toll-free 1-866-817-8888). http://www.siaonline.org

Formed in 1969, the Security Industry Association (SIA) provides its members with a full-service, international trade association promoting growth, expansion, and professionalism within the security industry by providing education, research, technical standards, representation, and defense of our member's interests. SIA has over 300 member companies representing manufacturers, distributors, service providers, integrators and others. SIA members are involved in several market segments such as, CCTV, access control, biometrics, computer security, fire/burglar alarms, home automation, just to name a few. Members work together to address issues facing the industry and develop programs to enhance the environment in which they sell products and services.