JUL 31 1996

SANDIA REPORT

SAND96-1130

Unlimited Release

Printed May 1996

Evaluation of Smart Gun Technologies Preliminary Report

RECEIVED

AUG 05 1996

OSTI

D. R. Weiss

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550
for the United States Department of Energy
under Contract DE-AC04-94AL85000

Approved for public release; distribution is unlimited.

SF2900Q(8-81)

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

MASTER

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
Office of Scientific and Technical Information
PO Box 62
Oak Ridge, TN 37831

Prices available from (615) 576-8401, FTS 626-8401

Available to the public from
National Technical Information Service
US Department of Commerce
5285 Port Royal Rd
Springfield, VA 22161

NTIS price codes
Printed copy: A05
Microfiche copy: A01

DRAFT

01/16/96

Evaluation of Smart Gun Technologies Preliminary Report

D. R. Weiss

January 1996

**This work was performed
by Sandia National Laboratories
for the National Institute of Justice
under contract IAA-94-IJ-R-021**

This page intentionally left blank.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

SAND96-1130
Unlimited Release
Printed May 1996

Evaluation of Smart Gun Technologies Preliminary Report

D. R. Weiss
Power Electronics and Custom Controllers Department
Sandia National Laboratories
Albuquerque, New Mexico 87185

Abstract

The goal of the Smart Gun Technology project is to eliminate the capability of an unauthorized user from firing a law enforcement officer's firearm by implementing user-recognizing-and-authorizing surety technologies. This project is funded by the National Institute of Justice. This document reports the project's second objective: to investigate, evaluate, and prioritize technologies that meet the requirements for a law enforcement officer's user-recognizing-and-authorizing firearm. This report details a smart gun system analogy, reviews and ranks various technologies that may meet the requirements of the law enforcement officers, and discusses the methodology used to obtain the results. The information in this report is based solely on the law enforcement requirements for a smart gun; the requirements for the general public are assumed to be different.

Acknowledgments

It would be negligent to not mention the contributions of Dale Brandt, and Kerry Tweet to the work done throughout this project. They have both assisted in countless ways to make this project a success. I would also like to thank the proof-readers who took time from their already busy schedules to make certain the information detailed in the report is presented fairly and accurately.

Reader Feedback

This report contains descriptions of various technologies that could be used in a smart gun system. We are constantly looking for ways to improve the information and processes contained in this report. Readers can provide the best suggestions for improvement. The reader is encouraged to submit any comments, criticisms, and ideas to be considered for future revisions to the following address.

Douglas Weiss
Smart Gun Technology Project
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0537

Fax: 505-845-9888

E-mail: drweiss@sandia.gov

Contents

ACKNOWLEDGMENTS.....	IV
READER FEEDBACK.....	V
CONTENTS.....	VI
EXECUTIVE SUMMARY	1
CHAPTER 1 THE SMART GUN TECHNOLOGY PROJECT.....	6
CHAPTER 2 INTRODUCTION.....	8
CHAPTER 3 A SMART GUN SYSTEM.....	9
CHAPTER 4 THE EVALUATION PROCESS.....	13
CHAPTER 5 ENGINEERING REQUIREMENTS	15
CHAPTER 6 AUTOMATIC ID TECHNOLOGIES.....	31
RADIO FREQUENCY IDENTIFICATION	31
REMOTE CONTROL.....	35
BAR CODES	36
TOUCH MEMORY	38
CHAPTER 7 BIOMETRICS TECHNOLOGIES	40
FINGERPRINT	43
VOICE RECOGNITION	45
HAND SHAPE.....	47
SIGNATURE DYNAMICS	49
BIOMETRICS ABOVE THE NECK	49
CHAPTER 8 MISCELLANEOUS TECHNOLOGIES	51
MAGNETIC ENCODING	51
LOCKS.....	52
LANYARD.....	53
CAPACITIVE SENSING.....	54
COLOR SENSORS	54
CHAPTER 9 LATCHING MECHANISMS	56
CHAPTER 10 SUMMARY OF EVALUATIONS.....	60
CHAPTER 11 CONCLUSIONS	69
BIBLIOGRAPHY	71
APPENDIX A SUMMARY OF USERS' REQUIREMENTS	73
APPENDIX B PATENTS	77

Executive Summary

The Smart Gun Technology Project has a goal to eliminate the capability of an unauthorized user from firing a law enforcement officer's firearm by implementing 'smart' technologies. Smart technologies are those that can in some manner identify an officer. This report will identify, describe, and grade various technologies as compared to the requirements that were obtained from officers. This report does not make a final recommendation for a smart gun technology, nor does it give the complete design of a smart gun system.

The National Institute of Justice (NIJ) is the sponsor of the Smart Gun Technology project. As part of the U.S. Department of Justice the NIJ sponsors the development of tools and technologies aimed at improving the effectiveness of law enforcement. Sandia National Laboratory is one of the Department of Energy's multiprogram laboratories. Sandia is conducting this investigation using a three step process: 1) define the requirements of an officer's smart gun, 2) investigate, evaluate, and prioritize technologies that may meet the requirements, 3) demonstrate various technology's strengths and weaknesses by building models.

Smart Gun Analogy

A smart gun system may be viewed as a type of security system for a firearm. As an analogy for the system it is described in terms of a key operated padlock. This is broken into three pieces: a key, a discriminator, and a latching mechanism. The key does not have to be a metal key like that of the padlock. The key can be any item that has some unique property that can be sensed. Items like a fingerprint, an electronic code, or a combination can all be considered a key. The discriminator is the device that distinguishes

the characteristics that make one key different from another. Each key has some associated technology that can distinguish its properties. The latching mechanism is like the shackle on the padlock; the latch physically locks the firearm and prevents it from being fired. When a smart gun system is made up of these three pieces, each piece can be evaluated against its particular requirements.

Before an officer could use a smart gun he needs to be authorized. A person becomes authorized by being enrolled. Enrollment consists of storing the unique characteristic of the officer's key into the discriminator so that it will be recognized in the future. Enrollment could take place on either the firearm itself, or when the firearm is attached to a separate system that stores the officer's key. After an officer is enrolled, then anytime that key is presented to the firearm, the firearm must allow the officer to fire. If the key is not a natural part of the officer's body, but is a carried device, the officer must remember the key or the firearm will not operate.

An evaluation method was needed that could trace the officer's requirements as the determinate factor in the rankings. A process called quality functional deployment (QFD) was used to transform the officer's sometimes general requirements into the more definite requirements needed by a designer. This process was able to find the relationships between the officer's requirements and the design engineer's requirements, while including how important various requirements were to the officers. After the engineer's requirements were listed, each technology could be ranked against each requirement to determine a final ranking between all the technologies. Since many of

the officer's requirements relate to the final implementation of a product, as opposed to a technology that may be worked into a product, some of the requirements could not be used for ranking purposes. Many of these items such as the amount of testing or documentation required for the system will not affect the rankings as shown in this report. The ranking that was completed, therefore, focuses on the basic operational aspects of the technology in a smart gun system.

This report includes the long list of engineering requirements that were refined from the officer's requirements. The officer's requirements were documented in the report previously released titled *Smart Gun Technology Requirements Preliminary Report*. Along with each requirement is a short description that gives the reader some background information describing the constraints placed on the technologies being ranked; this makes the reading of this section worthwhile to all readers.

Three categories of technologies are ranked in this report: Automatic Identification, Biometrics, and Miscellaneous. For each technology the same format is used which includes among other things, the current uses for this technology, some theory of how it works, and how it might be implemented into a smart gun system. The descriptions for these technologies cover both the key and its associated discriminator.

Automatic identification is a broad classification of technologies for devices that can be used to track items without manual effort. Generally speaking these are electronic devices that use some type of code for their unique key. Biometric technologies are those that base their key on some characteristic of the human body. These are also electronic devices that can sense the unique human property and use that information to lock or unlock a firearm. Miscellaneous technologies are other devices that were grouped into one chapter of the

report. Many of the devices are mechanical, which has a benefit of not necessarily requiring power like the electronic devices.

Latching mechanisms are the devices that physically disable the firearm. Each firearm has been designed to be effective and efficient. Most parts are not transferable between firearms. For these reasons the design and implementation of a latching mechanism is left to the firearm manufacturers. What is considered are philosophies of how to physically disable a device, and some devices available to perform these actions. Any critical piece in the firing chain can be restrained, removed, or destroyed, to stop a firearm's firing chain from operating. It takes some type of energy to perform any of these actions; the proper utilization of this energy (whether mechanical, electrical, magnetic, or other) influences the design. The implementation of the latch is critical to the functioning of the system.

Fifteen implementations of fourteen technologies were evaluated. The implementation of the technologies can affect ranking. The most appropriate implementations were ranked for each of the technologies, each maintaining the basic building blocks of the smart gun system analogy. Each implementation was scored according to how well it meets each of the requirements. These scores were summed to determine a final ranking. The scores were also multiplied by the importance ratings found in the QFD process to weight the requirements by what was important to the law enforcement officer and the designer. Figure 1 is done in a style similar to common consumer magazines for easy comparison between technologies. The figure shows the rankings for the technologies (without importances) compared to specific categories of requirements detailed in the report. The category headings are self evident descriptors of the requirements contained within that category. It is shown without the importances so that the readers can decide for themselves

	● = A+	● = A	⊙ = B	⊙ = C	○ = D	• = F			
Updated Engineering Requirements	Scope	Physical Characteristics	Power	Operation	Key	Discriminator	Interface	Cost	Environments
Radio Frequency Tag	●	⊙	•	⊙	⊙	●	⊙	•	●
SAW Tag	●	•	•	⊙	⊙	●	⊙	•	●
Active Tag	●	•	•	⊙	⊙	●	⊙	•	●
Remote Control	●	•	•	○	⊙	●	⊙	○	●
Touch Memory	●	⊙	•	⊙	⊙	⊙	⊙	○	⊙
Fingerprint	●	○	•	⊙	●	⊙	⊙	•	⊙
Magnetic Encoding (A)	●	•	•	⊙	•	○	⊙	○	●
Magnetic Encoding (B)	●	•	⊙	⊙	•	•	⊙	○	●
Voice Recognition	●	⊙	•	⊙	⊙	○	⊙	•	⊙
Finger Length	⊙	⊙	•	⊙	⊙	○	⊙	○	⊙
Bar Code	●	⊙	•	⊙	•	⊙	⊙	•	⊙
Capacitive Proximity	•	⊙	•	⊙	○	•	•	○	●
Lanyard	●	○	●	•	○	○	⊙	⊙	⊙
Key Lock	●	•	⊙	•	•	○	⊙	⊙	⊙
Combination Lock	●	○	○	•	•	○	⊙	⊙	⊙

Figure 1 Evaluation of Technologies Compared to Requirements

what is important. The symbols used in the rankings are shown in the figure.

Figure 2 shows that there is no perfect technology: one that will meet all the officer's requirements. There are numerous reasons for this. The companies who develop these technologies have not targeted a firearm for their products. Most of these technologies are built into buildings, and wired into the building's electrical systems. If developers saw a market in the firearm area some of the lower scores could be improved. Another reason is that although many of the technologies have been conceived of for years, it has only been recently that the manufacturing capabilities were available to turn them into products. The main reason that there is no perfect technology is that the set of requirements obtained for law enforcement officers are idealistic and thus very difficult. It will be the task of any

manufacturer who builds a smart gun system to decide how to leverage the requirements that can be met with those that cannot be met. Negotiations with officers will be essential to determine what requirements can be relaxed.

The previous column chart shows that the highest grade that any of the technologies received was a "B". More work needs to be done to all the technologies to bring them to a level that a law enforcement officer will value.

The radio frequency devices were at the top of the ranking. A reason for this is that radio waves travel through most substances so they are not hindered by the same environments as some of the other technologies. Another reason is that an electrical device uses a code that can be quickly transmitted and checked for errors giving it a high rate of accepting authorized users. The biggest concern of the

radio frequency devices is electromagnetic interference that would prevent the normal communication from occurring.

Touch memory technology scored rather high even though it has practical problems to overcome. This means that the qualities that it does have are important to the user, and the strengths outweighed its weaknesses. Again, an electrical device allows a repeatable communication of a unique code. A drawback is the alignment of the key.

Fingerprinting technology ranked as high as it did because of its key. The key is always available and is very stable. The problems have to do with the time it takes to obtain a

The magnetic technologies can use magnetic forces to turn the firearm on and off. This would alleviate the need for some type of on/off switch that would help conserve battery life. It is also possible for one of the implementations to not require the use of batteries at all. The concern is the alignment of the key with the discriminator.

Voice recognition is another biometric technology, but in this case the key is not as good as that of the fingerprint. The goal of voice recognition is to detect the vocal tract, but today most systems are based on detecting phonemes (the smallest units of speech). As the voice changes due to various reasons including sickness, stress, or age a

Figure 2 Rankings of Technologies

completed reading of the fingerprint, and with contaminants interfering with the reading between the key (fingerprint) and the discriminator.

person may have a difficult time being recognized. If the system is implemented with a spoken password as a key it means the activation requires a memorized action.

The next three technologies (finger length, bar codes, capacitive proximity) all have limited potential as a smart gun technology. They either lack a basic building block of a smart gun system, or lack a good implementation. Finger length and hand mass are not known to be unique in the method that a firearm would be used: gripping a curved surface. Bar codes need a method to be carried by the user so that the firearm could read the bar code's information.

The three final devices, the lanyard, the key lock, and the combination lock came in last as meeting the requirements for a law enforcement officer's firearm. These devices are less expensive than the other technologies and they may not require any power source. The problem these technologies have is that they do not automatically enable the firearm for the user but require the user to perform an action. This may not be able to be accomplished during a takeaway situation.

When importances are added to the rankings some changes in the rankings do occur. Different officers have different requirements that are important to them. These mainly depend on their specific duties. Because of these differences it is recommended that the reader use the ratings without importances, then decide from the included information what is personally most important. When the importances are included it can be seen that for the most part the rankings do not change, but some technology's scores will increase because of specific qualities that it has that are of higher importance to the users.

After a thorough review of the data there was no perfect technology: one that would meet all the officers' requirements. This indicates

that there are some characteristics of each technology that do not live up to the officer's expectations. This is not all bad since the officers' requirements were often highly idealistic. What it does mean is that there is still work to be done by technologists to resolve the officers' concerns. None of the top ranking technologies were found to have any problem that could not be solved from more research and development, or by reaching a compromise with the officers. Many of the technologies discussed did not exist even a few years ago as marketable products. Even during the evaluation period new advances were made in some of the technologies, with more being expected within the next few years. As technologies become mature the weaknesses listed in this report may be overcome. Much time and resources will have to be expended to overcome these weaknesses; this is difficult without a guarantee of a market place for the product when it finally becomes available.

Although there is no perfect technology there is a desire by many to have a more secure firearm available for use by law enforcement officers. Others would like to have more secure firearms available to the general public. The information in this report is based solely on the law enforcement requirements for a smart gun; the requirements for the general public are assumed to be different. It is hoped that the information contained in this report will spawn a move by technologists to review the results and use their expertise to resolve the shortfalls of their technologies. In this way reliable, safe, and secure user-authorized smart guns can be developed.

Chapter 1

The Smart Gun Technology Project

National Institute of Justice

As the research and development agency of the U.S. Department of Justice, the National Institute of Justice (NIJ) pursues a wide range of programs to prevent crime and improve the criminal justice system. NIJ is authorized to: sponsor research and development programs, and special projects; evaluate the effectiveness of new and promising crime control programs; support technological advances applicable to fighting crime and improving criminal justice; disseminate information from research, development, demonstrations and evaluations.

For more than 20 years, NIJ has had oversight for developing performance standards for law enforcement products including hand-held radios, metallic handcuffs, firearms, surveillance devices and body armor. With the development of tools and technologies aimed at improving the effectiveness of law enforcement being under NIJ's jurisdiction, NIJ is supporting a "smart gun" technology research and development proposal. The Smart Gun Technology project is an effort to define a user recognizing and authorizing firearm surety system as well as investigate, evaluate and prioritize existing technologies for potential use in a "smart gun." The results of this project will be used to further the goal of eliminating the capability of an unauthorized user from firing a law enforcement officer's firearm.

Sandia National Laboratories

Sandia National Laboratories (SNL), one of the Department of Energy's multiprogram laboratories, has for over four decades applied its talents, tools, and techniques to solving technical problems of national scale. Established in the 1940s as the engineering arm of the nuclear weapon development system, Sandia has since grown into one of the country's largest technical resources, now working in areas as diverse as environmental remediation, healthcare, transportation, manufacturing, and criminal justice.

During its more than 40 years of existence, Sandia has maintained an abiding commitment to technical and scientific excellence in meeting the Department of Energy's and the nation's needs. Sandia's industrial management heritage brings to the Laboratories an emphasis on developing theoretical concepts into useful solutions. The ability to transform knowledge from research laboratory to factory floor, from vision to application, is a Sandia strength.

The Smart Gun Technology project is a project for the Department of Justice. Since Sandia is not in competition with private industry, an unbiased look at the problem of firearm takeaways and technologies to address the problem can be conducted by Sandia. A separate goal of Sandia is technology transfer: the results of this project will be disseminated to private industry to direct the realization of a "smart gun."

Smart Gun Technologies Project Description

The goal of the Smart Gun Technology project is to eliminate the capability of an unauthorized user from firing a law enforcement officer's firearm by implementing user-recognizing-and-authorizing surety technologies. The project intent is not to produce a firearm, but to evaluate technologies capable of being used in a firearm that can recognize a user, as well as be highly reliable, very safe, very secure and meet stringent law enforcement requirements. The focus on law enforcement firearms dictates that authorized users must always be able to operate the firearm and unauthorized users should never be able to operate the firearm.

This approximately 20 month, \$620,000 project has multiple objectives. The first objective is to find and document the requirements for a user-recognizing-and-authorizing firearm technology that law enforcement officers will value. A prior report documented the requirements for the smart gun technologies that law enforcement officers would value.

The second project objective is to investigate, evaluate, and prioritize technologies that may meet the requirements for a user-recognizing-and-authorizing firearm. This document contains the preliminary results of this objective. Various technologies are evaluated regarding their potential to satisfy the

requirements. These technologies are ranked and the process documented.

The third project objective is to demonstrate and document various technology's strengths and weaknesses in models of a user-recognizing-and-authorizing firearm. Models will be fabricated to illustrate identification principles as well as demonstrate proof of concept of the most promising technologies.

Purpose of the Technology Report

The purpose of this report is to provide detailed written technical descriptions delineating the strengths and weaknesses of technologies as they pertain to the requirements for smart gun technologies. The document includes discussions on the investigation, and evaluation of a wide variety of technologies that, in principle, could be capable of meeting the law enforcement officers' requirements for a smart gun technology. The investigation consisted of systematically examining many technologies that could meet the law enforcement officers' requirements when placed in a smart gun system. The evaluation process ascertained the worth of the technologies in meeting the requirements individually and in proposed smart gun systems. From the information in this report the technologies can be prioritized for further work.

Chapter 2

Introduction

This report is written to guide the reader through various technologies that could be used in a smart gun system. The report attempts to contain enough information for a non-technical person to understand the strengths and weaknesses of the technologies. At the same time the report tries to give a technology specialist the background and special insights to the key problems that would need to be resolved with each particular technology.

It is impossible for every implementation that could be used in a smart gun system to be covered. The approach that was taken was to give an overview of as many technologies as possible within the resource constraints of the project. For some of the technologies the descriptions only give a snapshot of the state of these quickly advancing technologies. The stated implementations are not necessarily recommendations, but are thought to be the most appropriate implementation of the technology today and are used to show specific strengths and weaknesses.

The remainder of the report begins with a description of the general smart gun system. This gives an understanding of the basic building blocks of a smart gun system.

Next it is important to understand the process that was used during the investigations. By reviewing the methods in which the investigations were conducted the manner in which the rankings of the technologies are related to the user's requirements can be seen.

After the analysis method is described, an understanding of the requirements the

technology must meet is needed. This gives a clear picture of the challenge placed before each technology. The engineering requirements are expanded from the users' requirements, being more complete and measurable.

Finally with the groundwork laid, each technology can be discussed. There are so many possibilities for smart gun systems that it is impossible to discuss every variation. In the technology discussions various keys and their associated discriminators will be discussed. Each discussion will first present a general description of the key as a unique identifier independent of the application in a smart gun system. Even some keys that do not seem to have a feasible method of implementation in a smart gun system will be discussed. This is to leave room for the reader to conceive ideas, and not limit the report to the limitations of ideas of the authors. There are many possible ways to present the data. The many technologies that were reviewed have similarities and differences that lend themselves to different arrangements of the information. The grouping which consists of three broad categories of technologies tended to have the least overlap.

After the individual discussions of each technology, a summary of the evaluation is given. The summary includes the benefits and weaknesses of the technology as it might be incorporated in a smart gun system, according to the requirements stated in this report.

Chapter 3

A Smart Gun System

The generic smart gun technology system.

There is no one method of developing a smart gun system. There are many ingenious variations of smart gun systems possible and for the most part the system will contain the same building blocks. The three basic system building blocks can be explained through the analogy of a key operated padlock. The building blocks of a smart gun technology system are the key, the discriminator, and the latch. The framework of this report and the requirements are based off this generic concept. This is not to say that other concepts are not valid, if the user's requirements are met.

The smart gun system analogy

The analogy of a key operated padlock is beneficial to describe the concept of a smart gun technology system. The analogy works because both are security devices that allow authorized users access to protected items. The key is what allows the authorized user access by unlocking the lock. The protected items are secured (to the capabilities of the lock) from any user that does not have the correct key. The lock can be divided into two pieces, the discriminator and the latch. The discriminator is matched to the key. It will read the key and make the appropriate decision on whether the latch should be allowed to open. The latch is the object, the shackle in this analogy, which is used to

Figure 3 Smart Gun System Analogy

physically secure the protected item. Each of these building blocks will be discussed in reference to their application in a smart gun technology.

The Key

The firearm must somehow identify a user; this is accomplished by the use of a key. The key is the unique identifier that characterizes the user. The key can be a variety of objects such a fingerprint or an electronic tag. The key must be unique to the individual or group of authorized users. The firearm may allow access by only a single key, or allow multiple keys. Thus multiple authorized people can use a single firearm, or a single user may be authorized on multiple firearms. Some types of keys can be re-keyed (the uniqueness can be re-coded) while others cannot be easily changed. The key is the crux of the smart gun system; various types of keys will be fully discussed in this report.

The Discriminator

The discriminator distinguishes between different keys and enables the latch for authorized users. The discriminator stores the information needed to remember which keys are authorized. It then receives keys to acquire new readings. These readings are compared with the previously stored readings of authorized users. If a recognized key is detected then the discriminator enables the latch.

The Latch

The latch is the mechanism that physically disables the firearm. It must receive information from the discriminator to know the proper state of the firearm. The latch in a firearm will depend on the actual mechanical operation of the firearm. For this reason the implementation of the latch is left to the firearm manufactures to incorporate as each particular circumstance dictates. This report will not discuss the implementation of the latch, but will cover the latch requirements, and possible methods and devices that could be used.

The smart gun system

The smart gun system is an interdependent grouping of these three blocks to form a secure firearm. Each block alone must have a level of security commensurate with the needs of the system as a whole. This security level is one that will protect an officer from having his firearm taken and used against him, and at the same time not hinder the normal operation of the firearm.

The practical operation of the generic smart gun system.

Today, when an officer is in a circumstance that requires the use of his firearm, he simply draws the firearm from his holster, pulls the trigger, and the firearm fires. This is how officers desire a smart gun technology system to operate also. The following describes how the practical smart gun system might operate during each of these steps and the activities that may happen in the background.

An officer is enrolled

Before an officer is able to use a smart gun technology system he must train the firearm to recognize his key. This first step is referred to as enrollment. Enrollment means that a key is associated with the officer, and with the firearm. It is possible that the officer would enroll himself directly on his firearm, or he could use a separate enrollment machine located at the police department.

If the gun is equipped with the special enrollment features, the officer presents his key to the firearm and goes through the programming sequence. In this case each firearm is a stand alone system: it does not need an external programming device. This convenience does have some drawbacks, one is that each firearm must have all the circuitry and capabilities as an enrollment machine as well as its normal function. These could include buttons or keypad, indicators or alphanumeric display, and additional logic to perform the function. Because of the extra buttons and functions the firearm contains, the cost could increase and the reliability

decrease for each firearm. It also has a drawback that the firearm must be given to every person that will need to be enrolled; each of these users has to enroll themselves into every gun that they may ever want to use. Another problem is how permission is granted to enroll a new user. Typically someone (such as the owner) is assigned as the enrollment manager. This person has to be present to allow anyone else to enroll. Otherwise, anyone that picked up the firearm could enroll themselves.

A more likely approach is to have the officer use an enrollment machine. The downside of an enrollment machine is that now a separate piece of equipment is used to store all the templates, and there needs to be a method of communication between the machine and the firearm. Each police department would have to have access to an enrollment machine. The enrollment machine would store the unique characteristic of each user in a database that is maintained by the officer's department. Each user would only need to be enrolled one time at the machine and then this information could be downloaded into the appropriate firearms. This would insist that the biometric readers are standardized so that any reader produces the same resultant template, so templates would be transferable. To do this the officer takes his smart gun system to the station and plugs the firearm into the interface box. The database operator then programs the firearm with the officer's key. As officers join or leave the department the enrollment machine is updated, and then at some time each firearm needs to be brought to the enrollment machine to be updated. The enrollment machine's data base could easily track what users are authorized for any firearm. Once an officer is authorized he is able to use the firearm whenever the firearm has access to the key. The additional circuitry that the firearm needs is some means of talking to the programmer: a connector, an infra-red link, or some other interface. Although an officer could operate the machine himself, additional security can be

obtained if a separate enrollment manager for the department does the programming. The skill involved to program the firearm should be no more than that associated with making a withdrawal from an Automated Teller Machine (ATM), using equipment as simple as an interface box attached to a personal computer.

An officer goes on duty

Before an officer starts his duty shift he will want to make sure that he has all of his equipment. During this check he will make sure that his firearm is operational. To do this he will place his hand on the grip the firearm and check the indicator(s). There will be an indicator to show that the firearm recognizes the person holding it. If the smart gun system contains a battery there will also be a low battery warning indicator. This will show if the batteries need to be replaced. By checking these indicators the officer can be sure that the system is operational. The indicators need to meet the requirements stated in this report.

An officer needs to use his weapon.

Now that the officer is authorized, and knows that the system is operational, he is able to use his firearm any time the key is available. When the situation arises to use lethal force the officer grips the firearm in his hand. At this time the firearm's discriminator must read the officer's key. This is the first hurdle that the system designer must cross. It is never known when the firearm may be used. When the circumstance arises, there is not time for the officer to perform any special operations to wake up, or turn on, the firearm. The smart gun system must be able to sense the need to read the key. It is possible that the discriminator may be constantly looking for the key, but this constant looking may be impossible if other requirements such as the required battery life must be met. Possible methods for accomplishing this task are to have a switch attached to the firearm that is automatically closed when the firearm is in the hand of the user. In another method the system might sense the removal from the

holster, although this might limit other applications when the firearm is not holstered.

Now that the system has turned on, the discriminator's reader must read the key. The methods for this to be accomplished are the discussion of the majority of this report. After the key has been read, this new reading is compared with the readings of the authorized users that are stored in memory. The requirements for the memory depend on numerous factors. These factors include: how many users the firearm must be able to store, how much memory space each user's key requires, the time it takes to search all of the valid users and make a decision for the current users acceptability, if the memory must be reprogrammed, and if the memory must remember its contents without any power.

Now that the discriminator has performed a check to see if the new reading matches any of the pre-stored readings, the discriminator can enable the latch. The latch should currently have the firearm disabled; it should

remain disabled until the comparison is complete and the user is identified as an authorized user. At this time the latch should enable the firearm.

The officer pulls the trigger and the gun fires

All the reading and distinguishing of the key must occur in the time it takes for the officer to draw and pull the trigger of his weapon. In the circumstance that an officer has lost his firearm and has just regained control of it, these actions must occur in the time it takes for the officer to grip the firearm and pull the trigger.

Other system concepts

So many possible smart gun system approaches exist that they cannot all be covered. The approach described in this report is thought to be the most complete and adaptable. Other concepts do exist and have merit if the officers' requirements are met. As an example of another concept is one in which a safe zone is created around the "good guys" so that anyone can fire the firearm, but they cannot shoot the "good guys".

Chapter 4

The Evaluation Process

A common concern with applying existing technologies, developed for a specific purpose, to another application is that the wants and needs of the customer are forgotten or ignored in an attempt to make the technology perform its function. To overcome this concern, an approach for ranking technologies was needed that allowed the ability to trace the technology's ranking back to the law enforcement officer's requirements. In this manner as either the requirements or the importance of users' requirements change, the affect can be seen in the rankings of the technologies.

A quality function deployment was used as the basis for determining a more concise set of requirements, then this set was used for ranking each technology. Although a knowledgeable person's intuition may ultimately give the same rank order, this approach allows the review and tracability of the decision making process.

Quality Function Deployment

A quality function deployment (QFD) is a discipline for planning and development of a product that focuses on the customer's wants and needs. For this project, the QFD was used to assist in determining engineering requirements and importances. Although numerous other methods could be used, this approach keeps the focus on the wants and needs of the law enforcement officer. This study limited the analysis to the first phase of the QFD process, a matrix commonly called the House of Quality, that met the needs of the project.

It is difficult to rank technologies directly against an officer's requirements since these requirements often pertain to qualities of a smart gun. Instead of these qualitative requirements, a less subjective list of quantitative engineering requirements is needed. The QFD starts with the customer's requirements referred to as the "whats", meaning what the customer wants or needs. The QFD assists in the formation of engineering requirements, referred to as the "hows", meaning how the customer's whats will be met. Each what has an importance rating assigned. This importance rating was assigned from the information received from law enforcement officers during the process of determining their requirements.

A QFD matrix was built which provides a visual display of the interrelationships between the whats and the hows. Each interrelationship is assigned a weighting to identify if the technical how in any way has a bearing on satisfying the customer's what. The weighting is multiplied by the importance rating for each relationship. These products are then summed for each engineering requirement, this gives a measure (importance weight) of how important the engineering requirement is to be able to meet the user's requirements.

It is normally recommended that the number of whats and hows be limited in number. This keeps the matrix to a manageable size. To thoroughly understand the interrelationships between the customers' requirements and the rankings of the technologies, the size of the matrix was not

limited. A QFD matrix of over 8,000 relationships was built.

The result of the QFD process was a list of engineering requirements against which each technology could be ranked. Each engineering requirement resulted in an importance weight which gave a measure of its importance to the user. After the list of engineering requirements was formed from the user's requirement, the list was arranged in logical groupings and reviewed for completeness. Additional requirements were added as necessary to complete the set.

As another step in the QFD process each engineering requirement, as appropriate, is assigned a target value. This value is a goal for a designer to meet for the particular requirement. The target values must be specific and measurable. Each target value is assigned a direction for movement to indicate the desired direction for the design. Many of the requirements for this study were written as attributes, or features, that the technology would either have or not have. A correlation matrix can then be built to compare the engineering requirements with each other. This identifies complementary or conflicting relationships. The relationships are designated to the extent that they positively or negatively affect one another. This information is used to point out where trade-off decisions may need to be made; such as between the number of users that can be authorized to use a firearm and the time it takes to scan the list of users to identify the right one. For this project the correlation matrix was completed to a limited extent.

Ranking Process

The QFD process was followed by the ranking process. A separate matrix was formed to allow the list of engineering requirements to be compared to each technology to be evaluated. The technical requirements are often stated as attributes, requiring the presence of an item. This allowed the ranking process to be accomplished without having a precise implementation known.

Each technology was assigned a score indicating how well it could achieve the engineering requirement. This score was multiplied times the requirement's importance weight to affect the score according to the user's requirements. These products were summed for each technology to give a total score that could be used to rank the technology. The ranking scores show the ability of a particular technology to meet the wants and needs of the law enforcement officer. It should be understood that there is subjectivity in each step of the process and that the ranking results could be affected. To resolve this, information is provided with and without the importances included.

As a quick reference, the technologies are ranked against an abbreviated list of requirements as in popular consumer magazines. This allows the reader to quickly achieve an overview of the technologies compared to one another and the requirements.

Chapter 5

Engineering Requirements

The requirements listed in this section strive to build on the officers' ideal requirements as listed in *Smart Gun Technology Requirements Preliminary Report* and transform them into attributes that a smart gun system would or would not contain. More background is given in the previous report as to how the requirements were derived. An assumption that is made is that the requirements documented in the *Smart Gun Technology Requirements Preliminary Report* are valid. Those requirements are used as the basis for the comments stated in this report.

This report contains requirements referred to as engineering requirements because they are a refined set of the users' requirements, and are closer to what a designer would need to account for the features a product would entail. Some of the requirements pertain directly to a technology while other pertain to the smart gun system as a whole. The requirements are not meant to dictate a certain technology or design, but merely to state the users' ideal. It is still possible that officers would be willing to negotiate down from these idealistic requirements to simplify them or to make them less conflicting.

The requirements are listed in bold text followed by a brief explanation. Also included is a target value that states a goal for the requirement to meet. Many of the requirements were written so that the target value was listed as pass/fail, this means that the feature is either possible or not. Listing many of the requirements targets as pass/fail simplified the ranking process because many of the technologies theoretically could meet the requirement but have not used that

particular property in other applications. If a specific target value is listed then the preferred direction for the value is also listed in parenthesis. For example, the required number of users is listed as 'target value: 50 (more)' means that 50 is the targeted number of users, and the target can be improved by offering more than 50 users. For some requirements a target value is difficult to specify. The rank-able value is to indicate whether the requirement was used in the prioritizing of the technologies. Some requirements do not lend themselves to be used without an actual product to analyze.

Some readers may consider this lengthy section to be dry reading, but it will give the reader a deeper insight to the constraints placed on the technologies.

SCOPE

A smart gun technology system consists of an interdependent group of keys, discriminators, and latches integrated with a firearm.

This requirement states the need for a smart gun system to be developed as a system made up of the three basic building blocks of the smart gun system analogy (the key, the discriminator, and the latch).

Target value: Pass/fail

Rank-able: No

A smart gun technology system must have a unique identifier that can be associated with a user.

This requirement states the need for a key. The specific requirements for a key are found below.

Target value: Pass/fail

Rank-able: Yes

A smart gun technology system must have a means to discriminate between keys.

This requirement states the need for a discriminator. The specific requirements for a discriminator are below.

Target value: Pass/fail

Rank-able: Yes

A smart gun technology system must have a mechanism to latch the firearm so that it cannot be fired.

This requirement states the need for a latching mechanism that will physically enable or disable the firearm. The specific requirements for a latch are below.

Target value: Pass/fail

Rank-able: Yes

PHYSICAL CHARACTERISTICS

The weight that the smart gun technology adds to the firearm should be less than 3.5 ounces.

This requirement states the need for the technology to be lightweight. This weight should include any additional weight that must be added to the firearm because of the technology. Users' are concerned about firearms becoming too heavy. Officers must carry their equipment with them. A heavier firearm can adversely affect the officer's use of the weapon. The value of 3.5 ounces came from reviewing the weight of common laser sighting devices.

Target value: 3.5 ounces (less)

Rank-able: Yes

The size that the smart gun technology adds to the firearm should be less than 2 cubic inches.

This requirement states the need for the technology to be a small size. The firearm should not grow in size, becoming too large to carry and use. An increase in size can cause the officer difficulty in grasping the firearm, which could adversely affect weapon use. The value of 2 cubic inches came from reviewing the size of common laser sighting devices.

Target value: 2 cubic inches (less)

Rank-able: Yes

The addition of the smart gun technology should not change the firearms balance so that the use of the firearm is affected.

This requirement states the need for the placement of the technology not to upset the balance of the firearm. The balance primarily effects the response of the weapon to being fired. The balance, or feel, of the weapon is very subjective. By satisfying the weight requirement the balance of the weapon should not be affected.

Target value: No perceived change in balance.

Rank-able: No

The change in the firearm's shape should not affect their use in existing holsters.

This requirement states the need for the technology not to affect the shape such that other existing equipment, such as holsters, could not be used. It is not desirable for officers to have to change holsters if they change firearms.

Target value: NA

Rank-able: No

POWER

The technology used should not need an electrical power source. If a power source must be used it must meet the following power requirements.

This requirement states the goal for a technology not to need a separate power source. A power source, whether it is a battery or any other type, adds to the unreliability of the firearm. It also adds constraints such as increased scheduled maintenance times, and the need for an indicator.

A technology may be powered in a number of ways: rechargeable batteries, batteries in magazines, portable chargers in holsters. Different approaches need to be considered.

Target value: Electrical power not required.

Rank-able: Yes

The target value for the life of the power source is a replacement interval of greater

than 12 months or 1000 recognition attempts by a user, whichever comes first.

This requirement states the need for a power supply, if needed, to be of such long life that it is not a nuisance to an officer. If the battery can last long enough then the user does not have to be as concerned about having a dead battery when the firearm is needed. Since the life of the power source is dependent on both time and the number of uses, the user needs to determine how best to schedule a battery replacement. An annual scheduled time could be set to change the batteries for mostly unused firearms. A shorter scheduled time would be set for a well-used firearm. An indicator would still be necessary as a reminder, or to indicate a premature failure of the battery.

Target value: 12 months or 1000 recognition attempts (longer time or more attempts)

Rank-able: Yes

The power source must be of a standard size that can easily be obtained.

This requirement states the need for a power supply, if needed, to be easily obtained and readily available. The user should not have difficulty finding the proper battery for his firearm.

Target value: Standard size

Rank-able: No

The replacement of the power source should be able to be accomplished with no special equipment in less than 20 seconds.

This requirement states the need for a power supply, if needed, to be able to be replaced without being a hindrance to the officer. Battery replacement is more convenient if no special tools are needed.

The ease of battery replacement needs to be balanced against the requirements of failing armed and surviving certain environments. If the firearm's smart features are disabled without power (such as could be the case for a fail armed firearm), this easy access could be a hazard. If criminals learn that they can fire the firearm if they remove the batteries, and it only takes seconds to take the batteries out, then the officer has not been given enough

protection from having their firearm taken and used against them. An easy access may also make the firearm more prone to certain environments involving moisture and dirt. These environments could degrade the reliability if brought in contact with a power source.

Target value: less than 20 seconds (less)

Rank-able: No

A low power indicator must be available to indicate that the power source should be replaced.

This requirement states the need for an indicator to warn an officer of an impending need for replacement of the power supply, if used. Anytime a battery is used, an indicator should be available to monitor the status of the battery. The indicator must meet the indicator requirements stated later in this document.

Target value: Pass/fail

Rank-able: No

At 10 hours after the low power indicator first alerts the need for power source replacement the firearm must be able to fire 3 full magazines.

This requirement states the need for the low power indicator to alert the officer of the impending need for replacement of the power supply. Sufficient time must be given so the user can obtain and replace the power supply at their convenience, and not during a critical time. Three magazines is typical of what an officer might carry on his belt. These magazines should be able to be fired at the end of a shift, even if the warning indicator turned on at the beginning of a shift.

Target value: 3 full magazines fired after 10 hours (more rounds or longer time)

Rank-able: No

The number of steps to test the life of the power source should be minimized.

This requirement states the need for a simple method to test the power supply life. Observing a warning indicator is the simplest method. The ease of checking the requirements needs to be balanced with the indicator requirements. It is easy to simply

look or touch an indicator, but that indication may also be noticed by an adversary. An indicator such as a press-to-test button would require an action to check, but could be done at times acceptable to the officer.

Target value: One step (fewer)

Rank-able: No

OPERATION

The smart gun technology should not require any actions to activate or deactivate.

This requirement states the need for the device to be self actuating. The officer may not have the capabilities to do even a simple task like turning on the firearm at the instant the firearm must be used. The officer also may not have time or ability to turn the firearm off if someone is trying to take it from them. The firearm needs to automatically turn on and off, through the current interactions between the users' hand and it's presence on the firearm. Then the officer only has to grip the firearm to enable it, or let go to disable it. Some police trainers will instruct their students to use, as a last resort, the firearm's safety if they think that they will lose the weapon. Then they hope that the person that took the firearm does not know enough to disable the safety.

Target value: Zero actions

Rank-able: Yes

The smart gun system must have a method to reinitialize the identifying sequence.

This requirement states the need for a manual reset mechanism that restarts the mechanism in case of any type of malfunction. Officer's are typically taught the tap-rack-bang maneuver to reset a malfunctioning pistol. If a smart gun technology would for some reason malfunction, there needs to be a simple procedure to reset the smart gun system and re-read the user's characteristics.

Target value: Pass/fail

Rank-able: No

The system must detect when a new user is attempting to use the firearm.

This requirement states the need for the system to automatically recognize when a new user has gained possession of the firearm. The firearm should be able to detect a user picking up the firearm, or a transfer of possession from one user's hand to another. This could be incorporated in a number of ways each having different problems to overcome. One method is continuous sampling of the user's characteristic that takes both time and power. Another method could be a switch that is automatically pressed when the firearm is held.

Target value: Pass/fail

Rank-able: No

The system must detect and disable the firearm when an existing user has relinquished the firearm.

This requirement states the need for the system to become automatically disabled when the current user has given up possession of the firearm either voluntarily or involuntarily.

Target value: Pass/fail

Rank-able: No

The smart gun technology must automatically be able to repeatedly enable and disable.

This requirement states the need for the system to be reset and re-enabled automatically without special tools, as opposed to a system that becomes permanently or semi-permanently disabled. If an officer loses his firearm during a struggle, it automatically turns off, if he regains control of the firearm it automatically turns on.

Target value: Pass/fail

Rank-able: Yes

The smart gun technology must be able to be activated by a single individual without assistance from others.

This requirement states the need for the firearm to remain controlled by a single user with no help from others. A system must be controlled by a single individual, and not

dependent on having more than one person present. A possible exception to this would be the implementation suggested in the Remote Control section of this report. In this implementation the command and control functions are directed by a higher authority.

Target value: Pass/fail

Rank-able: Yes

The smart gun technology must be able to be operated with one hand.

This requirement states the need for the firearm not to require both hands for operation. A firearm must be able to be operated with one hand.

Target value: Pass/fail

Rank-able: Yes

The smart gun technology must be able to be operated with either hand.

This requirement states the need for the firearm not to be limited to use by either hand. Circumstances or individual user preferences may necessitate the use of either hand for firing the weapon.

Target value: Pass/fail

Rank-able: Yes

The smart gun technology must operate while the user wears gloves made of .063 inch thick leather, or .005 inch thick latex rubber.

This requirement states the need for the firearm to operate with gloves that might be used by an officer during duty. Officers sometimes have to wear gloves. The types of gloves that are worn vary. Some technologies cannot be operated through gloves. Either these technologies need to be ruled out, or a method to overcome the problem found. For the typical optical fingerprint reader one option would be to have finger-less gloves. Other options may exist.

Target value: .063 inches of leather, or .005 inches of latex rubber (thicker material)

Rank-able: Yes

The time for the smart gun technology to attempt to identify the user and enable the firearm must be less than .250 seconds.

This requirement states the need for the firearm to be ready to use before that the officer can fire the firearm. The time it takes for a system to enable the firearm is critical to the officer. Normally the firearm is carried in a holster and there is a finite time that it takes to draw and aim the weapon. The time may be much shorter if the officer retrieves the firearm from an adversary's hand. Some technologies take a long time to take a reading of the user's unique characteristic, to process that information, and then to latch or unlatch the firearm.

Target value: .250 seconds (faster)

Rank-able: Yes

The time for the smart gun technology to attempt to identify the user and disable the firearm must be less than .250 seconds.

This requirement states the need for the firearm to become disabled as soon as the officer has relinquished possession of the firearm either voluntarily or involuntarily. When the officer takes his hand off the firearm it should become disabled, either as the default state of the weapon or because there is not a valid user's hand on the weapon. Care must be taken so that the firearm never becomes disabled while the firearm is in the user's hand.

Target value: .250 seconds (faster)

Rank-able: Yes

The smart gun technology must not be able to cause the firearm to fire in and of itself.

This requirement states the need for the discriminator and the latching mechanisms to be separated in such a way that the recognition of the user cannot cause the firearm to discharge. The recognition of a user cannot act as a secondary trigger. No matter what state the weapon is in, cocked or not, the weapon can only discharge if the trigger is pulled.

Target value: Pass/fail

Rank-able: No

The smart gun technology must interface to the firearm in such a manner that the firearm will function if the technology becomes dysfunctional.

This requirement states the need for the latching mechanism to operate in such a manner that if the discriminator does not give any signal (i.e., the technology is not functioning) the firearm will still be able to be fired. This is the fail armed philosophy. It is much more likely that an officer will use his firearm in defense of himself or someone else, than to have his firearm taken and used against him. Officers have the desire that if the technology is not working the firearm will still operate. There are various approaches to do this. One is to have the firearm normally be enabled. When the user attempts to use the weapon, the firearm quickly attempts to recognize the user. If the user is not authorized, the firearm disables itself before the user can pull the trigger. This would become a race between how fast a user can pull the trigger, before the firearm becomes disabled.

Target value: Pass/fail

Rank-able: No

The smart gun technology should only be enabled if the firearm is in an authorized user's hand.

Firearms are designed to be held in the user's hand. If a firearm is not in the user's hand it should not fire.

Target value: Pass/fail

Rank-able: Yes

The smart gun technology should only be enabled if the key is within 6 inches of the discriminator.

The distance, or reading range, between which the smart gun's key and discriminator can communicate needs to be considered. It is important that the firearm is not enabled if there is too great a distance between the key and the discriminator. The greater the reading range the greater the possibility of the user's key being read in a circumstance that it should not be read, because it has accidentally entered the reading range. Also there is an

increased possibility for having other keys enter the reading range and having contention problems.

Target value: 6 inches maximum (less)

Rank-able: Yes

The smart gun technology system should not require the use of a memorized task.

This requirement states the need that an officer under stress may not have the mental facilities, the time, or the opportunity to perform a memorized task. It is known that for items such as a personal identification number, a large percentage of the people write the number down so that they can refer to it later. Often it is written on the card that it is meant to protect. This reveals that people do not always remember numbers even under benign circumstances.

Target value: Zero memorization

Rank-able: Yes

All users must be enrolled before use.

This requirement states that all users need to be authorized before they can be recognized. This should be obvious because the firearm must know who is authorized before it can allow anyone access to firing the weapon. Enrollment is discussed elsewhere in this report.

Target value: Pass/fail

Rank-able: No

The system should allow an untrained user to be enrolled in less than 5 minutes.

This requirement states the need for quick and easy programming of the user(s) in to the firearm's memory. No matter how the enrollment process is handled, it needs to be simple for the user. This benefits in reducing user frustration by reducing the time each officer is waiting to program or update the users in his firearm.

Target value: 5 minutes (Less)

Rank-able: No

The number of steps to test for an authorized user should be minimized.

This requirement states the need for a simple method for a user to verify that he is an authorized user of the firearm, without

actually firing a round. There are many times that a person may want to check to verify that the firearm recognizes them; at the beginning of each shift, on the way to a call, and during an inspection are only a few.

Target value: one step (fewer)

Rank-able: No

KEY

The key must be unique to an individual or a group.

This requirement states the need for a key to be exclusive to a user, or his group. This means that there must be a large number of different keys available for firearm users. Being unique eliminates the concern of an unauthorized user appearing as authorized because of a duplicate key. It is possible that groups of keys can be made identical, or have a similar feature so that multiple user could easily each other's firearms. If this is the case, it would be desirable that this feature could be changed. This is in case one of the keys is lost or stolen: the keys could be reprogrammed instead of replaced.

Target value: 1 million (more)

Rank-able: Yes

The key must be stable and non-changing for a known period of time.

This requirement states the need for a key that does not change it's characteristics. If the key changes with time, then the discriminator may not recognize it the next time it is tried. Some systems, by using neural networks or other means, can learn small changes each time it operates. This makes the system more complicated, but also makes the system more reliable. With frequent use small changes such as wear on a mechanical part, growth of a finger, or pitch change of a maturing voice, can be accounted for automatically.

Target value: Pass/fail

Rank-able: Yes

The key must not be easily copied.

This requirement states the need for a key to not be easily duplicated, either by the authorized or an unauthorized user. If all it takes is a photocopy of the key to duplicate it,

then there is not enough security associated with the key. To have the necessary security, either the key should not be able to be duplicated at all (being truly unique), or it should be so difficult that it would be a deterrent to the majority of adversaries.

Target value: Pass/fail

Rank-able: Yes

The key must be controlled in such a manner that no two users would inadvertently have like keys.

This requirement states the need for a process at all levels that will prevent the concern of an unauthorized user appearing as authorized because of a duplicate key. There may be some scenarios for some technologies, where a master key arrangement may be preferable. Normally, it would be inappropriate to have two users using the same key. Duplication needs to be prevented at all levels: manufacturers must have controls so that duplicate keys are not made, police departments may need controls to ensure that officers are not assigned duplicate keys, and officers need to not duplicate keys.

Target value: Pass/fail

Rank-able: Yes

The key should not be transferable, but uniquely associated to a person.

This requirement states the need for a key to be directly associated with a particular user and not transferable between users. Another user has to be enrolled to operate the firearm, and not just borrow a key. This requirement infers that biometric keys are the best, because they are unique to an individual. Any type of key that is transferable can be taken by, or given to, another user. This defeats the ideal of a user authorized firearm.

Target value: Pass/fail

Rank-able: Yes

The key must communicate with the discriminator.

This requirement states the need for the key to be compatible in operation with the discriminator. In the smart gun system analogy, the key must be able to pass on information to the discriminator. This

information includes the characteristics that make the key identifiable. Depending on the technology, the key may do nothing except be read by the discriminator's reader, or it may plan an active role in the reading process.

Target value: Pass/fail

Rank-able: Yes

The key should not be an item that must be separately carried by the individual such as an external device. If an external device must be used it must meet the following requirements.

This requirement states the need for the key not to be a separate item that could be lost or forgotten. The following requirements deal with the key as a carried item. Since the item should not be transferable (as stated above) these requirements elaborate on what a carried device must be capable if the device is carried.

Target value: Pass/fail

Rank-able: Yes

An external device must be able to be carried on at least two locations.

This requirement states the need for an external device to be conveniently carried by an officer. If a device must be carried it must be unobtrusive. Some officer's have aversions to wearing certain types of item while on duty. If the device can be carried in multiple locations then it may overcome the concerns of it being carried. Examples of this may be on either hand, on different fingers, on hand and wrist, on hand and torso, or on any combination of these.

Target value: two locations (more)

Rank-able: Yes

The size of the external device may vary depending on the intended carrying locations.

This requirement states the need for the size of the external device to be so small that it is unobtrusive to the officer performing his duties. If the size of the carried item is too large then it could interfere with the normal day to day operations that the officer must perform.

Target value: .5 cubic inch (less)

Rank-able: Yes

The external device must meet same standards as smart gun technology.

This requirement states the need for the carried item to meet the same standards as the smart gun technology. Not all the requirements apply, but most do. The item must be reliable, work in all environments, have a long life, etc.

DISCRIMINATOR

The discriminator must be able to identify and differentiate between multiple keys.

This requirement states the need for the reader to be able to distinguish between unique keys. The function of the discriminator is to be able to read the unique characteristic of the key and verify those characteristics as belonging to an authorized user. The discriminator must also be able to communicate with the latching mechanism in such a manner that the latching mechanism can lock or unlock the firearm.

Target value: Pass/fail

Rank-able: Yes

The memory required by the discriminator to store a user's unique characteristic should be minimized.

This requirement states the need to minimize the amount of information required to store each key's characteristic. It is often the case for devices that use memories, that the available memory becomes a limiting item. Minimizing the memory required to store an individual user allows for more users being able to be enrolled in the firearm for a given amount of memory, or allows a smaller amount of memory to be used. Minimizing the amount of memory also reduces the cost of the entire system.

Target value: 500 bytes per user (less)

Rank-able: Yes

The number of different users that should be able to operate a particular firearm should be greater than 50.

This requirement states the need for at least 50 officers to be able to be programmed into a single firearm. Enrollment by at least fifty

users allows the majority of the departments within the United States to program all of their officers into each firearm. The number of users that can be programmed into a smart gun is limited by the amount of memory or unique mechanical features in the firearm.

Target value: 50 (more)

Rank-able: Yes

The system should remember enrolled users until un-enrolled.

This requirement states the need for the firearm to retain authorized users in its memory until a user is removed from the data base. This is so that if power is removed from the firearm the memory is not erased. This prevents the need to reprogram all the authorized users each time the batteries are changed.

Target value: Pass/fail

Rank-able: Yes

The discriminator must be able to activate the latch.

This requirement states the need for the discriminator and the latch to be compatible in operation. For the smart gun system analogy to be complete the discriminator must be able to communicate with, or control, the latching mechanism. The extent of the communication necessary is whether the firearm should be locked or unlocked.

Target value: Pass/fail

Rank-able: Yes

The false acceptance rate (FAR) should be less than 5%.

This requirement states that the percentage of times that the firearm will inadvertently allow an unauthorized user to successfully operate the weapon should be less than 5% of the time. Current firearms do not limit the use of the officer's firearm at all. Since an officer is much more likely to fire the firearm in defense of himself or another person than to have it used against him, and because the FAR and FRR are related, the limit for FAR was set at 5%. Ideally this number would be 0%.

Target value: 5% (less)

Rank-able: Yes

The false rejection rate (FRR) should be 0%.

This requirement states that the firearm should never limit an authorized user from successfully operating the weapon. The system must never falsely reject an authorized user.

Target value: 0 %

Rank-able: Yes

The recognition score and the threshold value that is used to determine if a recognition is valid should be available in a test configuration.

This requirement states the need for the discriminator to have a means of measuring how well the key's characteristics are being measured. This assists in being able to compare scores when evaluating different technologies, especially for consistency and in different environments. It also assists in maintenance to allow readings to be compared to a baseline. This feature would only have to be available in a testing configuration. One possible implementation is to have this feature only available to be read by an external enrollment machine. This allows a quick and simple test of the discriminator that could be done at the convenience of the user.

Target value: Pass/fail

Rank-able: No

The smart gun technology must be able to perform the identification of the user without regard to the alignment of the key.

This requirement states the need for a discriminator to be able to read the key in multiple orientations and positions. The key during normal operation should be placed in approximately the same position. Under actual use conditions there could be some displacement or rotation. The discriminator must be able to read the key's characteristics if the normal alignment is not present. This means that the discriminator must be capable of accounting for the misalignment as it distinguishes the characteristics. This makes the discriminator more complicated.

Target value: Displacement = $\pm\frac{1}{2}$ inch (greater), Orientation = $\pm 180^\circ$.

Rank-able: Yes

The discriminator must not require special movement for the key to be read.

This requirement states the need for the discriminator to be able to not require the key to perform a special movement to be read. For many technologies it is critical that the key remain stationary for the discriminator to obtain a reading of key's characteristics. For other technologies the discriminator requires that the key be moving past the reader to obtain a reading. An officer using a firearm cannot be required to unnaturally hold the key stationary or perform a special movement when he is ready to fire his weapon.

Target value: Pass/fail

Rank-able: Yes

LATCH

The latch must be able to lock or unlock the firing state of the firearm.

This requirement states the need for the latching mechanism to control the state of the firearm. The firearm can be either locked or unlocked. The latching mechanism is the physical device that is able to block the firing action of the weapon until such a time that an authorized user is recognized by the discriminator.

Target value: Pass/fail

Rank-able: No

The latch should be matched to the characteristics of an individual firearm.

This requirement states the need for latch and the firearm system to be operationally compatible. Each firearm made by different manufacturers contains different pieces. The pieces may or may not be similar between manufacturers and models. It should be left up to manufactures how best to implement the latching mechanism into each particular model. Since there are many possible implementations, the manufacturers can decide what is in the best interest of their customers, and their company.

Target value: NA

Rank-able: No

The latch is activated by the discriminator.

This requirement states the need for the latch to be operationally compatible with the discriminator. For the smart gun system analogy to be complete the latching mechanism must in communication with the discriminator. The extent of the communication necessary is whether the firearm should be locked or unlocked.

Target value: NA

Rank-able: No

The implementation of a latching mechanism to lock the firearm for an unauthorized user should not affect the trigger pull level during normal use by the authorized user.

This requirement states the need for the latching mechanism not to interfere with the existing standards for trigger pull level when an authorized user is firing the firearm. When an unauthorized user is attempting to use the system the trigger pull may change either to a locked condition (infinite force needed) or unattached (zero force needed). This would be determined by the implementation of the latch, and the preference of the manufacturer.

Target value: Existing NIJ standards

Rank-able: No

The material strength of the latch must withstand the stresses of both normal and credible abnormal circumstances.

This requirement states the need for the latching mechanism to be strong enough not to be overcome by common threats such as dropping or increased trigger pull forces. The smart gun system must not be compromised by a broken latching mechanism.

Target value: Pass/fail

Rank-able:

INDICATORS

A feedback indicator should be present to show whether the firearm (the latch, not the discriminator) is enabled or disabled.

This requirement states the need for the officer to have a means of knowing the actual state of the firearms firing mechanism. The

indicator must show the present state of the latching mechanism not the discriminator. The discriminator makes a decision on whether the firearm should be enabled and communicates that information to the latching mechanism. It is possible that the latch did not receive the communication or it failed to respond. In this case if the discriminator was the sole indicator, the wrong indication would be present. If the indication comes directly from the mechanism that performs the enabling, then the actual state of the firearm is known.

Target value: Pass/fail

Rank-able: No

Any indication should be obtained with minimal actions from the user.

This requirement states the need for the officer to be able to know the actual state of the firearms firing mechanism with a minimum of actions. The officer should be able to check the state of his gun at anytime without interfering with his duties. The simple acts of looking at a light, listening to a sound, or feeling a protrusion are considered actions.

Target value: one action (fewer)

Rank-able: No

Any indicator should not distract the user's attention from their duties.

This requirement states the need for an indicator not to distract the officer from performing normal duties. Items such as lights, or sounds could distract the officer in certain circumstances.

Target value: Pass/fail

Rank-able: No

Any indicator should not be easily noticed by others.

This requirement states the need for an indicator not to reveal the officer to other individuals. Items such as lights, or sounds could jeopardize the officer in certain circumstances.

Target value: NA

Rank-able: No

DOCUMENTATION

Instructions of proper use must be available.

This requirement states the need for proper training, instructions, and cautions to be available for operation and maintenance of a smart gun technology firearm system. Even though the smart gun technology should not complicate the use of the firearm, officers need to be trained in the proper use and maintenance of all of their equipment.

Target value: Pass/fail

Rank-able: No

The amount of specialized ancillary equipment should be minimized.

This requirement states the need to minimize any additional pieces of equipment that must be used in conjunction with the smart gun technology firearm system. This includes any type of item that the officer may have to carry besides his firearm (i.e., a ring or controller), and any items that a department may need to operate, or maintain, the firearms. Although the number should be minimized, it may be to the officer's or the department's benefit to have certain types of ancillary equipment. One such item is a separate external enrollment machine instead of having each firearm having programming capabilities (as previously discussed).

Target value: zero

Rank-able: Yes

The number of special procedures should be minimized.

This requirement states the need to minimize any special operations or processes that accompany the firearm. This includes anything that the officer would not currently have to be concerned with in using his firearm. If there are any special controls, limitations, or procedures that are needed they should be listed. Departments must be concerned with items like lost firearms, lost firearm keys, trading of firearm keys, authorizing non-police on an officer's firearm, re-keying, and other possible issues.

Target value: zero

Rank-able: Yes

SAFETY

The smart gun technology should not contain material that contains known carcinogens.

This requirement states the long term exposure to the materials used in the construction of a smart gun system should not cause ill effects to the user.

Target value: Pass/fail

Rank-able: No

The smart gun technology should not emit known harmful emissions.

This requirement states the need for the smart gun system not to emit any type of substance or energy that would be harmful to the user.

Target value: Pass/fail

Rank-able: Yes

OTHER STANDARDS

The smart gun technology system must meet the existing applicable NIJ standards.

This requirement states the need for the smart gun system to meet or exceed any existing standards set forth by NIJ for firearms.

Target value: Pass/fail

Rank-able: No

The smart gun technology system must meet the existing applicable SAMMI standards.

This requirement states the need for the smart gun system to meet or exceed any existing standards set forth by SAMMI for firearms.

Target value: Pass/fail

Rank-able: No

ADVERSARIAL STRENGTH

The time for an adversary to defeat the smart gun technology system after being taken from an officer should be greater than 1 minute.

This requirement states the need for the smart gun system to be time consuming to defeat by an unauthorized person so that the authorized user has time to pursue other options. Time is critical when there is a firearm takeaway. If an officer is given even one minute they have been given an enormous opportunity. Now they are not hindered by the possibility that

the firearm that was taken from them could be used against them. They can use the time to regain control of the adversary, or to get assistance, or to run: what ever is the appropriate choice. Longer times benefit the officer in offering even more opportunities. Taken to the extreme, if it takes so long for an adversary to defeat the protection a smart gun system offers, then there will be no use for adversaries to take officer's firearms. This would also eliminate the reasons for stealing any firearm. Meeting this extreme may be a difficult requirement, unless designed into a product from the start. If the smart gun technology is integral to the firearm it may be possible to make the firearm incapable of being fired if the smart gun portion is defeated.

Target value: 1 minute (longer)

Rank-able: Yes

The smart gun technology system should not be defeated with tools readily available.

This requirement states the need for the smart gun system to be difficult to defeat by any means that an unauthorized person could reasonably employ at the scene of a takeaway attempt. Since takeaways are not typically planned events, special tools are not available. Common items such as knives, keys and hairpins could be available.

Target value: Pass/fail

Rank-able: Yes

An adversary must not be able to overcome the smart gun technology system in a manner that would make the firearm non-functional to the user.

It is important that an officer always be able to use his firearm. There cannot be a manner in which the smart gun technology can be overcome and thereby "jam" the firearm.

Target value: Pass/fail

Rank-able: Yes

TRAINING

The training on normal operation of a smart gun technology system should be less than 1 hour.

This requirement states the need for the smart gun system to be easy to learn and operate. Training for police is expensive because it takes officers off of duty. Once initial training is conducted no further special training should be required. Training may consist of reading the manual, and demonstrating a working knowledge of the firearm.

Target value: 1 hour (less)

Rank-able: No

Specialized training on smart gun technology system covering topics such as diagnostics and repair should be less than 4 hours.

This requirement states the need for specialized training to be given to appropriate people such as trainers and armorers. This additional training would cover topics in more depth such as technical operation, repair, and replacement of parts.

Target value: 4 hours (less)

Rank-able: No

MAINTENANCE

The smart gun technology system should be made up of modular parts.

This requirement states the need for the smart gun system design to be simple to repair, replace, and upgrade. Modular parts could make the task of repair capable of being completed by nearly anyone. They may also assist in making the technology integral to the firearm making it more difficult for an adversary to defeat the mechanism.

Target value: Pass/fail

Rank-able: No

The smart gun technology system should be tested with normal electrical bench-top equipment.

This requirement states the need for diagnostics to be able to be performed without the use of highly specialized equipment. Equipment should be able to

measure voltages, resistances, and possibly interface with a computer through serial communication channels.

Target value: Pass/fail

Rank-able: No

Modular parts should have features for easy alignment during assembly, testing, and replacement.

This requirement states the need for the pieces of the smart gun system to be easily assembled. This simplifies the product assembly, and makes repairs able to be done by people without extensive training.

Target value: Pass/fail

Rank-able: No

The smart gun technology system should have diagnostic test signals available.

This requirement states the need for features to make maintenance and troubleshooting simple by a trained person.

Target value: Pass/fail

Rank-able: No

The required routine maintenance of the smart gun technology system should require less than 1 hour per year.

This requirement states the need for the smart gun system to be maintenance free. This should include all the cumulative times of enrollment, replacement of batteries, and any other actions.

Target value: 1 hour per year (less)

Rank-able: No

The routine maintenance of a smart gun technology system must be simple enough to be performed by an untrained user.

This requirement states the need for the routine maintenance to not require special training.

Target value: NA

Rank-able: No

Routine maintenance of a smart gun technology system must not degrade the system performance.

This requirement states the need for the smart gun system not to degrade due to normal maintenance.

Target value: 1000 times a year (more)

Rank-able: No

INTERFACE

The mechanical layout of the smart gun technology system should be standardized for potential upgrade capabilities.

This requirement states the need for manufacturers to plan the firearm mechanical systems such that as incremental improvements become available they can be easily upgraded by a qualified user into the firearm.

Target value: Pass/fail

Rank-able: No

The electrical interface of the smart gun technology system should be standardized for potential upgrade capabilities.

This requirement states the need for manufacturers to plan the firearm electrical systems such that as incremental improvements become available they can be easily upgraded by a qualified user into the firearm.

Target value: Pass/fail

Rank-able: No

The information protocol of the smart gun technology system should be standardized for potential upgrade capabilities, and compatibility between different brands of firearms.

This requirement states the need for an information protocol that would allow a single key to be used on firearms from different manufacturers. This prevents users with multiple firearms from obtaining separate keys that work only on specific models or brands of firearms. This also allows for the consistency of readers to be maintained so that whatever discriminator reads a key the same result is obtained.

Target value: Pass/fail

Rank-able: No

COST

The incremental cost of a smart gun technology system should be less than \$60.

This requirement states the need for the additional cost that a smart gun technology would add to a firearm must be affordable.

Target value: \$60 (less)

Rank-able: Yes

The total cost of maintaining a smart gun technology system should cost less than \$5 per year.

This requirement states the need for the yearly costs associated with a smart gun system to be affordable. This includes the costs that a department incurs for using smart guns.

Target value: \$5 per firearm (less)

Rank-able: No

The total miscellaneous cost associated with a smart gun technology system should cost less than \$5 per year.

This requirement states the need for the miscellaneous costs of a smart gun system to be affordable.

Target value: Less than \$5

Rank-able: No

TESTING

All requirements must be sufficiently tested.

This requirement states the need for rigorous testing of smart gun systems, preferable to a standard. A self test could even be built into the firearm to perform a self analysis of its internal workings.

Target value: Pass/fail

Rank-able: No

The smart gun technology system must be trial field tested in actual use conditions.

This requirement states the need for testing in an actual use environment before the product is openly marketed.

Target value: Pass/fail

Rank-able: No

The smart gun technology system must be analyzed for failure modes and the effects of failures before fielding the system.

This requirement states the need for extensive study of the various ways a system could fail and what the effects of those failures would be, before a product is marketed. These results must be made aware to the officers so that an informed decision can be made about using the firearm.

Target value: Pass/fail

Rank-able: No

RELIABILITY

The smart gun technology system should be able to enable or disable the firearm after identifying the user with a reliability of 99.9%.

This requirement states the need for the smart gun technology to be reliable. One method of achieving this high reliability would be to implement two independent systems within the firearm, so that if either operates the firearm will discharge.

Target value: 99.9% (greater)

Rank-able: Yes

SERVICE LIFE

The lifetime of a smart gun technology must be at least 10,000 live rounds, and 100,000 enable/disable operations.

This requirement states the need for the smart gun technology to be able to function throughout the lifetime of the firearm: both live firings and check/testing functioning.

Target value: 10,000 live rounds (more), and 100,000 enable/disable operations (more)

Rank-able: Yes

ENVIRONMENTS

The smart gun technology system must operate independently of the amount of ambient light.

This requirement states the need for the technology to operate in all types of light conditions, not being dependent on the external light.

Target value: Pass/fail

Rank-able: Yes

The smart gun technology system should operate after submersion in water.

This requirement states the need for the technology to be water proof.

Target value: 2 hr. (longer) at 2 atm. (deeper)

Rank-able: Yes

The smart gun technology system should operate at temperatures up to 160 degrees F.

This requirement states the need for the smart gun technology to operate in extremely hot environments.

Target value: up to 160 degrees F. (hotter)

Rank-able: Yes

The smart gun technology system should operate down to -50 degrees F.

This requirement states the need for the smart gun technology to operate in extremely cold environments.

Target value: down to -50 degrees F (colder)

Rank-able: Yes

The smart gun technology system must operate after a drop of 4 feet on to a hard steel plate in any orientation.

This requirement states the need for the smart gun technology to survive the type of shock environment that could be expected in normal use.

Target value: 4 feet (higher)

Rank-able: Yes

The smart gun technology system should operate after vibration.

This requirement states the need for the smart gun technology to survive the vibration that could be expected in normal use.

Target value: 6 g/rms. for 30 minutes in any orientation

Rank-able: Yes

The smart gun technology system should operate after exposure to chemicals commonly used in or around firearms.

This requirement states the need for the smart gun technology to survive exposure to chemicals that might be used in or around firearm. These include items like cleaning fluids and oils.

Target value: Pass/fail

Rank-able: Yes

The smart gun technology system must operate during and after acoustical noise environments up to 130 dB.

This requirement states the need for the smart gun technology to operate in all types of noise environments, not being dependent on the external noise level.

Target value: 130 dB (louder)

Rank-able: Yes

The smart gun technology system should operate after exposure to a salt fog environment.

This requirement states the need for the smart gun to operate after exposure to an atmosphere that could be expected during a lifetime of use.

Target value: 10 days (longer)

Rank-able: Yes

The smart gun technology system should operate after exposure to sand and dust.

This requirement states the need for the smart gun to operate after exposure to an atmosphere that could be expected during a lifetime of use.

Target value: 96 hours (longer)

Rank-able: Yes

The smart gun technology system should operate after exposure to mud.

This requirement states the need for the smart gun to operate after exposure to an atmosphere that could be expected during a lifetime of use.

Target value: 96 hours (longer)

Rank-able: Yes

The smart gun technology system should operate after an exposure to a surf environment.

This requirement states the need for the smart gun to operate after exposure to an atmosphere that could be expected during a lifetime of use.

Target value: 96 hours (longer)

Rank-able: Yes

The smart gun technology system should operate after ice has been applied and removed.

This requirement states the need for the smart gun to operate after exposure to an atmosphere that could be expected during a lifetime of use.

Target value: 1/4 inch (thicker)

Rank-able: Yes

The smart gun technology system should operate after exposure to solar energy.

This requirement states the need for the smart gun to operate after exposure to an atmosphere that could be expected during a lifetime of use.

Target value: ten 24 hours cycles (longer)

Rank-able: Yes

The smart gun technology system must operate during and after exposure to radio frequency interference.

This requirement states the need for the smart gun to be operate during and after exposure to an atmosphere that could be expected during a lifetime of use.

Target value: 85 dBm $\leq$ 100MHz,
130 dBm $>$ 100 MHz

Rank-able: Yes

Chapter 6

Automatic ID Technologies

Auto ID is the abbreviated terminology for Automatic Identification. Auto ID and its related field Automatic Data Collection (ADC) generally describe the automatic collection of information or data about an object. Automatic ID includes those technologies that electronically detect and measure a unique characteristic of an item. ADC includes any technology that can be used to directly input data into a computer system without the intervention of a human. The reason these technologies are used so often in manufacturing industries is they eliminate the collection and entry of the data, both which can be very time consuming and error prone.

The same technologies are used in both fields, but they are configured differently. A few biometric technologies are also included in this area; for this report biometric technologies will be considered in their chapter. Each technology has its own specific advantages and disadvantages. This makes different technologies suited for different applications. Sometimes the technologies are used in conjunction with each other.

Radio Frequency Identification

Description

Radio transponders have been used for identification since World War II when aircraft used the identify friend or foe system. The transponder, or tag, would receive a radiated signal and then reply with another signal. Radio Frequency Identification (RFID) tags are a classification of devices which includes devices like those attached to

items in a store that will detect shoplifters by setting off an alarm if the item inappropriately leaves the store. Although those are very basic forms of a tag, more sophisticated tags operate similarly. Tags typically use an integrated data memory that can be read by radio waves. The devices are designed to be reusable and can be read whenever the tag is in the proximity of the specifically designed reader. Some tags contain pre-stored information that can only be read, while you can read and write to others. In a smart gun application the tag could be used as the key while the firearm would be the information reader and discriminator.

Examples of existing uses

Most RFID tags are used in the process of Identification. The most common application for an RFID tag is inventory control, such as identifying pallets moving in a factory. By using read/write tags, the pallets can become "smart", so that they store all the necessary information regarding the product on the pallet. Even though they are more expensive than bar codes, in many applications tags have replaced the bar code because of their read/write and reuse capabilities. Read/write tags can be read and written to by the same device, so information can be updated each time the tag is read. Companies strive for longer reading distances and faster reading times to meet the changing needs for the items being tracked. Some current applications for RFID tags are: automatic toll accounting for driving cars through toll booths; livestock, pet and zoo animal inventory; theft protection; and ski resort

tickets to reduce unauthorized use and analyze slope traffic patterns.

What is measured

The RFID tag contains information. The information is transmitted by radio waves from the tag to the reader. This information may be stored in different forms within the tag, but will normally be converted into a digital signal that is transmitted by radio waves. The information may be transmitted from ranges from near contact to several yards away. The reader then takes appropriate action based on the information received.

How it works

The typical RFID system consists of three pieces: the tag, the reader, and antennas.

The antennas are the elements that are used for transmitting and receiving radio frequency energy. Both the tag and the reader must contain some sort of antenna. The size and shape of the antennas will vary depending on the application and the specific requirements of the system. The system configuration will dictate whether the antennas will transmit, receive or do both. When the tag's antenna is within the reading range of the reader's antenna the data transmission may occur. Typically there are dead-spots within an antennas reading range. RFID readers usually depend on the tag traveling through the reading range to ensure that a proper read can be made. Dead-spots would be a concern in a firearm application, because the tag may not constantly be moving with respect to the antennas.

The tag is a transponder that contains the unique information that can be read by special purpose readers. Some tags are read only: they are manufactured with pre-stored information that cannot be changed. Other tags, referred to as read/write, contain some type of alterable memory that can be reprogrammed by the reader. Another distinguishing characteristic of the tag is if the tag needs a power source. If the tag has its own power source and does not require an

external control stimulus it is considered an active tag. Active tags are employed when a longer reading range is desired, or when data memories are used that require continuous power to retain their data. If the tag is able to operate on the power that the antenna receives from the radio frequency energy then it is considered a passive tag. Passive tags can be smaller and lighter because they do not need a battery, but they must contain memory that is not erased when power is removed. Passive tags are very reliable and have a very long life since there are no active parts, or batteries that can wear out. Passive tags place more power burden on the reader, because the reader must radiate power to the tag. Since the transmitted power diminishes quickly with distance, the shorter reading range of a smart gun application could make sustained battery life possible. Tags are relatively orientation independent at short distances. The change in orientation effects the amount of energy received which effects the reading range.

The reader is the brains of the RFID system. The reader contains both an antenna and a decoder. The reader's receiver must meet the requirements for high sensitivity, selectivity, and resistance to electromagnetic interference (EMI). After the reader receives the data from the tag it decodes the transmission using special integrated hardware or software. The reader then performs its specifically designed function for the application, such as disabling a firearm. For a passive tag system, the reader's antenna will transmit radio frequency energy and then wait for a response. The reader has to transmit sufficient energy to the passive tag's antenna to achieve the desired reading distance. For an active tag the reader's antenna only receives transmissions.

Modulated backscatter is a term used to categorize passive tags that change the radio frequency signal that the reader receives. Backscatter refers to the deflection of radio frequency energy back to the reader from any surface. For RF/ID to work, the tag must be able to change, or modulate, the signal in a

way that the reader understands. The signal's frequency, amplitude, phase, or information may change. Power is a major constraint in determining how the signal can be changed. Since all the power that is available to the passive tag is received through its antenna, only a limited amount is available for changing and re-transmitting the signal. This also limits the distance that the signal can be retransmitted. Another constraint is the required speed of the system. This determines the time that is allowed for modulation of the signal.

The tags commonly found attached to clothing and video tapes are reflective tags, whose input frequency is simply divided in half. Frequency division is a method that was developed for use in retail electronic article surveillance. Because the system is looking for a single, specific low radio frequency, it is able to eliminate: false alarms; de-tuning by weather, body fluids, or metal; failed detections. More complicated systems use a semiconductor memory in the tag, and transmit the information using radio frequency. The performance of these systems is dictated by various factors: the amount of memory contained in the tags; the speed of data transfer; the operating range; the operating frequency; the modulation technique used to transfer data.

The amount of memory available varies from around 20 bits in the read only tags to 32kbytes in read/write tags. A 20 bit memory can uniquely distinguish over 1 million tags. The advantage of more memory is that more information about the object can be stored if this is necessary, but this comes at the price of speed, frequency, and computing power. To read larger amounts of information a longer time or a higher frequency is required, and the processing power must be increased to handle the amount of data in the given time window. Reading rates up to 3,000 bytes per second are advertised by manufacturers.

The range for reading the information is another performance factor that is configured

for a particular system. Factors such as antenna configuration, transmission frequency, and power control the reading range. Range for the presently available systems varies from less than one inch to many yards. An important consideration is the frequency range of the system that should be selected by the needs of the specific application. The frequency must allow reliable reading of the information. For a firearm application it means having no dead-spots within the reading range. The frequency and power used determines the type of FCC regulations that apply. FCC regulations may protect the system from outside interference, but also may hinder the manufacturers in obtaining proper authorizations for their products.

The final performance measure to be discussed is the modulation technique used in the system. The techniques vary depending on how a digital "one" and "zero" are represented in an analog radio frequency signal passing between the antenna and the tag. Different techniques will each have their strengths and weaknesses in areas such as reliability, signal selectivity, and interference immunity. With any schemes the reader should implement error checking features to ensure that proper information was read.

Possible implementations of the technology

An RF/ID system could be implemented in a firearm as a smart gun technology by using the tag as the key and the firearm as the reader. There are many possible variations to each part of the described system. It will be attempted to give sufficient illustration to make the strengths and weaknesses of other variations apparent to the reader.

Each officer would be assigned a tag that has a unique code. The firearm acts as the reader. When the firearm is in the hand of the user, the firearm would transmit low power radio frequency from an antenna built into the firearm. If the passive RF/ID tag was within the reading range it would be powered from this energy and transmit the stored

information back to the firearm. The firearm receives the information from the tag and discriminates it. If the tag is one that was preprogrammed into the firearm as an authorized user the firearm would enable the firing mechanism. The firearm can be programmed to accept numerous codes so that multiple users can be enabled on a single firearm.

The tag would be carried by the officer in some manner. A likely location would be as part of a ring or wristband. Because of the small physical size of tags, it may be possible for a tag to be made part of, or able to connect to, existing jewelry. Although it is possible to attach the tag to other locations on the officer, the tag must be in a location so that if the firearm was taken from the user it would not still be in the reading range of the tag. This requires the reading range to be minimized to ensure that the firearm is no longer operable. For some existing commercial applications, hermetically sealed tags are implanted underneath the skin of animals. Implantation in the user's hand could be a possible implementation. Many factors such as federal approval, and civil liberties would have to be considered.

Since radio waves travel through most substances, an RFID technology does not have the same concerns as some other technologies. RFID are durable and will operate through gloves, dirt and other contaminants. Line of sight is not required between the tag and the reader. Since physical contact is not required, the opposite concern is that the reading range is too large and that a firearm taken from an officer may still be distinguished by the reader. This requires that the range of the reader be minimized for reliable reading only when an officer's hand is on the firearm.

Contention may occur when two tags are simultaneously interrogated by one reader's antenna. This could occur if the officer wants to be able to shoot with either hand and is wearing a tag on each hand. The concern is

that neither tag may be read accurately. Contention is minimized when steps are taken to ensure that only one tag is within the read range of the reader, such as limiting the read range, and controlling tag spacing. A similar problem would be if there were two firearms trying to read a single tag. This can be overcome by having readers not interrogate when another reader is interrogating. Systems are now being made which use multiple frequency scanning to sequentially read multiple tags in the same location.

Currently different manufacturers' tags are not compatible with each other. Each company has proprietary protocols used for reading their tags. This is referred to as a closed system: each company sets its own rules. The advantages to this method of operation are that each system has high security in that only a certain type of tag will communicate properly with the system, and each vendor can control the serial numbers of their tags to keep them unique, with no possibility of duplicate tags being fielded. The disadvantages are that smart gun systems from different manufacturers, using different types of tags would not be able to communicate. This means that the officer or department that uses more than one brand of firearm would have to have the appropriate key for that brand. In an open system the users have a tag that can be read independently of who manufactured the tag. This reveals the need for standards in the RFID communication protocol.

Another consideration is whether read only or read/write memory is preferred for a smart gun application. Both contain sufficient memory capacity. The read only memory contains a code that is placed into the tag when it is manufactured and cannot be changed. For this type you rely on the manufacture to not make duplicate tags. Read/write memory relies on the user to program unique codes in each tag, or have another scheme of identifying officers. This places the burden on the police departments, but also gives them much more flexibility.

Read only offers security in that the stored code is tamper resistant and cannot be changed, whereas read/write offers security in that if the code is compromised it can be changed.

Since these systems operate on radio frequencies there are two additional concerns: radio interference from an outside source, and harmful physiological effects of long term exposure to the radio frequencies. Problems due to outside interference can for the most part be reduced, but not eliminated. Having a short reading range with a large field strength reduces, but not eliminates, the probability that electrical interference would be strong enough to corrupt the communication. Physiological concerns are brought up with any radio frequency device. The relative level of field strength needed for this application is very low and should not present any health problems. The manufacturers of these devices state that the devices are intrinsically safe.

Similar Technologies

The Surface Acoustic Wave (SAW) device is a passive tag device that can uniquely encode a radio frequency signal. The difference between SAW devices and the above described RFID devices is the manner that the tag modifies the information. The implementation, strengths, and weaknesses for a SAW device are nearly identical as for a RFID device.

SAW devices are based on the theory that mechanical disturbances can propagate undisturbed on the surface of certain types of solids. They are unlike bulk acoustic waves because they travel only on the surface, not into the volume of the material. The basics of SAW technology have been known for more than 100 years, but they were not cost effective until the development of: the precise photolithographic techniques from the semiconductor industry; effective signal processing methods from today's telecommunications; antenna designs from satellite research. The use of SAW

technology eliminates the need for semiconductor components, switches, batteries and circuit boards that may fail over time and with exposure to certain extreme environments.

A known radio frequency signal can be modified by use of a SAW device. By attaching an RF antenna to a mechanical substrate with specialized properties, an acoustic wave is made to travel across the surface of the device. This unique signal can then be transmitted with another antenna to be received and decoded by a discriminator. This altered signal, made unique by the SAW device, can be used as a key. SAW devices are read only.

The SAW is composed of materials that are anisotropic piezoelectric, such as man-made lithium niobate or quartz crystal, and a small antenna. A very low power radio frequency signal from the reader is captured by the tag antenna and excites the thin film transducer on the surface of the lithium niobate crystal setting up an acoustic wave along its surface. The wave travels slowly enough along the surface of the crystal that etched metal "taps" of a second thin film can be used to send back to the reader a series of time delayed "reflections" of the original signal. This is an analog equivalent of a binary code and is made unique to each tag.

Remote Control

Description

Remote control is the technology used to operate a device from a distance. A common configuration is a small hand-held transmitter that sends a radio frequency signal to a receiver for interpretation and action. This could be used for remote disablement of a firearm. This is a slightly different philosophy than the other technologies in that the officer must perform an action instead of being automatically sensed.

Examples of existing use

Remote controls are becoming more popular on consumer products. Many examples of

remote controls can be found; TV remote controls, garage door openers, and car alarm controls are just a few. These devices are typically used for the convenience of the user.

What it measures

A remote control transmits a unique coded signal from the transmitting device to the receiving device. The information is then interpreted and used to control some operation.

How it works

The remote control requires some human action. The remote control transmits a signal, while a receiver in the device that is to be operated receives the signal. When a button on the remote control is pressed a signal is sent from the transmitter to any listening devices. Any device that receives the signal distinguishes whether it is a recognized instruction and if an action is required. Various transmission schemes are used depending on the device. Some types of the devices require line of sight between the transmitter and the receiver.

Possible implementations of the technology

For implementation into a smart gun system the remote control would be carried by the officer. The remote control could be made small enough to attach to an existing piece of equipment. The officer would press a button on the remote to enable or disable the firearm. This puts the officer in direct control of his firearm. At the beginning of a shift the officer could enable his firearm. Once the firearm was enabled it could be fired by anyone who would pull the trigger, it would not automatically sense who was using it. If someone tried to take the officer's firearm, the officer would have to push the button on the remote control to disable the firearm. Then the officer could regain control of the situation before re-enabling the weapon.

Many officers like this method of operation even though it goes against the requirement of the user being automatically sensed by the firearm. It gives them more of a feeling of control. This manual method of RF

disablement is an intermediary step to an automatic disablement. The major question is whether an officer could reach the remote control's button while another person is attempting to take his firearm. Other concerns are where to place the remote control, should it attach to the duty belt, to a badge, or some where else. The remote should not be carried in a pocket or somewhere where it could not be obtained easily. The concern about having it easily accessible is that if the criminals know that they can disable an officer's firearm by simply pressing a button, it may become almost a game to them. Contention problems could also exist with remote control devices if a single firearm is trying to listen to more than one transmitter at a time. As with other radio devices interference is a concern.

Similar Technologies

The active tag is a cross between the passive tag and a remote control. Like the passive tag it contains a unique code. Like the remote control, the active tag broadcasts the information to any discriminator that may be listening. The active tag itself is larger than a passive tag because of the need for its own power supply. The active tag is always transmitting so it does not require an external control stimulus such as pressing a button. The range of the broadcast must be controlled so that the firearm would not be enabled unless intended by the officer.

Bar Codes

Description

A bar code is a symbol consisting of light and dark bars forming a unique code. Depending on the symbology chosen the bar code can represent either numeric or alpha-numeric characters. The symbol is specifically designed for easy optical reading and automatic decoding, while also capable of being mass produced. The bar code is probably the most common method of automatic identification used today. Although the bar code has many strengths as

a technology, no suitable smart gun implementation was determined.

Examples of existing use

Bar codes are prevalent in society today. The common UPC code found in retail environments is an example of current use. The majority of retail items that can be purchased in a store have a bar code attached. These bar codes contain the unique code necessary for the identification of the item which then relates to other pertinent information such as the price. Bar codes are also used for inventory applications from tracking video tapes and library books, to computers and vehicles.

What is measured

The bar code symbol contains the unique identifying information stored as a series of bars that form a dark and light code. The information is encoded by varying the size and placement of the elements. Depending on the symbology used, either the widths of the bars or the spaces between the bars may contain the encoded information. Most of the code symbologies are based on the binary number system, and include means to verify the validity of the code read by including a control character.

How it works

The bar code can be located on many types of surfaces. These include printing the code on paper or labels, and etching on plastic or metal. The manner that the bar code is attached influences the type of reader that may be appropriate and the distance that the code can be read. The goal of reading a bar code is to discriminate between the light and dark elements. To be able to read, the bars must have a direct line of sight between the bar code and the reader. The bar code must also be visible, either with an external light source, or light from the reader itself. The light elements will reflect light while the dark elements will absorb light. The contrast between these two elements is detected by the reader's photoelectric receiver and used to decode the stored information.

Many types of readers are available depending on the application. A bar code can be read over a wide depth of field ranging from contact to several feet depending on the type of reading equipment and the size of the bar code. The least expensive reader, the pen reader, operates on contact as the pen is swept across the surface of the bar code at a constant rate. Charge Coupled Device (CCD) readers use the same types of sensors used in cameras. The image of the bar code is projected through a lens onto the CCD array. The image is scanned and converted into a digital signal so it can be analyzed and decoded. Both the pen reader and the CCD rely on externally generated light. Another type of reader, the laser scanner supplies its own light. Laser scanners have the largest range of reading distances. The laser light is diffused with rotating mirrors to scan a bar code that is within the reading range. The scan rate can be adjusted by the speed of the rotating mirrors.

The bar code orientation is a consideration in reading the code. When the orientation of the code is known the reader can be positioned to properly scan the information. If the orientation is not known or if the bar code must be able to be read in any orientation, a more complex scanning operation must be accomplished or a specialized bar code must be used. Multiple scans are desired to diminish the effects of any imperfections in the bar code.

Possible implementations of the technology

Bar codes are the most widely used form of automatic identification today. The current applications require an identification method that is very cheap, and they also allow for large scanners that account for the variation in the orientation of the bar code. Even though bar codes are inexpensive, can be placed on many surfaces, and can be read from distances from contact to many feet, no practical method of implementation was found for the use of a bar code as a smart gun technology.

The placement of a bar code on the officer is the first problem. The bar code would need to be attached to an item such as a glove that would be required to be worn, or semi-permanently marked on the officer's hand or uniform. Since line of sight is required between the reader and the bar code, it would be difficult to read a bar code placed on a uniform. Also, the scanners would have to account for a large variation in orientation of the bar code. For most types of readers either the bar code or the reader must move to make a reading. This movement could be accomplished for a bar code on a hand if the hand properly moved across the firearm's scanner. This does not seem practical. Other problems with bar codes are: the contaminants can easily interfere with the dark and light bars on the bar code, a light source would have to be available, and the durability of the optics in the reader.

Similar technologies

As with bar codes, the following technologies were not found to have a practical implementation as a smart gun technology.

The magnetic stripe is the most widely used technology for handling person-based transactions, just as the bar code is the most prevalently used method for handling item based transactions. The most common location for a magnetic stripe is on the back of some type of media such as paper or plastic cards. Credit cards, subway or airplane tickets, and identification badges often use the magnetic stripe to store information. Standards are available for reading and writing to magnetic strip cards. Data is recorded on the thin magnetic layer referred to as the stripe. This process is similar to that done with cassette tapes. To read or write from the card it is placed in a reader, like that of an ATM machine. The magnetic record/writing head must be in contact during the reading/writing process. The card must remain moving past the head. Some readers are set up for the user to 'swipe' the card, but more will 'eat' the card so that the speed is controlled. In this way

the digital ones and zeros that are magnetically stored on the tape can be read, along with the clocking information that was stored at the same time. Similar to bar codes, the implementation of magnetic stripe devices is difficult.

Smart cards are similar to magnetic strips in that they are suited for the credit card industry, but are finding other applications such as on car keys. Smart cards use a small integrated chip that contains relatively large amounts of data. Data can be added, deleted or rearranged within the smart card. Implementation of smart card technologies has the same concerns related to bar codes, or to touch memories. A different use of smart cards would be to store the enrollment information template for an officer. The smart card would then contain all the necessary information about the officer's key that the firearm would need to know. If an officer needed to use another officer's firearm that he had not been pre-programmed for, he could insert his smart card and then be able to use the weapon.

Optical character recognition is the process of electronically identifying printed text. This is often used to automate sorting and data entry of pre-printed material, such as those different looking numbers on the bottom of checks and bills. By scanning the text and recognizing the shapes of the letters, or even properties of the ink, it is possible for the reader to recognize the text. Again similar to bar code, implementation is difficult.

Touch memory

Description

The touch memory is a technology used to automate the identification of items. The device consists of a digital memory device placed in a small can. The can acts as both the reader interface and physical protection for the memory. The information in the memory can be read by simply touching the can with a reader. Although Touch Memory is a trademark for a product made by Dallas

Semiconductor, for this report touch memory is used to describe any type of device containing a memory that has to be physically contacted by a reader to read the contents of the memory.

Examples of existing use

Touch memories are used in numerous applications, typically for inventory control purposes. Touch memories can be used on production lines to store product information. Companies use touch memories placed on equipment for inventory control, and on personnel badges for access control, and even for time and attendance record keeping.

What it measures

Information stored in memory is read and used as a unique piece of data. Various sizes and types of memory can be used in a touch memory device. The memory could be a predefined serial number that is unique to that device, or it could be a read/write device. A read/write device allows the information to be updated.

How it works

Touch memories are read through physical contact between the device and a reader. The contact completes an electrical circuit so that the data can be serially read. The reader supplies both the power to the memory device and the necessary logic signal to read the memory. Attachments are available for use with the touch memory that can transmit the information by radio frequency. With this attachment the device becomes an RF tag.

Possible implementations of the technology

For a touch memory to work it must have physical contact made between the reader and the memory device. A likely implementation would have the touch memory mounted on a ring, and a reader built into the grip of a firearm. In this implementation, when the firearm was in the hand of an authorized user the touch memory would be in physical contact with the gun. The memory could be read and the firearm could be enabled.

One major strength of this type of system is that it is very similar to existing firearms, in that the user's hand must be in physical contact with the firearm for the firearm to be enabled. The concern is the type of contact that is required. An electrical contact must be made between the metal package of the touch memory, and the metal contacts of the reader. Many problems could occur that would hinder this communication channel from operating reliably. These include any type of contaminants that could get on the electrical contacts of the ring or the reader, such as dirt, oil, or blood. This also includes water that could short the contacts. Wearing gloves while firing would also be a problem with this type of device.

The major weakness of this and other similar technologies is the alignment of the touch memory device on the firearm. To make contact, the memory and the reader must be aligned. If the memory is placed on a ring it must be designed so that it will be in the right orientation to be read no matter how the user's hand is placed on the firearm. The reader must be positioned on the firearm such that it does not interfere with the normal gripping of the weapon, but still has the proper tolerances to make the necessary contact. An officer cannot worry about whether the ring has rotated on his hand, or if it is not in exactly the right position.

The unique item being sensed is the memory. Different strategies could be employed, but some care needs to be taken to ensure how memory content is controlled. Typically each memory would have a different unique number stored that would identify the user. The Touch Memory device has a serial number encoded that is controlled by the company and is unique to that device. Another scheme would be to have some part or all the memory alike for a particular set of people. This would require that the code be periodically changed in case it was compromised, but could allow organizations in the same location to use each others firearms if the need arises.

Chapter 7

Biometrics Technologies

Introduction to Biometric devices

A *biometric* is a measurable, unique physical characteristic or personal trait used to identify or verify the identity of a person. The characteristics can fall into two classes: physiological and behavioral. A physiological characteristic is a relatively stable physical feature that does not change without injury to an individual. Common physiological characteristics that are unique are fingerprint and eye retinal patterns. The behavioral characteristics are based mainly on a person's psychological makeup; unique behaviors include handwriting and typing patterns. Some characteristics like voice prints have a combination of physiological and behavioral attributes. The characteristic must be unique, that is being the only one of its kind. Uniqueness implies that the characteristic does not change over time, and is not easily copied. Physiological characteristics are considered to be more reliable because of the normal lack of variability, compared to behavior characteristics. Behavior based systems need to compensate for the variability, which may reduce the reliability of identification.

It is important to recognize the distinction between the two types of biometric processes that exist: identification and verification. Identification is the process of comparing a sample to all the templates that are stored to see if there are any matches. This process is like looking into a crowd, seeing a person, and asking yourself "Do I recognize you?". The important fact is that the person did not do anything except let you look at them (let a sample be taken of their unique

characteristic): the system did all the work of identifying the individual. In the verification process the person claims an identity and then presents a sample of their characteristic to the system. This is like answering the question "Are you who you say you are?" When Jane Doe gives you information about herself, you only need to look at her file (reference template) to verify her identity. Verification simplifies the search for identities because the system has to compare the sample that was just taken with only one previously stored template instead of all of them. The drawback of verification is that the user must do something before being verified, such as entering a personal identification number (PIN). While a PIN is used as a secure password in an automated teller machine, for a biometric system the PIN is just an index to the stored template.

Biometric systems, or devices, are automated devices that measure the unique characteristics and compare, decide, and indicate whether an identification or verification has been achieved. The living personal characteristic has to be captured in an analog or digital form. This reading has to be processed, stored, and compared with a previously stored reading for a decision to be made. A comparison score gauges how close the measurement is to the previously stored pattern. If the new reading surpasses a predetermined threshold it is considered a match. Biometric systems attempt to operate in much the same manner as humans to recognize an individual. A *reference template* containing the specific data of the characteristic must initially be stored so that a

later comparison can be done. This template is similar to you being shown a picture, or a description, of a person you will be meeting for the first time. Now when you are trying to identify a person in a crowd, you are taking a *sample* of each person you see and are comparing each of them to the reference template. Many systems will update the information in the template each time the person uses the system, in this manner the system learns of any subtle changes that have occurred in the person's characteristic. Many systems also attempt to verify that the sample taken is from a live person so that imitations can be more easily detected.

Since the system needs a reference template for each person that will ever need to use the system, each person must first be enrolled. If a person does not have their characteristic stored in a template on the system, that person cannot be identified. The manner in which a person is enrolled depends on the system. Some controls must be maintained to ensure that only authorized users are enrolled. During enrollment the enrollee submits the characteristic being measured to the machine that will store it as a template. This may require repeated samples until a template that reliably matches the person can be produced. Algorithms are used to convert the measured characteristic into a series of ones and zeros that can be used in a computerized system. The process used for conversion is normally made so that the original information cannot be reverted from the template. This relieves the privacy issues of storing the biometric templates. Templates are typically stored in a centralized system that can be accessed by the appropriate sources. Templates can also be stored on magnetic stripe cards, or smart cards, if the template needs to be available to the user, as in some verification systems.

Existing biometric systems are most commonly used for access control. They are used for access to some of the most secure military laboratories and also for college cafeterias. Biometrics do not give a positive yes/no recognition like other technologies.

They give a relative measure of how close the user matches the pre-stored template, such as what percentage of the comparison process matched. Inside the system, a threshold is set to determine what percentage of a match is required before access is allowed. If the threshold is set very high so that no unauthorized users will be allowed, then it is also more likely that a valid authorized user will be rejected. This is referred to as a false rejection, or Type I error. Conversely, if the threshold is set low so that authorized users will always be identified, then it is more likely that an unauthorized user will also be authorized. This is referred to as a false acceptance, or Type II error. These error rates are related to each other: as one improves the other deteriorates. Rates for both types of errors are specified by manufacturers of biometric systems, and are usually used to compare different products. Like any manufacture's claim, the numbers need to be scrutinized. It must be understood how the numbers were obtained, by whom, in what circumstances, and how many attempts the users were given during each transaction. A user typically needs to expect some false rejections on their first few attempts to use the system; these need to occur during training as they learn how the system obtains a good reading. Training is the most effective method to reduce false rejections.

A biometric as smart gun technology

The basic biometric smart gun system follows the lock and key analogy. The key is the biometric that is being measured. The discriminator contains one device that measures the characteristic, and another that processes the measurement. This new reading is compared with the previously stored templates that are stored in the system. A discrimination is performed to determine if a match is found so the latch and the indicators can be enabled and the firearm allowed to function.

Should a smart gun technology use a characteristic that is physiological or behavioral? Both processes are valid for use

in a smart gun system. Physiological characteristics are slow to change and are more prevalent in industry, which are both positive attributes. Behavioral biometrics have not been reliable because the characteristics are subject to change. An individual's behavioral characteristics vary more than their physical ones. This variation within the same individual can be a more difficult problem than dealing with the differences between people. They require frequent use to update the users' characteristics. A slight twist on behavioral biometrics would be to train a characteristic into law enforcement officers that could then be detected. This is briefly discussed in later sections.

Should a smart gun technology use identification or verification? The ideal method of operation for a smart gun system is an identification system. This is because the user does not have to perform any operations other than presenting their biometric. All possible enrollees are checked in an identification system without them having to claim an identity. Depending on the number of enrollees in the system this could take a long time. In verification systems the user must claim an identity, usually by entering a PIN, which for a firearm system adds complications. One complication is that the officer would have to remember to enter his PIN or his template, possibly by inserting a magnetic stripe or a smart card. This usually would be done at the beginning of duty (and simplifies the system if only one officer will use the firearm), but to use another officer's firearm in the field he would first have to remember and enter the PIN under stressful conditions. Industry surveys have shown that many people have trouble remembering their PIN under normal circumstances. Another complication is the time it takes to enter the PIN, which in some circumstance may be limited. Another complication is that the firearm would have to have the means for an officer to enter his PIN or his template. This adds to the complexity of the firearm by

incorporating an additional data entry feature such as a keypad, or a card reader.

What type of error rates should a smart gun technology have? Ideally both the false rejection rate and the False acceptance rate would be zero. Existing systems do not meet the ideal, but both error rates need to be as low as possible. For smart gun technologies the detection threshold should be available to the user. At a minimum this allows testing of the device and comparison between different devices. If the threshold is also made user change-able the amount of security added to the firearm can be determined by the user. Proper education would be needed for users to understand the implications of changing the threshold. Too high of setting could keep the officer from reliably using his firearm, while too low of setting could allow anyone to use it. Biometric smart gun systems must also be designed for first attempt identification. All statistical data must be reported as related to the first attempt at using the system.

What other topics should someone be aware of when it comes to biometrics? Today's biometric systems, designed for access control into buildings, have changes to make to meet the requirements of a smart gun technology. The following is a list of concerns that fit the majority of existing devices. 1) Existing systems are typically located in benign environments and are not movable. The robustness of systems must be analyzed for the particular environment if it greatly differs from the norm. 2) The majority of systems are verification systems that require the user to first enter a PIN to claim an identity. For typical access control situations the user is given up to three chances to properly be identified. Not operating on the first attempt may not be a problem if it only delays a user from entering a work area, but if it stops the user from performing a life critical operation the delay could be deadly. 3) The time it takes for biometric systems to perform identity checks is typically too long. For many systems it

takes a few seconds for the system to complete its work. 4) The size of existing units has not been a factor for many of their applications; the firearm application will push the devices into a new realm. 5) Existing devices are typically wired into the existing electrical system. The power consumption of the technologies is another concern. 6) The costs of biometric systems are very expensive today, often in the range of thousands of dollars. Although as more manufactures are entering the market place, and as more products are being fielded, the cost continues to drop.

A biometric technology needs to have the following characteristics. It must be reliable, rugged, fast, and accurate. It must be able to balance false acceptance and false rejection rates. It must be high performance, and inexpensive. It must be a complete system, be secure and safe, and be accepted by the user. It must recognize a living person, and not be affected by the methods of the user. It must be immune to environmental factors.

So which biometric technology is best for a smart gun? The following is a list of some of the biometric technologies that are being studied today. The following sections will describe biometric characteristics that can be measured, and review technologies that are being studied to measure the biometric.

Fingerprint

Description

Fingerprinting is the most well known method, and the accepted law enforcement method, to identify individuals. The capturing of the pattern formed by the ridges and valleys of a person's fingers is a biometric that has been studied for hundreds of years. The traditional form of fingerprinting is accomplished by making an ink impression of the fingertips using an ink pad and a piece of paper. The impressions are traditionally manually classified by a very labor intensive process. Becoming more widespread is the use of computerized

systems to automatically scan and verify a person's fingerprints.

Examples of existing use

The use of fingerprints as a means of personnel identification is increasing in popularity. The general public is more accepting of fingerprinting than many other biometric technologies. Besides law enforcement, fingerprinting is currently used for identifying a wide range of people that includes workers needing government clearances to children whose parents fear the possibility of abduction.

In law enforcement, a type of system known as the Automated Fingerprint Identification System (AFIS) is the accepted norm. This system was developed to be able to automate the existing technique of coincident sequencing used in law enforcement. This process consists of obtaining a set of fingerprints from a suspect or a crime scene and then comparing this set to every other record stored within the system. The result is the identification of a list of similar fingerprints that can be further scrutinized by hand if necessary.

The majority of fingerprint systems being developed today are verification systems. Many companies are developing systems, but there are relatively few that are ready to be purchased off the shelf. The applications that the new systems are being developed for extend past the normal security applications to the point-of-sale applications and automatic teller machines.

What it measures

The uniqueness of fingerprints is found by the unchanging and repeatable pattern the ridges create. The gross patterns have typically been classified into a number of key patterns that include loops, whorls, and arches. The smaller characteristics, known as minutiae, occur where ridges end and where they divide. Many minutia relationships can be recorded to distinguish between fingerprints by answering questions similar to the following: Is the feature the end of a ridge or

a division?; where is this feature positioned in comparison to the other features?; what are the angular relationships between this feature oriented and the other features?; how many ridges fall between this feature and the other features? The new commercial systems will determine the answer to these or similar questions to create a template.

How it works

A user's identity is recorded by an automated fingerprint system. By some means such as an electro-optical scanner that incorporates light, lens, and charged-coupled-device (CCD) image sensors, a high-resolution picture of the fingerprint is taken. The live scanned image may be manipulated to obtain a form that better reveals the minutiae. This manipulation may include filtering, edge extraction, and using features included in video frame grabbers. The minutiae are chosen and recorded by methods that are unique to the individual company's machine that is used. The minutiae are assigned a coordinate, a direction, a relationship to other minutiae, or other characteristics. For criminal identification purposes there are minimum numbers of features that must be used, these vary between countries, but is typically a number in the teens. For civilian use a lower number is generally accepted as sufficient. More features than are required are often acquired, and then a template is made after a minimum number are matched. The templates for fingerprint systems often require relatively large amounts of memory. The template is referenced to a personal identification number. Future live scan readings will be compared with this template to perform a verification when the PIN number is entered. The template is not the stored image of the fingerprint itself, but is the stored result of the comparisons done on the minutiae. The actual fingerprint cannot be reconstructed from the template.

Possible implementations

Implementation of fingerprinting as a smart gun technology has various possibilities. For an authorized user to operate a firearm, the

person's fingerprints must be available to the firearm. There are numerous places that a scanner could be placed on a firearm. The ideal location for the scanner is on the trigger. Having the scanner on the trigger conforms with the basic safety rule of the firearm not being able to fire unless there is a finger on the trigger, but could cause officers to frequently place their finger on the trigger to test that the system is operating correctly. The sizes of current triggers are thin, which would only give a small slice of the whole fingerprint. Depending on the size of the slice and the portion of the finger on the trigger, this may limit the number of minutiae that are present and limit the uniqueness of the fingerprint. This could be overcome by enlarging the width of triggers to accommodate a larger surface contact with the finger. The trigger finger of each hand could be programmed into the firearm so that an officer could fire with either hand. By reading the fingerprint from the trigger, the trigger fingers of the officers would have to remain in uniform condition: not having cuts, scrapes or contaminants interfering with the minutiae. Having the scanner on the trigger offers the scanner the protection of the trigger guard. This would assist it from the majority of abuse that may harm it.

Other locations for fingerprint scanners of firearms are on the side of the grips to read one or more of the non-trigger fingers, or on the thumb rest to read the thumb print. While a scanner on the trigger would only require one scanner for an officer to use either hand, these other locations would require a scanner on each side of the firearm to accommodate both left and right hand operation. Two sets of scanners have many undesirable attributes such as additional cost, volume, and weight. The benefit of having scanners on the side of the firearm is that more than one fingerprint can be read. This leads to a higher reliability since the probability of obtaining a good reading of at least one of the fingerprints increases.

No matter which location for the scanner is chosen, other concerns must be addressed. The most frequently used scanners today consist of optical scanners and CCD arrays. The sizes of these devices are prohibitive for use on a firearm. All manufacturers are striving to reduce the volume required by their readers and it is only a matter of time for a reader small enough for firearms is available. Other reading methods are also being brought to market, one being ultrasonic readers. Ultrasonic waves travel through many substances and may be able to read fingerprints through contaminants on the skin or on the reader. This may or may not be able to overcome the hurdle of the officers' desire to be able to wear gloves while shooting. The wearing of gloves by officers continues to be a major obstacle to keep fingerprint technology from becoming an acceptable smart gun technology.

Another complication in current systems is the time that is required to accomplish the entire reading and verifying cycle. Most, if not all, systems currently take over one second to verify a user's identity. This cycle time must be reduced to meet the officers' requirement. For a smart gun application the best fingerprinting system would be an identification system. This makes the timing requirement more difficult to accomplish by having to search each possibility. In a verification system a PIN number is entered which reduces the search for the proper user to a single individual, thus reducing the time to authorize the user.

Similar technologies

Another biometric that is very similar to fingerprinting is to use the user's palm print for identification. The concept for palm printing is identical to that of fingerprinting. The creases on a person's palm are measured. This uniqueness could be recorded, and a person identified, by use of a scanner in the firearm's grip.

Another new biometric that is beginning to be brought to market is identification of sweat

pores on the fingertips. One system uses a sensor smaller than a postage stamp to record the ridges and sweatpores on the fingertip. The silicon sensor contains the equivalent of thousands of contact sensitive switches. The algorithms are also supposed to reduce the time of verification to less than 100 ms. All of these attributes would improve the performance over the optical systems.

Voice Recognition

Description of Voice Recognition

Voice recognition as a biometric is becoming increasingly popular. Individuals may be identified by recording their voice and distinguishing differences in their vocal tract characteristics. The field is separated in to various categories to separate the identification of an individual speaker from a group, and to separate a set of predefined words from any word that may be spoken.

Examples of Existing Use

The most well known use for voice systems is probably the telephone companies latest products. Now a person can dial a telephone number by speaking the persons name into the telephone receiver. These names and numbers are recorded into the telephone system during a short training session. The number of people that are allowed to be stored are limited. Using this system saves the user from memorizing commonly called phone numbers.

A market that has even larger growth potential is speech dictation into computers. For handicapped individuals and for numerous industries this offers great potential for increased productivity. Even inexperienced typists could enter characters quickly if the computer understood the spoken word. The goal for dictation is to understand continuous speech (where words are run together into phrases) as compared to discrete speech (where slight pauses are required between each word).

The most common use of voice verification, as with most biometric technologies, is for

access control in to secure areas. Many specialized algorithms for many different applications are being worked on by universities, laboratories, and private industry.

What it measures

The goal of voice recognition technologies is not as much to recognize the sound, but to recognize the object that produced the sound. The focus is on the characteristics that produce the speech. These characteristics include the various speech producing mechanisms along the human body's entire vocal tract: the throat cavity, the nasal cavities, and the mouth itself. Since each person's physical characteristics are different, even a well-trained mimic could not jeopardize the system.

Voice systems are separated into two classes: speaker recognition, and speech recognition. Speaker recognition attempts to discern the person from their spoken words, in other words determining *who* said it. Speaker recognition can be either identification or verification of an individual. Sometimes the terminology gets confusing because different words are used. Sometimes *voice* is used for *speaker*, and sometimes *authentication* is substituted for *verification*. If the speaker recognition system can recognize the speaker no matter what he says then it is a text independent system. In a text dependent system, recognition can only be done when the speaker says a word from a small set of words. The ideal speaker recognition system would be a system capable of identifying any speaker (speaker identification) saying any phrases (continuous speech) which includes any type of word (text independent). These systems are not available.

Speech recognition, also known as text recognition, is determining *what* was said. Speech recognition can be either text independent or text dependent, depending on the limitations set on the words that will be recognized. Speech recognition also has other factors that affect recognition. The

ideal speech recognition system would be system capable of working with any speaker (speaker independent) saying phrases (continuous speech) which include any type of word (text independent). These systems are not available. What is available are systems that are highly constrained: speaker dependent, discrete speech, and small vocabulary.

How it works

The user's voice needs to be recorded. This requires a microphone and some means to turn the analog signal into a digital signal that can be processed. The microphone needs to be placed very close to the user's mouth to minimize background noises and directional influences, or at a minimum placed at a consistent distance in a consistent environment. Processing consists of a wide variety of filtering, scaling, and compression to enhance the utterance, and retain all the characteristics useful for comparing to the previously stored template. Some type of algorithm is used to match the processed utterance to the template and a decision is made as to if it is a recognized word, or user. The types of algorithms used are very complicated and often proprietary.

The goal is to be able to recognize speech and speakers based on the physical characteristics of the vocal tract. Different sounds are made by different parts of the vocal tract: the lips, tongue, roof of the mouth, throat, and even the nose, are all involved in the sound of the utterance. Over time a person's voice will change, and an adaptive system should be used. A great amount of research is being done on both speech and speaker recognition systems.

Possible Implementation

Implementation of a voice recognition system follows the basic analogy of the smart gun system. The person's voice, or what the person says, is the key. A microphone mounted on the firearm receives the voice input and sends it to the discriminator. The discriminator then attempts to recognize the

speaker, or the utterance. If the recognition is completed successfully then the latching mechanism is enabled.

In this system the firearm must be able to hear the user's voice through the microphone. Existing systems require a person to talk directly into a microphone. This increases the signal from the voice of the user compared with any extraneous noise from the environment. If the environment of the user is so noisy that the user cannot be heard then the system would not be able to recognize the user. The position of the microphone is critical to make these systems operate reliably.

A user would have to be enrolled by speaking into the system multiple times until the system can recognize the characteristics of his voice. This may be done by repeating a small set of predefined words multiple times, or by reading a portion of selected text. The process depends on the particular recognition algorithms being used, and could be a very short process or it could take a long time to totally recognize a user's voice.

A great deal of work is being done by companies involved in voice recognition work. There are commercially available single-chip products available, but they use simple algorithms that are not as reliable. Most systems are computer based, some requiring large amounts of processing power. For the firearm application the size of the processors could need to be reduced to fit within a firearm.

A smart gun system could be based on a text dependent system, where the firearm would recognize a predefined list of words. In this case the officer would call out a "password" that the firearm would recognize, but there is some concern of whether the officer in a highly stressful situation would remember the "password", if he could articulate it accurately, and if the system could recognize his voice due to stress related changes. This is a good reason for a text independent system that recognizes any words. So as the officer

is speaking the firearm is constantly enabled. Also this is why the system should recognize the characteristics of the voice and not the sound of the voice. Only the most sophisticated algorithms attempt to take into account any changes in the voice due to stress, or hoarseness.

Time to recognize the individual is also a concern. Many systems take between 2 and 15 seconds to authorize a user in a verification system. This time must greatly be reduced for a firearm system based on voice recognition to work.

Hand Shape

Description

Among the unique characteristics of humans are the lengths of their fingers. Scanners that verify the three dimensional representation of a user's hand are among the most common biometric device used in access control today.

Examples of existing use

The majority of uses for hand verification readers have been for access control. The technology has been used for nearly two decades. Readers can be found in locations from college cafeterias to nuclear facilities. Sites for hand recognition continue to increase because of the ease of use: simply placing your hand flat on a surface. Another reason for popularity has been the readers low error rates: an authorized user is rarely rejected.

What it measures

A hand recognition device measures and verifies characteristics of the human hand. Items such as the finger length, width, area, and height can be measured. One dimensional to three dimensional systems are possible.

How it works

The characteristics of fingers can be measured by various methods. The simplest method is to use photoelectric cells to measure the length of each finger. A more common method is to use a CCD camera to

capture the complete outline of the hand; the third dimension of hand height is also sometimes recorded. This captured image is measured using the software algorithms within the device. The result is compared to the result that was stored during enrollment. Since these are verification systems the user entered PIN determines which stored template is used for comparison. The size of an individual's hand is not so much unique compared to any other hand, but unique when compared to the characteristics stored with the associated PIN. The template for hand geometry recognition is small compared to many other biometrics.

Although other methods have been tried, the successful approaches have been to lay the hand flat on a plate with fingers placed against pins for alignment. The less successful approaches include capturing the hand's details while the hand is held in free space, reading the creases on the inner side of the fingers, or laying the hand flat with no alignment pins.

Possible Implementation

Implementation of a hand recognition would require a method to determine the hand's characteristics while gripping the firearm. Having a repeatable manner in which characteristics are measured is the primary concern. Officers are well trained and probably have a more repeatable grip than many other firearm users. Even so, alignment features would most likely be necessary to even further enhance the repeatability of the grip. Some officers use contoured "combat grips" today, but other officers dislike them or are forbidden to use them on service firearms. Whatever alignment method is chosen it needs to accommodate both left and right handed users.

There are many reasons that the method of obtaining a hand geometry measurement on a firearm is more complicated compared to some other applications. These limitations make the job of using hand geometry

measurements for identification, rather than verification, even more difficult.

On a firearm system it is difficult to measure the hand in three dimensions, this limits some of the information available. After the fingers are aligned, then the question arises about the uniqueness of a user's hand when it is wrapped around a curved surface such as a firearm grip. Existing systems measure the hand when it is held with fingers outstretched. The successful use of systems has depended on this approach; no research was found on the uniqueness of measuring finger length on a curved surface.

Sensors must be placed on both sides of the grip to accommodate both left and right handed users. CCD cameras usually have focusing optics that do not fit this application. Photoelectric cells have potential if an array of sufficient quantity is used to measure the small changes in the measured characteristics. The frequency of light used must also be considered. Visible light will be effected by the ambient light conditions. Some other frequencies will have some percentage of light absorbed into the finger causing other variations in the measurement such as blood flow and oximetry.

Another approach would be to use contact sensors. The contact sensors that are being developed for fingerprints could easily be adapted to measure the contact surface of the fingers. Again the concern is that the contact surface is not the same as the outside dimensions of the finger, and that changes due to other factors may change the measurements. Pressure sensors would operate like contact sensors, but also measure the amount of pressure being applied at each location. Capacitive proximity sensors could also be used to determine the mass characteristics of a person's hands; this is discussed in the section on capacitive proximity sensors.

No matter what method of measurement is used it must be reliable and repeatable. It has to be able to measure the finger dimensions

and not other attributes that change like internal blood flow, the length of fingernails, or whether the user is using a one or two handed grip. Also the matter of wearing gloves is again a concern because gloves change the appearance of the finger characteristics. One thing that should not affect the readings are environmental effects such as cold, hot, wet, dry, or dirty hands.

Signature Dynamics

Description

A person's signature has been used for years in the banking industry as of means of identification. Signature recognition is a behavioral biometric that is used to verify a user's identity based on their handwritten signature. It is included in these discussions as an example of how a behavioral biometric could be used in a firearm application, specifically a person's draw characteristics.

Examples of existing use

Today signatures are being electronically captured by overnight delivery services. Although these devices are not used to recognize the signature, systems are on the market that will verify the signature by comparison with a stored template. Since signatures are already an accepted form of identification much work is continuing to develop improved systems. Another "signature" based system looks at the rhythm of keystrokes on a computer keyboard to verify not only a password but the person typing the password.

What it measures

Signatures are typically visually compared with a signature card or another known valid signature. Visual comparison only allows the general formations of the letters to be compared, so clever forgeries or photocopies will be similar or identical. Other traits of a person's signature can be characterized by electronically capturing the signature. These traits such as the amount of pressure at various points, the rhythm, and the speed and acceleration of the pen strokes make a

signature nearly impossible to duplicate. In the same manner the characteristics of an officer's grip, draw, and trigger pull may visually look similar to other officers but may have special attributes unique to that officer.

How it works

Depending on what is being measured various types of sensors are used to measure the speed, or location of an item at any point in time.

Possible Implementation

For a firearm system, are there behavioral attributes that could be measured that would verify one officer from another? Or could officers be trained to perform a special action, such as flexing a certain muscle, that then could be sensed and used to enable the firearm? The answers to these questions are unknown, but it is possible that traits could exist. The drawing of the firearm from the holster, the manner in which the grip is squeezed, or the way that the trigger is pulled, could all be compared to how the officer normally performs these actions.

Since these are all behavioral, not physiological traits, the trait may change due to factors such as stress, or injury, or simply be forgotten. Also whatever trait is measured would have to be valid even if the firearm was not drawn from the holster but in any circumstance that may arise. This is where a trained simple action performed by the officer may be a very good option.

Biometrics Above The Neck

Description of the head's biometrics

Many unique features of the human are found on a person's head. These are what each of us typically use in identifying each other on a daily basis. These features include recognizing the face, the eye, and even the ear. Although the manner in which these might be used in a handgun is not obvious, they may have better applications in rifles.

Examples of existing use

The most successful of this category of biometrics is the retina scan. This scanning of the retinal vascular pattern on the back surface of the eye provides some of the highest security possible. New systems are becoming available for security applications which base verification from other facial features.

What it measures

Various parts of the head can be measured and reviewed for unique characteristics. Eyes have many unique qualities from the color, and shape, to the routing of the blood vessels inside. Ears have different shapes and curves. Faces have different bone structure, height to width ratios, and temperature profiles. Using various techniques, all of these characteristics can be measured and compared to previously stored images to make a decision of a person's identity.

How it works

Facial feature recognition records the face of the user and then compares certain features each time the user attempts to use the system. Using video cameras and frame grabbers a representation of a person's face is captured. The face is then analyzed using advanced image processing techniques to map the facial geometry. Neural networks, that attempt to mimic the way the human brain learns, then classify the faces so they can be recognized. These systems attempt to map the facial geometry in such a way that changes like beards, hair styles and color, shadows and lighting, head position, and expressions do not affect the recognition process.

Facial thermography is another method to recognize the face. The heat being released from the face, caused by underlying vascular pattern, is mapped. Manufacturers claim that this pattern is different for each individual,

even twins. Using infrared imaging, related to the kind used in night goggles, the heat patterns are stored and used to recognize the individual.

Retinal scanning measures the vascular pattern on the back of the eye by shining a weak infrared light through the pupil and capturing the reflected pattern. This pattern can be analyzed and compared to previous readings to verify an individual. These systems are among the most reliable in recognizing users and not accepting unauthorized users.

Iris scanning is another method of verifying an individual. The colored part of the eye contains characteristics known as contraction furrows, striations, pits, collagenous fibers, filaments, crypts, serpentine vasulature, rings, and freckles, all of which make each iris unique. A video picture of the iris is stored and compared to a previous version through algorithms and image processing techniques.

Ear detection is a relatively newcomer to the biometric field. Images of a person's ear are used to make a map that can be used to verify the person.

Possible Implementation

Implementation of these types of biometric identifiers in a handgun may not be possible because of the different locations of the head and the firearm. There may be potential applications for firearms with scopes. A scope offers the eye alignment possibilities that are needed for the retina and iris scanning systems. By looking through the scope the necessary capturing of the eye details needed could be taken without any notice from the user. The drawback of eye systems used in security applications thus far have been the user's fears of holding their eyes up to the scanning devices.

Chapter 8

Miscellaneous Technologies

Many different devices have been used for centuries to only allow authorized persons access to protected items. Still today, mechanical locks on doors are the most prevalent. In this section various items have been placed which did not fit into the other categories of technologies.

Magnetic Encoding

Description

Magnets have a north and south pole, and attract ferromagnetic materials. These properties can be used in different implementations of a smart gun. Hall effect sensors can be used to sense magnetic poles, such as a code produced by a series of magnets. Alternatively, the force produced by the magnet could also be used to physically move mechanisms to enable or disable a firearm.

Examples of existing use

Magnets are used in so many places that people forget that they are present. Refrigerator doors are covered with advertisements attached to small magnets. Magnets often hold that same door closed. Magnets are used in magnetic padlocks, rpm sensors, and kids' toys. A magnetic device called the Magna-Trigger was one of the first commercially available smart gun technologies.

What is measured

In general terms the magnetic field strength, or the magnet's attractive force, is being measured. The north and south poles of ferromagnetic materials, such as iron, are the result of the alignment of the individual small

magnetic fields produced by spinning electrons. Electricity is produced by the movement of electrons, thus electricity and magnetism are related. This relationship led to the invention of electrical sensors able to measure the magnetic field strength.

How it works

Magnetic reed sensors have been used for years to act as a simple magnetically activated mechanical switch. Hall effect sensors measure the effect of a magnetic field placed on an electrical conductor in the sensor. The electrical current in a conductor is produced by moving electrons. As the electrons pass through a magnetic field they are attracted or repelled to one side of the conductor. This change in current density can be measured by a hall effect sensor.

Possible implementation

There are two general methods of using magnets in a smart gun device. One is to use the magnet's attraction to ferromagnetic materials to physically move an item. Another is to use reed switches or hall effect sensors to read a code produced by magnets arranged in a specific pattern.

One of the first commercially available smart gun technologies involved the use of magnets. The Magna-Trigger used a magnet on a ring to physically move a lever in the grip of a revolver. The movement of this lever would enable or disable the firearm. The complaint that officers have said about this device is that the orientation of the user's ring on the firearm grip was critical. If the ring rotated on the finger, or if the user's grip was not normal, then the firearm would not operate.

Although it was not possible to validate these complaints they are very understandable. If the magnet is localized on the ring, then if the ring rotates it would not be in the proper position to operate the lever. Also since magnetic forces between poles are inversely proportional to the square of the distances between them; if the placement was not accurate the magnet would not be strong enough to attract the lever. A very strong magnet would have to be used. Of course, gloves would hinder the operation. Another problem with this simplistic approach is that the key is not unique: any magnet placed in the proper spot would enable the firearm. The best strength of this approach is that there are no batteries needed: all the energy is supplied by the magnetic forces.

The second type of implementation uses magnets placed in a known orientation on a ring as a unique code. The code can be read by using hall effect, or similar types of sensors, in the firearm grip. The more sensors that are used, the more likely that the alignment problems can be overcome, but it also increases the cost. The ring still could rotate on the users finger if not designed correctly. The physical size of the magnets could limit the number of unique codes that could be placed on a ring, or make the ring unusually large. The magnets also must be strong enough to create a measurable magnetic field strength, and they should be permanent magnets to alleviate the concerns of the magnets becoming demagnetized due to certain severe environments. A handgun using a magnetic technology is being produced by Fulton Arms, Houston, Texas.

Locks

Description

A lock is a device used to hold, or secure, an item. There are numerous types of locks having different means of entering a key to verify a user. The most common types are key and combination locks.

Examples of existing use

Examples of locks surround each person, although some are not always thought of as locks. Locks can be found on almost everything that needs in some way to have limited access. Houses, cars, desks and computers all have locks. Locks are accepted methods of securing items.

What it measures

There are different kinds of locks each having a distinct means of controlling its opening. Key locks measure the key cut: the amount of material removed from the key. Combination locks measure the knowledge and input of a sequence of numbers or letters.

How it works

Each lock must distinguish the appropriate type of key. The typical key lock used pins and tumblers to create a sheer line that allows rotation when the proper key is inserted. Mechanical dial combination locks consist in a series of gated wheels. When all the gates are aligned, the lever and fence will drop in to the gates and allow the latching mechanism to open. Other technologies employed in locks like magnetic key actuated, keypad operated, and push-button operated, all use different keys and discriminators but operate on the same principles.

Possible implementations

Numerous implementations of mechanical locks on firearms exist. All of these demand a user action to unlock the lock. A concern with each of these implementations is having the key available, and the time and skill it takes to insert the key. A major strength of these technologies is that they could be made very reliable and require no batteries.

Key locks on firearms could be easily implemented. By simply inserting a key, the lock could enable or disable the firearm. Implementations of combination locks are similar. Typically for a firearm application a push-button combination is assumed, instead of a dial. This type of mechanism would assist an officer in storing his firearm, but could cause problems for a police officer on

duty. For these implementations the duty officer would have to find the key or remember the combination, then he would have to insert the key or combination into the firearm before he could use his firearm.

The time, and the mental and physical facilities, it takes to do these operations would be unacceptable for an officer facing a shooting situation. The key would have to be available for use. The combination would have to be remembered. Inserting these into the firearm would have to be done in any environment: the dark, the rain, or snow. The environments could hinder the officer, or it could hinder the operation of the device itself. Many people have experienced the difficulty of inserting a key in the dark, or having ice or dirt build up inside a lock. Some say for a combination lock time could be reduced by entering all except the last number. This would decrease time, but also reduces the level of security for the officer. Now the adversary would have a higher probability of opening the lock by entering the last number correctly, and if the officer or an adversary hits the wrong button then the sequence must start from the beginning.

A major problem with these devices is that after the firearm is enabled, it can not automatically disable itself when it leaves the officer's hand. An automatic disable feature could relatively easily be designed into a firearm, but then the enabling time must re-occur. If the officer just was struggling for his firearm and was able to regain control, the last thing he wants to have to do is take out a key to insert into the firearm and then have to fight over the key. This is supposing that the officer did not mistakenly leave the key in the firearm and the adversary was able to re-enable the firearm.

Lanyard

Description

A lanyard is a cord that is attached to an item. In this context it is a cord attached to a key

that is inserted into the firearm which becomes disabled when it is removed.

Examples of existing use

Lanyards are attached to numerous items, but are often referred to under a different name. Lanyards have been used in the past for firing cannons, and are still used to attach weapons to military aircraft. Another use for a lanyard, known commonly as ripcord, is for deploying parachutes.

What it measures

The lanyard itself does not measure anything, but controls the occurrence of something when removed.

How it works

A typical operation for a lanyard is to start a sequence of events when it is removed. The lanyard will consist of a device at the end of the cord, which can be as simple as a pin, that keeps the sequence from starting. This pin may keep an item from moving, or trigger another device to start.

Possible implementations of the technology

A lanyard as applied to a smart gun would disable the firearm when it was removed. The firearm would always be enabled as long as the lanyard was in place. When the lanyard was pulled out, the firearm would become inoperable. Depending on how it was implemented the pin could be reinserted for immediate use, or require some disassembly of the firearm to re-insert the pin.

Typically lanyards are not unique: a simple pin. There is nothing prohibiting the use of a 'keyed' pin, that would operate much like a key lock. This would add security by making the lanyards be keyed to a single, or group, of firearms.

The concern of a lanyard device is if the officer can remove the lanyard if an adversary attempts to get his firearm. The lanyard could be permanently attached to numerous places on the officers uniform so the firearm would only be allowed to extend to the normal reach of the officer. Another concern

is that the adversary could pull the lanyard to disable the officer's firearm.

Capacitive Sensing

Description

Proximity sensors have been developed with the capability of sensing when an object is nearby. This knowledge can be helpful to avoid collisions between objects. Various types of proximity sensors are available, one using capacitance as its measure.

Examples of existing use

Capacitance proximity sensors are used in various industrial applications. The common use is in controlling a process when a product is close, or to position the product for the next operation. The sensors are also being developed for avoidance systems for automated vehicles and robotic arms.

What it measures

Capacitance is the capability of an object to store electric charge. A capacitance sensor measures the change in its stored charge as it is brought nearby or in contact with another object.

How it works

There is electrical capacity between any two electrical conductors. This capacity varies with the area of the conductors, and the dielectric properties of the space between them. The capacitance sensor generates a known electric field in the space between its conductors. As the sensor is brought near another object the changes in the electric field are measured in terms of the change in capacitance. The sensor needs two electrodes, although the object being sensed can act as one of the electrodes. Two electrode configurations allow a better defined starting point, and make the sensor less sensitive to the electrical properties of the object being sensed.

Possible implementations

The state of the art in capacitive sensing today is only sensing if an object is nearby, and some gross attributes about the object: it

cannot identify the user of a firearm. Although it is not possible today, one of the goals of proximity sensing is to be able to make a three dimensional map of the object being sensed. This would allow machinery to know exactly what is approaching and how it should be handled.

Since the gross size of an object can be measured it would be possible to develop a firearm that would be able to detect a small hand, such as that of a child, on the grip as opposed to a large hand. This even has problems though if other materials would be around the firearm, or the child used two hands.

Using a different approach, the proximity sensors could be used not identify the user, but require the user to know something specific about the firearm. Such implementations can be visualized as secret switches on the grip that can not be seen. Some of these switches would have to be closed (by covering them with parts of the user's hand), while others would have to be left open. If taken to the extreme, with an infinite amount of sensors, this would be the same as measuring the user's hand size, or finger length. This approach could also be implemented with pressure sensors, or contact switches.

A capacitive sensor could work in conjunction with other technologies by telling the firearm when to turn on or off when a hand is present. This could be useful to battery operated technologies that need to be turned off when not in use.

Other types of proximity sensors are available but are thought to have less potential as smart gun technologies.

Color Sensors

Description

Color is not a physical quantity, but a visual phenomenon. This makes color more difficult to measure than some other items. Since many items are purchased based on

their color, manufacturers realize the importance of accurate sensing of the colors. Sensors that determine the color of items have been developed to automate the inspection of colored items.

Examples of existing use

The majority of uses for color sensors are in factories to detect the presence or absence of an item. Items range from the color of a wire going into an electrical connector, to making sure all the ingredients were placed on top of a frozen pizza.

What it measures

Color sensors measure the amount of light in specific frequency bands. Normally, color is discussed in terms of intensity, hue, and saturation. Human perception of color is subjective, different combinations of frequencies can make the same visual effect. Sensors can objectively measure color.

How it works

The typical color sensor is a photosensor and a set of filters. The photosensor is a device that has electrical properties that change when light is incident upon it. When placed behind a set of filters these semiconductor devices exhibit changes that are directly related to the amount of light passing through the filters. The filters are chosen to match the range of colors being sought. Many sensors include a

red, green, and blue filter to describe the attributes of the color. Since CCD color cameras have become available there are also methods being used to use them as the input device to sense the color.

Possible implementations

For color used in a smart gun technology system, the key would be a color that the firearm could recognize. This area of color would have to be in a location that a color sensor on the firearm could see. Possible locations for an area of color would be on a ring, or glove that the officer was wearing. Each officer could have a different color. The firearms would distinguish the color's attributes and compare them the authorized colors stored in the firearm's database.

Concerns that would have to be overcome include where the color is located on the officer. Industrial sensors use their own light source so that they are independent of the ambient light, this could be difficult in firearm use. Also, there must be a direct line of sight between the sensor and the colored item. If anything, including dirt, gets in the way the sensor may not operate. Also the color, like any good key, must not change. The color cannot fade, or be bleached out from ultraviolet light, or multiple hand washings.

Chapter 9

Latching Mechanisms

The latching mechanism is the third piece of the lock and key analogy. It is the physical mechanism in the smart gun system that allows or inhibits the firearm from being fired. The term latch is used to infer that the lock must be intentionally enabled (by the discriminator), but can be automatically reset. As discussed in the preceding sections the key and the discriminator must work very closely together. The latch must work together with the discriminator and the firearm's mechanisms. When a user has been authorized by the discriminator the latch must be notified. While the latch only has to be activated by the discriminator, it must operate closely with the internal workings of the firearm. The latch needs to be matched to the characteristics of the firearm. The implementation must be such that the firearm's characteristics, such as the trigger pull, still meet existing standards for an authorized user.

Latching mechanisms are separated into this section of the report because it was determined that it was not a task of this project to determine an implementation for a firearm latch, but only possible mechanisms that could be used for latching. Each firearm has a variety of pieces in their mechanism. Over the years the designs have been improved to make each mechanism operate both efficiently and reliably. It is the responsibility of the firearm manufacturer to understand the firing chain of their individual firearms insofar as they know the best manner to incorporate a latch into a particular model. There is not a single latching mechanism that can be easily placed in every firearm. In this

section of the report an overview of different latching philosophies, a description of some design options, and some prime moving devices will be discussed.

The latch, in a security sense, is used as part of a delay system that impedes the use of the firearm. The latch is an important part of the entire smart gun technology system. In cooperation with the discriminator the latch provides the actual locking of the firearm. It must be remembered that given sufficient skill and time all locks can be defeated. The goal is to have the latch portion of the smart gun technology system to match the capabilities of the rest of the system. There is no sense in making the latch any weaker or stronger than the rest of the system.

Throughout these discussions the requirements for the latch must be considered. Besides those discussed above, there are other considerations. The material properties of the latch must resist not only normal use environments, but also an adversary's attempts at defeating the mechanism. This includes everything from a very strong pull on the trigger to the use of external tools. It must be determined if the latched firearm should lock the trigger from being pulled or simply allow it to move freely without engaging any other part of the firing chain. The user community needs to be consulted on these decisions. The latch must be able to disable a firearm no matter what state it is in, for example either single or double action. The latch must not be able to act like a second trigger. No matter what state the firearm is in, the enabling of the

latch must not cause the firearm to discharge a round, unless the trigger is intentionally pulled.

For this discussion, a simplified firearm firing system is used. This will bring out the main points without being burdened by explaining the differences between the various types of systems. The critical components, or elements, in this generic firing chain are the loading (ammunition feed), trigger (cocking device), the spring (energy storage device), and the firing pin (bullet initiating device). These components must be intact and functional in order for a handgun to fire ammunition. It is assumed that the design of a handgun is such that, if any one of the critical components of the firing chain is missing or nonfunctional, the firing chain is severed and the weapon is inoperable. To prevent stolen firearms these pieces must be so integrated into the design that if they are removed or modified the firing chain can no longer function, or it takes so long to do the modifications that it is not worth the effort. Therefore, a smart gun latch must be capable of affecting one or more of these critical elements in a manner that breaks the firing chain and prevents unauthorized use of the weapon.

LATCHING METHODS

A smart gun latching mechanism must be capable of affecting at least one of the critical elements in the firing chain. Latching may be achieved with one or more of the following philosophies: Critical Element Restraint, Critical Element Positioning, or Critical Element Destruction.

Critical Element Restraint. Each of the elements in the firing chain must be able to move to complete their action. If the motion of a critical element within the firing chain is restrained, the smart gun would be prevented from functioning. If the element restraint is removed, the weapon is capable of firing ammunition. The advantage of this method is that it may be fairly simple to block the

motion of one critical element. The disadvantage of this type of latch is that even with the critical element restrained the element is still present in the firing chain. This may compromise the firearm surety.

Critical Element Positioning. Each element has a role in the firing chain, if that element is not present that function cannot take place. One or more of the critical elements can be positioned such that it is no longer a component of the firing chain to make the smart gun nonfunctional. Once the critical element has been positioned outside the firing chain, any motion of that critical element shall have no effect on the firing chain. If the critical element is repositioned into the firing chain, the handgun is functional. The advantage of this philosophy is a higher degree of surety because the critical element is completely removed from the firing chain. The disadvantage of this method is that the system design may be complicated, which could compromise functional reliability.

Critical Element Destruction. One method of removing an element is by having it destroyed. If at least one critical element is irreversibly destroyed, the weapon is rendered permanently inoperable. The advantage of this method is that, once the element has been destroyed, the smart gun is absolutely nonfunctional. The disadvantage is that the latch is irreversible and the smart gun would be permanently disabled, which is undesirable for law enforcement applications.

LATCH DESIGN

There are an infinite number of mechanism designs that could function as a latch. However, each latch design will utilize energy in a specific way, regardless of the form of energy used, which may be mechanical, electrical, or a combination of both. The following latch designs are categorized in terms of the way they use energy and not in terms of a specific mechanism design.

Continuous Energy Device. One method of locking is achieved with a continuous supply of energy. If the energy supply is stopped, the system becomes unlocked. An example of a continuous energy device is a mechanism that is locked (or held unlocked) with a powered solenoid. When solenoid power is removed, the mechanism changes its state. Another example is a push-button mechanism that requires continuous hand pressure to maintain the unlocked condition. The advantage of this type of device is that the locking mechanism design is simplified. However, increased power consumption becomes a concern.

Energy Storage Device. Another method of locking is achieved with an energy storage device such as a spring, a permanent magnet, or a capacitor. Examples of this type of device are a ratchet mechanism that maintains position using a spring, repelling magnets, or stored charge in a capacitor. The advantage of this device is that it requires only a short pulse of energy for locking, or unlocking, to occur. However, the introduction of the energy storage device into the latching mechanism may increase system complexity. What is more important, a new critical element has been introduced and the mechanism that releases the energy must be carefully scrutinized. Now any false signal, environment, or accident that can release the stored energy, performs the same function as the valid method of energy release.

PRIME MOVERS

A prime mover is any device that supplies the motion required to actuate the latch system. In general this will be a device that converts electrical energy to mechanical motion, however, a prime mover may also take the form of a person's hand. (One method of ridding the battery, or at least minimizing the power required, may be to use the energy from the pull of the trigger, or from the gripping of the weapon, to be the prime mover.) There are many types and manufacturers of prime movers and this

section is not intended to be review of all possible prime movers. Information presented in this section is based on prime movers selected for their small size, which is one of the most important characteristics for a handgun application.

DC Motors. These are electromagnetic actuators characterized by small volume, low power consumption, and high speeds. In addition, these actuators are relatively low in cost. Another advantage of DC motors is their drive signal; they require only a simple DC voltage for operation. The primary disadvantage of these motors is that to achieve accurate motion control, a feedback system is necessary, which increases both volume and system complexity. Another disadvantage of DC motors is that they tend to have low torque output. Some details follow. Volumes of 0.06 cubic inches can be achieved and no-load current and voltages on the order of 12.5 milliamps and 3 volts, respectively, are typical. Speeds as high as 14,000 rpm can be expected. Typical prices for quality DC motors are in the tens of dollars. Stall torque to volume ratios average approximately 0.9 in oz/in³ for these motors.

Stepper Motors. The primary advantage of stepper motors is their ability to provide accurate motion control without any external feedback system. These motors also have good torque capabilities. The disadvantages of stepper motors include their larger size, higher power consumption, and higher cost. Another concern of stepper motors is their drive signal and the accompanying electronics. Steppers require a drive signal consisting of two square waves 90 degrees out of phase and the added electronics required to produce this signal can consume additional volume. Some details follow. Stall torque to volume ratios average approximately 1.7 in oz/in³, which is almost twice that of DC motors. Volumes of smaller size steppers are on the order of 0.22 cubic inches. Typical no-load drive current and voltages are 390 milliamps and 28 volts,

respectively, per phase. Their cost can range as high as hundreds of dollars.

Piezoelectric Traveling Wave Motors. Piezoelectric traveling wave motors convert electrical energy directly to mechanical motion by the piezoelectric effect. They are characterized by high torque output in a small package, which is their primary advantage. Another very important characteristic of piezoelectric traveling wave motors is that they require large frictional forces to convert oscillations of the piezoelectric element to rotary motion of the output shaft. This frictional drive results in a high detent torque, which is the holding torque a motor possesses with no power. The high detent torque of piezoelectric traveling wave motors makes them an excellent candidate for an Energy Storage Device. In addition, piezoelectric actuators are insensitive to magnetic fields. There are three primary disadvantages of piezoelectric traveling wave motors. First, one piezo motor requires two high frequency sine waves as a drive signal. The drive frequency must be continuously varied to match the resonance frequency of the piezoelectric element, which will change with load and temperature. Thus, the drive electronics for these actuators can be very complex and volume consuming. Secondly, this is a relatively new technology and there are few commercial suppliers. Consequently, their cost is high. Thirdly, piezoelectric motors are moderately high power devices. Some details follow. Typical no-load drive current and voltages are 60 milliamps and 28 volts peak-to-peak, respectively. Stall torque to volume ratios of 8.0 or higher can be expected and volumes as low as 0.009 cubic inches are achievable. Currently, prices for

small traveling wave motors can be as high as thousands of dollars.

Solenoids. Solenoids come in two types, linear and rotary. They can have volumes comparable to DC motors. They are relatively simple devices that require only a DC signal for operation. Additionally, they are low cost actuators. However, solenoids require more power than that of a comparable sized DC motor. Also, linear solenoids provide only linear motion and, consequently, are more susceptible to external forces, such as those due to dropping shock, which tend to be linear and not rotational. Some details follow. Solenoids can be priced as low as ten dollars. No-load current and voltages average approximately 300 milliamps and 10 volts, respectively.

LIGA Actuators. LIGA is a technique for making three-dimensional microstructures in metals, plastics, and ceramics from a process that combines lithography, electroforming, and plastic molding. The primary advantage of LIGA actuators is their extremely small size. Volumes as small as 0.0018 cubic inches can be achieved. The primary disadvantage of LIGA actuators is that the technology is relatively young. Performance characteristics of these actuators, which can be either a stepper or a solenoid, are mostly unknown. Also, commercially available actuators may be years away. However, since LIGA motors are batch manufactured in much the same way as computer chips, their cost is expected to be reasonable. A design issue associated with these motors is the interaction between the very small LIGA actuator and the larger piece parts normally found in handguns. This is a concern that will have to be addressed before LIGA actuators make their way into smart guns.

Chapter 10

Summary of Evaluations

Fifteen implementations of fourteen technologies were taken through the entire evaluation and ranking process. The technologies are a subset of the ones that have been reviewed in this report. The specific list of technologies also lent itself to referring the results to other similar technologies that have similar characteristics even though they may have totally different theories of operation. The six technologies required by the project contract are included in this list.

IMPLEMENTATIONS OF EVALUATED TECHNOLOGIES

Because the implementation may affect the evaluation scores, the following gives a brief description of the implementations of the technologies that were ranked. The evaluated implementations approximated the most appropriate methods for the technology if they were to be built today.

The RADIO FREQUENCY TAG technology was evaluated as a passive system using a tag placed on a ring or a wristband. The firearm included an antenna that transmits radio frequency energy to the tag whenever the firearm is in the hand of the user. The tag includes a receiving antenna that powers a small integrated memory from the radio frequency energy, and another antenna that transmits the memory's data back to the firearm. Another antenna in the firearm receives the information from the tag, and validates whether it is one of the predefined authorized users and controls the latching mechanism.

The SAW TAG technology has an identical implementation to the Radio Frequency Tag.

The ACTIVE TAG technology was evaluated as a radio frequency transmitter that the officer would carry as close to the firearm as practical to minimize the transmitting range. The active tag would constantly transmit unique information. A firearm being held in a user's hand within the range would receive the data from the active tag, validate whether it is one of the predefined authorized users, and control the latching mechanism.

The REMOTE CONTROL technology was evaluated as a push button activated transmitter that would transmit a unique signal to any firearm within range when the user presses the button. The firearm contains an antenna to receive and validate whether the signal is one of the predefined authorized users and controls the latching mechanism.

The TOUCH MEMORY technology was evaluated as a contact-read memory device attached to a ring that the user would wear. The firearm included in its grip a special reading surface that could read the memory when the memory was in contact. The contact of the memory itself is enough to start the reading action, evaluate the signal, and control the latching mechanism.

The FINGERPRINT technology was evaluated as a firearm with multiple optical scanners placed on the trigger or grip. When the user's hand is on the firearm his fingerprints are scanned and analyzed. The firearm then validates whether it is one of the

predefined authorized users and controls the latching mechanism.

The MAGNETIC ENCODING technology was evaluated with two implementations. Both use a ring with a magnet with north and south poles arranged in a pattern. The magnetic fields can be used to initiate the reading action. Implementation (A) uses an array of electronic sensors around the grip to distinguish the magnetic field pattern. Implementation (B) uses magnetically actuated mechanical switches in the grip to sense the pattern. The firearm then validates the pattern to determine whether it is one of the predefined authorized users and controls the latching mechanism.

The VOICE RECOGNITION technology was evaluated with a firearm that includes a microphone and all the processing electronics necessary to distinguish the utterance that the user is required to speak to enable the firearm. The latching mechanism can then be appropriately controlled.

The FINGERLENGTH technology was evaluated with multiple optical transmitters and receivers that are arranged to measure the length of the user's fingers while they are gripping the firearm and aligned by ridges on the grip. It was never determined if the length of a user's fingers was unique when gripped on a curved surface.

The BARCODE technology was evaluated with an optical scanner on the firearm grip that would scan a bar code when the firearm was in the user's hand. An exact method to attach a bar code to a user was never adequately determined.

The CAPACITIVE PROXIMITY technology was evaluated with sensors placed on the firearm that would sense a large mass disturbing the field created by the sensor. It was never determined how to make a user's hand mass appear unique.

The LANYARD technology was evaluated with a uniquely shaped lanyard (similar to a door key) inserted into a firearm. The firearm

would distinguish the lanyard through a mechanical discriminator that would be integrated with the latching mechanism. The lanyard strap would have to be pulled to remove the lanyard and disable the firearm.

The KEY LOCK technology was evaluated with a metal key (similar to a door key) inserted into a firearm. The firearm would distinguish the key through a mechanical discriminator that would control the latching mechanism. The firearm would be enabled or disabled by turning the key.

The COMBINATION LOCK technology was evaluated with a lock that can be unlocked by a memorized combination of button presses on the firearm. The firearm includes the keypad to enter the combination, and could distinguish the key through either a mechanical or electrical discriminator that would control the latching mechanism.

SUMMARY OF THE TECHNOLOGY EVALUATIONS

The evaluation of the technologies took place by reviewing each of the engineering requirements against the implementation described above. Each technology was assigned a score from 0 to 10 as to how well it could meet that requirement. The scores were assigned according to the capabilities of the technologies today. Changes such as repackaging and reduction in size were assumed to be possible for the technologies except where technical challenges ruled them out. For some requirements it was impossible to assign a score, because there is not an actual product to analyze. The scores were then summed for each technology. Two summations were made: one made directly from the scores, and the other from the score multiplied times the officers' importance for that requirement as obtained through the QFD process. Both of these summations were compared with the maximum score possible for the ranked requirements. By this comparison each of the technologies was

graded within a category of requirements, as well as with the whole set of requirements.

The scores were assigned to bullets that represent a grade (A, B, C, D, or F). An A+ signifies that the maximum score available was achieved (100%). The other grades signify a percentage of the maximum score available was achieved as follows: A = 90-99%, B = 80-89%, C = 70-79%, D = 60-69%, and F < 59%. The bullets were chosen so that comparisons between technologies could be reviewed by a glance of the eye.

Figure 4 and its accompanying notes show the summarized results of the rankings of the technologies without importance ratings compared to the various categories of the engineering requirements detailed in this report. Shown are only the categories of engineering requirements that contained requirements which were ranked. The reason that the importance ratings are not shown in this figure is that it allows the reader to make their own opinion as to what is important to them. The notes attached attempt to summarize all the significant qualifications that exist for that particular ranking for all the requirements that could be ranked. The notes are independent of whether the importance is included. In general the notes are negative qualifiers (thus more notes generally imply that more concerns are present). A brief verbal description of the figure follows.

In Figure 4 it can be seen that two of the technologies reviewed did not meet the basic scope requirements. Both the finger length and the capacitive proximity technologies have keys that are questionably non-unique. If the key is not unique it is not possible to distinguish one user from another. Finger length is one of the best biometrics used today, but that is when the hand is measured on a flat plate, and not a curved surface. More characterization of finger length must be done before any attempt is made at measuring finger length on a firearm grip. Other attempts at measuring unconstrained finger lengths have had limited success.

Also, when finger length is used for security applications it has been in the verification and not identification process. For capacitive proximity sensing of the mass of a hand, the sensing is too crude and the mass too non-unique to be used today.

The physical characteristics of all the technologies are less than perfect. Most are currently too large, although most could be made smaller if there was some incentive for the manufacturers to proceed. For some technologies the sensors would need to be placed on both sides of the firearm to reliably sense both left and right handed user's. This means that for officer's to be able to use either hand to discharge the firearm the technologies must be made even smaller than if only one sensor had be fit in the available volume.

Most of the technologies require some type of power supply. Typically this means batteries. Because power consumption is a concern, it is recommended that the technologies have some type of on/off switch to control when the technology is looking for an authorized user. (Ideally this switch might be the trigger if a technology could operate fast enough and be reliable enough that an indicator was not required.) Otherwise the technology has to constantly be using power to look for a user's key. This switch needs to automatically turn on whenever the firearm is in the user's hand. The technologies that were entirely, or mostly, mechanical scored higher in the category of power requirements. All the technologies except the lanyard were assumed to have at least power used to operate the latching mechanism. Some of the technologies that require a mechanical action, such as the key or combination locks, could use that mechanical energy directly or indirectly to latch the firearm. The technologies requiring two batteries were penalized more than those requiring only one.

The operational requirements describe functional requirements. Since for most technologies an on/off switch is required for

power consumption, this also allows it to be used for automatically enabling and resetting of the firearm. Otherwise only a few could meet this requirement. Some technologies require the use of two hands to enable or disable the firearm; one hand to hold the firearm and the other to perform an operation such as manually entering a code. Other concerns that some technologies have in this area are carrying an item that the firearm would recognize, memorizing an action to enable the firearm, and being able to wear gloves while using the firearm. Other comments are contained in the notes attached to the figure.

Biometric keys have the advantage over any key that comes from an external device. The biometric key is a permanent part of the user, will not be forgotten at home, does not require two items to be carried like may be required by rings, and is free. A key that is attached to an external device such as a ring could be lost, forgotten, or stolen. If it is not being worn the firearm will not fire. The uniqueness of these devices must also be controlled by the manufacturer so that duplicate keys are not available.

The discriminators main function is to authenticate the key. The discriminator needs to be able to read the key without concern of special alignment or movement between the two. It also has to be able to retain the list of authorized users for the particular firearm. Most of all it has to have a low false acceptance and false rejection rates.

The interface requirements that were ranked dealt with the existence of industry standards for the technologies. Most technologies do not have industry standards: each manufacturer uses a proprietary interface to communicate between their discriminator and their key. This means that their product does not work with any other manufacturer's device. This is not unlike the locks on various things today. Even though locks operate on the same principles, people have to carry a string of keys each one specific to a

single or a small number of locks. The goal for a smart gun product is to have a standard interface.

Cost is a factor for all the technologies. The mechanical systems are less expensive: they are relatively simple devices and are commonly available. The electronic devices will continue to drop in price as the demand rises.

The ability to operate and survive through various environments is a challenge to many of the technologies. All the technologies must be able to survive the explosive environment associated with the firearm discharging a round. The technologies that require some type of an optical scanning can be upset by environments that can block or distort light: dirt, contaminants, frost, perspiration. Some have specific concerns such as noise for a voice recognition system. With proper packaging the technologies should be able to survive most environments.

DRAFT

01/16/96

● = A+	● = A	⊙ = B	⊙ = C	○ = D	• = F
--------	-------	-------	-------	-------	-------

Updated Engineering Requirements	Scope	Physical Characteristics 3	Power 4	Operation	Key	Discriminator	Interface 46	Cost 47	Environments 49
Radio Frequency Tag	●	⊙	•	⊙ 8,9,10,11	⊙ 24,25,26,27	● 35	⊙	•	● 50
SAW Tag	●	•	•	⊙ 8,9,10,11	⊙ 24,25,27	● 35	⊙	•	● 50
Active Tag	●	•	• 5	⊙ 8,10,11	⊙ 24,25,27,28	● 35	⊙	•	● 50
Remote Control	●	•	• 5	○ 10,11,12,13,14,15,16	⊙ 24,25,27,28	● 35	⊙	○	● 50
Touch Memory	●	⊙	•	⊙ 9,10,14,17,18	⊙ 24,25,27,28	⊙ 35,36,37,38	⊙	○	⊙ 51
Fingerprint	●	○	•	⊙ 8,15,18,19,20,21	● 29	⊙ 35,37,38,39,40	⊙	• 48	⊙ 52,53,54,55
Magnetic Encoding (A)	●	•	•	⊙ 9,10,14,15,18,20	• 24,25,27,28,30	○ 35,38,40,41,42	⊙	○	● 53
Magnetic Encoding (B)	●	•	⊙ 6	⊙ 9,10,14,18,20	• 24,25,27,28,30	• 37,38,40,41,42,43	⊙	○	● 53
Voice Recognition	●	⊙	•	⊙ 8,11,15,21,22,23	⊙ 29,31	○ 35,38,39,40	⊙	• 48	⊙ 56
Finger Length	⊙ ₁	⊙	•	⊙ 8,18,19,20	⊙ 32	○ 35,37,38,40,42,44	⊙	○ 48	⊙ 52,53,57
Bar Code	●	⊙	•	⊙ 8,9,10,11,18	• 24,25,26,27,29,31	⊙ 35,37,38	⊙	•	⊙ 52,53,55,57
Capacitive Proximity	• ₂	⊙	•	⊙ 8,18,19	○ 33	• 35,37,40,42	•	○ 48	● 53
Lanyard	●	○	● 6	• 10,12,13,14,15,16,20,21	○ 24,25,27,31	○ 37,38,41,43,45	⊙	⊙	⊙ 53,57
Key Lock	●	•	⊙ 6	• 10,12,13,15,16,20,21	• 24,25,27,31	○ 37,38,41,43,45	⊙	⊙	⊙ 53,57
Combination Lock	●	○	○ 6,7	• 12,13,15,16,20,21,23	• 24,25,27,31,34	○ 37,38,41,43,45	⊙	⊙	⊙ 53,57

Figure 4 Evaluation of Technologies With Notes

NOTES:

- 1 Not known if finger lengths are unique over curved surfaces, and not valid for identification.
- 2 Hand mass is not unique, discriminator is weak.
- 3 All technologies have problems with their size and/or shape, and the placement of the discriminators on the firearm. (Each of these scores were increased by .2 to show some distinction between them.)
- 4 Most technologies require power for at least the discriminator and the latch.
- 5 Two batteries are needed.
- 6 May be entirely mechanical system.
- 7 Possible electronic keypad and or latch.
- 8 Some type of on/off switch is necessary to simulate passive operation; to allow the system to reset, turn off, or disable; to signal when to take a reading and conserve power.
- 9 A key may need to be worn on each hand.
- 10 Must remember to carry the key
- 11 Key may be read from some distance. The distance needs to be controlled.
- 12 Must manually enter key, this takes time, effort, and the key must be readily available.
- 13 Two hands may be required for enabling and/or disabling the firearm (one for firearm, other for the key).
- 14 The technology itself may be used as an on/off switch.
- 15 Activation and/or discrimination may be too slow (possible up to seconds).
- 16 Will not automatically sense new user.
- 17 Electrical contact required for communication between key and discriminator.
- 18 Wearing gloves could be a problem.
- 19 Must store biometric from each hand.
- 20 Near contact required to read key.
- 21 Enrollment of a new user with unique key may be time consuming.
- 22 Must be able to speak to enable firearm.
- 23 The key must be memorized.
- 24 Key could be transferred.
- 25 Key is an external device that has to be carried.
- 26 Key could be made semi-permanent part of body.
- 27 Manufacturer would have to control keys for uniqueness to be maintained.
- 28 Key is physically larger than many others.
- 29 Key is not stable, it may change due to time, stress, input direction, or contaminants.
- 30 Limited number of unique combinations available.
- 31 Key is more easily copied.
- 32 Finger length around a curved surface is not known to be unique.
- 33 Hand mass is not known to be unique, any item of correct mass could enable firearm.
- 34 The key must be memorized.
- 35 Requires a method to retain stored authorized users (non-volatile memory, battery backup...).
- 36 Electrical contact required for communication between key and discriminator.
- 37 Alignment between key and discriminator must be controlled.
- 38 Special movement may be required between the key and discriminator (may require movement or non-movement).
- 39 Template for key storage may be rather large.
- 40 False rejection rate (FRR) and false acceptance rates (FAR) need to be proven.
- 41 Difficult to obtain the required number of users.
- 42 Limited discrimination because of limit uniqueness of key.
- 43 May incorporate mechanical discriminator.
- 44 Finger length around a curved surface is not known to be unique.
- 45 Multiple keys may greatly reduce security.
- 46 Each manufacturer of existing technologies maintain their own standards. One manufacturer's discriminators may not recognize another one's key. Some existing standards are not documented or applicable.
- 47 Mechanical based technologies are most cost effective when dealing with mechanical firearms. Technologies that do not commercially exist were given the benefit of low prices. There is a very large range of prices within the F category.
- 48 Biometric key is free.
- 49 Must survive firing environment.
- 50 Must protect against radio interference.
- 51 Exposure to water could electrically short the discriminator.
- 52 Frost could cause problems at cold temperatures.
- 53 Any substance that can alter the key or discriminator is a problem (mud, blood, etc.).
- 54 Excessive perspiration could have adverse effects on reading the key.
- 55 Sensors may crack with shock.
- 56 Affected by acoustically noisy environments.
- 57 Affected by external light conditions.

Figure 5 Ranking of Technologies (without importances)

Figure 6 Rankings of Technologies (with importances)

FINAL GRADES

The following describes the final rankings of the technologies and gives a brief description of reasons for the ranked position. For more detail on the technologies refer to the specific sections contained within this report.

The ranking of technologies reveals the relationship between the various technologies compared to how they meet law enforcement officers' requirements. Figure 5 shows the ordered ranking of the technologies without importances compared to the maximum number of points that were available for the requirements that could be ranked. Figure 6 shows the same information with the importances factored into the numbers.

The first thing that should be noticed is that the highest score of any technology, when compared to the maximum score possible, is in the eighties. This reveals that all the technologies have some further development to be done before they can meet the idealistic officers' requirements. Next, when the two figures are compared, there is very little change due to the importance ratings being included. If they were greatly different this would say that the requirements that are important to both the officer and the smart gun designer overwhelmed the requirements that were not as important. Instead since this was not the case, either the importances were too alike to make a difference or the technologies intrinsically contain the traits needed to meet the important requirements. Most likely it is a combination of the two. For these reasons it is suggested that the values without importances are used as a baseline.

In reviewing the ranked order of the technologies, the radio frequency technologies came out ahead. The reasons for this are that the radio waves travel through most substances and therefore are not affected by many of the environments that hindered the other technologies. The radio waves can transmit information through mud, blood, and other contaminants, as well as through glove

materials which most other technologies could not. Speed is not a problem, nor is signal integrity since electronics containing error checking codes can check if a valid transmission was received and if not try again. The possible concern for the radio frequency devices is electromagnetic interference that could effectively keep the firearm from receiving the necessary signals.

Ranked after the radio frequency devices is the touch memory device. Although in practice the touch memory has problems to overcome, it also has some good attributes. Its strong point is that it is a relatively simple device that can work fast with good discriminating capabilities. Its weaknesses are that it requires a ring to be worn that needs to contact the firearm with an electrical connection to perform its communication. This presents concerns with both alignment and certain environments.

Next in order of ranking is fingerprint technology. The reason that fingerprinting is ranked this high is that as a key it is unique and available, assuming gloves are not being worn. The main problem with the fingerprinting technology is any contaminant that could get in between the key and discriminator and prevent a proper reading from taking place. The other concerns are the slow speed to scan and analyze the fingerprint and the cost of the current devices.

Magnetic rings are next in order of ranking. Magnetic rings improved when the importances are included in the rankings in part because the magnetic energy itself can be used to turn the firearm on and off, therefore no separate mechanism is needed to conserve battery power. It is possible that a battery would not even be necessary although this is unlikely in order meet other requirements. Problems with magnetic rings are that besides having to carry the ring, the magnets need to be strong (therefore expensive) or large in size. They also have concerns with the alignment of the magnets to the sensors, and

the number of unique codes that can be produced.

Voice recognition is another biometric technology, but in this case the key is not as good as that of the fingerprint. The goal of voice recognition is to detect the vocal tract, but today most systems depend on phonemes. As the voice changes due to various reasons including sickness, stress, or age a person may have a difficult time being recognized. If the system is implemented with a spoken password as a key it means the activation requires a memorized action.

In theory finger length, bar codes, and capacitive proximity technologies all have limited potential as a smart gun technology. In practice their implementation, or lack thereof, lowered their ranking. Finger length and hand mass are not known to be unique in the method that a firearm would be used: gripping a curved surface. Research could reveal the validity of their uniqueness. Assuming they are unique, a method of measuring them needs to be developed that does not depend as much on the exact alignment of the biometric and other environmental conditions. Bar codes need a method to be carried by the user so that the firearm could read the bar code's information. They are able to be reliably read in normal environments, but any contaminants will interfere with a reading.

The three final devices, the lanyard, the key lock, and the combination lock came in last as meeting the requirements for a law

enforcement officer's firearm. These devices are less expensive than the other technologies and they may not require any power source. The problem these technologies have is that they do not automatically enable the firearm for the user but require the user to perform an action. The action must be performed with an external item that is not as easily carried as a ring, and may even require a memorized event. Other problems include having being able to discriminate between the required number of users while not reducing the security of the firearm, and being able to copy the key.

Many of the requirements could not be ranked but are very important to consider. The main reason that some requirements were not ranked is that they were too dependent on the final implementation and realization of a smart gun. Many important requirements that could not be ranked include the entire requirement categories of reliability, service life, testing, maintenance, adversarial strength, latch, indicators, and with other individual requirements. What this means is that while the rankings that were done display the state of the technologies in meeting the ranked requirements, a large piece of the puzzle that is missing is the ranking of the actual product implementation. Even the perfect technology could be improperly implemented and not be successful as a final product. At the same time, by proper implementation of a lower ranked technology it could surpass others as a final product.

Chapter 11

Conclusions

A documented study of various technologies that could be used in a user authorized firearm, a smart gun, has been compiled in this report. This report contains information regarding the engineering requirements for a smart gun system, an overview of a smart gun system, explanations of various technologies and why some are better than others, and the methods used during all of these steps.

A generic system model based off of a key operated padlock was used. Three distinct pieces must exist in any smart gun technology system. The key must be an item that can uniquely identify the firearm user, the discriminator must be able to identify the key, and a latching mechanism must be able to physically lock the firing mechanism.

The work in this report was based off of law enforcement officers' requirements as documented in *Smart Gun Technology Requirements Preliminary Report* and updated with information received since release of the report. The assumption is made that these are correct. With the requirements obtained from law enforcement officers as a base, technologies were investigated, evaluated and ranked. The technologies that were chosen were all ready being used in other security applications, had been tried on firearms before, or were thought to have some potential in this application. Many different implementations of each technology are possible and the ones ranked were chosen to highlight the strengths and weaknesses of the technologies.

The difficulty throughout this study was that evaluations were done on what a technology

could do if developed into a smart gun product; this is unlike normal evaluations that are done on existing products. Decisions were made based on engineering judgments from available information. On many issues it was impossible to make any judgment because the requirements were based on a final implementation in a product, in these cases the requirements were not ranked at all. Sometimes a feature of a technology would be a strength in one area and a weakness in another, so depending on how the feature would be implemented in a product could change the rankings. The information is presented in a manner that allows readers to make up their own minds as to what is important to them.

After a thorough review of the data there was no perfect technology: one that would meet all the officers' requirements. Considering all the requirements that were ranked, the highest ranked technology could only be given a grade of B. This indicates that there are some characteristics of each technology that do not live up to the officer's expectations. This is not all bad since the officers' requirements were often highly idealistic. What it does mean is that there is still work to be done by technologists to resolve the officers' concerns. None of the top ranking technologies were found to have any problem that could not be solved from more research and development, or by reaching a compromise with the officers. Many of the technologies discussed did not exist even a few years ago as marketable products. Even during the evaluation period new advances were made in some of the technologies, with

more being expected within the next few years. As technologies become mature the weaknesses listed in this report may be overcome. Much time and resources will have to be expended to overcome these weaknesses; this is difficult without a guarantee of a market place for the product when it finally becomes available. The technologies developed into products may not depend as much on what the technology can currently do, but of the remaining things that it cannot do. Technologists can leverage which of the problems are left to solve against the most benefit that will be gained in making the user community satisfied. The technology does not have to be perfect to be fielded, but law enforcement officers need to be aware of any limitations that the product may have. It should be expected that mistakes will be made in early prototypes, but these need to be discovered and fixed before a wide distribution of the product is made.

Although there is no perfect technology there is a desire by many to have a more secure firearm available for use by law enforcement officers. Others would like to have more secure firearms available to the general public. The information in this report is based solely on the law enforcement requirements for a smart gun; the requirements for the general public are assumed to be different. It is hoped that the information contained in this report will spawn a move by technologists to review the results and use their expertise to resolve the shortfalls of their technologies. In this way a reliable, safe, and secure user-authorized smart gun can be developed.

Bibliography

- R. Adams, Sourcebook of automatic identification and data collection, Van Nostrand Reinhold, NY. 1990.
- D. Barvenik, R. Renick, and R. Tun, Personalized Handgun Anti-Fire Safety Equipment, a student project sponsored by Johns Hopkins Injury Prevention Center.
- D. Black, A Short Course in RF/ID Technologies, in *IDSystems*, February 1994.
- G. R. Doddington, Speaker Recognition - Identifying People by their Voices, *Proceedings of the IEEE*, Vol. 73, No. 11, November 1985.
- M. Elkins, GunID Small Arms User Validation System.
- R. E. Floyd, Access Control with RF/ID, *IDSystems*, October 1993.
- K. T. Gee, S. H. Scott, M. G. Wilde, and S. E. Highland, Overview of Locking Systems, Sandia National Laboratories report SAND93-2030.
- D. Guinier, Identification by biometrics an introduction and a survey, *SIGSAC Review*, Summer 1990.
- J. Hollingum, Automated Fingerprint Analysis Offers Fast Verification, *Sensor Review* Vol. 12. No. 3. 1992 pp. 12-15.
- J. P. Holmes, L. J. Wright, and R. L. Maxwell, A Performance Evaluation of Biometric Identification Devices, Sandia National Laboratories report SAND1-0276.
- C. Jennings, Biometrics - When The Person Is The Key, *Sensor Review*, Vol. 12 No. 3. 1992 pp 9-11.
- M. F. Lewis, On Rayleigh Waves and Related Propagating Acoustic Waves, in Rayleigh-Wave Theory and Application. Editors: E. A. Ash, E. G. Paige.
- C. Loughlin, Tutorial: colour and colour measurement, *Sensor Review*, April 1990.
- A. Macintyre, Magnetic Field Sensor Design, *Sensor Review* Vol. 11 No. 2, 1991, pp. 7-12.
- P. MacGregor and R. Welford, Veincheck Lends A Hand For High Security, *Sensor Review* Vol. 12. No. 3. 1992 pp. 19-23.
- L. H. McCarty, Electronic System Makes Remote Identification, *Design News* 10-7-85.
- B. Miller, Vital signs of identity, *IEEE Spectrum*, February 1994.
- E. Newham, The Biometrics Report, 1995
- J. R. Parks. Biometrics: the people sensors, *Sensor Review*, April 1989.
- R. D. Peacocke and D. H. Graf, An Introduction to Speech and Speaker Recognition *IEEE Computer*, August 1990
- A. P. Plummer, Colour makes it easy, *Sensor Review*, July 1990.

- D. R. Richards, ID Technology Faces the Future, *Security Management*, April 1994.
- J. R. Rodriguez, F. Bouchier, and M. Ruehle, A Performance Evaluation of Biometric Identifications Devices, draft Sandia National Laboratories report SAND93-1930.
- P. E. Ross, I can read your face, *Forbes*, December 19, 1994.
- R. B. Starkey, The Human Face - A Unique Pattern?, *Sensor Review* Vol. 12. No. 3. 1992 pp. 16-18.
- D. Tynan, What you say is what you get?, *PC World*, January 1995.
- D. White, Harnessing the Hall effect for today's technology, *Sensor Review*, April 1989.
- L. J. Wright, Coded Credentials - A Primer, Sandia National Laboratories report SAND 88-0180.
- AIM USA. Internet home page containing general information on automatic data collection.
- AM Sensors, Inc. Advertising information on Alphasensors.
- Amtech. Advertising information on Intellitag products.
- Association for Biometrics. Internet home page containing general information on choosing biometric technologies.
- Captive Breeding Specialist Group. Working group on permanent animal identification. Memorandum test report on transponders.
- Dallas Semiconductors. Automatic Identification databook.
- DataLogic, Inc. Data book on Automatic Identification.
- Digital Biometrics Inc. Advertising information on fingerprinting equipment.
- Dragon Systems. Advertising information on Dragon Dictate.
- Fulton Arms Inc. Advertising information on the SSR-6.
- Gun safety system, applauded as 'revolutionary,' fails to trigger response from larger agencies, *Law Enforcement News*, Vol. IV, No. 20. November 27, 1978
- Phillips Semiconductors. Advertising information on RF identification transponders.
- Proposed European Standard for Biometric Technology Projects Testing & Evaluation: Glossary of Terminology. Sponsored by the Association for Biometrics, draft working document, February 18, 1994.
- Radio Frequency Identification Reference Book. Innovative Insights, Inc. Unpublished book.
- RFID Technologies CC. Internet home page containing general information on the Supertag.
- TEK Inc. Advertising information on Tek Touch System.
- Texas Instruments. Advertising Information on TIRIS tags.
- TrueFace Applications. Internet homepage containing information on TrueFace.
- TRW. Advertising information on VeraFind automated identification system.

Appendix A

Summary of Users' Requirements

The following are the officer's requirements as found in the *Smart Gun Technology Requirements Preliminary Report*. A more detailed review can be found in that report.

1. PHYSICAL CHARACTERISTICS

1.1 FEEL

- 1.1.1 The addition of smart gun technologies cannot appreciably change the weight, size, or balance of existing firearms.
- 1.1.2 The smart gun technology should not affect the carrying of firearms in existing holsters.
- 1.1.3 The smart gun technology must not affect the existing trigger pull standards.
- 1.1.4 Addition of batteries should not greatly change the physical characteristics of the firearm, i.e., size, weight...

1.2 APPEARANCE

- 1.2.1 The smart gun must have the general appearance of an existing firearm.
- 1.2.2 The addition of smart gun technologies cannot add appendages which would appreciably increase snagging compared to an existing firearm.
- 1.2.3 Any external device should have optional methods for attachment to the person, i.e., multiple fingers; fingers or wrists; implantable...
- 1.2.4 Ideally external devices can be attached to existing items, i.e., rings, watches, badges...

1.3 MISCELLANEOUS CHARACTERISTICS

- 1.3.1 The addition of a smart gun technology to a firearm should be operationally transparent to the user.
- 1.3.2 The smart gun technology must be applicable to multiple types and brands of firearms.
- 1.3.3 The technology should also be applicable for use on multi-user weapons. i.e., shotguns.
- 1.3.4 Ideally no external devices are needed to operate the smart gun technology.
- 1.3.5 Any external devices must be consistent with other smart gun technology requirements, i.e., reliability, durability, easy to maintain, small, accessible, simple...

2.0 PERFORMANCE

2.1 FUNCTION

- 2.1.1 A single individual must be able to activate a smart gun technology without assistance from others.

- 2.1.2 The ideal smart gun technology operates without action by the officer.
- 2.1.3 The smart gun technology should become enabled or disabled without action by the officer.
- 2.1.4 A smart gun technology must operate within the capabilities of an officer in a highly stressful situation.
- 2.1.5 A smart gun technology must be capable of ambidextrous one-handed operation.
- 2.1.6 The smart gun technology must operate while wearing gloves typically worn by officers.
- 2.1.7 The addition of smart gun technologies must not increase the time of drawing and firing when the decision for using lethal force has been made by any authorized user.
- 2.1.8 A smart gun technology for law enforcement officers should fail armed, such that the failure of the technology does not inhibit firing of the weapon.
- 2.1.9 The addition of a smart gun technology must not complicate the use of the firearm.
- 2.1.10 Smart gun technologies must not be alignment critical.
- 2.1.11 Proper documentation for operational use must be supplied.
- 2.1.12 The smart gun technology should only be operational while in the officer's hand.
- 2.1.13 The operational range of any external device must be consistent with other requirements.
- 2.1.14 Smart gun technologies should be capable of being used by an off duty officer.

2.2 RECOGNITION

- 2.2.1 The smart gun technology must properly recognize, and limit the use of the firearm, to the authorized user.
- 2.2.2 The smart gun technology should be capable of being used by multiple users.
- 2.2.3 The technology must operate for a single individual on multiple firearms.
- 2.2.4 The smart gun technology must operate on the first verification attempt.
- 2.2.5 For applicable recognition technologies the actual recognition score, rather than a simple go/no-go indication, should be available in a testing configuration.
- 2.2.6 For applicable recognition technologies, a method of adjusting the recognition threshold by a qualified person is recommended.

2.3 POWER REQUIREMENTS

- 2.3.1 Ideally the smart gun technology would not require the use of batteries.
- 2.3.2 A low power indicator must be supplied if batteries are used in a smart gun system.
- 2.3.3 If batteries are used, they must be easily obtained, and factored into the cost of maintaining the equipment.
- 2.3.4 Ideally a battery used in a smart gun system would last longer than 1 year.
- 2.3.5 The minimum lifetime of a battery used in a smart gun system would allow an officer to fire 3 magazines, 10 hours after first indication of a low battery.

2.4 INDICATORS

- 2.4.1 A simple test to confirm that the smart gun technology is functioning properly must be available.
- 2.4.2 An indicator cannot be distracting to the officer.

2.5 READINESS

- 2.5.1 The addition of a smart gun technology must not significantly reduce the circumstances in which the firearm will operate, compared to existing firearms.

2.6 SAFETY

- 2.6.1 The addition of smart technologies should not affect existing gun safety rules.
- 2.6.2 Smart gun technologies must meet the existing law enforcement standards.
- 2.6.3 The addition of smart technologies cannot act as a second trigger.
- 2.6.4 Smart gun technologies and external devices should not cause medical side effects.

2.7 RELIABILITY

- 2.7.1 The smart gun technology must operate in a predictable manner.
- 2.7.2 The addition of a smart gun technology must not significantly reduce the reliability of the firearm system compared to existing firearms.
- 2.7.3 The addition of a smart gun technology must not effect the primary use of firing the weapon by the authorized user.
- 2.7.4 Simple procedures must be available to allow an officer in the field to quickly reset the recognition system in case of a technical malfunction.

2.8 SECURITY

- 2.8.1 A smart gun technology must not be easily disabled by an adversary.
- 2.8.2 The technology must be such that even with full knowledge of how the system operates it cannot be easily defeated.
- 2.8.3 The technology used in a smart gun must have a unique characteristic that is not easily replicated, or jammed by an outside source.

2.9 COMPATIBILITY

- 2.9.1 The smart gun, compared to existing firearms, should not cause a loss of capabilities.
- 2.9.2 The ideal smart gun technology could be installed in existing firearms without reducing the existing firearms capabilities.
- 2.9.3 Smart gun technologies must meet existing applicable firearm standards.

2.10 TRAINING

- 2.10.1 Smart gun technologies must cause only minimal additional training, such as transitional training and in service training on proper use.
- 2.10.2 Smart gun technologies must enhance and not eliminate weapon retention training.
- 2.10.3 Smart gun technologies training must extend beyond the use of technologies and include training for armorers and others as appropriate.

2.11 MAINTAINABILITY

- 2.11.1 Maintenance requirements for smart gun technologies must be held to a level that the average officer will do.
- 2.11.2 There must be a method for armorers and manufacturers to test the smart gun technology.
- 2.11.3 Individual smart gun product lines should ultimately have interchangeable parts that are not easily misassembled and can be replaceable without special tools.
- 2.11.4 The smart gun must be capable of repeated maintenance without damage or a decrease in performance.
- 2.11.5 Department's armorer or trained personnel should be able to perform most diagnostic tests and repairs.
- 2.11.6 The technology should be upgradable when the next incremental version of the technology is introduced.
- 2.11.7 Batteries should be easily replaceable, even in the field.

3.0 ENVIRONMENTAL

- 3.0.1 The smart gun technology must operate in all likely environmental conditions.
- 3.0.2 The remainder of the Environmental requirements are found in Appendix A of *Smart Gun Technology Requirements Preliminary Report*.

4.0 EXTERNAL EQUIPEMENT

- 4.0.1 Ancillary equipment needed must be identified.

5.0 MISCELLANEOUS

- 5.0.1 The additional production cost to incorporate a smart gun technology to a firearm should not add more than approximately \$50 to the purchase price.
- 5.0.2 Any additional costs associated with the use of smart gun technologies should be minimized.
- 5.0.3 The limitations of smart gun technologies must be made known so the technology is not declared the end all solution to the problem of weapon takeaways.
- 5.0.4 Recommendation of special procedures must be listed.
- 5.0.5 A systematic test program must be performed before actual field testing a smart gun technology which at a minimum includes studies of long term performance issues, and design failure modes and effects analysis.

Appendix B

Patents

The following are a few of the patents that exist pertaining to smart gun technologies and systems. This list is given as a place to start looking for references: the list is not intended to be a complete record. No endorsement is being given by being listed, as well as no disapproval by being absent.

Patent number: 03939679 (also see 4003152)
Issue Date: 02-24-1976
Inventor 1: Barker; James N.
Inventor 2: Cartwright; Edward A.
Title: Safety system
Abstract: Normally disabled electrical and mechanical devices are caused to be enabled to operate by remote control signals having predetermined distinctive characteristics, such signals originating from enabling control equipment transported by an authorized person or persons. Receiving equipment providing output enabling signals only in response to received signals having the predetermined distinctive characteristics is preferably made integral with the mechanical or electrical devices involved and is coupled through appropriate electronic or electromechanical devices to the disabling means in the mechanical or electrical devices to be enabled.

Patent number: 03978604 (also see 4067132, 4110928, 4135320, 4154014)
Issue Date: 09-07-1976
Inventor 1: Smith; Joseph E.
Title: Trigger inhibiting mechanism
Abstract: Trigger safety device for firearms is provided having a pivotally mounted magnetically attractable bar positioned on the inside of the handle adjacent the trigger, with the bar directed toward the trigger or on the rear of the trigger, with the bar directed toward the handle. When the pin is oriented centrally, sufficient movement of the trigger is inhibited to prevent firing. The bar is mounted in a non-magnetizable casing. The user of the gun, by wearing a magnetic ring, displaces the bar from its central orientation and allows for sufficient movement of the trigger for firing.

Patent number: 04105885
Issue Date: 08-08-1978
Inventor 1: Orenstein; Henry
Title: Hand operated instruments having non-magnetic safety switch

- Abstract:** Operator controlled devices in the form of hand operated instruments in which a ring worn by an operator is configured to be insertable into a recess in a hand holdable portion of the instrument. The recess includes a fixed contact configuration that is engagable by a non-magnetic bridging contactor on an outer peripheral face of the ring, so that the instrument becomes operational when the contactor is inserted into the recess and engages the fixed contact configuration.
- Patent number:** 04136475
Issue Date: 01-30-1979
Inventor 1: Centille; Edward E.
Title: Safety device for firearms
Abstract: The invention provides a safety device for firearms wherein a key operated lock actuates a locking pin to lock the firing mechanism. The locking pin is controlled by a rack and pinion gearing linkage which moves the locking pin to alternately engage or disengage a trigger seat.
- Patent number:** 04162586
Issue Date: 07-31-1979
Inventor 1: Pachmayr; Frank A.
Title: Gun with cushioned grip safety
Abstract: a gun having a pistol type handle with a trigger at the front of the handle and a grip safety at the back of the handle mounted for limited pivotal movement and acting to prevent actuation of the trigger except when the grip safety is squeezed forwardly, and with the back surface of the grip safety being formed as a layer of cushioning material for contacting the user's hand
- Patent number:** 04261127
Issue Date: 04-14-1981
Inventor 1: Karkkainen; Alpo
Title: Safety lock for firearms
Abstract: The invention relates to a device for locking a firearm preferably provided with a wooden stock (1) comprising a so called pistol end. the locking device according to the invention comprises a cylinder lock (4) mounted from beneath into the pistol end of the stock (1) behind the trigger (2) and mechanical means preferably comprising a flexible shaft (5) for transmitting the movement of a turnable element of the cylinder Lock from the cylinder lock (4) to a member (6) essential for the function of the firing device of the arm.
- Patent number:** 04354189 (also see 04488370)
Issue Date: 10-12-1982
Inventor 1: Lemelson; Jerome H.
Title: Switch and lock activating system and method
Abstract: A system and method are provided for opening a lock or activating a switch by electronically controlled means. In one form, a finger ring is provided which contains a code recording supported within or adjacent the crown thereof. when the hand of the person wearing the ring is held near a reading device, such as to dispose the crown within a receptacle containing the reading device, the code is automatically read and electrical signals generated thereby are applied to close or open an electrical switch or operate a motor or solenoid For opening a lock

and/or drive a door to open. If the signals generated in reading the ring recording is a code, they may be applied to a comparator for operating the lock or switch if the code is an enabling code. The reading device may comprise a photoelectric cell or bank of cells adapted to read variations in reflectivity of the ring code. In another form, the ring may contain an electronic circuit or devices which generate a code in the presence of a radiation field generated in the vicinity of the receptacle for the ring upon sensing the presence of the ring. In another form, the ring may contain a battery and electronic circuit means for generating the enabling code when a switch is closed. In another form, the combination of the code generating means of the ring and a separate circuit such as a circuit card, may be required to enable the switch to close or the lock to open. Improvements are also provided in the constructions of electronic keys in the configurations of finger rings, wrist watches, cards and the like, for use in switch and lock activating systems, security and transaction systems and the like.

Patent number: 04457091
Issue Date: 07-03-1984
Inventor 1: Wallerstein; Robert S.
Title: Firearm safety lock
Abstract: A firearm combination safety lock is disclosed. The safety lock includes a plurality of independently actuatable members, which in the preferred embodiment, are four push button switches connected to an electronic circuit. The electronic circuit compares the sequence in which the buttons are pushed and will operate an interlock means when the sequence matches a predetermined sequence. The pushbuttons are preferably provided in the finger grip of the handle of the firearm.

Patent number: 04467545
Issue Date: 08-28-1984
Inventor 1: Shaw, Jr.; Frederic A.
Title: Personalized safety method and apparatus for a hand held weapon
Abstract: A hand held weapon is fitted with a safety device responsive to the palm or fingerprint of one or more individuals. The safety device is activated by heat sensed when the device is hand held. Unless the palm or fingerprint of the person holding the device matches a prestored pattern, a blocking safety mechanism, normally preventing operation of the weapon, is maintained in its "blocking state" and the weapon will not fire.

Patent number: 04563827 (also see 04682435)
Issue Date: 01-14-1986
Inventor 1: Heltzel; James
Title: Safety system for disabling a firearm
Abstract: A safety system for selectively disabling a firearm which is fired by a mechanical movement is disclosed. The safety system includes a block which is moved between an engaged position whereby the mechanical firing movement is blocked and a disengaged position whereby the mechanical firing movement is not blocked. The block has a bearing surface which engages a relatively immovable part of the firearm when the block is in the engaged position. A moving device is also provided for moving the block from the disengaged position to the engaged

position, with the moving device normally biasing the block to the disengaged position. A remotely controlled actuating device for actuating the moving device includes a transmitter which selectively transmits a signal and which is designed to be carried by the operator of the firearm. A receiver is located adjacent the moving device. The receiver receives the signal from the transmitter and operates the moving device. Where the mechanical movement includes a member which moves parallel to a metal surface, the block is an elongate bar which is extendable through an aperture in the metal surface. The block can also be a lever which is pivoted intermediate two opposed ends. Conveniently, the moving device is a solenoid.

Patent number: 04672763
Issue Date: 06-16-1987
Inventor 1: Cunningham; Jerry M.
Title: Safety device for preventing the unauthorized firing of a weapon by releasing the hammer spring
Abstract: A safety device for preventing the unauthorized firing of a weapon, such as a pistol. The device has a hammer, a handle, and a leaf spring inside of the handle. The leaf spring places tension on the hammer, when the weapon is enabled. The leaf spring is held by a stop member, which is movable. When the stop member is moved to a lower position, the spring is released, and the weapon is disabled. The stop member is moved by a strap and a ring, connected to the stop member. The handle must be taken apart in order to return the spring and the stop member to the enabled condition.

Patent number: 04730407
Issue Date: 03-15-1988
Inventor 1: Decarlo; Dean S.
Title: System for converting firearms to electrical ignition
Abstract: A system for converting firearms to electrical ignition for firing of electrically primed ammunition. The system includes a drop in module to replace the conventional trigger, hammer pin, and other firing mechanism parts, and which has either included or separate structure to replace conventional firing pins. The module contains a safety interlock system, indicator lights, an on-off switch, an actuator switch, ammunition contacts and appropriate connecting circuitry to a power supply means.

Patent number: 04763431
Issue Date: 08-16-1988
Inventor 1: Allan; Robert E.
Inventor 2: Allan; Robert M.
Title: Handgun locking and unlocking apparatus
Abstract: Locking devices for guns operate to lock the guns against inadvertent or unauthorized firing, and at the same time enable quick and controlled unlocking of guns, to enable their use, as against home intruders.

Patent number: 04833811
Issue Date: 05-30-1989
Inventor 1: Wilkinson; Earl

Title: Safety for pistols
Abstract: a safety for hammer-equipped pistols, which includes a lock pin slidably mounted in the handle of a pistol, a companion lock pin spring biasing the lock pin inwardly of the handle toward the hammer, a locking rod slidably mounted in the handle in angular relationship with respect to the lock pin, the upper end of which locking rod is adapted to normally engage a seat provided in the lock pin and a release pin normally located in a release pin seat provided in the base of the handle, for engaging the opposite, or lower end of the locking rod and preventing relative movement between The locking rod and the lock pin. in a preferred embodiment, one end of a release pin cable is attached to the release pin and the opposite end of the cable is secured to the pistol holder, wherein seizure and extension of the pistol beyond the length of the cable pulls the release pin from the release pin seat and allows the locking rod to slide downwardly inside the pistol handle and facilitate forward projection of the lock pin responsive of the lock pin spring and locking of the hammer to prevent firing of the pistol.

Patent number: 04970819
Issue Date: 11-20-1990
Inventor 1: Mayhak; Gary D.
Title: Firearm safety system and method
Abstract: Actuation of the firing mechanism of a firearm is prevented until grip pattern sensing means on the handgrip of the firearm supply to a microprocessor signals corresponding to a grip pattern stored in a programmed simulated neural network memory. All of these components are contained within the firearm. programming of the neural network memory is accomplished by using a host computer with a simulated neural network to train that network to recognize a particular grip pattern using grip pattern signals generated by the grip pattern sensing means as the sensing means is repeatedly gripped for the person for whom the firearm is to Be programmed.

Patent number: 04987693 (also see 5090148, 5140766, 5229532, 5335521, 5408777, 5457907)
Issue Date: 01-29-1991
Inventor 1: Brooks; Frank
Title: Firearm safety mechanism
Abstract: A firearm safety mechanism includes a lock with engagement structure. The engagement structure has a locked position in which the engagement structure operatively engages a portion of the firing mechanism to prevent discharge of the firearm. The engagement structure also has an unlocked position permitting operation of the firing mechanism. The lock includes selection structure permitting movement of the engagement structure from the locked position to the unlocked position upon the reception of a predetermined selection criteria. The firearm can be locked against unauthorized use and unlocked by an authorized user without resort to external accessories.

Patent number: 05016376 (also see 5123193)
Issue Date: 05-21-1991
Inventor 1: Pugh; Kenneth J.
Title: Magnetic actuated firearms locking mechanism
Abstract: This invention teaches a safety for preventing unauthorized firing of a weapon (h)

of the type having a trigger (19) and mechanical firing mechanism (21) for firing the weapon. A solenoid (s) controllably actuates or deactuates upon the application of an electrical signal. A decoder (d) is mounted with the weapon for detecting a signal from an authorized user and selectively activating the solenoid upon the signal from the authorized user. Such decoder (d) is electrically connected to at least a power source (p) and to the solenoid (s). An encoder (e) creates the signal indicating that the possessor is authorized to use the weapon. A linkage (l) connects the solenoid (s) and the firing mechanism (f) for controllably enabling or disabling the weapon from being fired upon the desired activation of the solenoid.

Patent number: 05022175
Issue Date: 06-11-1991
Inventor 1: Oncke; Ockert P. H.
Inventor 2: Van der Merwe; Sarel B.
Title: Safety arrangement for firearms
Abstract: A safety arrangement for selectively disabling a firearm is provided. The firearm includes a handle, a trigger, a hammer, and a barrel. The hammer, in an unlocked condition, is movable into a functional position for being actuatable by the trigger for striking a magazine causing firing of a bullet and, in a locked condition, is mechanically locked so that it cannot be actuated by the trigger for causing firing of a bullet. the arrangement includes a control unit adapted in the locked condition to lock the hammer and, in the unlocked condition, to unlock the hammer; an electronic decoder unit adapted to decode input signals and to provide corresponding output signals; an electronic driver stage being adapted on receipt of the output signals from the electronic decoder unit, to cause corresponding operation of the control unit for locking and unlocking the hammer as the case may be; and a keypad unit having a number of key buttons, the key buttons being adapted on operation thereof to provide input signals to the electronic decoder unit when The keypad unit is electrically coupled thereto.

Patent number: 05042185
Issue Date: 08-27-1991
Inventor 1: Justice, Sr.; Jerry P.
Title: Semi-automatic pistol safety lock apparatus
Abstract: A locking mechanism for a semi-automatic pistol that completely disables the weapon when in the locked position. The mechanism includes a set screw that is inserted in a small hole drilled in the side of the pistol side plate behind the trigger. the set screw has attached to it a small button such that when the mechanism is in a locked position, the button located on the screw is extended into a blind hole formed in the hammer, thereby preventing pivotal movement of the hammer, and consequently preventing operation of the trigger and the slide. When the mechanism is in an unlocked position, the weapon functions as originally intended by the manufacturer.

Patent number: 05062232
Issue Date: 11-05-1991
Inventor 1: Eppler; Larry D.
Title: Safety device for firearms

- Abstract:** A safety device for firearms having trigger interrupting means operably connected to the trigger mechanism of the firearm. The code generating means worn by the user or operated by the user generates a signal which is detected by detection means on the weapon to disengage the trigger interrupting means to permit the weapon to selectively be fired by an authorized user.
- Patent number:** 5068989 (also see 5192818, 5423143)
Issue Date: 12-03-1991
Inventor 1: Martin; John M.
Title: Mean for reducing the criminal usefulness of dischargeable hand weapons
Abstract: Methods and apparatuses for reducing the criminal usefulness of a dischargeable hand weapon wherein the weapon is temporarily or permanently linked to a relatively heavy, bulky or long object by either a cord, cable, or signal, wherein the weapon may be prevented from discharging immediately after or a certain amount of time after it becomes unlinked from the object and wherein the object must be moved with the weapon when the weapon is taken to a relatively distant location for discharging, thereby effectively reducing the portability and concealability of the weapon for distant locations where it is more likely to be used for a crime.
- Patent number:** 05168114
Issue Date: 12-01-1992
Inventor 1: Enget; Jerome M.
Title: Automatic gun safety device
Abstract: An automatic gun safety device is provided which consists of a mechanism for transmitting radio signals. Another mechanism is built into a firearm for receiving the radio signals. A solenoid is electrically connected to the receiving mechanism and is normally in engagement with a trigger of the firearm, so that the firearm can only be fired, when the transmitting mechanism is within range of the receiving mechanism and a properly coded signal is being received by the receiving mechanism. The receiving mechanism which is housed within the firearm will activate the solenoid to disengage with the trigger of the firearm, allowing the trigger to be depressed to fire the firearm.
- Patent number:** 05171924
Issue Date: 12-15-1992
Inventor 1: Honey; Michael T.
Inventor 2: Osborne; Kendall S.
Inventor 3: Ruston; Richard D.
Title: Flagged firearm lock method and apparatus
Abstract: The invention comprises a system for facilitating the locking of a firearm to prevent its unauthorized firing. The system provides an easily noticeable flagging device to facilitate visual affirmation that a firearm lock is engaged; and the firearm cannot be discharged until it has been unlocked. The locking system utilizes a locking wedge that activates a set of locking spurs so as to engage the interior of the firearm and disable the firing mechanism. The system provides for quick and simple enabling of the firearm to facilitate a quick response in an emergency. The system makes use of locking device that can be inserted or extracted through the barrel of a firearm using a key rod. The locking device is

not readily apparent or accessible externally to an observer. The system may be used to lock a firearm that is either loaded or empty, although it is obviously preferable and a proper precaution to apply the system only to empty firearms.

Patent number: 05235763
Issue Date: 08-17-1993
Inventor 1: Nosler; Robert A.
Inventor 2: Lewis; William I.
Title: Key-actuated safety for handgun
Abstract: A key actuated safety mechanism is described for mounting in the hand grip of a revolver or other hand gun. The safety mechanism includes a rotary operator having an eccentric projection which upon rotation to a locked portion directly engages the hand gun firing mechanism as a stop to prevent firing, or is coupled too such firing mechanism by a lock bar which acts as the stop. An improved key actuated rotary lock for use with such safety mechanism is also described having a cam actuated, spring biased plunger operated by the key inserted into an opening through such plunger for enabling the lock to be rotated between locked and unlocked positions.

Patent number: 05303495
Issue Date: 04-19-1994
Inventor 1: Harthcock; Jerry D.
Title: Personal weapon system
Abstract: A personal weapon system comprises a microprocessor-controlled and electronically fired "blow-forward" handgun with a firing parameter memory device, digital security lock and safety device, directional compass, electronic rounds counter, integral keyboard and liquid crystal display, laser designator capability, programmable piezo-resistive trigger, and high frequency A.c. ignitable Primer. A microprocessor receives information from a real time clock, hall-effect rounds counter, and an integral hall-effect compass. The processor displays this information on the lcd display for the operator. When a round is fired, the microprocessor records time and date, number of rounds fired, and direction of firing for crime lab analysis. The trigger pressure required to fire the handgun is programmable by the operator, and a corresponding trigger detonation mark is displayed on the lcd display. Trigger pressure exerted by the operator is displayed on the lcd display as a bar graph which lengthens in proportion to trigger pressure applied. The weapon fires when the bar graph reaches the trigger detonation mark.

Patent number: 05361525
Issue Date: 11-08-1994
Inventor 1: Bowes; Kenneth E.
Title: Gun safety lock
Abstract: An improved gun safety lock is disclosed which employs a barrel key to enable the firing mechanism of the gun. The barrel key is inserted in the handle of the gun to allow the hammer of the weapon to be moved into a cocked or firing position. The barrel key is unique for each gun. The barrel key is held in the gun by retaining lugs. A lanyard attaches to the barrel key on one end and to the owner of the gun on the other end. Pressure on the lanyard causes the key to pull

out of the gun and thereby disables the gun.

Patent number: 05392552
Issue Date: 02-28-1995
Inventor 1: Mccarthy; Joseph
Inventor 2: Hochstein; peter A.
Title: Lighted locks for firearms
Abstract: An electronic firearm lock (10) includes a housing (18) and a locking plate (28) which are locked together rendering the trigger (12) of a firearm (16) inaccessible. The housing (18) includes a locking lever (36) which engages a sawtooth surface (34) of the locking member (32) of the locking plate (28). The lock is unlocked by entering an input code via keypad (44). The keypad (44) is illuminated prior to the pressing of any button (100) by touching two conductors (62) simultaneously by the same object, i.e., a finger allowing the operator to see the keypad (44) before the needing to begin entering an incorrect code. an alarm transducer (82) signals both when a plurality of incorrect codes are entered, indicating an unauthorized person was attempting to access the firearm (16), and when the voltage level of the battery (74) is low

Patent number: 05419069
Issue Date: 05-30-1995
Inventor 1: Mumbleau; Dean W.
Inventor 2: Mumbleau; Craig T.
Title: Firearm locking mechanism
Abstract: A firearm locking mechanism comprising block or body having a conventional pin-tumbler or cylindrical lock mounted generally vertically therein. The block or body is received within the exposed area between the breech and open breech block in a firearm directly above the magazine, with an engagement member connected to the bottom of the lock being received within the top of the magazine and rotated by the lock. The engagement member engages beneath and between the cartridge-retaining surfaces at the top of the magazine to secure the lock and body to the top of the magazine, thereby preventing the breech block from closing or the magazine from being removed. The locking mechanism similarly prevents moving the firing pin assembly into proximity with any cartridge remaining in the barrel or magazine.

Patent number: 05433028
Issue Date: 07-18-1995
Inventor 1: Novak; Vicente N.
Inventor 2: Fard; Amir H. F.
Title: Gun's trigger locking mechanism
Abstract: This device selectively locks the trigger of a firearm by the action of a hollow pin that, pushed by a spring, fits inside a cavity made at the bottom of the trigger. This hollow pin is welded to a flat steel bar that fits along a groove inside the horizontal part of the trigger guard. This trigger guard is made of a non-magnetizable material. The flat steel bar pivots by the use of a horizontal pin that can be locked at the front of the trigger guard, depending of the needs of the designers of the different guns. This flat steel bar has an up and down motion to lock and unlock the trigger. To release the trigger, the user of the gun wears a flat

magnet with a magnetization pattern parallel to its thickness. This magnet should be attached to the exterior surface of the second phalanx of the middle finger of the shooting hand either mounted to a ring or sewn to a glove. In this way the magnet will be located under the trigger guard when the gun is held, and the pulling of the magnet will move the bar and the locking pin (hollow pin) down, unlocking the firearm. If the gun is dropped or taken away from the owner, it will not shoot. Neither will shoot if someone takes the gun unaware of the need of the magnet.

Patent number: 05448847
Issue Date: 09-12-1995
Inventor 1: Teetzel; James W.
Title: Weapon lock and target authenticating apparatus
Abstract: A lock and target authentication apparatus for handguns and rifles. the apparatus is designed to fit into handgrips that replace the factory provided handgrips. Flexible membrane circuitry is contained within the handgrips as well as the power source for the apparatus so that the unit does not have to make part of the weapon and can easily be added afterward. The only other modification of the weapon that is necessary is to make a slight change to the trigger assembly or trigger bar. An infra red signal is communicated from a remote transmitter that unlocks a solenoid mechanism that prevents the weapon from being fired. The signal is unique to the weapon. the apparatus also features a target authentication ability so that a number of weapons can communicate with one another to prevent a weapon from being fired at them if that weapon receives a preselectable infra red signal that indicates to the apparatus that the other weapon is a "friend" and not a "Foe".

Patent number: 05459957
Issue Date: 10-24-1995
Inventor 1: Winer; Guy T.
Title: Gun security and safety system
Abstract: A security and safety mechanism for a firearm including a disabling unit that interacts with a firearm grip safety in order to enable/disable the firearm. The firearm will remain in a disabled state unless a verification means determines that a firearm user is an authorized firearm user. The security and safety mechanism utilizes voice recognition technology in order to ascertain whether a firearm user is an authorized firearm user.

Patent number: 05461812
Issue Date: 10-31-1995
Inventor 1: Bennett; Emeric S.
Title: Method and apparatus for a weapon firing safety system
Abstract: This invention teaches a novel method of safeguarding and protecting a weapon from being accidentally fired or misused by an unauthorized person. Without a verified pre-registration signal, an arming safety solenoid remains in a fail-safe position, preventing use of the weapon. The electronically actuated solenoid enables the use of trigger only when a valid identification signal is received. The system is comprised of microminiature circuits contained within the grip of the weapon and a ring that is worn on same hand that uses the firearm. :When the

weapon is first pickup by the intended user, a switch closure in the grip of the gun turns on a transmitter, which sends a low power, limited range interrogation signal to the finger ring. Upon receipt of this signal, a transponder mounted within the finger ring responds by sending a coded signal that contains a serial number identification. A microprocessor contained within the weapon then compares this decoded signal with one preregistered serial number stored in memory and if the comparison is valid, actuates the arming safety solenoid, allowing the gun to be fired. Arming the weapon for firing can only be accomplished upon receipt of a verifiable identification signal from the finger ring; the finger ring must be worn by user and be within the range of the electromagnetic transceivers and must be within the range of the magnetic metal sensors.

Distribution:

1	Raymond L. Downs	
	National Institute of Justice	
	633 Indiana Avenue, NW	
	Washington, DC 20531	
1	MS9018	Central Technical Files, 8523-2
5	MS0899	Technical Library, 4414
1	MS0619	Print Media, 12615
2	MS0100	Document Processing, 7613-2
		For DOE/OSTI
1	MS0769	D Miyoshi, 5800
1	MS0762	D Spencer, 5861
1	MS2643	D Plummer, 2643
1	MS2643	K Tweet, 2643
1	MS0509	D Williams, 2300
1	MS0537	M Mundt, 2314
1	MS0537	D Brandt, 2314
2	MS0537	D Weiss, 2314