SANDIA REPORT

SAND96–1131
Unlimited Release
Printed May 1996

Smart Gun Technology Project Final Report

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)

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

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: A08
Microfiche copy: A01

Smart Gun Technology Project
Final Report

D. R. Weiss

February 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.

SAND96-1131
Unlimited Release
Printed May 1996

Smart Gun Technology Project Final Report

D. R. Weiss
Power Electronics and Custom Controllers Department
Sandia National Laboratories
Albuquerque, New Mexico 87185-0537

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 (or "smart") surety technologies. This project was funded by the National Institute of Justice which is the research and development agency for the U.S. Department of Justice. This report lists the findings and results of the project's three primary objectives. First, to find and document the requirements for a smart firearm technology that law enforcement officers will value. Second, to investigate, evaluate, and prioritize technologies that meet the requirements for a law enforcement officer's smart firearm. Third, to demonstrate and document the most promising technology's usefulness in models of a smart firearm.

Acknowledgments

Thanks go out to all of people who supplied the information to make this report possible. This report consists of the aggregate ideas of many people who work in, and are knowledgeable about, the law enforcement profession, firearms, and various technologies. Special thanks go to team members Dale Brandt (the lead electrical engineer, and designer of the demonstration models), Kerry Tweet (the lead mechanical engineer, who also drafted Chapter 11 and Appendix A), and Debbie Spencer (Criminal Justice Coordinator). Without their efforts this project would not have been possible.

Reader Feedback

This report is the final documentation for the Smart Gun Technology Project. Even though this is the final report for this project there is still much work to do before a smart gun system can be fielded for use. We are constantly looking for ways to improve the information and the processes documented 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 research 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

Table of Figures

Preface

The following guide is to assist those readers that have read the projects previously released preliminary reports.

With the following exceptions all of the material presented in this final report is new:

Chapters 1, 2, 4, 5, and Appendices A, B, and C are from the project's first report: *Smart Gun Technology Requirements Preliminary Report*. There are no significant changes to the content of these chapters.

Chapters 1, 3, 6-12, and Appendix D are from the project's second report: *Evaluation of Smart Gun Technologies Preliminary Report*. There are no significant changes to the content of these chapters.

This page intentionally left blank.

Executive Summary

Issues and Findings

Discussed: A research and evaluation project was completed to determine if technologies are available that could meet law enforcement officers' requirements for a user authorized firearm.

Key Issues: The questions researched during this project include:

- What are the law enforcement officers' requirements for a smart gun?
- Do technologies already exist that can meet the officers' requirements?
- How would a smart gun operate?

Key findings: The results of this project include:

- Numerous officers have been killed by adversaries who obtained an officer's firearm (See Figure 1).
- Officers have very idealistic requirements for a smart gun technology.
- Many technologies have favorable attributes to meet a subset of the officer's requirements, but there is not currently a perfect smart gun technology.
- Demonstration models illustrated operational concepts and validated both the officers' requirements and technology evaluations.

The Smart Gun Technology Project

By Douglas R. Weiss

"It will never happen to me," and "The only officers that are killed with their own guns are those who give them away" are the types of comments that were sometimes heard from law enforcement officers when research on firearm takeaways in law enforcement began. When the records are studied it is seen that numerous officers have been killed in the line of duty with their own service firearm, as many as nineteen in a single year (See Figure 1). A smart gun technology, one that could enable a firearm only after identifying an authorized firearm user, is one method of eliminating or reducing the number of these deaths.

The Smart Gun Technology Project was funded by the National Institute of Justice (NIJ) in April 1994. The research that the NIJ requested was organized into three primary objectives: first, to find the requirements that a law enforcement officer has for a smart gun technology; second,

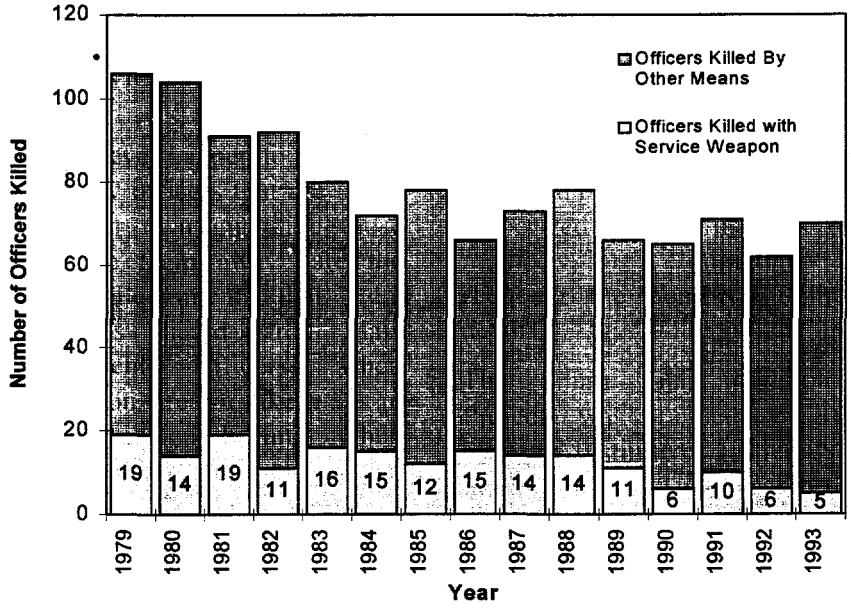


Figure 1. Number Of Officers Killed With A Service Firearm

to evaluate various existing technologies by comparison with requirements obtained from officers; third, to develop models to demonstrate how a technology might operate in a smart gun system. All of these objectives are focused on meeting the project goal of eliminating the capability of an unauthorized user from firing a law enforcement officer's firearm by implementing *user-recognizing-and-authorizing*, or "smart", technologies.

Gathering Requirements

Information was needed on the occurrence of takeaways to prove the need for smart gun technologies to officers (see "Is There A Takeaway Problem?"). Actual takeaway data was used to show officers that takeaway incidents occur. When officers realized that an average of 16% of the all the officers killed in the line of duty are killed by an adversary with a service firearm, either their own or another officer's, they were more interested in looking for a possible solution to the takeaway

Is there a takeaway problem?

Most officers underestimate the number of officers who have been killed with a service weapon, either their own or their partner's, because it was obtained by an adversary. Officers that have been through the experience often do not like to talk about it. It is said that some may not even report the incidents. It needs to be remembered that whenever an officer enters a situation there is a firearm present.

From survey results, only a few officers offered that weapon takeaways are not a problem and other more critical topics should be studied. The majority of officers have never seen the statistics surrounding takeaways. There are also false rumors circulated, such as the only time an officer is killed with his own firearm is when the firearm was surrendered to the suspect.

Some indirect evidence that there is a takeaway problem can be seen by the amount of emphasis placed on firearm retention training at police training academies, the wide selection of security holsters available, and the Federal Bureau of Investigations (FBI) continued interest in tallying the number of these deaths.

The FBI gathers information on officers killed in the line of duty. One of the items that is tracked is the number of officers killed with their own weapon. The total is published in the FBI's Law Enforcement Officers Killed and Assaulted report. A box is checked if an officer is killed with his own gun, and the tally of these boxes gives the official number of takeaways for the United States. If an officer is killed with another officer's service firearm it is not included.

FBI reports from 1979 to 1992 were analyzed to extract information concerning officers killed with service weapons. Officers deaths were reviewed to include other officers, such as partners, that were killed with a service firearm by an adversary. Since the FBI's tally does not include these other deaths, their number is conservative. Deaths that neither calculation includes are non-law enforcement personnel that are killed when an officer's firearm is taken. (While the FBI tracks officers that are killed during takeaways incidents, much less information is known about the number of takeaways that do not result in a death.)

Research revealed that during this time frame an average of 16% of the officers killed were killed with a service firearm, either the officer's own or another officer's, in the hands of an adversary. This totaled 182 officers killed in 178 separate incidents during the fourteen year period.

Fortunately the number of these deaths has been decreasing since a peak in 1986 (as seen in Figure 1). Some possible reasons for the decline in deaths may be increased awareness of the problem, the more frequent use of security holsters, changing from revolvers to semiautomatics, and the increased use of body armor among officers.

Over half of the total number of takeaway incidents resulting in an officer death have occurred in the

problem. The percentage could be made to look worse if the officers that are killed in non-firearm related incidents (accidental deaths) are removed from the calculations.

To understand the attitudes of the officers toward smart gun technologies a survey was developed. The survey questions were designed to understand the conditions that influence officers' thinking and actions when dealing with their firearms. The responses were characterized to determine the types and number of concerns of officers (See "Survey of Officer's Concerns). The concerns found in the surveys were combined and validated with information from other sources such as live interviews and periodicals. The principal result of this process was a list of officers' concerns about smart gun technologies.

South region as defined by the FBI. Following the South (56%), in order, are the Midwest (19%), West (14%), and Northeast (10%). The reason that the South region has had more than twice the takeaways resulting in death than the next closest region is not known. When compared to other regions the answer is not directly related to population or the number of officers.

Other takeaway facts:

- Incidents occur in various locations, mainly along a roadway after a traffic stop. Quite a few occur while transporting prisoners, and at police departments.
- The most common motive for an attack on an officer is to escape from the officer[1].
- A struggle usually ensues prior to a takeaway. In only 8% of the documented incidents were the firearms taken by another means such as by surprise, or stolen.
- The physical condition of the victim officers are average or above average[2].

Officer's Requirements

For each of the officers' concerns a deductive approach was used to document the reasons behind their viewpoint. This approach allowed requirements for the smart gun technologies to be extracted from their concerns. While the set of smart gun technologies describes the idealistic "wants" of law enforcement officers, it is understood that the actual "needs" are a subset of the wants. These wants set a target for the optimum smart gun technology. Although it may or may not be possible to meet the officers' ideal, this sets a standard that can be used to rank various implementations of technologies.

Figure 2 shows the officers' concerns relating to smart gun technologies compared to the number of survey responses. The primary concern that officers expressed was the effect of a smart gun technology on the reliability of the firearm system. To the officer the firearm is another tool that is available to be used. The difference is that the firearm is only used when the circumstances of the officer's work demand that lethal force be used. Then the firearm must work because the officer's or another person's life is at stake.

The second most frequently listed concern by officers requires that the smart gun technology be able to operate in all the circumstances and environments in which an officer could conceivably find himself. The officer's firearm must operate in the worst possible environments the officer may face.

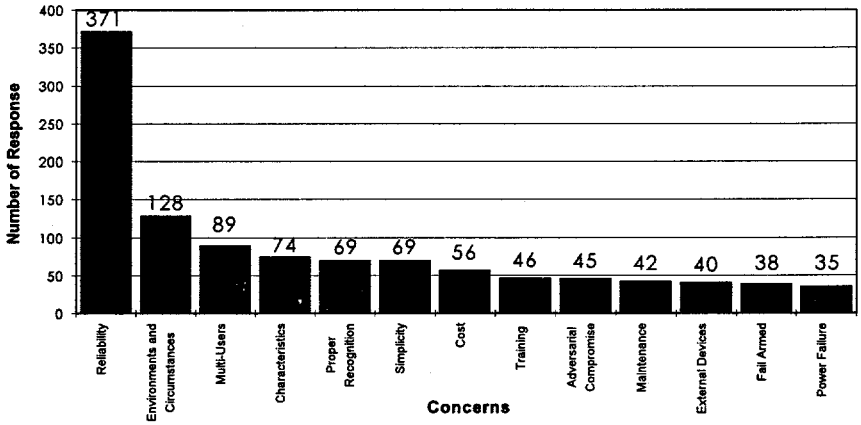


Figure 2. Officer's Concerns Relating to Smart Gun Technologies

Gaining an officer's trust in a smart gun technology is a hurdle that must be overcome. The technology must be able to separate the authorized users from unauthorized users. Officers want the capability to use another officer's weapon if the need arises. They also want to be able to use a weapon with either hand. The technology must be simple and affordable. The encompassing desire that officers have is that a smart gun technology does not interfere with the manner in which current firearms operate, except by limiting the use to an authorized individual.

Survey of officers' concerns

A survey was used to obtain information from law enforcement officers. Questions were designed to draw out officer's attitudes about smart gun technologies. Surveys were mailed to police departments, distributed at law enforcement conferences and published in the American Society of Law Enforcement Trainers Journal. The method of distribution was not intended to give a scientific sampling of law enforcement, but did result in a broad sample.

Analysis of the information included both the interpretation of the open ended questions, and calculation of statistics from the closed ended numerical responses. Follow-up interviews were conducted in person and by telephone until the trends of the answers were repeating. The interviews sought to check the interpretation of the questions to validate the survey, to understand the importance of the answers, and understand any extenuating circumstances that may have influenced the answers.

Responses were received from across the country, with the returns generally matching the population characteristics of the regions. The exception was the greater return from the South region (58%) as defined by the FBI. This is also the region that had the greatest percentage of officers killed in takeaway incidents. The majority of the returned surveys were from city, or municipal, police departments (63%), the next largest percentages of respondents were from county agencies (11%). These two types of agencies jointly provide most of the law enforcement service in the Nation. Surveys were also received from training academies, Federal, State, Tribal, University, and unknown agencies.

A wide range of personnel responded to the survey, from management positions, to trainers, to patrol officers. The majority of the responses came from officers having field duties, and over a quarter came from officers involved in training. The officers also had a wide range of experience. Over half of the officers were in the range of 11-25 years experience in law enforcement.

Evaluating Technologies

An evaluation method was needed that could trace the officers' requirements as the determinate factor in the rankings. A process called quality functional deployment (QFD) was used to transform the officers' sometimes general requirements into the more definite requirements needed for the evaluations. After the specific requirements were listed, each technology was ranked against each requirement to determine a final ranking between all the technologies. Since many of the officers' requirements relate to the final implementation of a product, as opposed to a technology that may be included into a product, some of the requirements could not be used for ranking purposes. The ranking that was completed, therefore, focuses on the basic operational aspects of the technology in a smart gun system.

Three categories of technologies were investigated: Automatic Identification, Biometrics, and Miscellaneous. Automatic identification is a broad classification of technologies for devices that can be used to track items without human involvement. Generally speaking these are electronic devices that use some type of code for their unique key. Biometric technologies are those that base their uniqueness 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. Other devices were

Demonstration Model Evaluations

The third objective of the smart gun technology project was to demonstrate the usefulness of promising technologies in models. Five models were developed to show the strengths and weaknesses of various technologies. The purpose of the models was to illustrate the principles showing how a smart gun technology would operate, and provide a visual aid when discussing the project with law enforcement officers and others. Five models were fabricated: Touch Memory, Remote Control, RF Tag, Fingerprint, and Speech Recognition.

The breadboard models are not functional prototypes, although they have features that approximate those of a final product. Each of the models were built into an identically sized box that held any additional electronics necessary to show how the technology would recognize an individual. The models performed an enabling operation that was displayed for the user.

The breadboard models were built from existing commercial equipment that was modified into configurations to emulate a smart gun. Even though the models were not functional firearms, they had to give the impression to a professional firearm user that the device was acting like a smart gun would operate.

Technologies were selected not only to show how a particular implementation of a technology would operate, but also to show how a class of technologies with similar characteristics might operate. By proper selection of the technologies to be modeled, the comments that officers made during reviews could be extrapolated to different technologies with similar characteristics.

What the models could not demonstrate to the officers were non-tangible items like the technology's cost, reliability, and adversarial strengths. Items like these will remain a concern for officers until a fieldable prototype is thoroughly tested.

grouped into the miscellaneous technologies category. Many of these devices are mechanical and have the benefit of not necessarily requiring a power source like the electronic devices.

Demonstration models were fabricated after the initial evaluations were complete. The models were chosen to highlight the strengths and weaknesses of selected technologies (See "Demonstration Models"). The models were demonstrated to law enforcement personnel to obtain comments. In this way both the officer's requirements, and the ongoing evaluations could be validated.

The Results

Fifteen implementations of fourteen technologies were evaluated in detail. The implementation of the technologies can affect the ranking. What was considered to be the most appropriate implementations were ranked for

each of the technologies, each maintaining the basic building blocks of a smart gun system (see "Smart Gun Analogy"). Each implementation was scored according to how well it met 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 both the law enforcement officer and the designer. Done in a style similar to popular consumer magazines, Figure 3 shows the rankings for the technologies (without importances) compared to specific categories of requirements. The category headings are self evident descriptors of the requirements contained within that category. In this case the rankings are shown without the importances so that the readers can decide for themselves what is important. The symbols used in the rankings are shown in the figure.

Figure 4 shows that there is no perfect technology: one that will meet all the officer's requirements. Existing technologies that have been optimized for other commercial applications were evaluated. The companies who develop these technologies have not targeted a firearm application for their products. The chart shows that the highest grade that any of the technologies received was a "B". The grades were obtained from the numerical scores for all the ranked requirements. More work needs to be done to all the technologies to bring them to a level that a law enforcement officer will value.

The top four technologies all are radio frequency devices. One 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 these electrical devices use a code that can be quickly transmitted and checked for errors giving it a high rate of

● = 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 3 Evaluation of Technologies Compared to Requirements

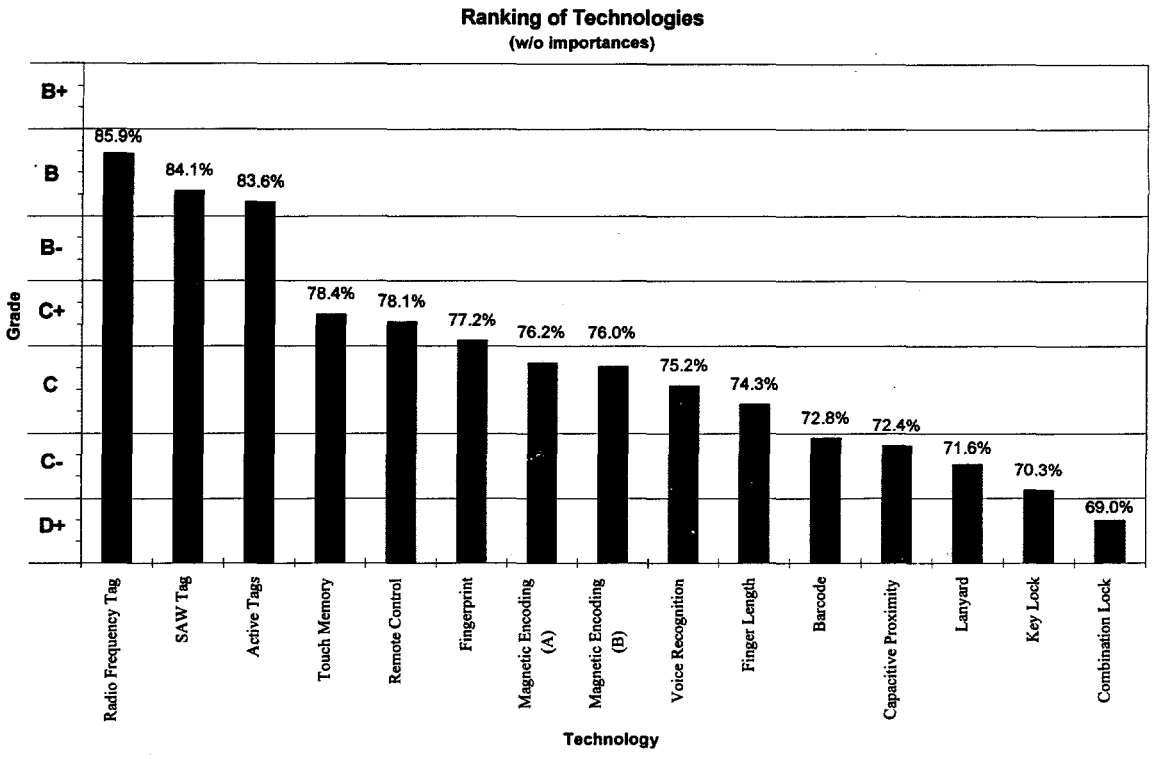


Figure 4. Ranking of Technologies (without importances)

accepting authorized users. The biggest concern of the radio frequency devices is electromagnetic interference that would prevent the normal communication from occurring. Officers reviewing the radio frequency models liked that there was not critical alignment, or any contact, between the model's key and the discriminator. The radio frequency models could also be operated while wearing gloves. For the remote control model, a few officers liked the control of manually turning the firearm on or off, even though this contradicted their own requirement of not requiring an action.

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. Officers evaluating the touch memory model were concerned about the alignment necessary between the key and the discriminator, and that contaminants could interfere with the communication channel. Many officers also are concerned about any technology that requires them to wear an item such as a ring, or a watchband, that they could forget.

Fingerprinting technology ranked as high as it did because of the uniqueness of its key (fingerprint). The key is always available to the officer: it cannot be forgotten. The problems have to do with the time it takes to obtain a completed reading of the fingerprint, and with contaminants interfering with the reading between the key and the discriminator. Officers trying the fingerprint model were primarily concerned with the size and speed of the technology. Also, an injured finger, with simple cuts, scrapes, or blood, may not be recognized by the firearm.

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. While implementation A has a better discriminator making it less orientation critical, implementation B may not require the use of any power source. The concern is the alignment of the key with the discriminator.

Voice recognition is another biometric technology, but in this case the key cannot be discriminated as well as a 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 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.

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

Smart Gun Analogy

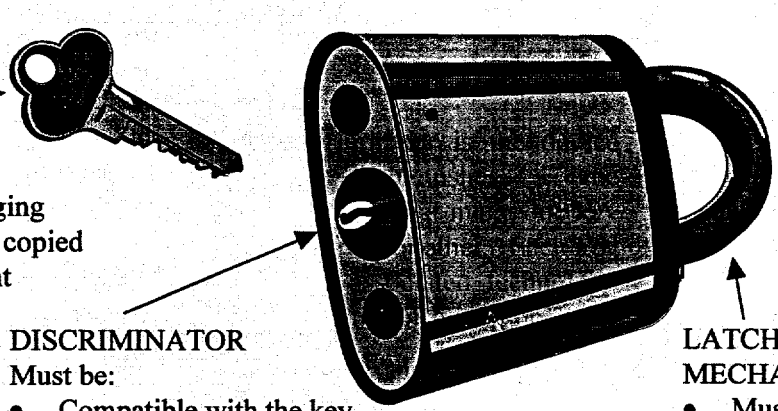
A smart gun system may be viewed as a type of security system for a firearm. As an analogy, it is described in terms of a key operated padlock. The analogy is organized into three pieces: a key, a discriminator, and a latching mechanism.

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.

The Smart Gun Technology project focused on the evaluations of potential combinations of keys and discriminators. The design and implementation of a latching mechanism is left to the firearm manufacturers. This makes sense because this is their expertise: each firearm's mechanism has been optimally designed, and this limits the reliability and liability concerns of having a mechanism being put into the firearm.



KEY
Must be:
- Unique
- Non-changing
- Not easily copied
- Convenient

DISCRIMINATOR
Must be:
- Compatible with the key
- Able to distinguish between keys

LATCHING MECHANISM
- Must be able to disable the firing mechanism

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 by an officer during a takeaway situation.

Conclusions

The National Institute of Justice was correct when they recognized that a number of officers are being killed each year with their own service firearms. The research validated the problem of takeaways and revealed that up to 19 officers a year have been killed during takeaway incidents. The number of deaths may not be as large as some other categories of officer deaths, but at an average of 16% of all the officers killed it is a significant percentage.

Officers have a very difficult set of requirements for a smart gun technology. One reason that the officers' requirements are so difficult is that the documented set of requirements contain the idealistic wants of the officers, which is suspected to be greater than their actual needs.

Officers want their firearm to operate predictably: the firearm must remain reliable in all the environments and circumstances that an officer may encounter. This summarizes the most important requirements that need to be satisfied. It is expected that if these items can be met, then the other requirements become negotiable.

The requirements led to an analogy for a smart gun system. The system can be viewed as a lock and key for a firearm. The key is any unique item that the firearm can recognize. The lock is divided into a discriminator and a latching mechanism. The discriminator recognizes the key, while the latching mechanism physically enables or disables the firearm.

The officers often gave very qualitative requirements that made evaluation of technologies difficult. Using quality techniques a quantitative set of requirements was formed that could be used to score each technology.

Evaluations of fourteen technologies showed that each technology had characteristics that scored high in individual categories. Mechanical technologies ranked high for low power consumption and being less expensive. Electronic technologies scored high for their ability to discriminate digital codes. Biometric technologies scored high for being unique as a key. However, the evaluation revealed that no technology currently meets all the officers' idealistic requirements.

Demonstration models were vital for showing officers how smart gun technologies operate. The models stimulated comments that were used to validate the requirements and learn other insights from the officer. Officers generally liked the particular characteristics of each of the technologies that ranked high in the evaluations.

Many of the rankings are so close that a small change in a technology's capabilities, or in the ranking algorithms, could tilt the scales in favor of another technology. 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 documented weaknesses may be overcome.

The consensus among law enforcement officers is that a smart gun is a good idea and could be very beneficial to their work, if it will meet their requirements. 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 obtained during this project is based solely on the law enforcement requirements for a smart gun.

Developing a smart gun that meets law enforcement officers' idealistic requirements is a very difficult task. It may take a generation of smart gun systems to come and go before a smart gun is not only common but is favored over a non-smart gun; this is much as it is with other new technologies. To accomplish this goal a great deal of time and resources will have to be expended to optimize the technologies for the smart gun application.

SECTION 1

INTRODUCTION

Chapter 1

The Smart Gun Technology Project

Firearms are used by assailants in most of the attacks on law enforcement officers that result in serious injury or death. In some of these attacks the officer is killed by his or her own firearm. While the total number nationwide killed in this manner may not be large, the potential threat is present for every officer facing violent and unpredictable subjects. In research back to 1979, as many as 19 deaths per year have occurred from an assailant's use of an officer's firearm.

The 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[3].

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 22 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.

The second project objective is to investigate, evaluate, and prioritize technologies that may meet the requirements for a user-recognizing-and-authorizing firearm. 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 were fabricated to illustrate identification principles as well as demonstrate proof of concept of the most promising technologies.

Initial Comments for the Reader

The following are a set of miscellaneous comments to assist the reader:

- The requirements are given from the viewpoint of the end user, the law enforcement officer. The end user requirements stated are for the technologies used in a smart gun, not for the firearm itself. Sometimes the boundaries between the technology and the smart gun system are not evident. It should be understood that the technology is only one part of the total system along with the officer and the firearm, and that the technology may only meet a requirement in combination with the entire system. It is expected that technologists are able to extract the necessary information to meet their particular needs.
- This report often describes the idealistic "wants" of law enforcement officers; it is understood that the actual "needs" are a subset of the wants. These wants set a target for the optimum smart gun technology. Although it may or may not be possible to meet the ideal, a standard can be set to rank various implementations of technologies.
- The masculine pronoun will be used throughout the report for ease of reading. This is not intended to overlook the role of the female police officer in law enforcement.
- The geographic regions and divisions of the United States used in this report follow those used by the Federal Bureau of Investigation (FBI).
- The report uses phrases such as "officers killed with service weapons" to include both an officer killed by an adversary using his own firearm, as well as an officer killed by an adversary using another officer's firearm. Deaths due to friendly fire, unintentional discharges, etc. are not included by these phrases.

- It is realized that it is easy to offer suggestions to particular instances in hindsight. In any comments about actual incidents of law enforcement officers we are not attempting to second guess their actions.
- Round off error may be detected in some of the figures throughout the report. All calculations were completed before rounding.
- Although rifles, shotguns, and other weapons may be candidates for using smart gun technologies, they will not be specifically addressed in this report.
- Although the potential exists for smart gun technologies to be used in all firearms, the focus of this report will be for law enforcement handguns.

Chapter 2

Firearm Takeaways

The Need For Investigation

Are officers being killed with their own weapons? Are there enough officers being killed with their own weapons to consider it a problem? The answer to the first question is definitely yes. Not only are officers being killed with their own weapons, other officers and even citizens are being killed with officer's service weapons. The answer to the second question is largely a manner of opinion. Some consider a single officer being killed in any manner a problem; others look at the problem statistically for an answer.

From the survey results, only a few officers stated concerns that weapon takeaways are not a problem and other more critical topics should be studied. The majority of officers have never seen the statistics surrounding takeaways. There are also false rumors circulated, such as the only time an officer is killed with his own firearm is when the firearm was surrendered to the suspect. Some officers who have not been involved in a struggle for their firearms believe that training alone can solve the problem. Officers who have been in fierce struggles for their firearms seem to believe that even though training is important, in these situations survival takes over where the training leaves off. If officers being killed with their own weapons were not a problem, there would not be as much emphasis on gun retention training as exists today, and there would not be the availability of products like security retention holsters for the officers. Awareness training of the problem can reveal to officers the extent of the problem of weapon takeaways.

Available Data

The annual report titled Law Enforcement Officers Killed and Assaulted, published by the Federal Bureau of Investigation (FBI), contains the best documented information in the area of takeaways. One problem with this report is that it is a difficult source from which to extract information; the report is sometimes lacking in details or completely fails to include incidents. The process in which the FBI obtains its information depends on the processes of the individual states that are required to supply accurate information on a timely basis. These processes may be lacking, and could affect the accuracy of the report. Information received directly from the FBI data base did not exactly match their own reports; for this document the information was extracted only from the FBI reports. Examples of text from the FBI reports follow (*warning: these are not pleasant reading*):

> Florida, 1991. On January 18 at approximately 8:10 p.m., a 29-year-old patrolman with the Ft. Pierce Police Department for nearly 4 years was shot and killed. After stopping a vehicle going the wrong direction on a one-way street, the patrolman ran record checks on the driver who had given several false names. Since no driver's license could be identified, the patrolman arrested the driver and had him exit the vehicle. While attempting to handcuff him, a struggle ensued during which the driver obtained the patrolman's Sigarms Model P226 9-millimeter semiauto-

matic service weapon. The patrolman was shot once and collapsed on the street. Allegedly, the driver then stood over the patrolman and shot him 12 more times. Although the patrolman was wearing body armor, many of the shots were below his vest. A total of nine rounds entered the patrolman's body; his vest stopped four. An 18-year-old suspect on probation for burglary charges was apprehended about an hour later and charged with Murder.[4]

Illinois, 1990. Two 20-year veteran officers from the Chicago Police Department, ages 43 and 46, were shot and killed at 9:10 p.m. on May 13. The two responded to a domestic quarrel between a grandmother and her grandson at her residence. A struggle ensued when the officers confronted the grandson in the residential garage. During the struggle, the offender managed to obtain one of the victim's service weapons, a Colt Trooper .38-caliber revolver, and shot both in the head, back, and chest. Neither victim was wearing body armor, and both were pronounced dead at the scene. A 23-year-old male was apprehended and charged with two counts of murder.[5]

It can be seen from these examples, some are more descriptive than others. The information in this report reflects our interpretation of the information contained in summaries such as these. This information was later compared to the data extracted from the FBI's database.

In collecting and entering information into their database, the FBI uses the forms submitted by the individual states. One of the pieces of information included is whether the officer was killed with his own service weapon. The FBI data does not reflect if an officer was killed by another officer's firearm (as was one of the officers in the second example). It also does not present data on the number of takeaway attempts, or assaults on officers involving their own service weapons. Only when an officer was killed with his own service weapon was it included in the FBI data; this means the FBI reports contain the most conservative numbers. In reviewing the FBI data we included the number of other officers killed, but did not include deaths due to officers' firearms when turned on others. It is not unusual for a suspect to use the firearm taken from an officer, and used to kill that officer, to wound or kill others, such as innocent citizens, or to take his own life.

There are many cases where the officer's firearm is stolen after he is killed with the suspect's firearm. A smart gun technology may also help eliminate the value in stealing officers' weapons.

Time Frame of Study

FBI reports were analyzed to extract information concerning officers killed with service weapons. Data available from 1979 to 1992 was used for this study. The 1993 detailed FBI report was not yet available, but the information that was available was used where appropriate. This represented a 14-15 year time history to be reviewed. This was considered a sufficient time frame to be reviewed. Included within this time period is the introduction of the security retention holster to law enforcement, and the publishing of other studies that may have increased the awareness of retention problems.

Security Retention Holsters

Various companies that supply duty gear to law enforcement agencies include retention, or grab-resistant, holsters in their product line. The exact year of introduction of these holsters was not determined, although it is known that the holsters grew in popularity during the early to mid 1980's. As with most new equipment it has taken a few years for the retention holsters to become accepted and to fit into police department purchasing cycles, but now many larger departments are changing to retention holsters. Retention holsters are not a panacea.

There is not an industry standard for retention holster operation; this means that any company can name their retention levels any way they like. Holster suppliers state the importance of taking necessary precautions to keep from losing control of a firearm. No holster can completely secure a firearm from being removed by another person or from coming out during vigorous activity. The officer is still responsible for keeping his weapon secure.[6] A few officers complain that retention holsters slow down the natural draw of the holstered weapon, but others say that after some training and practice there is no difference. Retention holsters, with proper training, appear to be the best product available for use today as a preventive measure against firearm takeaways.

Other Studies

Also within the time frame investigated in this study there were reports written documenting the problem of firearm takeaways. One of these reports was released by the California Commission of Peace Officer Standards and Training (POST).[7] This report covered data from 1980 through 1986, and stated in its summary of findings of California officers killed, that the officer's weapon was used by suspects in 15% of the killings; this included both the victim officer or another officer's firearm. They also stated that of those officers assaulted but not killed, 7% were assaulted with their own or another officer's firearm. In their analysis they found that even though the method by which the suspect obtained the officer's firearm varies, the majority of the officers killed or assaulted lost their firearms during a "physical altercation" with the suspect. It is also important to note that the physical condition of the victim officers were average or above average. In the killing incidents, 50% were above average, and the remainder were average physical condition. In the assault cases: 21% were above average, 76% were average, and 3% were below average. One of the training guidelines for officers, resulting from this study, was that each officer should be required to demonstrate proficiency in techniques to prevent the handgun from being taken by the suspect.[8]

In a follow up study, POST investigated the three year period between 1987 and 1989.[9] This report documented many facts concerning incidents where California officers were killed or assaulted. After takeaway incidents agencies often changed training on gun retention, and recommended changes to a more secure holster, ones that impede weapon takeaways. They stated that the most common motive for the felonious killing attacks was to facilitate an escape from the officer. In comparing data to the previous report, they found that the frequency of weapon takeaways resulting in deaths was nearly identical for the two studies: 15 percent for the previous study and 16 percent for this study.

In a special report published by the FBI in 1992, the issue of weapon retention was also addressed.[10] Of the 762 law enforcement officers killed from 1981 through 1990, 110, or 14 percent, were killed with their own weapons. The question was asked, 'How much time is provided for teaching officers weapon retention techniques?' No answer was given.

Takeaways in San Francisco

The San Francisco Police Academy is one of the few agencies that could be found that keeps excellent statistics on weapon retention.[11] These statistics are then used for developing training programs for the officers. The information that is gathered includes the number of attempted and successful takeaways, as well as information on the officer, suspect, and circumstances. An attempt, for the San Francisco data, is defined as anyone making an effort to gain control of an officer's firearm. A success is defined as the officer losing primary control of his weapon. Neither number includes facts about killed or assaulted officers, although 5% of the assaults result in weapon takeaway attempts.

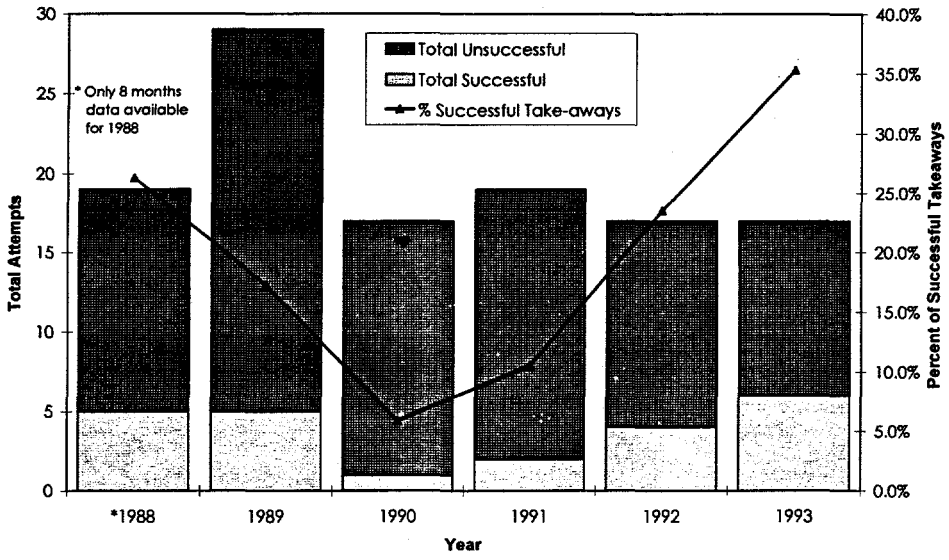


Figure 5. Takeaway Attempts in San Francisco

In Figure 5, numerous things can be observed. Note that for 1988 only 8 months of data was available. If the monthly average of takeaways for that year stayed constant, it would have been worse than 1989. The first thing that is noticed is that in 1990 there was a significant decrease in both the total number of attempts, and the percentage of successful attempts. Since 1990 the number of attempts have remained relatively constant but the percentage of successful takeaways have returned to their original levels and is possibly on an increase.

During 1988-89 there was a 2 hour block of weapon retention training added for the San Francisco officers. It is possible that this training was the cause of the decrease, although if it was the reason, the results were short lived. California POST requires some retention training, but individual agencies decide what and how much to implement. Three hours of retention training has again been added to the current training cycle, with an optional three day course available which officers say helps because of the additional training and practice they receive. In-hand retention is also being taught to the officers, suggesting they use the firearms external safeties. Many adversaries are not proficient with firearms and, if the officer knows he is about to lose his weapon, the simple act of pressing the magazine release or safety may save the officer.

Some of the firearm takeaway trends being found in San Francisco follow. While these trends for attempts in San Francisco do not necessarily match the typical scenario for officers killed around the United States, some valuable information can be obtained.

- Some suspects have practiced weapon takeaways.

  This alarming trend may indicate why successes are increasing. Officers have reported suspects using the same maneuvers they have been taught at the police academies. Other takeaway techniques are taught in magazines and self defense classes for the general public.

- Suspects have typically used alcohol or narcotics.

  Alcohol or narcotics use is indicative of the majority of assaults on officers, and not only for firearm retention. The FBI reports that 76% of cop killers interviewed stated they were engaged in drug or alcohol activity at the time of the killing of the law officer.[12]

- There are typically multiple officers present.
- Successful suspects are typically the same size or smaller than the officer.
- Officers typically have 6-10 years experience.
- Officers are slow to detect that the suspect has turned from a defensive to an offensive role.

These last four trends could suggest that officers let down their guard at certain times or in certain circumstances. Proper tactics must always be used by the officers to eliminate the possibility of takeaways occurring.

Separate statistics on attempted takeaways come from the survey respondents. One of the survey questions asked if a suspect had ever taken, or attempted to take, their firearm. Over one third (38%) of the respondents at some time during their career had been a part of a weapon takeaway attempt.

Typical Takeaway Incidents in the United States

From the data researched for the last 14 years of officers killed, the following information has been charted to understand the typical takeaway incident that resulted in death of an officer.

How many Officers are Killed with a Service Weapon?

The percentage of the officers killed with a service weapon compared to officers killed by any other means varies year to year. Figure 6 shows the number of officers killed with a service weapon as extracted from the FBI reports. These numbers include an officer killed by a suspect using his or another officer's firearm. The number for 1993 is the FBI stated number because the 1993 detailed information was not yet available.

This information reveals that an average of 16% of the officers killed in the line of duty are killed by a suspect armed with a service firearm, either the officer's own or another

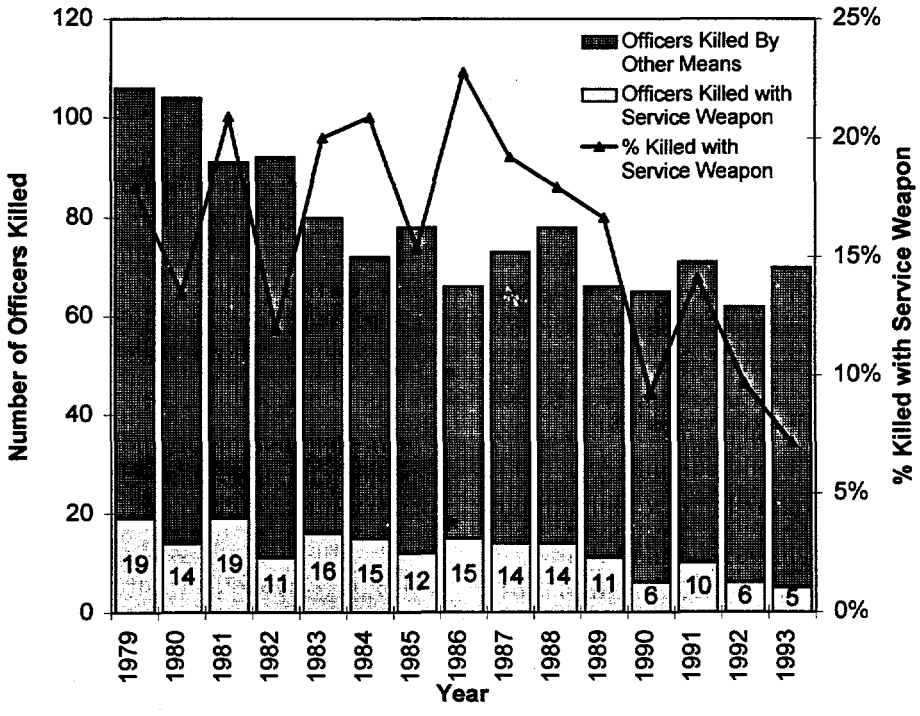


Figure 6. Officers Killed With Service Weapons

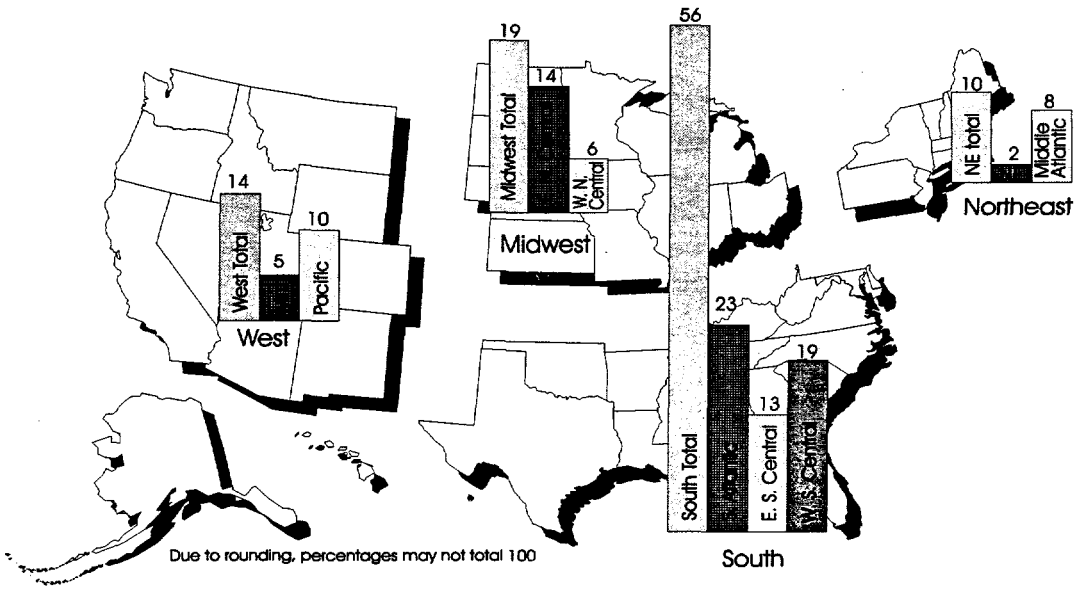


Figure 7. Percent of Total Takeaway Incidents (1979-1992) by Region and Division

officer's. Since a peak in 1986 there has been a downward trend in the percentage of officers killed with a service weapon. While this chart displays the number of officers killed, it says nothing about either the number of assaults on officers with service weapons, or the number of attempted takeaways. Some possible reasons for the decline in deaths may be increased awareness of the problem, the introduction of security retention holsters, a transition from revolvers to pistols, and the increased use of body armor among officers.

In the 14 years of data reviewed, a total of 178 takeaway incidents resulting in an officer's death were reviewed. The number of officers killed in these incidents was 182, giving an average of just over one officer killed per incident where a death occurs. Only seven takeaway incidents occurred which had greater than one officer killed with a service weapon. In all of these incidents two officers were killed; sometimes with one service weapon and sometimes with two. Of the seven incidents where two officers were killed, all were in the South and Midwest regions, with two being in Chicago.

Where do takeaways occur?

Over half of the total number of takeaway incidents resulting in an officer death have occurred in the South region. Following the South, in order, are the Midwest, West, and Northeast regions. Figure 7, shows the percentage of the total incidents for each region, this is then broken down into individual divisions. The reason the South region has had more than twice the takeaways resulting in death than the next closest region is not known. The South does have the largest population of citizens, and ranks second in officer to population ratio. The Northeast, ranked last in takeaways, has the second greatest population and ranks first in ratio of officers.[13]

Showing more detail, Figure 8 displays the takeaway incidents resulting in death by State. While this shows the total number of takeaway incidents during the time period studied it does not show a relationship to the number of officers in that state. Figure 9 shows the number of takeaway incidents per region normalized by the number of full time officers in that division.[14] In this view again the South region stands out as having the most officers killed during takeaways.

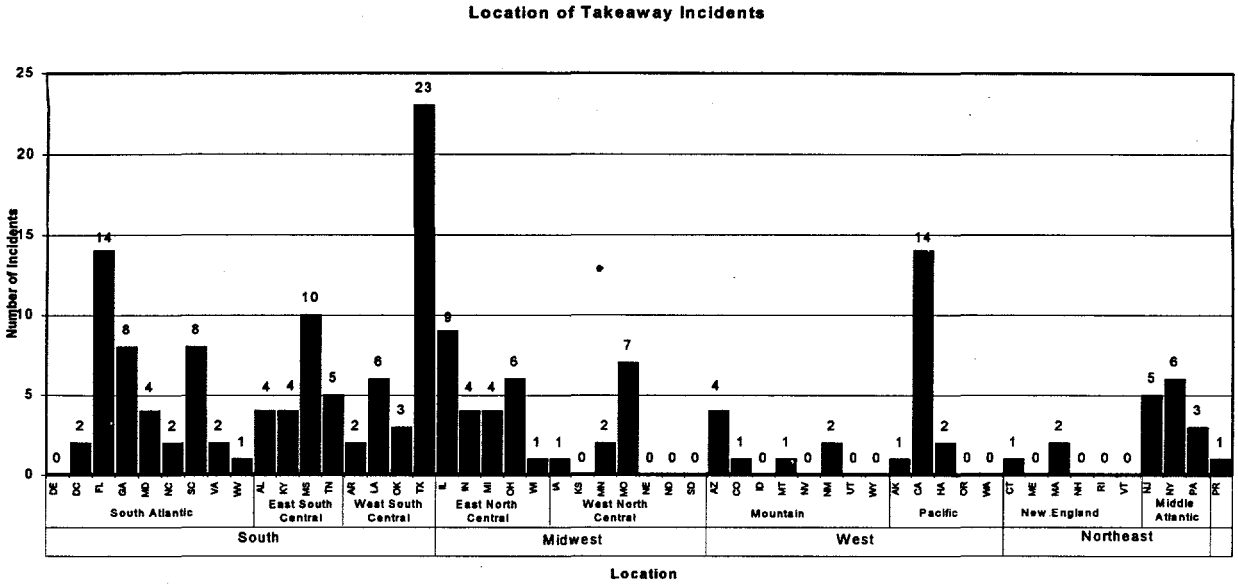


Figure 8. Location of Takeaways Incidents by State, Division, and Region

A typical Incident

The typical takeaway incident starts as a typical call, either to someone's home or a traffic stop. The person is going to be placed under arrest and starts in some manner to resist the arrest. At this time a struggle occurs and at some point in the struggle the suspect realizes he may be able to take control of the officer's firearm and the takeaway attempt begins.

Many variations of this example exist, but some common facts can be seen. Since officers carry firearms, there is a firearm in every situation that the officer enters. Most of the time the firearm is never used, but it is always available to the officer and possibly to the adversary. Most of the incidents occur along a roadway or in a residence, although quite a few occur in transporting prisoners and at police departments. The most common motive for an

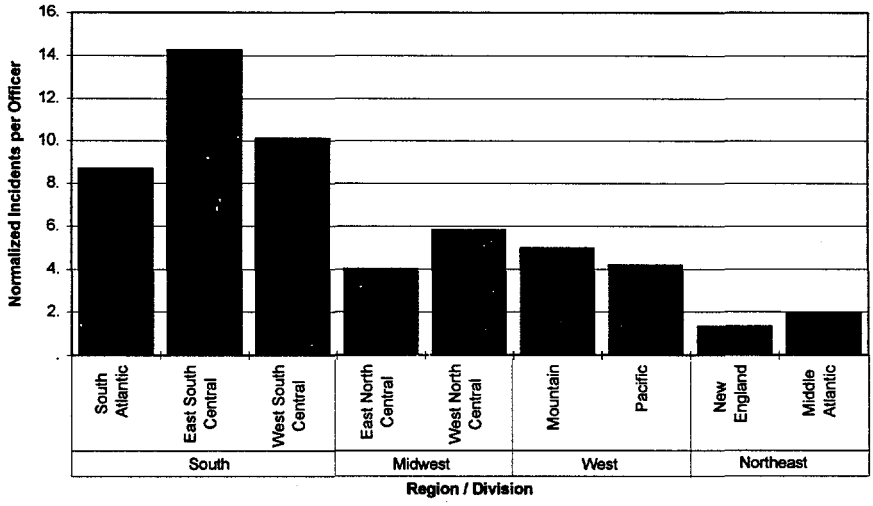


Figure 9. Officers killed in takeaways normalized by the number of officers employed in the division

attack on an officer is to escape from the officer.[15] This attack may result in an attempted takeaway.

A majority of the officers involved in takeaways resulting in their death were killed after a struggle. From the data analyzed, 79% of the incidents involved a struggle, in 13% it is unknown if a struggle occurred. It is not known if the officer was able to draw his firearm in these incidents. Officers relinquishing a firearm to an adversary is not a major cause of takeaway deaths. In the 8% with no struggle, various approaches were taken. These methods include stealing officers' weapons, removing them from their holsters by surprise, or taking officers' weapons after they have been wounded by some means other than a struggle.

The majority of the officers and suspects involved in takeaways are male. Ninety-four percent of the takeaway deaths involved male officers, and 6% were female. The most likely reason for this is that there are more male officers than female. Females make up 8% of the sworn officers in the Nation.[16] Also in the FBI's interviews with offenders they found that some offenders, all males who had killed male officers, stated that they would not have committed the act had the officer been female. The average killer of a law enforcement officer may or may not receive higher status in the prison society for his or her crime, but the one individual interviewed who had killed a female officer found little to boast about within the prison setting. He was even reluctant to talk about the fact that he killed a female.[17]

Officers that are killed with a service weapon are usually killed with their own weapons (86%) rather than another officer's (14%). They are usually in a one on one situation with the suspect. Figure 10 shows the ratio of officers to offenders in the incidents studied. In 78% of the incidents the officer killed was older than the suspect, which is typical for a crime of any type.[18]

The information also shows that the less experienced officer is more likely to be killed with a service weapon. This data is shown in Figure 11, one should note that this is not normalized by the number of officers in each age category. This trend is similar to the historical FBI data for officers slain.[19] This is different from the San Francisco data on attempted takeaways that finds that most takeaway attempts occur to officers in their mid-career years. This may indicate that while more takeaway attempts are made on experienced officers, their experience enables them to remain in control of their firearm.

A takeaway attempt can occur at anytime. Figure 12 shows the known times of takeaway incidents, the greatest percentage or takeaways occur during swing shift hours. This is similar to the historical FBI data for all officers slain[20].

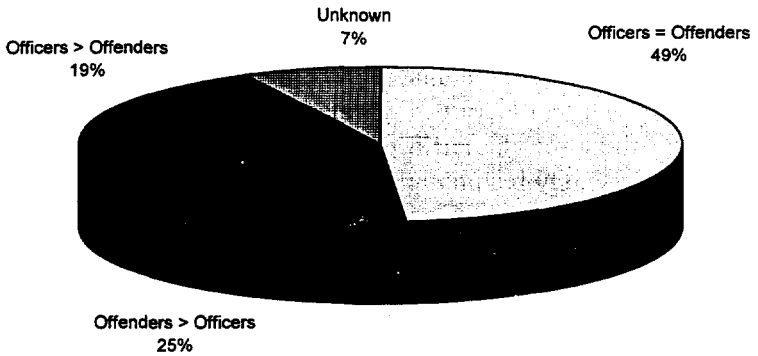


Figure 10. Ratio of Officers to Offenders During Takeaway Incidents

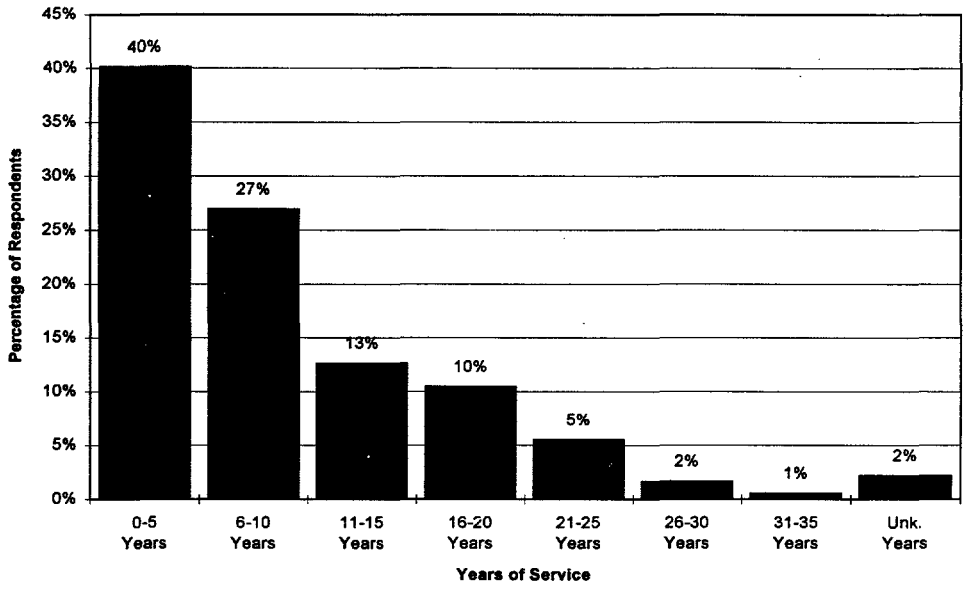


Figure 11. Years of Service of Officers Killed During Takeaways

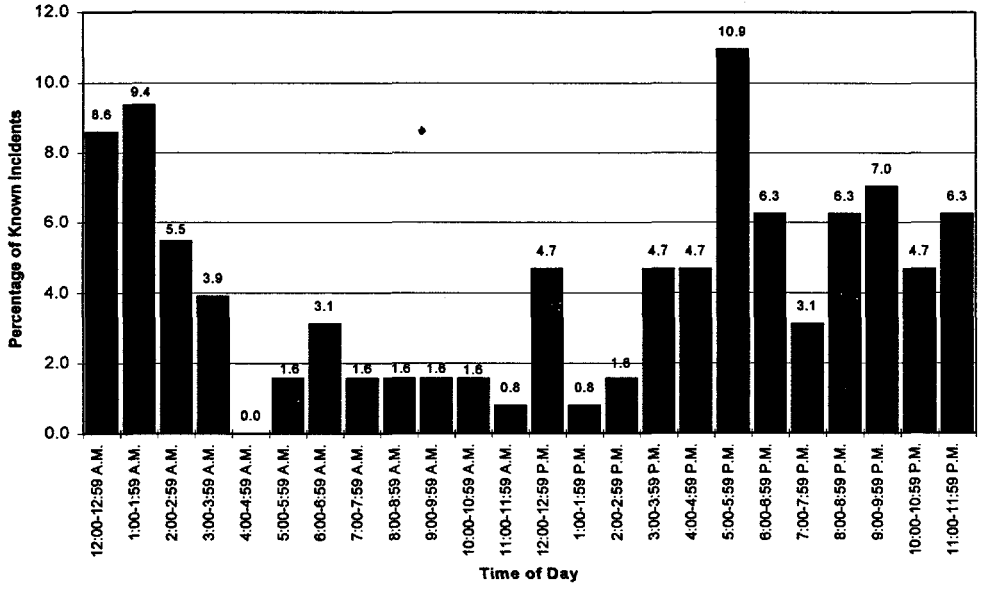


Figure 12. Time of Takeaway Incidents

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 the item that 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 physically secure the protected item.

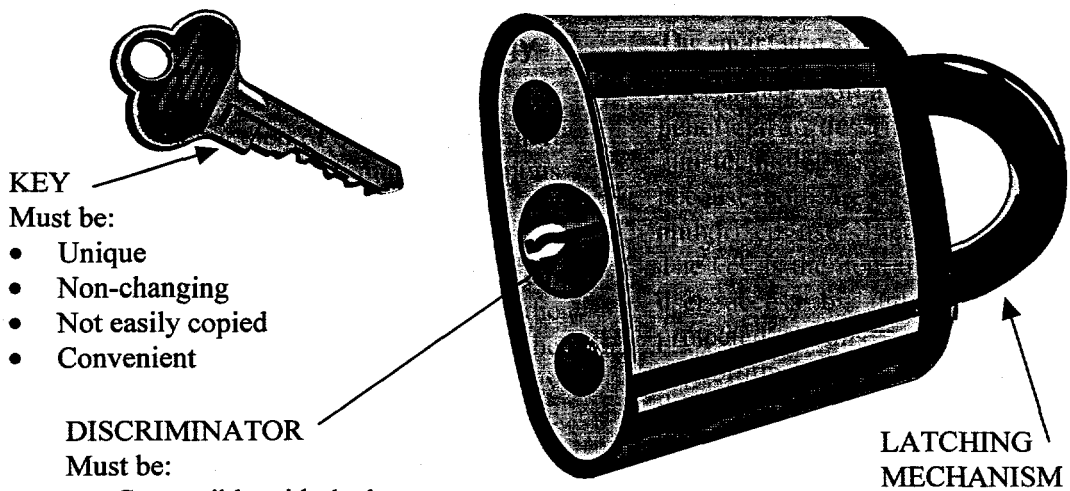


Figure 13 Smart Gun System Analogy

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 were evaluated during this project.

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 project did not address the implementation of the latch, but did 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 firearm 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 primary results of this project. 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 chapter 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".

SECTION 2

THE REQUIREMENTS FOR A SMART GUN TECHNOLOGY

Chapter 4

Requirement Gathering Process

Methodology Overview

To correctly determine the requirements for a smart gun technology a logical approach was taken. Research was conducted to understand the officers, their firearms, their duties, and their requirements for a smart gun. A questionnaire was developed and distributed to officers. This survey was designed to focus on specific smart gun technology issues. The survey was followed with personal and telephone interviews as time allowed. Finally the information was digested into a set of requirements for the technologies. To formulate the requirements for smart gun technologies all the information collected, from the literature, survey analysis, and interviews, was studied for commonalties.

Data Gathering Process

The process followed to gather data, and described in this section, is modeled after the approach used by AT&T Bell Laboratories.[21] The process flow is shown in Figure 14. The process is discussed in detail to disclose the exact techniques used.

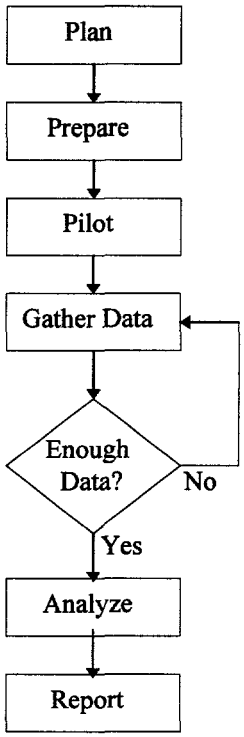


Figure 14. Data Gathering Process Flow

Planning Stage

A broad reaching method was needed to quickly understand the wants and needs of many officers. Information from officers, at all ranks and in various types of law enforcement, was needed to understand officer's viewpoints on a number of issues. During the planning stage of the process the survey objective, and methods of obtaining information were developed. The type of information that was needed was determined, and the location of that data was documented. Initial plans were developed for each stage of the process and a Data Gathering Plan drafted.

Preparation Stage

The process continues with the preparation stage. In this stage the areas to be covered in the survey were developed through preliminary conversations with officers and literature

searches. A survey was designed to collect the needed data, yet not require more than 5-7 minutes to complete. Appendix B contains the questionnaire.

The surveys were made up of questions to determine the attitude of individuals. Attitudes are the mental states of individuals composed of their feelings, knowledge, and the way they act. These attitudes are the conditions that influence how they take in and use information as the basis for action. The survey included both open and closed ended questions.

Open ended questions were used to obtain opinions and to probe the attitudes of the officers. The responses were characterized to determine the range and number of concerns of officers, and to be able to capture responses in the respondents' own words. It is always possible that open ended questions can be misinterpreted. To minimize this, all open ended questions were interpreted by at least two analysts.

Closed ended questions were used to measure attitude intensity. Closed ended questions used a Likert-type scale. This response format developed by R.A. Likert (1932) represents a bipolar continuum. The low end represents a negative response while the high end represents a positive response.[22]

Respondents were informed that they were not required to answer all the questions. They were specifically informed that the demographic information was optional.

An informational page was distributed with the surveys to explain more fully the project goals and objectives. A cover letter was also sent with the mailed surveys asking the respondent to circulate the surveys to appropriate people.

Pilot-Test Stage

The questionnaire was pilot tested before being publicly distributed. Independent reviewers, data analysts, and human subject testing experts reviewed the content, questions, instructions, and mechanics of the survey. Individual trials of the questionnaire were completed with both a set of police officers and persons that would be analyzing the data. Questions were reviewed to assure a consistent understanding (reliability) that would stimulate accurate information (validity). The survey was revised as necessary throughout this stage.

Data Gathering Stage

The surveys were distributed through numerous methods. Surveys were mailed to police departments, distributed at law enforcement conferences, published in a law enforcement professional journal (American Society of Law Enforcement Trainers Journal), and copies passed on from these people to others. People were encouraged to distribute copies to other knowledgeable people. Officers from various organizations at all levels of law enforcement were covered.

This method of distribution was not intended to give a scientific sampling of law enforcement, and no extrapolation to a larger population of officers is intended. Because of the manner of distribution it is impossible to establish a response rate.

A postage paid return envelope was included with the survey when distributed by mailings or direct distribution. Surveys were returned by mail, fax, and e-mail. Surveys were logged into a computer system as they arrived.

Analysis Stage

Analysis started at a date selected to meet project deadlines. At this time sufficient surveys were received (319) to meet the survey objectives, and trends could be seen in the data. After this date new survey results were not tallied with the rest, but each was reviewed for any comments that would not support the existing data, none were found.

Qualitative data was received from the open ended questions on officers' concerns. The analysis goal of this information was to reduce the numerous responses into a meaningful few. All open ended questions were interpreted by at least two analysts. The information was categorized, sorted, and rechecked for

consistency within the category. Quantitative, or numerical, data was collected from the close ended questions. Descriptive statistical information was collected to look for central tendency and variability.

Follow-up interviews were conducted in person and by telephone until the trends of the answers were repeating and time demanded completion. The interviews were used to check the interpretation of the questions to again validate the survey. The interviews were sought to understand the importance of the respondents' answers and any extenuating circumstances that may influence an answer. During the interviews answers could be elaborated upon and inconsistencies could be questioned. In depth personal interviews were conducted with officers during the swing shift at the Kansas City Police Department, and the day shift at the Albuquerque Police Department.

Reporting Stage

All of the information collected and analyzed, from preliminary interviews, literature searches, law enforcement conferences, the surveys, follow-up interview, and other means, was used in the analysis of the officers' requirements. This report documents those findings.

Survey results are presented throughout this report with the appropriate sections of text as quantifiable attitudes of the surveyed officers. Data is presented in various manners depending on how it can be best understood in the context of the information presented. The officers' concerns are often used exactly as written on the surveys, or are paraphrased, in the text of the report. The officers' identities are not given for protection of their personal privacy.

Characteristics of Respondents

A wide range of law enforcement personnel responded to the surveys. The goal was to include varied types of officers and this goal was achieved. Some characteristics of the respondents are charted here.

The persons responding to the survey, as shown in Figure 15, generally match the population characteristics of the Nation, except for the South. The South had a much greater response than the other regions. One reason for this may be that since the percentage of law officers killed is much greater in the South, the officers are more concerned about their safety and methods of prevention. The number of takeaway incidents is also the greatest in the South. Surveys outside of the United States were received from Canada, Puerto Rico, and

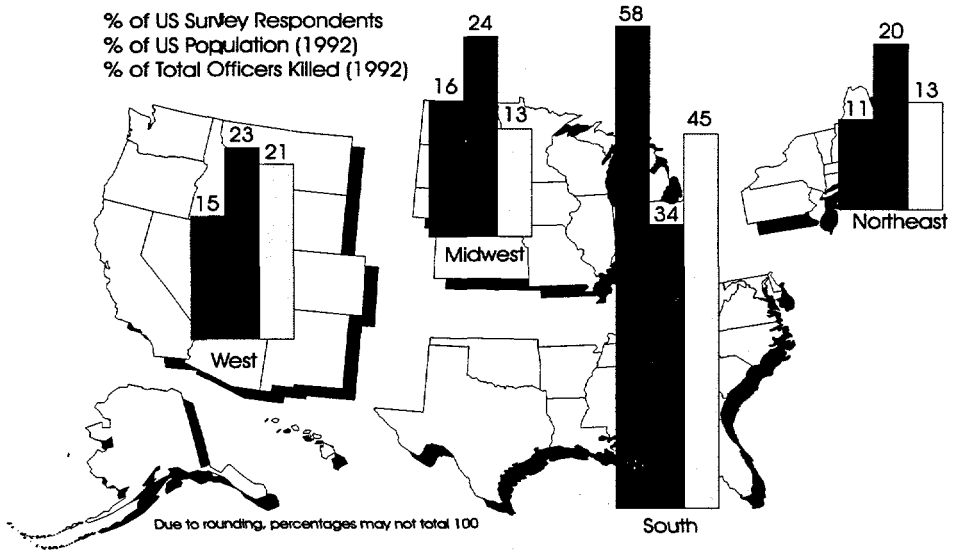


Figure 15. Survey Respondents By Region

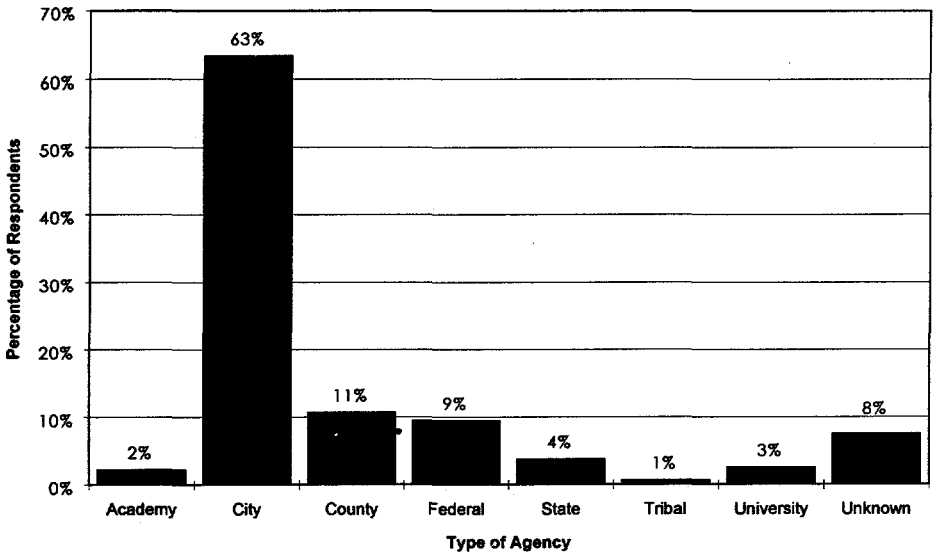


Figure 16. Survey Respondents By Type Of Agency

the United Kingdom.

Figure 16 shows the percentage of respondents and the type of agency with which they are affiliated. A wide range of agencies responded. The majority of the respondents were from city, or municipal, police departments. The next largest percentages of respondents were from county agencies. Of course, these two types of agencies jointly provide most of the law enforcement service in the Nation.[23]

Figure 17 shows the percentage of survey respondents by the title placed on the survey. Many officers listed more than one position, and usually the first title listed was used. A wide range of personnel responded to the survey, from management positions, to trainers, to patrol officers. This variation of people allows the information to not be biased by only one category of people responding. Although only 6.3% of the respondents had titles of instructors, a total of 26.9% of the respondents worked in the training areas at various levels. People in the area of training are involved because they are usually well informed on the needs of the officer. They are often responsible for tracking statistics on the officers, as well as recommending and implementing training programs.

The responses that were analyzed came from officers with a wide range of experience, as seen in Figure 18. Over half of the officers were in the range of 11-25 years experience in law enforcement. These are officers that have seen many ideas in law enforcement come and go and have definite opinions on the way things should operate. A smaller percentage of younger officers also responded These officers often like the concept of advancing the technology of law enforcement. Officers with more experience were usually in administrative roles including planning, teaching, as well as some Chiefs of Police.

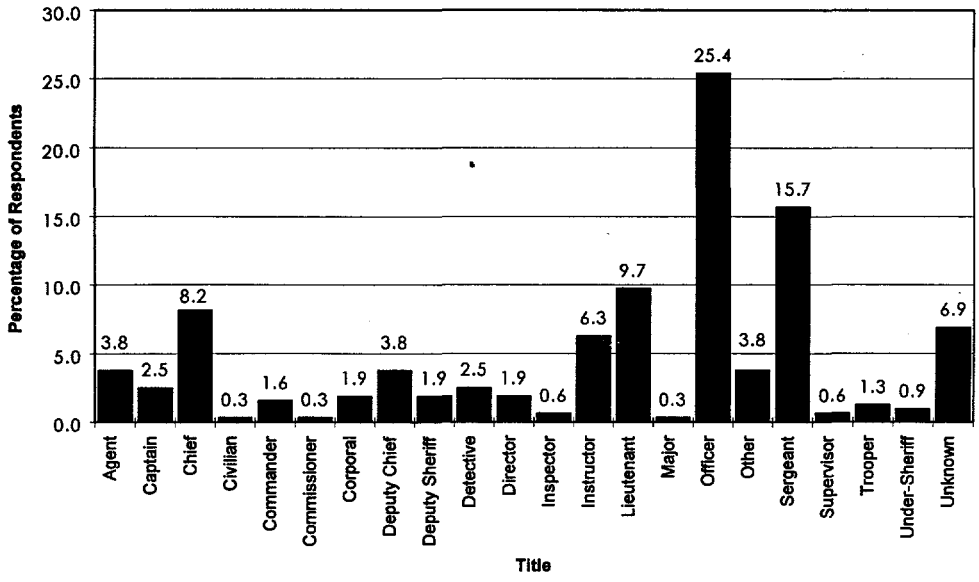


Figure 17. Titles of Survey Respondents

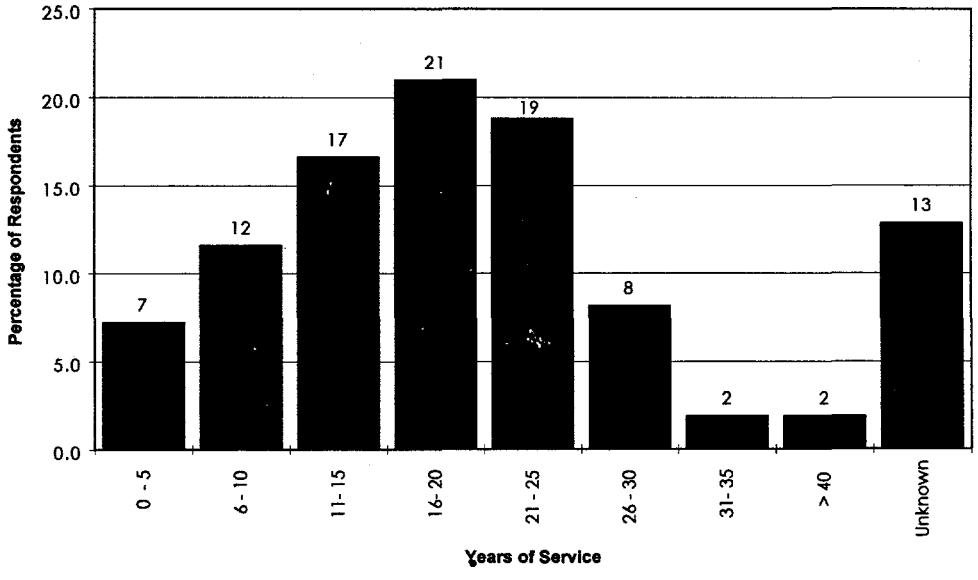


Figure 18. Survey Respondents Years of Service

Chapter 5

Officers Concerns

From Concerns to Requirements

One method of determining the requirements of the law enforcement officers is to understand, and address, their concerns. From all of the gathered data, the officers' concerns were listed. In the questionnaires distributed to law enforcement personnel, two open ended questions were asked. One sought to understand the officers two main concerns about smart gun technologies, and another sought any two problems that a smart gun technology could cause them. The responses from these two questions were categorized and tallied. The interpretations of some comments were subjective. At least two analysts categorized each response to minimize bias. The responses were then analyzed in various ways to see if certain concerns ranked higher than others. No matter which way they were characterized, the rankings did not significantly change. Figure 19 shows the total number of tallied concerns in any single category. Each of the respondents' concerns will be addressed by category in this chapter of the report; with associated requirements assigned.

As can be seen from Figure 19, the overwhelming concern of the officers is the effect that the addition of a smart gun technology has on the reliability of their firearm. The number of respondents that stated a reliability related concern is almost three times that over any other concern. Many of the other concerns listed by officers have a hint of reliability in them. When the survey results are

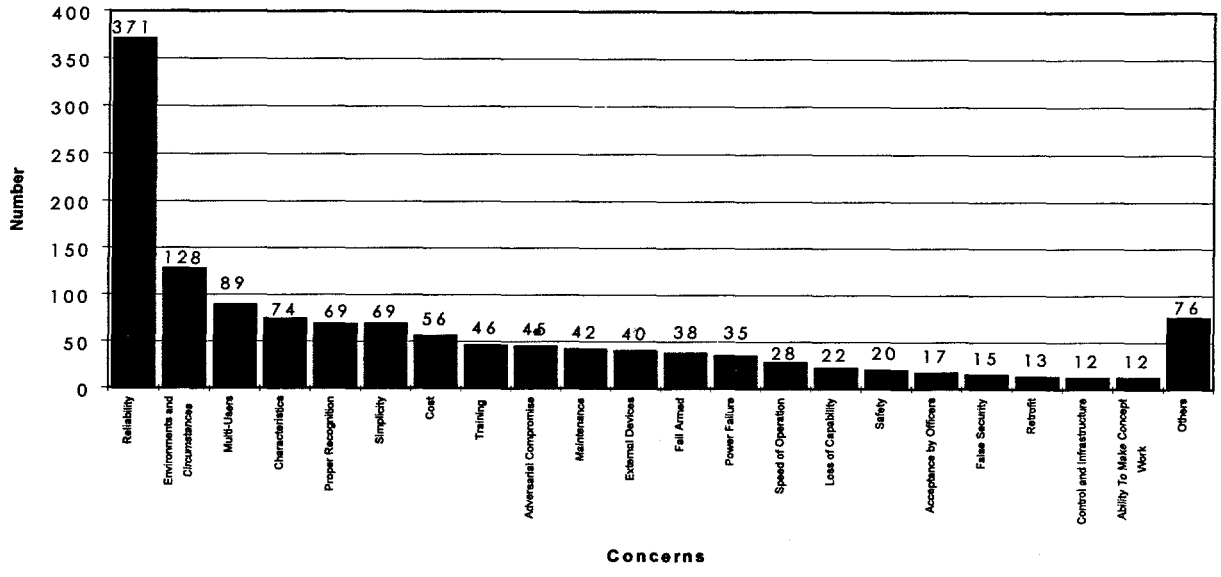


Figure 19. Officers' Concerns Relating to Smart Gun Technologies

compared to the data gathered by other means, the results show consistent concerns. It is unlikely that the survey questions influenced the officers concerns.

Discussions of Concerns

There are numerous methods of documenting the information collected during this study. The following sections of this chapter list officers concerns. Each of the concerns listed will be addressed in decreasing order of significance as determined by the number of respondents stating it as a concern. For each concern a deductive approach is used to explain the reasons behind an officer's viewpoint, concluding in a list of requirements. A summary of requirements can be found in Appendix C.

Reliability

Without a doubt the most important aspect of a smart gun technology is that the entire system must be reliable. Numerous terms are used to describe the concern of not operating properly. After personal interviews and follow-up calls, words such as the following, in the correct context, indicated a concern for a reliable technology: reliability, foolproof, fail-safe, malfunctions, disabled, zero-error tolerance, dependability, failure rate, breakdowns, and works every time.

To the officer, the firearm is another tool that is available to be used. The difference is that the firearm is only used when the circumstances of an officer's work demand that lethal force be used. Then the firearm must work because the officer's life is at stake. Lethal force can only be used after the officer determines that his life is in danger. These facts explain why the number one concern among officers is the reliability of the smart gun technology.

The military has very stringent reliability requirements. Handguns used by Special Operations personnel are designed for a service life of 30,000 rounds without repair or replacement of parts. These specialized firearms can also demonstrate a minimum 10,000 Mean Rounds Between Stoppages (MRBS), where the only class of stoppages allowed are those that can be cleared by the weapon operator within 10 seconds. Another way that the reliability is sometimes stated is: the probability of firing a full magazine without stoppage should be greater than 99.9% probability.[24]

Law enforcement standards require firing a total of 600 rounds with a verification of measured parameters after the test. A total of 1 or 5 malfunctions are allowed for revolvers[25] and pistols[26], respectively. Information on service life can be found in Appendix A.

However the reliability is stated, either as percentages or MRBS, the addition of a smart gun technology cannot significantly reduce the reliability of the firearm system compared to existing firearms.

Requirement: The addition of a smart gun technology must not significantly reduce the reliability of the firearm system compared to existing firearms.

Environments & Circumstances

A primary concern of officers is that the smart gun technology operates in all conceivable circumstances and environments in which they could find themselves. It was not possible to separate the concerns of operating in all circumstances from operating in all environments, when answering the open ended question about concerns of the officer. Some of the phrases that were interpreted to be contained in this category were the need to operate: at the worst possible moment, in extreme conditions, as needed, through use and abuse, in all weather climates, in all expected and unexpected situations and conditions, during critical confrontations, in all field conditions, and with all types of contaminants such as dirt or blood.

After studying these concerns one learns that the officers working conditions are unpredictable. The environmental conditions that officers face depend mainly on their locale. The same firearms are used by police departments in Florida as in Alaska. This means that a single technology must also operate in the environments presented by those states. For specifics on the environmental requirements of a smart gun technology see Appendix A.

The circumstances that an officer may face are also unpredictable. The people that the officer deals with are often unpredictable. Adversaries may be calm and rational or they may be out-of-control on drugs. The adversary may simply be an average citizen that has gotten themselves into an unintended or embarrassing circumstance, or the adversary may have trained and practiced for the crime they have committed. The officer may deal with a single adversary or be confronted by multiple people. The officer may be alone or have a partner, or backup, available.

The officer must also deal with the particular conditions of the situation. An officer may be called to duty on a hot sunny summer day on a sandy beach, or a cold snowy winter night. The call the officer responds to may be a quiet swampy area, or a barroom with deafening music and screaming people. The officers described in the above scenarios could be sweaty, sandy, wearing gloves, snowy, wet, and shouting. No matter what the circumstances the officer may find himself in, his firearm must still operate.

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

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

Requirement: The smart gun technology must operate in all likely environmental conditions.

Multi-Users

Officers often think in worst case scenarios. This is not unusual when you consider the number of situations that can arise for an officer. One worst case scenario is that an officer may need to use another officer's firearm after he has run out of ammunition or his firearm has failed, and the other officer is incapacitated to a point that they cannot use their firearm (or vice versa). Although actual statistics could not be found on the number officers having to use another officer's firearm to defend themselves, it is thought that it is a very infrequent occurrence. We do know that these situations occur. Accounts can be found in the FBI Law Officers Killed and Assaulted reports.[27] Officers are concerned about losing the capability of using another officer's firearm when their life may depend on it.

Some of the people that officers thought should be able to use their firearms included: partners, other officers within the department, officers from another county/state/jurisdiction, gunsmiths and armorers, trainers, and friends of the officer such as helpful citizens or spouses. In follow-up talks, the majority of officers said that it is not important for friendly citizens to use officer's weapons. Officers cannot depend on citizens to protect them when it is their duty to protect the citizens. Officers agree that it is unlikely that they would ever use one of their fellow officers firearms, some had never even considered it a valid possibility. They felt that it is even more unlikely that they would have to use the firearm of another jurisdiction that would not be compatible with their own firearm. Also with more semi-automatic weapons with larger magazines available, the chance of running out of ammunition and needing to use another officer's weapon is even less. Officers were also concerned that the smart gun technology may be only found on a certain model or type of firearm. This would not only limit selection

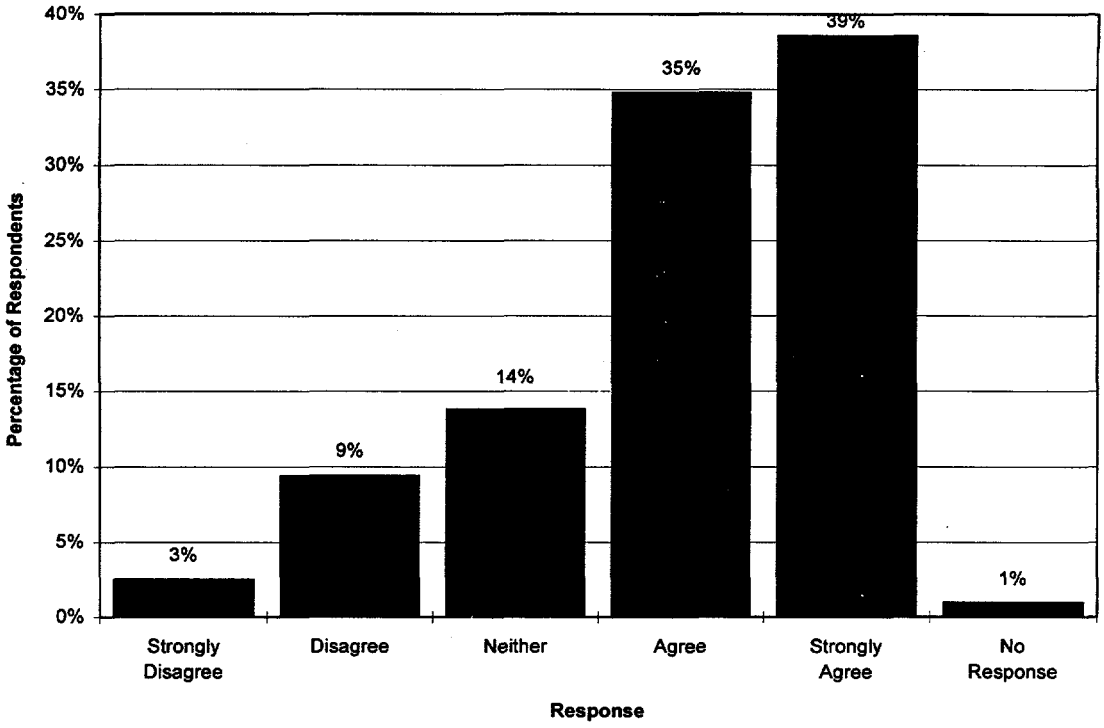


Figure 20. Survey responses to: Other authorized people should be able to use my firearm.

and personal choice of firearms, but also may drive up the cost.

Officers realize it is highly unlikely that they would use another officer's firearm. Despite this fact, in responding to the survey statement, 'My partner, or other authorized people, have to be able to use my gun,' they overwhelmingly agree that others should be able to use their weapon. This is shown in Figure 20. This concern is part of not wanting to lose an existing capability of their firearm. While operating between multiple users may not be a requirement, it definitely is something the officers desire and may be needed to gain full acceptance.

Not all police firearms are single user firearms. Frequently in police cars there is a rifle or shotgun that is common to all who use that car. The smart gun technology should also be applicable for use on multi-user firearms.

In some departments, officers are allowed to carry backup firearms. Officers who carry backups desire the capability of using the same means of identification for the backup as for their primary weapon. This means that the officer could switch between firearms without any special actions.

The number of officers that any one firearm might need to recognize could greatly vary. There are approximately 860,000 police officers in 17,000 departments across the United States. While that works out to be an average of 50 officers per department that statistic is misleading. Currently the size of police departments in the United States is small: only two departments have more than 8,000 officers, 90% have fewer than 24 officers, and 50% have fewer than 12 officers.[28]

There is no such thing as a standard police firearm. A few departments require that officers use a specific firearm, with the goal of uniformity of training and interchangability of parts. Some departments may offer a choice of a few makes and models, and other

departments have no stated preference on make or model as long as it operationally meets a departmental standard operating procedure. Information from the survey respondents shows that within this small number of officers, seven different makes of firearms are used. Within these seven makes, there were over 60 different models of firearms used. This information shows that many makes, and many different models within those brands are used by officers.

Requirement: The smart gun technology should be capable of being used by multiple users.

Requirement: There must be a method for armorers and manufacturers to test the smart gun technology.

Requirement: The smart gun technology must be applicable to multiple types and brands of firearms.

Requirement: The technology should also be applicable for use on multi-user firearms. i.e., shotguns.

Requirement: The technology must operate for a single individual on multiple firearms.

Requirement: Individual smart gun product lines should ultimately have interchangeable parts that are not easily misassembled and can be replaceable without special tools.

Characteristics

Officers are concerned about both the appearance and characteristics of their firearm. Sorting through the responses it is found that much of this concern is due to resistance to change and having to relearn how to fire a new weapon. It is assumed that after the appropriate time of getting familiar with any new device, the officers would use it if it had merit. The concerns mentioned by officers deal mainly with the physical qualities of the firearm.

The firearm should physically look like existing firearms, preferably identical to them. If a suspect cannot recognize the weapon, then the officer may not have the desired intimidation over them. A smart gun needs to look like an existing firearm. Both officers and suspects need to be able to recognize a lethal weapon when they see one. There have been numerous shootings when toy guns have been drawn on officers. If suspects cannot tell if the firearm contains a smart gun technology, if they try or even succeed in obtaining an officer's firearm, the officer will still have an upper hand on the suspect. If suspects could tell the difference, it is possible that they may look for officers who do not have smart guns. Figure 21 shows that officers agree that 'a smart gun should look just like an existing gun.' Officers would like some recognizable feature on the smart gun so that the trained eye could identify one, even from some distance. This allows them to tell what type of firearms other officers are using.

The other part of the concern deals with the actual physical characteristics of the firearm. Weight of the firearm is a concern. Officers must carry on their person all the equipment that they are likely to need in performing their duties. When the situation arises, they are not able to run back to the car to get the equipment that they need. An officer's duty belt is heavy when loaded with equipment such as: their loaded firearm (40 oz.), a pair of extra magazines or speed loaders, a flashlight, handcuffs, keys, chemical agent dispenser, baton, and gloves. Not only is the equipment heavy, it also creates difficulties in getting in and out of the car without snagging objects. The smart gun technology cannot create an appreciable additional weight to carry or cause additional appendages to the firearm that would increase the difficulties in movement while carrying the firearm.

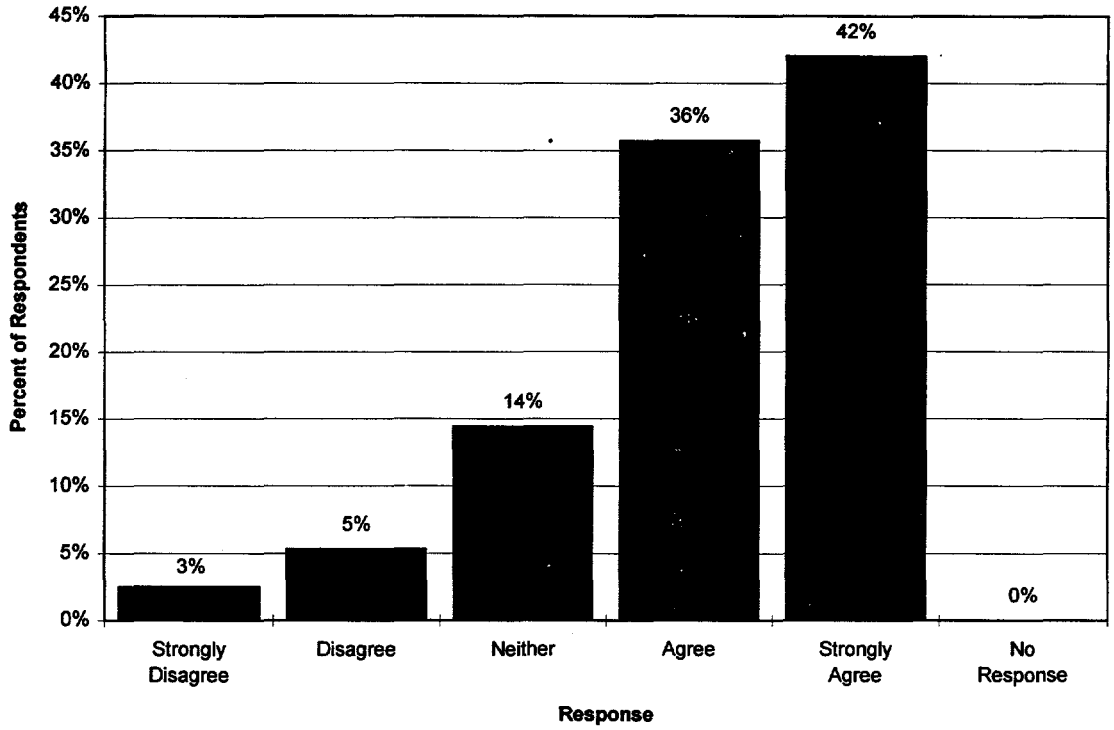


Figure 21. Survey responses to: A smart gun should look just like existing firearms.

The technology should not affect the existing standards that exist for trigger pull. If the trigger pull is too light it could be considered a safety hazard. If it is too heavy the trigger may be too difficult to pull and shoot accurately. In general, laboratory tests and field experience has determined that more than 18 pounds is a difficult trigger pull for most shooters to maintain accuracy.[29]

The smart gun technology should also not greatly affect the size: the firearm needs to be manageable. Officers with smaller hands need to be able to properly grip the firearm. Some officers will change the grips on their firearm to a more comfortable grip. If the firearm is too bulky or cumbersome it may hinder the officers use, retention, or concealment of the weapon. The additional technologies should not alter the balance of the weapon that could effect the accuracy. Existing holsters should be able to be used. The devices should not affect gripping the weapon, or limit the manner in which the firearm must be held.

Requirement: The smart gun must have the general appearance of an existing firearm.

Requirement: The addition of smart gun technologies cannot appreciably change the weight, size, or balance of existing firearms.

Requirement: The addition of smart gun technologies cannot add appendages which would appreciably increase snagging compared to an existing firearm

Requirement: The smart gun technology should not affect the carrying of firearms in existing holsters.

Requirement: The smart gun technology must not affect the existing trigger pull standards.

Proper Recognition

Another concern that officers have with a smart gun technology is that it may not recognize them properly when it comes time to operate

the weapon. The comments received from the officers concerning proper recognition included statements such as the smart gun technologies must: be owner loyal, recognize the handler, identify authorized persons, recognize legitimate users, and not recognize unauthorized users. In talking to officers, many of these concerns came from unfamiliarity with the technologies that may be applied in a smart gun. The officers' concerns are valid; definite error rates in recognition exist, both for not being accepted by their own firearms, and for adversaries being accepted by officer's firearms.

Error rates are described as percentages of occurrence per verification attempt. Attempts are defined in various ways. An attempt as used to describe a smart gun technology is defined as one cycle of an individual using the technology as proof of being a validly authorized user. In some applications more than one try is allowed per attempt, where a try describes a single presentation of the individual to the technology for measurement.[30] For smart gun technologies a try and an attempt are equated: the firearm must operate on the first try (attempt) that an officer makes to use his firearm.

A false-rejection rate (FRR) is the percentage of times an authorized user who makes an honest attempt to be verified is rejected. This is the case when an officer attempts to use his own firearm but is falsely rejected. A false-rejection error is called a Type I error. A false-acceptance rate (FAR) is the percentage of times that an unauthorized user is accepted as authorized. This would be the case where an assailant tries to use on officer's firearm and is successful. A false-acceptance error is called a Type II error. The type of false-acceptance we are referring to here are passive attempts, where the assailant submits himself as the authorized user, and not an overt act of the assailant to mimic the item being recognized (covered later). Techniques, such as the use of personal identification (PIN) numbers, can be implemented to reduce both error rates. Although these terms are most often used in association with biometric sensors they will be applied to the other technologies as well. In general, either of the error rates can be described as follows:

$$\text{Error Rate} = \frac{\text{Number of False Recognitions}}{\text{Number of Attempted Recognitions}} \times 100\%$$

In actual application most recognition technologies use a measurement of what is being recognized compared to a threshold to make decisions. Depending on the technology a number of attributes may be measured and a score determined. This score should be able to be retrieved in some test configuration so that information can be used during specialized diagnostics, training, and for quantifiable ranking of technologies. Many recognition technologies have a threshold that can be varied to change the level that the decision for acceptance or rejection is made. Thus, a police department or officer could set the threshold to control the probability of false rejects versus false accepts. A positive feedback indicator of acceptance is desired by most officers (see section on Indicators).

Requirement: The smart gun technology must properly recognize, and limit the use of the firearm, to the authorized user.

Requirement: The smart gun technology must operate on the first verification attempt.

Requirement: For applicable recognition technologies the actual recognition score, rather than a simple go/no-go indication, should be available in a testing configuration.

Requirement: For applicable recognition technologies, a method of adjusting the recognition threshold by a qualified person is recommended.

Simplicity

Today's firearms are relatively simple devices designed to do one thing: fire a round when the trigger is pulled. Although the firearm designs

have become more efficient and less likely to accidentally discharge, the operational designs have not significantly changed in the past few decades. Various models have different internal or external safety mechanisms, but none are difficult to learn. The addition of a smart gun technology must not effect the primary use of the weapon. The addition of a smart gun technology to a firearm should be transparent to the user.

Officers agree that the addition of a smart gun technology must not complicate the use of their firearm. The KISS principle, "keep it simple," applies. The reasons that officers are concerned about the added complexity cross over to many of their other concerns. In conjunction with the primary concern of reliability, officers fear that the more complex the firearm gets and the more parts it contains, the more likely it will be to fail when it is needed.

The smart gun technology device should also be able to be used during any stressful circumstances. A passive device that requires no actions by the officer is favored. The device should not have too many steps to operate, or be a hindrance to the officer. The device must not be so complicated that it would take too long to operate: it must be ready to operate instantly. It must not "take a rocket scientist" to operate: it must fit into the comprehension level of the officer with the minimum required amount of training and skills. It must be simple to maintain, even possibly in the field. Most of these topics are covered in their individual sections.

Requirement: The addition of a smart gun technology must not effect the primary use of firing the weapon by the authorized user.

Requirement: The addition of a smart gun technology to a firearm should be operationally transparent to the user.

Requirement: The addition of a smart gun technology must not complicate the use of the firearm.

Cost

Cost is an issue for any law enforcement product. Police departments are often funded to only the minimal levels necessary to maintain a status quo in the protection of the general public. The greatest part of a typical department budget is spent paying salaries, and only a small percentage is available to purchase equipment. Many departments cannot afford to supply or update their existing equipment to the latest technologies available. Discretionary equipment that is available to assist the officer in their job may not be purchased until the next model comes out and the price drops, if at all.

An additional factor is that most departments are small and do not have the buying power to get large quantity discounts. This also hurts the manufacturers, in that the law enforcement market is so fragmented it becomes hard for them to recoup their development costs in a time frame such that they can make the product more affordable. Technology experts say that because the law enforcement market is so limited, only one technology could be used for all law enforcement firearms to get volume production costs, or the market would have to be expanded to the general public.

Officers typically have to purchase their own firearms for their jobs. Even for those departments that were to subsidize officers in purchasing new firearms, the cost must be in a range that it is affordable. Officers have views of what is affordable that cross the entire spectrum of possibilities. Some officers suggest that the safety and peace of mind of knowing that someone cannot use their firearm against them would be worth spending up to twice what a current firearm costs. This argument is somewhat supported by the cost of the one commercial magnetic ring firearm that is available and is marketed to the general public; it costs approximately twice that of a normal firearm. On the other extreme, some officers rationalize that if this is a safety device it should be included as part of the firearm without any additional cost. In conversations with various product manufacturers, a possible

target for a smart gun technology may be approximately 10% additional cost in volume production.

Officers also mentioned concerns regarding the financial constraints of departments. Training officers is expensive and if a smart gun was available, a department may reduce training in the area of gun retention to offset the additional cost of the smart gun technology. Also there are other costs that must be considered. These include the routine maintenance of the firearm, which includes purchases such as batteries, and also the cost of any additional infrastructure needed. It is not known whether a department, which would mandate the use of smart guns, could receive a reduced premium for liability insurance.

Requirement: The additional production cost to incorporate a smart gun technology to a firearm should not add more than approximately $50 to the purchase price..

Requirement: Any additional costs associated with the use of smart gun technologies should be minimized.

Training

Training is important for all aspects of an officer's job. Today this is not only true for the need to enhance officer safety, but also for the need to reduce the possible liability of the department. Officers must be trained in the proper use of each piece of their equipment. Although all departments have requirements for training, the requirements will change from department to department. Training may only be implemented after an incident brings the need into the focus of the department, and possibly the community.

There are two general types of gun retention training: awareness training and physical training. Awareness training is to inform officers of the threat of having their service weapons taken from them. It may cover the frequency of occurrence, the typical scenarios, and warnings to be prepared. Physical training is to train the officer in various tactics that can be used to prevent a takeaway when in the situation. It may also cover awareness training, but the focus is on the practice of holds and maneuvers that will give the officer the advantage to keep, or regain, control of the situation. The most well known gun retention training techniques may be those started at the Kansas City Police Department by Jim Lindell in the 1970s.

Approximately 27% of the responses to the survey were received from training officers at various levels from academy directors to trainers. One of the main concerns listed by these trainers was that gadgets cannot replace training of officers: no matter how smart the gadget, what is needed is a smart officer. This expresses the concern that officers may become more dependent on a technology and less dependent on their training. A false sense of security may occur when officers depend too much on their equipment and not their own capabilities, because technologies can fail.

Some trainers suggest that with enough training there would be no weapon takeaways. This may have some truth, but is an over statement when all the possible scenarios are reviewed. Of the survey respondents who have been involved in takeaway situations, it is seen in Figure 22 that a wide range of physical responses, from survival to training, were involved. In follow-up conversations, officers said that training is the starting point to remain in control of their firearm during a takeaway incident, and is often all that is needed. The trained responses continue until they are no longer effective, then survival takes over the officer's actions.

Officers are concerned that departments may eliminate training on gun retention if smart guns become available. This would save the department money. Any change in training is time consuming and costly. It can become a logistical problem to cycle officers through new training programs that take them out of the

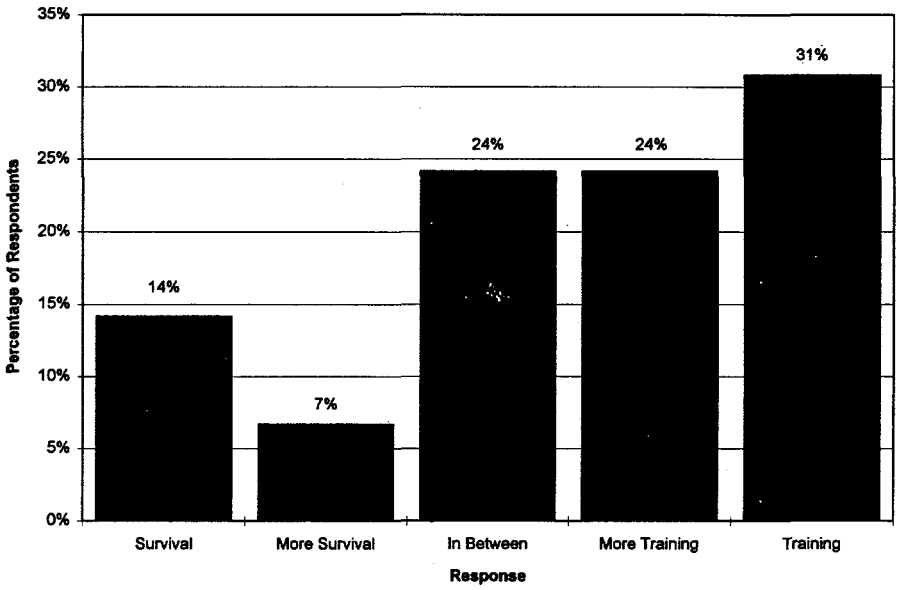


Figure 22. Survey responses to: The behavioral response used during a takeaway incident.

field. The new training programs may have to be developed. The transition to new equipment and training can cause problems if different equipment is in service and all officers have not been properly trained.

Trainers are concerned about the amount and complexity of new training that would be required. Trainers say that with proper training any new conditioned response can be developed. What is needed is an education of how a smart gun technology would work, at least to the level of understanding the required maintenance and proper operation. Officers fear that in stressful situations they may revert to old training and habits. When new equipment becomes available new recruits will usually transition easily. Many departments grandfather in existing officers when new equipment becomes available because of the officers concerns of changing old habits, or even sometimes because of union constraints. Training at the range and in class must also be considered as a way to get officers to know and trust this new technology. The training of the trainers, the armorers, and others should also be considered.

All of these concerns are not specific to smart gun technologies. Many of these same concerns are used when any change occurs, such as the transition from revolvers to semi-automatic weapons. The issues raised are more easily dealt with when the officers and trainers understand the need for change, and desire the change to be made.

Requirement: Smart gun technologies must cause only minimal additional training, such as transitional training and in service training on proper use.

Requirement: Smart gun technologies must enhance and not eliminate weapon retention training.

Requirement: Smart gun technologies training must extend beyond the use of technologies and include training for armorers and others as appropriate.

Adversarial Compromise Of Technology

The majority of scenarios of police officers being shot with their own firearms are not planned attacks. Although there are exceptions, the adversary does not usually plan to find an officer and take his firearm. The question that is still on the mind of many officers is: "How secure can a smart gun be?".

Just as hackers attack computer networks, it is a fact that the criminal element will try to find out how to defeat the smart gun technologies. Any technology such as this becomes widely known. Many officers feel that the general public should not be allowed to have a technology such as this. They feel that in the hands of the general public the "secret" will be out, and they will be left having a useless firearm. The general public will probably have this technology available to them. It is unlikely that the judicial system will allow the firearm industry to withhold any feature that could reduce fatalities caused by firearms from any sector of the population.

The technology must not be easily defeated even with full knowledge of how the system operates. The technology used in a smart gun must have a unique characteristic that is not easily replicated, or jammed by an outside source. The identifier that enables the firearm must be unique. There must not be a method by which an aggressor can easily override an officer's firearm and make it useless. If this is possible, the problem is no longer officers being killed with their own firearms, but officers left with useless firearms leaving them helpless against armed criminals.

Requirement: The technology must be such that even with full knowledge of how the system operates it cannot be easily defeated.

Requirement: The technology used in a smart gun must have a unique characteristic that is not easily replicated, or jammed by an outside source.

Maintenance

The amount and type of maintenance necessary for a smart gun technology is a concern to many officers. Comments from numerous officers reflected the statement of one who said: "Most police officers do not maintain their weapon very carefully," and another who said, "...the average shooter/officer will not maintain the system". The consensus is that there is a history of poor maintenance by officers. The maintenance requirements for smart gun technologies must be held to a level that the average officer will do. Proper documentation must be supplied.

There are maintenance time and costs associated with both the acquisition and/or installation of the technologies, as well as while the firearm is in service. The smart gun must be capable of repeated maintenance without damage or a decrease in performance. Problems may occur if the maintenance is increased to a level that is too complicated. Officers may not perform the normal suggested maintenance. It could become so technically complex the department's armorer could not repair them. The technology might be so advanced that service and repairs could not be done on site and would require factory service. If there is a problem, there needs to be a way that officers can easily use another firearm if theirs is in for repairs. Repair time should be short for any failures. Any auxiliary equipment associated with the smart gun must also be simple and easy to maintain, and the technology should also be upgradable as the next version of the technology is introduced.

Once the system is set up the officer should need to do little to keep it operational. A once a day check of the recognition technology, and possibly a battery check is the most that seems practical for the average officer. There should be an equivalent method to a "tap-rack-bang" maneuver to check for and reset possible malfunctions quickly in the field. The existing maintenance and cleaning that is performed must not harm the smart technologies.

Many officers feel that maintenance is a training issue. Officers can be trained to complete proper maintenance. From the interviews, an observation made is that those officers volunteering that they had prior military experience were the same that kept their equipment well maintained. These officers did not have concerns about normal maintenance issues.

Requirement: Maintenance requirements for smart gun technologies must be held to a level that the average officer will do.

Requirement: The smart gun must be capable of repeated maintenance without damage or a decrease in performance.

Requirement: Department's armorer or trained personnel should be able to perform most diagnostic tests and repairs.

Requirement: Simple procedures must be available to allow an officer in the field to quickly reset the recognition system in case of a technical malfunction.

Requirement: The technology should be upgradable when the next incremental version of the technology is introduced.

Requirement: Proper documentation for operational use must be supplied.

External Devices

There are many methods by which a firearm could recognize an authorized user. Two of the possible categories are biometrics, and tags. Biometrics would include those technologies that recognize a characteristic of the person, tags would include those technologies that recognize something that the person carries. Officers have some concerns about the specifics of this second category: external devices that the firearm would recognize. External devices could be any piece of equipment that was necessary in conjunction with the operation of the firearm. Possible examples are rings, wristbands, and buttons to be pushed.

The first widely known "smart gun" was the Magna-Trigger Safety System, this was invented in the early 1970s as a modified Smith & Wesson .38 revolver that was enabled by a magnet on a ring. Although only a few departments had their firearms modified, the information that was spread around the law enforcement community, true or not, was that the ring placement was critical. If the firearm was not gripped exactly right, it was said, the firearm would not operate. This first-of-its-kind product of 20 years ago still influences officer's opinions about any type of smart gun technology.

Officers have the same concerns about the external devices as the smart technology itself. The external devices must meet the same requirements as the technologies themselves. The external device must be reliable. It must operate in all possible environments that an officer may encounter. It also must be easy to carry.

The majority of officers agreed with the survey question 'I would be willing to wear something such as a ring, or wristband, that my gun would recognize' as shown in Figure 23. The officers who do not like the idea say that their firearm should not depend on something they would wear. They do not want to have to depend on another device to operate their firearm, another thing that could go wrong. The device would also be one more thing that they would have to carry or wear. For them to wear a device it has to be comfortable and unobtrusive. Some officers still do not wear soft body armor because of these complaints. It can not be affected by the weather, be broken in a physical altercation with an individual, or be affected by apparel such as gloves or long sleeves. Many officers had concerns that they might lose the device or just forget to wear it to work. Sometimes officers borrow equipment from others who are coming off duty when they forget to bring something to work. The device could also be stolen from them.

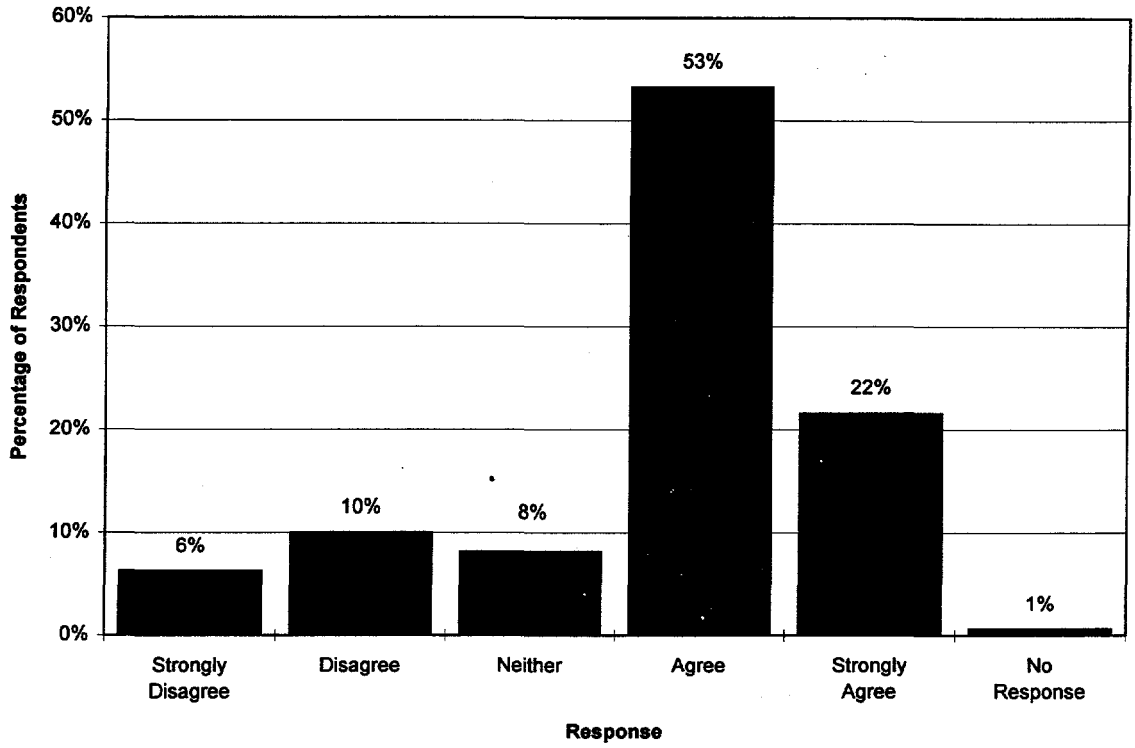


Figure 23. Survey responses to: I would be willing to wear something such as a ring, or wristband, that the firearm would recognize.

In operation the external device has many constraints. It must be safe to the user, it cannot cause medical effects to the officers, such as the fears raised by radar guns or contain common items that cause allergic reactions. It must be simple because it has to work in stressful situations. The officer must know where the device is, be able to obtain it quickly, and remember how to use it.

If the device is a ring, it should not interfere with the officers grip on the firearm, or be easily snagged or caught on other objects such as fences, ropes or clothing. It cannot be so big as to cause sufficient additional injury to a suspect in a physical alteration that it could be viewed as a weapon in itself. One officer said that he could not wear jewelry, and another mentioned that her hands swell and she cannot always wear her rings. Some officers suggested that implanting something in their hand would be a lot more convenient, although others were disgusted with the idea.

External devices that could be easily identified as enabling devices concerned some officers. In some departments the officers are required to carry a firearm while off duty. There are also undercover agents that need to be able to go undetected as a police officer. If an external device is unique to a police officer it could blow their cover or just identify them as an off duty officer. An obvious device could give a felon an upper hand knowing that an officer is nearby while the officer would not know there is a felon present. Most officers were not concerned about being known as police officers while off duty.

There are two general classes of external devices. Those devices that would actively control the firearm and those devices that the firearm would look for to identify a user. An example of an active control would be similar to a remote control firearm. A model of this technology has been seen by numerous people. With this technology the firearm can be

enabled or disabled at the push of a button. As seen in Figure 24, there are mixed feelings about this concept. What officers like about this concept is that their firearm is always ready to be used when they need it, and they have the choice when to disable it. The main concern is being able to get to the button to disable the firearm when in a struggle for the firearm. Most agree that with proper training this would not be a concern in most of the situations where takeaways occur. In scenarios where the officer is unconscious it could cause a problem if the adversary knew where the button was located on the officer. This raises another concern, if the adversaries know where the officer's disable buttons are located, then they may go around hitting officers in the common storage locations to disable their firearms. Of course the officer could re-enable the firearm. Unintentional pressing of the button is also a concern. Stories exist about officers walking around without any magazines in their firearm because the release button was pressed by accident. Many officers are in the habit of frequently feeling that the magazine *is* fully engaged. An indicator would likely be needed to alleviate the concerns of officers that they disabled their firearm by unintentionally pressing the button.

The other class of external devices is where the firearm looks for the device to identify the user. Instead of identifying a characteristic of the officer, the firearm identifies a device that the officer carries. For this type of device there are a number of characteristics that must be considered.

What type of device would the officer wear? Officers generally liked to have an option. If the device would be something like a ring they would like to be able to modify their existing rings. Many liked the idea of a wrist band better than a ring. The range the device works over is an important consideration. The

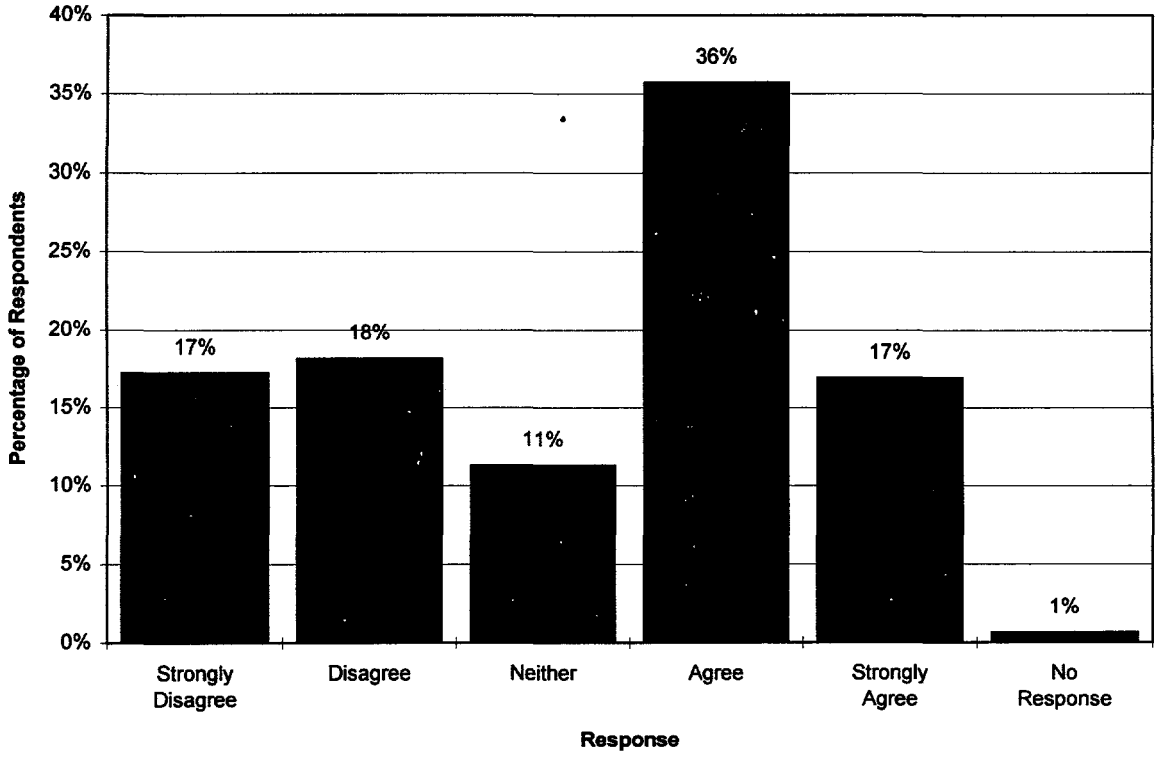


Figure 24. Survey responses to: I would be willing to do something (like press a button on my uniform) to disable the firearm if it was taken from me.

majority of all the scenarios have the officer and the suspect in very close proximity when the officer is shot. If the device operates over too long of a distance it may operate even when the suspect has the firearm. This leads to the need for ring and wristband type identifiers, as opposed to body mounted devices that would have a range of at least the officers arm length. Most of the incidents involve a struggle for the firearm. Officers may have to be retrained to let go of the firearm and remove their identifiers from the proximity that could make the firearm operable. Officers understood that they would have to wear two devices to be able to shoot with either hand. This did not effect the opinions of the officers as long as they could have a choice of things to wear. The identifier should also be a passive device not needing a power source. An additional power source, the associated maintenance concerns, and the size of the identifier device may be too great of a hindrance to officers.

No matter how the external device may operate it must be such that it cannot be easily duplicated. Felons must not be able to simply recreate the identifying device. The device must be such that it can work with other officer's firearms. The device must also not be alignment critical. In stressful situations, or situations where the officer's hand has been injured, the officer can not be concerned with proper orientation of the device.

Requirement: Ideally no external devices are needed to operate the smart gun technology.

Requirement: Smart gun technologies must not be alignment critical.

Requirement: Any external devices must be consistent with other smart gun technology requirements, i.e., reliability, durability, easy to maintain, small, accessible, simple...

Requirement: Smart gun technologies and external devices should not cause medical side effects.

Requirement: Any external device should have optional methods for attachment to the person, i.e., multiple fingers; fingers or wrists; implantable...

Requirement: Ideally external devices can be attached to existing items, i.e., rings, watches, badges...

Requirement: The operational range of any external device must be consistent with other requirements.

Fail Armed

An officer must be able to operate his firearm at any time. Today's firearms, having efficient designs, are relatively easy to understand and correct misfire situations. Pistol users are taught the "tap-rack-bang" to correct the most common failures simply and quickly. One concern of officers is what happens when the smart gun technology fails. Overwhelmingly, the officers desire a smart gun that will still fire if the smart technology fails. Their ideal is to err on the side of reliability and not security. The term officers often use is "fail-safe" meaning guaranteed not to "fail to fire." For the purposes of this project we will use the term "fail armed" meaning if a failure occurs the device is left in an armed, ready to operate, condition. The last thing an officer wants is a useless firearm.

The officers need to trust that the technology will not fail, but if it does fail they want the firearm to operate. This means that if the technology was somehow damaged during a struggle, if it was not maintained properly, or if the batteries just ran out, they would rather have their firearm be able to be used by anyone and not just themselves. This is reasonable when you realize that statistically a police officer will fire his weapon in defense of himself or another, more often than he will be fired upon by his own weapon. A weapon that is functioning will more often help the officer than the adversary.

Many different implementations of a fail armed feature are possible. Two optional ideas that were mentioned for use instead of a fail armed

system were a semi-permanent disable or timed lock-out. In a semi-permanent disable system, once the firearm was disabled it could not be easily reset in the field. This would leave the officer with the choice to manually disable his firearm knowing that it would remain useless until it could be reset. For the timed lock-out system the firearm would be disabled for a predetermined time if the officer chose to manually disable his firearm.

The problem that could be caused by a fail armed system is if a weakness is found that can easily disable the smart gun technologies. Criminals may learn the weaknesses of a certain model of smart gun: that by removing the batteries, or by rapping the firearm in a certain manner on the ground, the technology may become inoperable.

Requirement: 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.

Requirement: A smart gun technology must not be easily disabled by an adversary.

Power Failure

Smart gun technologies may either use active or passive technologies, meaning that they may or may not require separate power. Many of the potential smart gun technologies are active devices. The most probable type of power source would be the use of batteries. Officers have concerns about the reliability of battery operated devices. A battery is one more thing that could go wrong in a system. Many officers opinions are that batteries run down, need recharging, corrode, and are generally unreliable. For a firearm that their life depends on, officers want to minimize the number of things that could go wrong. Other officers do not have a problem with batteries. They say they depend on their radios for their life more frequently than their firearms. They have instituted a maintenance program for their radio batteries, and the same could be done for their firearms. They have no problems using rechargeable batteries that work fine.

Figure 25 shows that although the greatest single category of officers responding to the

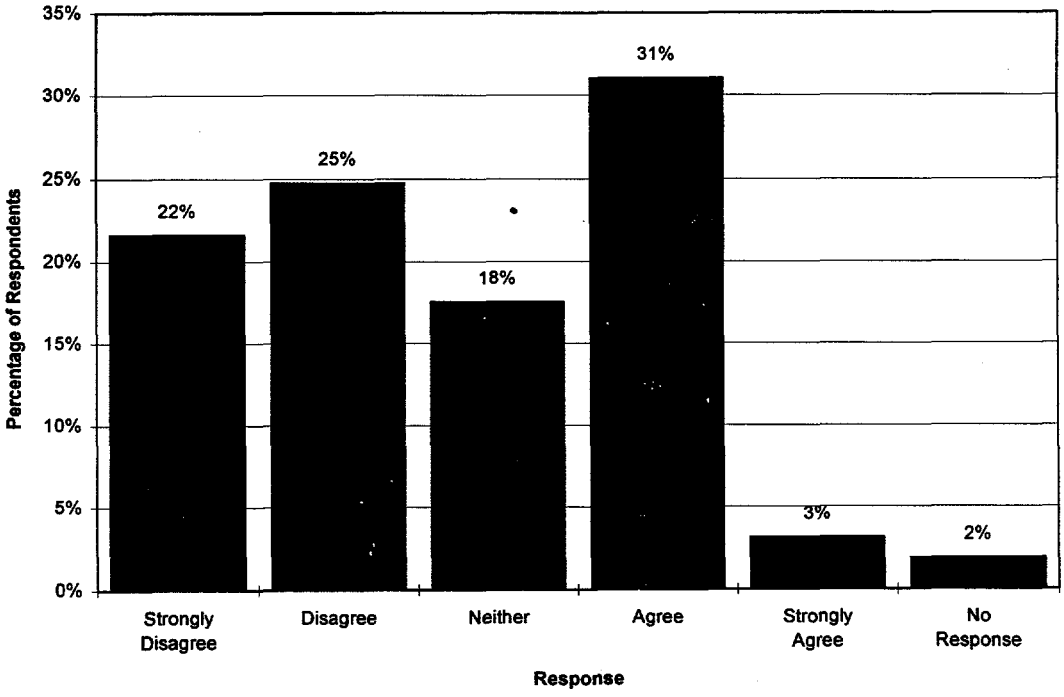


Figure 25. Survey responses to: It is acceptable to have batteries in firearms.

survey chose that they agree the statement 'it is OK to have batteries in my gun', a greater total majority disagree. Many of the officers dislike batteries because of the bad experiences they have had with their battery powered equipment. Flashlights and tape recorders seem to be the biggest culprits of promoting a bad reputation, although not all officers have problems. Other bad experiences come from departments not having batteries in supply when needed, and buying lower quality batteries in bulk to save money.

These bad experiences along with the personality types of officers lead to a common dislike for batteries. Many officers are notorious for not maintaining their equipment; others are extremely conscientious about maintenance. Often the best maintainers of equipment are those with previous military experience, both because of the regimented military maintenance programs and because of the fear of malfunctioning equipment. Batteries will have to prove themselves to officers to gain their confidence.

Since maintenance is a key factor, departments may have to enforce that batteries are checked and changed at regular intervals. Low power indicators may help promote proper maintenance. The indicator would have to meet the same requirements as in the indicator section of this report. Officers would rather not have to replace their batteries frequently. They would like to be able to change them in the field if necessary. Officers do not want to have to check their batteries more often than at the beginning of the shift. This means that the reserve capacity of the battery, assuming that the low power indicator came on immediately after it was checked, should allow the officer to fire three magazines approximately 10 hours later. Three magazines is the maximum a typical officer carries on his person, and 10 hours later implies that the officer is working longer than an eight hour shift. Ideally the officer would only have to change batteries at closer to one year cycles. Officers suggest that redundant power supplies may alleviate many officers concerns.

Two other concerns are as follows. One concern that is brought up when batteries are discussed is the bulkiness of the firearm. They fear that large batteries will increase the size and weight of their firearm. Another concern, along with the concern of maximizing reliability, is the officers desire that if the batteries fail, that the firearm not be rendered useless. The firearm should fail armed if the batteries fail.

Part of the engineering design of a smart gun system must include how to initially turn on the firearm when it is needed. Some technologies may allow power to be on continuously; others will have to be turned on only when needed. This turn on feature may be as challenging as other parts of the system.

Requirement: Ideally the smart gun technology would not require the use of batteries.

Requirement: If batteries are used, they must be easily obtained, and factored into the cost of maintaining the equipment.

Requirement: Ideally a battery used in a smart gun system would last longer than 1 year.

Requirement: 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.

Requirement: A low power indicator must be supplied if batteries are used in a smart gun system.

Requirement: Batteries should be easily replaceable, even in the field.

Requirement: Addition of batteries should not greatly change the physical characteristics of the firearm, i.e., size, weight...

Speed of Operation

Officers many times have to make split second decisions. Their lives and the lives of others may depend on the outcome of that decision. 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.

Officers are taught how to cover suspects: to be in a ready position with firearms out aimed at the ground 4-6 feet in front of them, having the advantage of seeing and responding to the first threatening movement of an attacker. Experience has shown that officers can reliably hit an 8 inch circle at about 10 feet in .5 to .7 seconds from a ready position.[31] Drawing from a holster adds some additional time.

Officers are concerned that the addition of smart gun technologies could affect the readiness of their firearm by increasing the time needed to draw the firearm from the holster. The smart gun needs to fit existing holsters. It needs to be able to clear the holster quickly. Access to their firearm cannot be delayed. Once the firearm is drawn, it must be ready to use. Whether on or off duty, quick use in an unexpected situation is primary to officer safety. The device cannot be so secure that it delays the intended use.

Things that could slow an officer down are extra steps that would be required before use. Activation or deactivation may take too long, in either a normal or a takeaway scenario, if it is too complicated or must be done manually. Also, the exchange between officers should be with a minimum delay.

Another decision for the smart gun system designer is how to initially tell the firearm to look for the user, and whether to re-authorize the user between each round. This affects the power and speed that the technology can operate. For instance, in the following scenario the firearm should not operate. A suspect has his hand on the firearm and the officer's hand is on the suspect. The identification ring on the officer's hand has enabled the firearm. When the officer removes his hand from the suspect's hand, and the suspect's hand is still on the firearm, the firearm should become disabled.

Requirement: 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.

Loss of Capability

Firearms have not significantly changed for decades. Officers are familiar with their operation. Anything new is going to cause a concern about losing a capability from the old model. Officers do not want to lose any capability that they now have with their firearms. The smart gun, compared to existing firearms, should not operate dramatically differently, should have the same performance, and should not detract from the officers effectiveness.

As mentioned in the discussions of other concerns, the smart gun technologies must be as reliable as present firearms. Sacrifices cannot be made in the use of the weapon in imperfect circumstances. The smart gun must be as fast and accurate as current weapons.

Requirement: The smart gun, compared to existing firearms, should not cause a loss of capabilities.

Safety

While many officers view a smart gun technology as another firearm safety it is better considered as a security feature. A safety is a device designed to prevent accidents from occurring. A security device prevents unauthorized use. A smart gun technology may add both safety and security to a firearm. Whatever it is called, firearm safety is on the mind of officers since they must carry their firearm with them each day. Every situation that an officer is involved in has a firearm present: their own. Safety concerns in the survey can be broken into two major

categories. The first category includes the basic rules of firearm safety and how they relate to a smart gun technology. The second category includes the physical safety mechanisms in place within firearms today.

The basic rules of gun safety are[27]:

1. All firearms are loaded. This is a state of mind that should be used when handling firearms. A person should never allow themselves to be comfortable with the theoretically unloaded firearm.
2. Never permit your muzzle to cover anything which you are unwilling to destroy. This rule is often violated among new firearm users and contributes most to tragic unintentional discharges. New firearm owners are sometimes taught to imagine that a powerful laser is aimed out the barrel that can never be turned off, such that anything it crosses is destroyed.
3. Keep your finger outside the trigger guard and on the receiver until beginning the shot. This is the second contributor to tragic accidental discharges. Unless an immediate discharge of the weapon is acceptable, the fingers should not be on the trigger.
4. Be sure of your target and its background. The target must be identified as appropriate to hit. Officers have been killed by other officers firing at muzzle flashes.

All of these rules should involve subconscious programming. The addition of smart technologies should not affect these or other gun safety rules.

The second category of safety is the internal safety mechanisms built into today's firearms. Even firearms that do not have a visible external safety device have internal protections. NIJ has standards that establish the minimum performance standards for "combat ready" police revolvers[32] and autoloading pistols.[33] The Sporting Arms and Ammunition

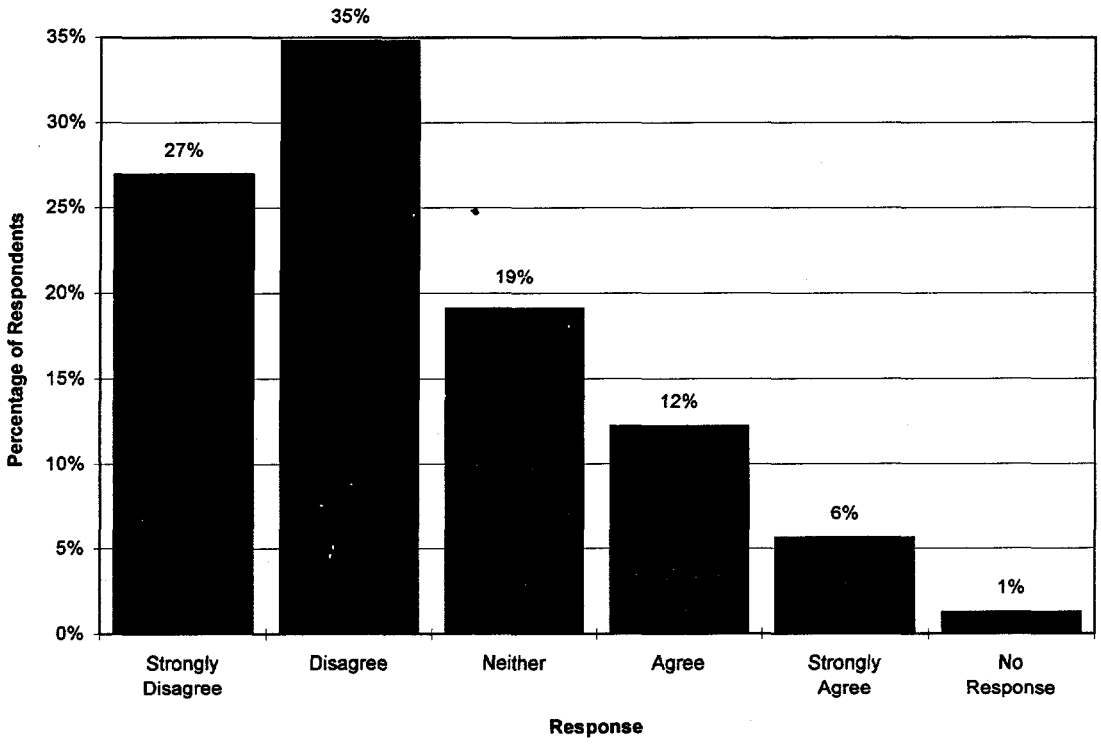


Figure 26. Survey responses to: A smart gun technology should replace existing firearm safety mechanisms.

Manufacturer's Institute, Inc. (SAAMI, pronounced "sammy") also maintains voluntary standards.[34] Among other topics, these standards include items dealing with safety. See the section on law enforcement standards for more details.

As seen in Figure 26, officers disagree with the statement 'the smart gun's identification feature should replace my gun's existing safety mechanisms'. Officers agreed that the addition of smart gun technologies should not interfere with, unduly complicate, or replace the existing safety mechanisms. The manufacturer's safety functions should exist with the additional enhancements of the smart gun technologies.

A separate concern is that the smart gun technology can not in any way operate as a second trigger. There should be only one manner in which the firearm can be fired, that is by pulling the trigger. There should be no way that the addition of smart technologies can cause an unintentional discharge of the weapon, i.e., the sequence: cock, press disable button, press enable button, and the gun fires. One method to help protect against this is not to pre-store energy or information needed to activate the firearms locking mechanism.

Requirement: The addition of smart technologies should not affect existing gun safety rules.

Requirement: Smart gun technologies must meet the existing law enforcement standards.

Requirement: The addition of smart technologies cannot act as a second trigger.

Acceptance By Officers

One of the hardest requirements may be to gain the acceptance of law enforcement officers. The majority of officers are interested in how smart gun technologies would work, and would like to try one. Figure 27, shows the response to 'I think it would be valuable to have a gun that only fires for an authorized person, such as

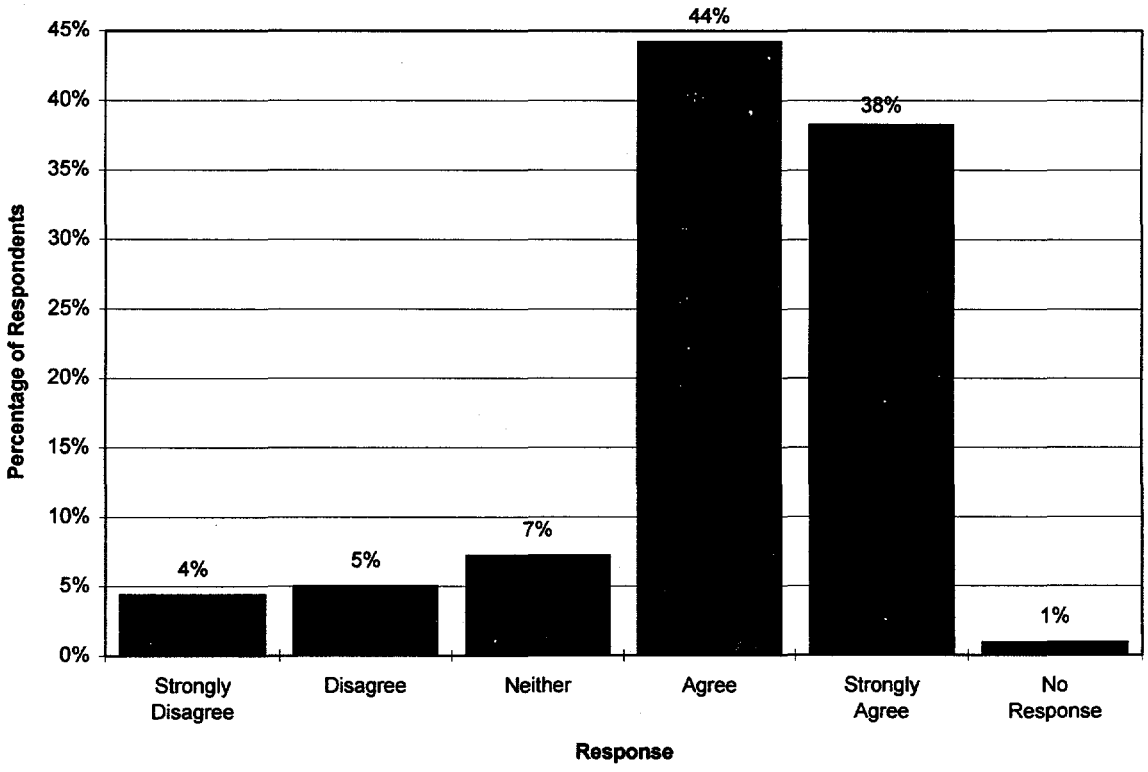


Figure 27. Survey responses to: Smart gun technologies have value.

law officer'. When asked, 'If a smart gun was available I would be interested in trying one', even more officers responded favorably. There is a difference in curiosity and acceptance. Prior user recognition technologies using magnetic rings have not been accepted by law enforcement. One soft body armor manufacturer voluntarily included thousands of brochures about the magnetic ring guns with their own material, but the concept still did not catch on.

Many officers have the "it can't happen to me" attitude; many of those same officers have never seen the statistics on the number of officers killed with their own firearms. Educating officers about the need is one step in gaining this acceptance. Police departments recognize that a problem does exist or they would not offer gun retention training. Industry knows that a problem exists or security holsters would not be marketable.

One pitfall of smart gun technologies are those who declare that a smart gun is the total solution before it is proven and accepted. Officers are concerned that smart guns may be less reliable than standard firearms and would thus create more of a hazard to the officer than they would potentially counter. The smart gun technology must operate in a predictable manner. A proper test program, demonstration program, and field trials will be necessary to gain the confidence of the end user.

Requirement: The smart gun technology must operate in a predictable manner.

False Security

As new inventions add conveniences to products, people start to rely on those conveniences. When the new invention adds security, opposed to convenience, the danger lies in people putting full reliance on the technology and not paying attention to other signals of danger.

This is the concern of many officers when it comes to smart gun technologies. Police trainers are concerned that officers are already depending more on technology and less on training. This can cause over-reliance of the weapon's safety mechanisms rather than retention skills in takeaway situations. Officers need to be trained so as not to have a false sense of security, or become complacent. Trainers are having a difficult time convincing officers that gizmos are not a substitute for safe practices. It is possible that departments may also fall into the same trap and de-emphasize traditional firearms training.

Requirement: 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.

Retrofit

The ideal situation for firearm owners is that they could have a smart gun technology installed in their existing firearm. Replying to the survey question, 'I would want to be able to install the smart gun device in my existing gun' the majority of respondents agreed, as shown in Figure 28. Since many officers have to pay for their service weapon themselves this would save out of pocket expenses. This may also make the multitude of existing firearms able to be made more secure.

There are concerns about retrofitting existing firearms with smart technologies. The main concern is whether the technologies could be added to existing firearms. Is there enough volume within the firearm, would it affect normal operation, could it adapt to all the different models? If a firearm was retrofitted, what happens to a manufacturer's warrantee, who is liable for the changes that were made, how much would it cost, and who would do the installation? Could the firearm manufacturers be forced to retrofit existing firearms? These

are all questions that do not currently have complete answers.

Retrofitting all existing firearms is a very complicated, if not impossible job. Even within one manufacturer, the various models are different to a point where one device may not fit them all. If modifications to older weapons are made, it is difficult to know what effect it would have on the normal operation of the firearm since it was not initially designed to operate in the same fashion. For these reasons the implementation of a smart gun technology may best be introduced into a new generation of firearms.

Requirement: The ideal smart gun technology could be installed in existing firearms without reducing the existing firearms capabilities.

Control and Infrastructure

With the addition of smart guns, the addition of other equipment may be necessary. This equipment would be used to manage the information stored within the firearm (if applicable for that technology). If multiple users are allowed to use a firearm then there must be some way to program that firearm: to verify who is authorized, as well as add and delete users. The enrollment process should be relatively quick and easy. This type of re-coding equipment could be available for use at police departments, practice ranges, and even firearm dealers.

The system can be imagined as a very basic computer that has a database with valid user names and identification numbers. The database system should be able to tell which officers are authorized to which firearms.

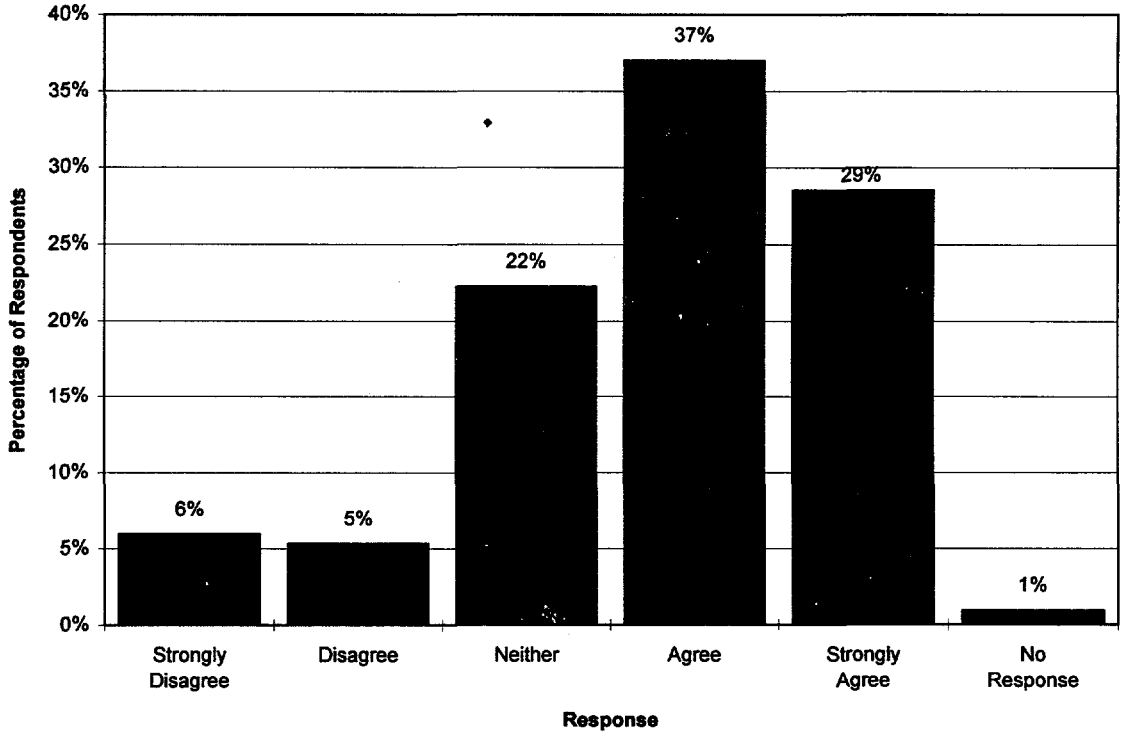


Figure 28. Survey responses to: A smart gun technology should be retrofitable.

Protocols must be established for a common interface and communication scheme between this ancillary equipment and all brands of firearms. This will eliminate the possibility that each manufacturer develops a separate piece of equipment that only works with their firearms so that departments would have to purchase multiple systems.

Departments would have to establish standard operating procedures on how identification codes would be secured and managed. It would have to include who would be authorized to use a particular officer's firearm, i.e., everyone in the department, only his partner, or even a spouse. The procedure would include the security of the identification numbers so that criminals could not obtain the information and more easily duplicate identification devices. Also included would be steps for reprogramming the appropriate firearms if an authorized officer loses an identifying device, and how often identifying numbers are changed (if ever).

Requirement: Ancillary equipment needed must be identified.

Requirement: Recommendation of special procedures must be listed.

Ability To Make The Concept Work

A few officers responding to the survey had doubts about the ability to find technologies that could make a smart gun meet needed requirements. This is a valid concern, and that is part of the purpose of this project. In interviewing officers, many of those who had doubts were relieved when the goals of the project, the systematic approach being taken, and some of the technologies that could be applied were explained to them.

The majority of the comments received in this area were attached with questions about how a smart gun would identify the user, and how it would be made reliable.

Other Concerns

Works Under Stress

A situation where the use of lethal force may be necessary, whether during a weapon takeaway or not, is a stressful situation for an officer. If the firearm becomes too complex, or requires the officer to do something complicated, the less likely an officer will use it effectively under stressful conditions. They may forget how to work the device or there may be too much confusion during the "heat of the moment" if officers are looking for a button mechanism instead of reacting to the situation.

In a very high stress situation such as a takeaway attempt, all but the most well trained officers will tend to change from training techniques toward survival. Their physical responses will follow this trend. The officer may only be able to use gross body movements. Expecting officers under stress to do something using fine motor skills is unacceptable. In these situations officers may forget steps of operations, their voice may change, the will to survive may take over.

Requirement: A smart gun technology must operate within the capabilities of an officer in a highly stressful situation.

Meet Law Enforcement Standards

As this chapter has tried to make clear, law enforcement officers have a unique set of requirements for their firearms. Some officers are concerned that smart gun technologies would not meet these standards. To be acceptable, any technology that is introduced must meet current standards: acceptable reliability, performance, range of ammunition calibers, models, and meeting individual agency criteria. Some of these concerns stem from the original Magna-Trigger device that could only retrofit to one model of firearm.

There are existing standards for firearms. NIJ has standards that establish the minimum

performance standards for "combat ready" police revolvers[32] and autoloading pistols.[33] The Sporting Arms and Ammunition Manufacturer's Institute, Inc. (SAAMI) also maintains voluntary standards.[34]

In these standards, items such as User Information, Visual Inspection, Dimensional Requirements, Functional Requirements, Firing Requirement, Drop Safety Requirement, Drop Function Requirements, Hammer Safety Requirement, Drop Test, Exposed Hammer Test, Jar-off Test, and Criticality of Requirement are included as applicable to either revolvers or autoloading pistols. Detailed information can be found in the standards themselves. Summary information can be found in Appendix A.

Requirement: Smart gun technologies must meet existing applicable firearm standards.

Gun Control

A small number of officers fear smart gun technologies may be used to promote gun control policies. While this is out of the scope of this project it is worthwhile to separate the issues of who should be able to own a firearm, and who should be able to fire a firearm. A smart gun should simply limit who can operate the weapon, not own it. One former police internal affairs officer said that this type of device may assist in the investigations of police involved shootings by limiting investigations to authorized individuals.

Unconscious or Incapacitated Officer

Some officers are concerned about the scenario where during a takeaway the officer is unconscious or incapacitated. Although this does occur, it is a small part of the officer deaths due to takeaways. Some officers would like to have the smart technologies operate even if the officer was incapable of doing anything. Therefore, there would be no ability to push a button, enter a code, or say a code word to deactivate the system. The system would have to be passive, in that when it is not in the officers hand it will not fire.

Requirement: The ideal smart gun technology operates without action by the officer.

Override

A few officers have suggested that they would like to see a manual override of the smart technology. Their real concern is the reliability of the device, and that if it fails they will be without their firearm. An override is possible, and it would let anyone use the device without the smart technologies operating. This override, depending on its implementation, could contradict the feature of not allowing a criminal to easily override the system. Whatever the override system, it cannot be kept a secret. Criminals would have a wide open "backdoor" to defeat the system. If the requirements for reliability of the smart gun technologies can be met, there is not a need for an override. If the smart gun fails enabled, then there is not a need for an override. If a system can be implemented which can only be overridden by the authorized user there is not a problem with an override, but this would have the same concerns as the technology itself.

Off Hand

The cases where an officer must fire with their off hand are statistically very few. Many officers do not even know of a time when someone has had to fire with their off hand, outside of police academy training. Figure 29, in asking 'a smart gun has to work with my off-hand' shows the majority of the officers still refer to the need to be able to shoot with either hand, just in case.

There are documented cases where officers have had to fire with their off hand. Injuries

often happen to an officer's shooting hand since it is their strong hand that is likely to be used to physically defend themselves. Officers will hold a baton or flashlight in their weak hand so that their strong hand is ready to draw their weapon if needed. Officers have already stated their concern about losing capabilities in changing to a smart gun, shooting with either hand is one of those capabilities. It is also not improbable to be shot in the hand or arm. Trainers observe this trait in practice with video and picture systems when the officer is confronted by an adversary holding a gun. When a person's attention is placed on the other's firearm, shots will sometimes center around the gun instead of center of mass.

Requirement: A smart gun technology must be capable of ambidextrous one-handed operation.

Off Duty

Some police departments require that officers carry a firearm while off-duty. Officers are concerned about how they can use their firearm in an emergency or unexpected situation off duty. Many will carry a separate, smaller firearm off duty. Officers asked if a smart gun system would be too cumbersome to be practical for off duty use. They also wondered about wearing an identifying device all the time. This could let felons know that they are an off duty officer while there is no way to identify the felons. Most officers were not concerned with being recognized as an off duty officer.

Requirement: Smart gun technologies should be capable of being used by an off duty officer.

Proven Thorough Testing

Before a smart gun technology is fielded it must be thoroughly tested. Many officers already have a bad feeling because of the previous magnetic ring guns. It would only take one mishap to lose officers trust in the

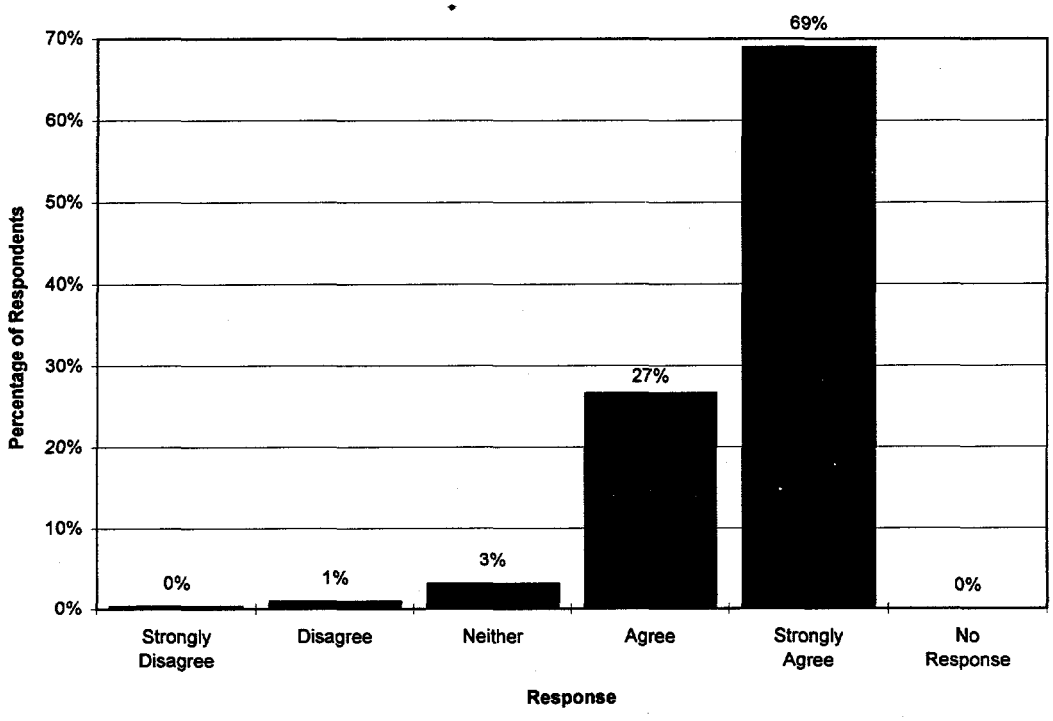


Figure 29. Survey responses to: A smart gun technology must operate with either hand.

system. All malfunctions must be eliminated before field testing. A systematic test program must be used to cover all aspects of the design before actual use. Long term performance issues must be understood.

Along with the normal testing that a firearm manufacturer does both in development and during production, additional testing of the smart technologies must be performed. It will be necessary for a standard to be produced to adequately inform consumers about possible sub-standard products.

Requirement: 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.

Passive Technologies

Officers prefer a passive device that would become disabled without the officer having to initiate any actions. For incidents when the officer is unconscious or incapacitated this may be the only manner of successful operation. This also may help the officer who is in a struggle for their firearm, so that they do not have to actively disable the device. The question may be, for some types of technologies, how to define the definition of out of the officer's hand. Proximity sensors operate over a range of distances. If the suspect's hand is on the officer's firearm, and the officer's hand is on the suspect's hand, some proximity devices may still operate. This concern also infers that the firearm becomes enabled as soon as the weapon enters the officer's hand.

Requirement: The smart gun technology should become enabled or disabled without action by the officer.

Requirement: The smart gun technology should only be operational while in the officer's hand.

Gloves

The question of whether a firearm needs to operate while the officer is wearing gloves continues to be an issue. While Figure 30, shows the officers agree to the statement 'A smart gun has to work if I am wearing gloves' few concerns were along these lines. Firearm instructors say that officers are trained not to shoot while wearing gloves. With a glove the same sensation is not felt by the trigger finger and it is possible that unintentional firings may occur. Officers in the northern states insist that the firearm must operate while wearing gloves. They agree that they would rather not have their gloves on if they have to fire their weapon, but if they have to be outside on a winter night without gloves their hands may be so numb that they could not use the weapon anyway.

A number of other types of officers also wear gloves on duty. Bicycle, motorcycle, and mounted police often wear gloves as part of their uniform for safety reasons. Also more and more officers are carrying some type of glove to be worn while frisking a suspect during an arrest. The common types of gloves that are worn by officers include thin leather gloves, latex gloves, or the newer kevlar gloves.

Requirement: The smart gun technology must operate while wearing gloves typically worn by officers.

Liability

Legal concerns are everywhere. Law enforcement is not excluded from law suits of every type. Departments and officers are brought into court for reasons from using excessive force, to improper training and use of equipment. There are probably more unanswered questions in this area than any other at the current time. This is partly because until cases are tried there is not a precedent to

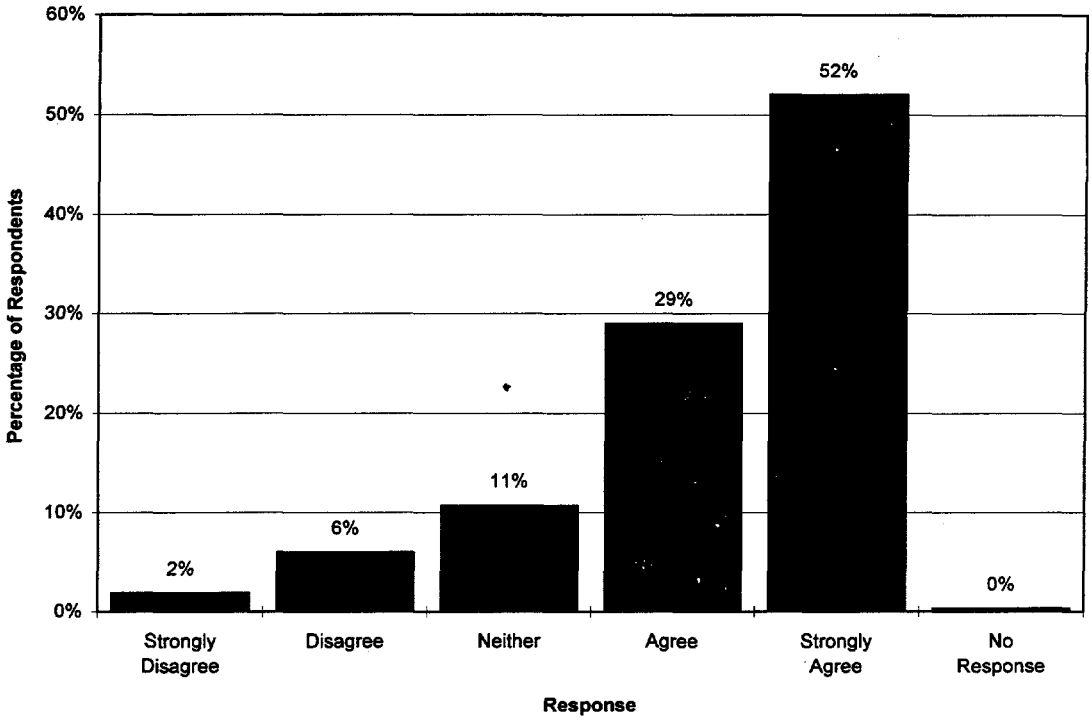


Figure 30. Survey responses to: A smart gun technology must operate while the officer wears gloves.

understand how varying incidents may be received in the courts.

For smart gun technologies, some of the liability concerns include weapons warranty & liabilities if the device failed to operate, or issues involving the use of deadly force if an officer loses a smart gun. More possibilities exist in conjunction with retrofitting a firearm.

The question exists of whether an officer's smart gun in the hands of an assailant should be considered a deadly threat. One scenario could be that an officer loses his smart gun to a suspect who is now threatening the officer with it. A backup officer arrives and sees the suspect with a firearm aimed at the officer. The backup officer shoots and kills the suspect who, because of having the officers smart gun, may be interpreted as being unarmed. The appropriate legal bodies must clarify the liability aspects of smart gun technologies to the law enforcement community.

Indicator

An indicator can be any type of status monitor. For a smart gun application it could be a light or buzzer that tells that the firearm recognized the user, or that the battery is getting low. While most officers say that indicators are necessary, others say that status monitoring is a training and maintenance problem and no indicators should be used. The latter indicates that the user must trust their firearm without relying on an indicator as a crutch.

Because smart gun technologies are a new concept and not yet accepted, most officers want indicators that they can use to build confidence in the device. Figure 31, shows the sum of the responses from the two questions 'An indicator is needed to show that the smart gun can identify me as an authorized user', and 'An indicator is needed to show if the gun is safe or enabled'. The fear that the device will not function reliably is too great not to have an indicator. Officers today frequently check to

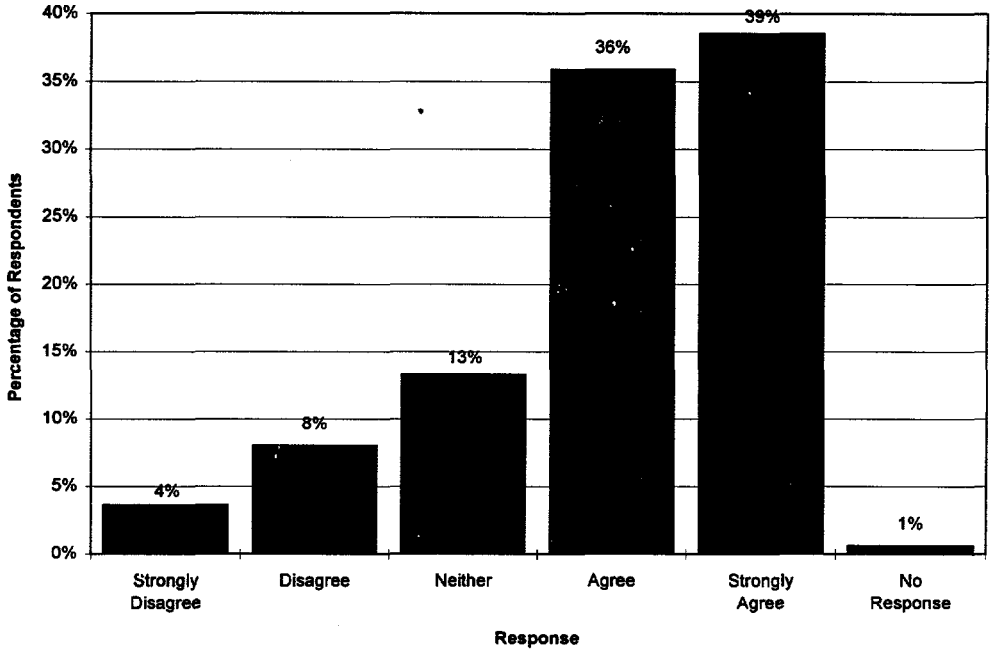


Figure 31. Survey responses to: Is an indicator necessary?

make sure that their magazines are engaged and that they have not inadvertently pressed the release button making their firearm inoperable. A simple test is needed that can be performed by the officer whenever desired to confirm the device is functioning properly without firing the weapon. This may be a feature whose importance will diminish as time passes and officers gain trust in the reliability of the firearm.

Two types of monitors are normally mentioned. One indicates whether a user has been accepted as an authorized individual. The other is a low battery monitor to warn when batteries are about to fail. Officers would like to check their weapon when they first arrive on duty and then maybe on the way to a 'hot' call. Otherwise the firearm only needs to warn them if something is wrong. Officers say the indicators cannot be distracting. Fighter pilots are known to turn off distracting alarms in stressful situations. Officers have different suggestions on what is good and bad. Some suggest a light as part of the sights, others want to be able to see the indicator while the firearm is holstered. Buzzers and other noise making indicators are generally not liked. If they could be heard when needed by an officer in a noisy situation, then they could also be heard by a perpetrator when the officer was trying to be quiet. Some liked the idea of something they could feel, whether a knob that sticks out or an internal thump or click, they would not have to look at the weapon to tell the status. A press to check indicator may allow independent monitoring without constant current drain to the batteries. The power indicator must be noticeable enough that it will not be overlooked, and be at a time that the firearm will still operate for some period, as mentioned in other sections of the report.

The following are some possible drawbacks of indicators that should be avoided. One is causing the officer to look at the weapon instead of the situation at hand. Another is if the indicator would somehow delay the firing of the weapon. If the indicator fails to indicate the proper status is another problem. One final concern if an indicator is present may be the scenario where a suspect has obtained a smart

gun. They could continue to try various tricks to make the smart gun technology operate and they would know if they had succeeded. This should not be a concern for a properly designed smart gun.

Requirement: A simple test to confirm that the smart gun technology is functioning properly must be available.

Requirement: An indicator cannot be distracting to the officer.

SECTION 3

THE EVALUATION OF SMART GUN TECHNOLOGIES

Chapter 6

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 7

Engineering Requirements

The requirements listed in this section strive to build on the officers' ideal requirements and transform them into attributes that a smart gun system would or would not contain. These requirements are 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 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 is 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 = ±½ inch (greater), Orientation = ±180°.
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 be 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

RELIABLILTY

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 operate after exposure to an atmosphere that could be expected during a lifetime of use.
Target value: 85 dBm $\leq$ 100 MHz
130 dBm $>$ 100 MHz
Rank-able: Yes

Chapter 8

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.

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 that 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 it's 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 handing 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 9

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 that 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 it 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. Manufactures 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 10

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. This firearm was not able to be reviewed and may or may not have addressed these concerns.

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 bought 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 11

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 previously, 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 used 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/in^3 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/in^3, 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 12

Technology 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 an 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 32 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 32 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.

● = 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 32 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.

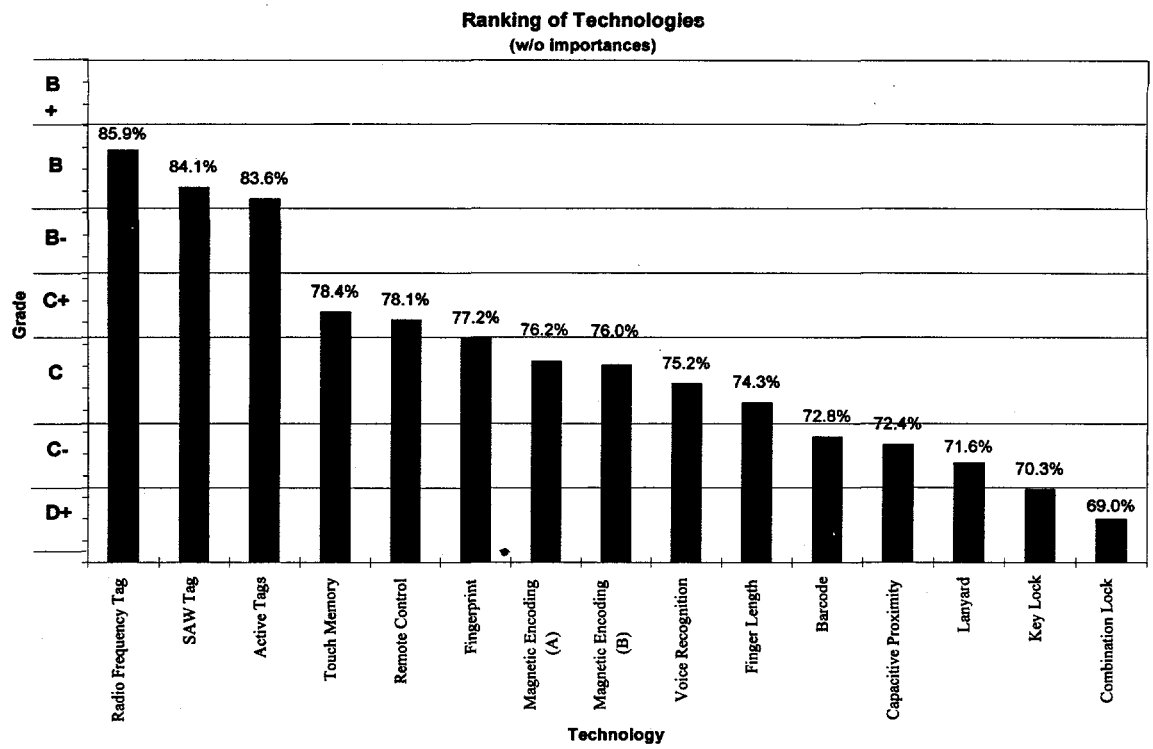


Figure 33 Ranking of Technologies (without importances)

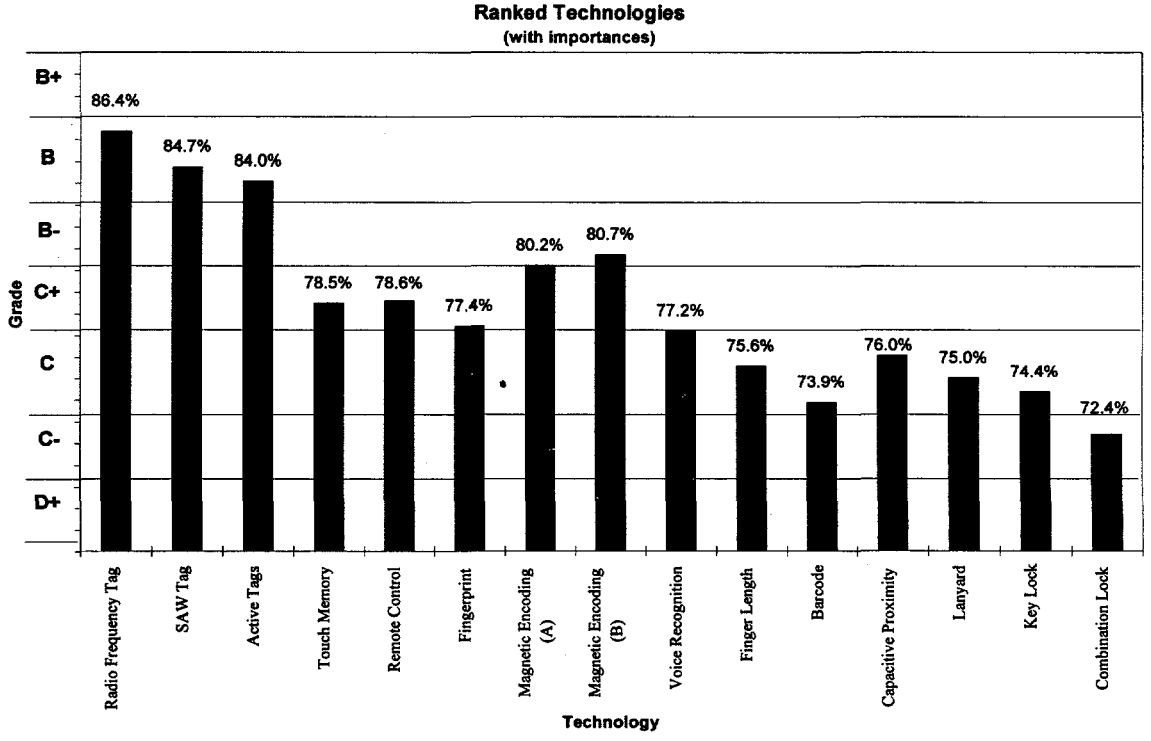


Figure 34 Rankings of Technologies (with importances)

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 33 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 34 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 know 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.

SECTION 4

SMART GUN TECHNOLOGY DEMONSTRATION MODELS

Chapter 13

Development of Demonstration Models

The third objective of the smart gun technology project was to demonstrate promising technology's usefulness in models. Five models were developed to show the strengths and weaknesses of various technologies. The models were referred to as breadboard models which is a term used for experimental models, as opposed to functional prototypes. Another term that is used is demonstration models.

The purpose of the models was to be illustrative of the principles showing how a smart gun technology would operate. The models provide a visual aid when discussing the project with law enforcement officers, and others. Having a model that can be seen and touched causes individuals to make comments that might not otherwise be made. The downside of showing models is that, in being breadboards, some people get the wrong impression that they are very close to a final product. Engineers are also helped through the development of the models by identifying areas that require further investigation.

The breadboard models do not have components assembled within firearms, although they have features that approximate those of a final product. Each model was built into an identically sized box that held any additional electronics necessary to show how the technology would recognize an individual. The models then would perform an enabling operation that was indicated to the user. Each of the models contained the signals that would be generated by the user to enable or disable the latching mechanism.

The goals for the models were to have a tool that could be transported to various locations for law enforcement officers and others to review. The models would show the concept of how the technology would recognize a user and then indicate the completion of the recognition process. Each model would have the same look and feel so that a person would not be influenced by changes in the model's appearance. Even though the models were not functional firearms, they had to give the impression to a professional firearm user that the device was acting as a smart gun would operate.

The breadboard models would have to be built from materials that could be obtained in the cost and time constraints of the project. Existing commercial equipment would have to be modified into configurations that would emulate a smart gun.

Technologies were selected not only to show how a particular implementation of a technology would operate, but also to show how a class of technologies with similar characteristics might operate. By proper selection of the technologies to be modeled, the comments that officers made during reviews could be extrapolated to different technologies with similar characteristics.

Five models were fabricated: Touch Memory, Remote Control, RF Tag, Fingerprint, and Speech Recognition.

Touch Memory Demonstration Model

The touch memory model was built to represent a technology that requires a firearm

user to wear an external device like a ring that would have constraints on the ring's alignment. In this way, the model also represented other technologies like magnetic rings and possible bar codes. The model allows up to four different memory devices to be recognized.

To operate the touch memory model the user has to wear a ring that contains a memory device that is read when it comes into contact with the reader. The ring's memory contains an identification number that would be unique to a single firearm user.

The discriminator is built into the firearm's grip. In this case the model includes two parallel rails inset in the grip. The top and bottom rails are of one electrical potential and are spaced with close tolerance so that the touch memory can just be placed between the rails. A second conductor is placed at the bottom of the inset so that an electrical circuit is made when the touch memory is placed in the inset. This allows the memory to be read, and discrimination between authorized and unauthorized codes to occur.

The signal generated by the discriminator is used for the actuation of the latching mechanism: on the model this is displayed by a "user verified" light. The trigger of the model is connected to the "weapon fired" light and indicates whether the firearm would have fired when the trigger was pulled.

RF Tag Demonstration Model

The radio frequency (RF) tag model demonstrates how a smart gun would operate with the user wearing an external device such as a ring that does not have strict requirements on the ring's orientation with respect to the firearm. The model allows up to four different tags to be recognized.

To operate the RF tag model the user has to wear a ring that contains a memory device that is read when it comes within range of the reader's transmitting signal. The ring contains a passive tag in which an identification number that would be unique to a single firearm user is stored.

The discriminator is built into the model. In this case the reader transmits an RF signal which powers the tag which in return transmits an RF signal back to the reader. This return signal contains the code that is stored in the tag's memory. The code is read to determine if the contents of the memory is that of an authorized or an unauthorized user.

The signal generated by the discriminator is used for the actuation of the latching mechanism: on the model this is displayed by a "user verified" light. The trigger of the model is connected to the "weapon fired" light and indicates whether the firearm would have fired when the trigger was pulled.

Fingerprint Demonstration Model

The fingerprint model demonstrates how a biometric technology that requires contact between the biometric and the reader could be used in a smart gun. The model allows up to four different fingerprints to be recognized.

The model contains an optical scanner that is used to read the user's fingerprints. Because of the size of the commercial reader, it is not placed on the grip of the firearm, but on the base of the model. To control when the fingerprint is scanned a switch is placed on the back of the firearm. When this switch is squeezed, as it would whenever being gripped by the user, the fingerprint can be scanned. If this switch is ever released, then the a new scan must be taken. The user must first be enrolled and train the system to recognize his fingerprint. After this, whenever the user's fingerprint is scanned, the system will attempt to recognize it.

After a fingerprint is scanned and analyzed by the discriminator, the result is displayed on the "user verified" light. The trigger of the model is connected to the "weapon fired" light and indicates whether the firearm would have fired when the trigger was pulled.

Voice Recognition Demonstration Model

The voice recognition model demonstrates how a biometric technology that does not require

contact between the biometric and the reader could be used in a smart gun. The model allows up to four different voices to be stored and recognized in the speaker recognition mode, and allows unlimited users to be recognized in the speech recognition mode.

The model is attached to a small computer that contains a commercial sound card that is compatible with the voice recognition software that is used. The firearm user must wear a high fidelity microphone headset to capture his voice. This is necessary to eliminate as much background noise as possible and to create a repeatable recording not possible with a hand held microphone. In the speaker recognition mode the user enrolls by training the model to recognize his voice by saying any word they desire. When this word is repeated the model attempts to recognize the word and its speaker so the system can be enabled. In the speech recognition mode, the user can say either of two pre-stored "secret" words. The model will attempt to recognize the words and enable the system

After the user's voice is recorded and analyzed by the discriminator, the result is displayed by the "user verified" light. The trigger of the model is connected to the "weapon fired" light and indicates whether the firearm would have fired when the trigger was pulled.

Remote control Demonstration Model

The remote control model is used to demonstrate a different approach to smart gun technologies. While the general smart gun concept is to identify the user and enable the firearm, this approach gives the user the command and control authority over the firearm.

A simple coded remote control transmitter is used to control the state of the model. The actual controller used is capable of transmitting two different radio frequency signals. One signal enabled only the user's firearm, the other would enable all firearms within range. The radio frequency receiver is acts as the discriminator. The receiver is built into the model and controls the state of the firearm.

For a user to operate this model, he presses one of the buttons on the transmitter which sends a coded signal to the firearm. The discriminator reads the signal and determines if it is from an authorized user. If the signal is recognized then the a "user verified" light is turned on. Now anytime the trigger is pulled, by anyone and not only the authorized user, the gun would fire as shown on the model by turning on the "weapon fired" light.

Chapter 14

Reviews of Demonstration Models

The smart gun technology models were made to educate law enforcement officers, and others, by demonstrating the strengths and weaknesses of various technologies. The normal manner for models to be demonstrated was at a conference. Sometimes the demonstration was associated with a formal presentation, other times as part of a display in an exhibit hall. The models were taken to various types of conferences. When possible the models were taken to police departments and demonstrated for officers. A few locations where at least some of the models were displayed include: Montgomery County Training Center (VA), Law Enforcement in the 21st Century Conference (DC), National Sheriffs Association (TX), American Society of Law Enforcement Trainers (NM), Houston Police Department (TX).

During presentations of the models, officers would be educated about the specific concepts the models were made to show. Officers would be guided through some of the known concerns with the technologies and then encouraged to offer comments and questions. They were also encouraged not to limit their thinking to the exact technology and features the models included, but to extend the concepts to other similar technologies. Often the officers just asked questions as they were learning more about the models, but even the questions revealed hidden concerns. Special features were included on certain models to ascertain officer's opinions on other aspects of their requirements not directly related to recognition. Although it is always nice to hear praise from the law enforcement community, it is more helpful in the early stages of a project to hear officer's criticisms: officers were encouraged to reveal what they saw and did not like, and what was missing that they wanted to see. This way corrections can be made in the requirements and designs early in the project. Because of this approach the officer's comments often sounded very negative.

The following section will summarize the strengths and weaknesses presented to the officers, and their comments in a paragraph form. The comments are not from any one individual, but are the composite of many officer's ideas and concerns about the models and technologies. Along with the comments are a simplified response, detailed information about officers' concerns and technologies are addressed throughout this report. The comments are grouped by models.

Touch Memory Demonstration Model

Officers examining the touch memory model could readily understand what it would mean to have a smart gun that would require the user to wear a ring that was alignment critical. Remember that these comments are steered towards the touch memory demonstration model, but may apply to any technology that requires an alignment critical ring.

The first comment that officers often make has to do with wearing a ring. Officers say that a ring can be forgotten, lost, or stolen. Any of these things would leave the officer without the use of his firearm. Since the police officer's job is not predictable it may be easier to forget an item that is not part of their uniform.

Officers admit that this is an item that they, for the most part, have complete control over. It would be up to an officer to remember to wear his ring whenever he had his firearm with him. Officers said that once they learned that the firearm and the ring were a pair it would be a normal to always have both items available.

It was said that an adversary could incapacitate an officer and take both his ring and gun. This is true, and in a small number of cases this is how officer's firearms are taken from them in the first place. The typical scenario does not occur in this manner. Also stated by officers is that many people today do not know how to operate firearms, and some officers have been saved by simply turning on the safety. In the same way, some people would not know that the officer's ring is critical to the operation of the firearm.

Some officers do not wear jewelry while on duty. Items on the hands and arms can become snagged during duty. A ring that snags on a car door or fence could injure the officer, while jewelry that snags another person could injure that person. Many officers currently wear at least one ring, and a watch.

Officers also mentioned the necessity of having to wear two rings to be able to fire with either hand. Officers understood that firing with either hand meant that a ring would have to be worn on both hands.

Many of the concerns about the touch memory ring came from the large size of the ring and that the ring had to be worn backwards. The ring used with the demonstration model was large: it was a commercially available ring. The reason that the model's ring had to be worn backward is that the memory device on the commercial ring was located on the outside, but for the memory to touch the reader in the firearm's grip it needs to be in the back. A ring can be designed that could greatly reduce the size over that used in the demonstration and have the contacts in the back.

The major concern of the officers trying the touch memory model was the alignment criticality of the ring. As the ring for the touch memory model is made smaller, the criticality of the alignment may increase. This is because there are two smaller areas that need to be aligned. The ring needs to be read where ever it happens to land on the grip. Even if the ring is turned so that the contacts are not squarely placed on the grip.

With the touch memory model, contacts are present on both the ring and the grip. These contacts must make an electrical connection for communication to occur. This causes concerns that contaminants of any type could interfere with the communication. Gloves could be considered a type of contaminant for this model because they would interfere with the communication.

RF Tag Demonstration Model

Officers examining the RF tag demonstration model could easily recognize the advantage of a system where alignment of the ring was not critical.

The benefit of the RF tag was that the firearm would become enabled as their hand approached the weapon, and not after finding the proper grip. This would work even if the officer was wearing gloves. This increased the comfort of many officers, although the officers still had the general same concerns about wearing rings as they had with the touch memory model.

The proximity that the firearm could become enabled now became the concern. If the firearms reading range was too great then two problems could occur. First if another officer was nearby while the firearm was trying to read the users tag, there might be contention between which tag is read. It is possible that no tag would be read. Second, when an officer is in a takeaway situation and an adversary obtains control of his gun, then that officer must make sure that his tag is out of range so that the firearm would become disabled.

Another concern was the possible interference problems that may exist between common electronic devices and the RF communication

required by the firearm. Interference can be caused by any device that can create a signal that is similar, much more powerful, or blurs the intended signal that the discriminator is expecting. Contention between two or more tags can be considered as a form of interference. This is a valid concern for all RF technologies.

Fingerprint Demonstration Model

Officers examining the fingerprint demonstration model were shown how a biometric technology relying on physiological attributes could operate in a smart gun. Many of these comments could be applied toward similar technologies such as finger length, or palm prints.

The first thing that officers would notice is that the fingerprint sensor was not on the model's firearm. The large size of the technology's reader immediately became apparent to them. This lead to questioning the placement of the reader on the firearm. Similar to having to wear two rings, if anything other than the trigger finger is used, two readers would have to be placed on the firearm.

When using the demonstration model the lengthy amount of time that is required for the scanning and processing of the fingerprint information was seen. The time was too long.

Again similar to the touch memory model, concerns were raised regarding the necessity of a physical touching of the reader. Again any contaminants could interfere with the discrimination process, but now abrasions to a person's fingers could also cause interference.

Voice Recognition Demonstration Model

Officers examining the voice recognition demonstration model were shown how a biometric technology that has behavioral attributes could operate in a smart gun. Comments may be compared to other technologies that have a behavioral component or require the officer to act in a certain manner.

The obvious item on the voice recognition model is the necessity to wear a headset that holds the microphone steady to obtain repeatable voice recordings. The effect of background noise can be seen during demonstrations. Extraneous noise causes a degradation in the discrimination process. Slight variations in the utterance of a word can effect the discriminating capabilities.

Both speaker recognition and speech recognition could be tried on the model. The speaker recognition allowed the officer to choose any enabling word he wanted. Even though discrimination is based on the speakers uttering the word, added security could be obtained by keeping this word secret from other individuals. With the speech recognition the password must be kept secret (while being spoken aloud) since the discriminator does not care who says the word, as long as the word is recognized.

Another concern is that of the effect of stress on the discrimination of the user's voice. The officer has to remember the proper words and then be able to say them recognizably independent of whether he is exhausted or excited. Saying a work requires an action by the officer, but this was more acceptable because it did not require the use of the officer's hands which could be busy during a takeaway scenario.

Remote RF Demonstration Model

Officers examining the remote RF demonstration model could see that there are other possible methods to formulate a smart gun system. Many officers liked the authority that the remote control offered. Being able to enable or disable the firearm at their command.

The fact that an adversary could operate their firearm if it was taken from them while it was enabled did not bother some, probably because this is equivalent to what they have now. Much of the reason may have had to do with the firearm already being in the enabled state (assuming it was carried that way) and nothing "magical" needing to occur before it will fire.

Some of the magic that some officers are concerned about is the unknown of exactly how

the electronics operate. In general the younger officers are more favorable toward any type of high-tech device, whether it is a radio or a firearm, than older officers. More experienced officers have two opinions about this: some say the younger officers have grown up in a high tech world and take it for granted, and others account for it by a lack of experience and respect for the difficulties of the job.

Some apparent contradictions in officer's comments between the different models are: the ability to carry a remote control but not wear a ring (that other technologies might require); and being able to press a button on the remote to disable the firearm, but not having the time to accomplish other actions that a technology might require.

A remote control can be carried as part of the uniform. This means that the officer does not have to remember to put on an additional piece of equipment (like a ring). In this way officers may think that they are not carrying anything new.

In a takeaway situation the officer would have to press a button to disable the firearm. This may be difficult if not impossible in some scenarios. Officers are of varying opinions whether the capability exists to manually disable the firearm. If the officer does have the capability to perform this action, they may also have other capabilities that they have not considered which could be done to turn on or off the firearm during critical situations.

Other Model Items

Information was also gathered from officers' comments on other features that were included on the demonstration models.

All the models had indicator lights as a visual means to tell whether the user was recognized. No negative comments were received on the lights, but since they were part of all the models the officers seemed to expect them. The remote control model was also supplied with an adjustable audible indicator. Indicators did not receive as many comments as the recognition portion of the models. The audible indicators did cause some concerns on both extremes of being too loud to be heard by others, or most likely not being able to be loud enough to be heard during an actual incident.

The fingerprint model was fitted with an on/off switch on the rear of the grip. This switch was built similar to the grip safety switch appearing on some pistols. This switch was normally viewed as just another thing that could go wrong with the system, one more link in the unreliability chain.

On both the biometric models the enrollment process could be evaluated. It can be seen that the enrollment process, even for a model, can be done simply and quickly and give acceptable results.

There are many items that the models could not demonstrate to the officers. A few of these are the technology's cost, reliability, and adversarial strengths. Items like these will remain a concern for officers until a fieldable prototype is thoroughly tested.

Even though the officers' comments often had a negative content this should not deter others from further investigations into these or other technologies. The technologies used in the models were not developed specifically for a smart gun application. They were made to fit this application in a model that was designed to show both the technologies' strengths and weaknesses. In this way officers could be educated about both the things they should look for and the things that they should avoid, and smart gun designers could learn from their likes and dislikes.

SECTION 5

CONCLUSIONS

Chapter 15

Conclusions and Recommendations

The National Institute of Justice (NIJ) recognized that a number of officers are being killed each year with their own service firearms. Acting as the principal research branch for the U.S. Department of Justice, NIJ funded Sandia National Laboratories (SNL) to perform research on one method of increasing the security of firearms and reducing these deaths: smart gun technologies. Smart gun technologies are those technologies that could equip a firearm with the intelligence necessary to tell if the user is authorized to discharge the firearm.

SNL is familiar working in the many areas that should be included in smart gun research: security, safety, reliability, weapons. SNL had previously done basic development activities on smart gun technologies for a security branch of the Department of Energy. A three objective project was developed: 1) find the requirements that a law enforcement officer has for a smart gun technology, 2) evaluate various existing technologies against those requirements, and 3) develop models to demonstrate how a technology might operate in a smart gun system.

Validating the Takeaway Problem

Little previous work could be found that specifically targeted law enforcement firearm takeaways. The FBI and individual states had summarized takeaway events. This project brought together the available research and added a detailed look at other factors that have occurred since 1979, such as location and types of officers. It was found that no officer is immune to being involved in a takeaway situation, and while the adversaries are becoming better trained the officers may be becoming overconfident. As many as 19 deaths per year have occurred from an assailant's use of an officer's firearm. Fortunately the number of officer deaths during takeaways is decreasing, down to five in the past year. There are numerous possible reasons this that could be researched in more detail, these include increased awareness of the problem, increased specialized training, increased use of security holsters, and the transition from revolvers to pistols.

An analogy was developed which described the smart gun system as a lock and key. The key is the item that is unique to the officer, the item that the firearm recognizes. The lock consists of the discriminator that determines if an authorized key is present, and the latching mechanism that physically enables or disables the firearm.

Finding Officer's Requirements

Having the problem validated helped explain the need for a smart gun technology to officers. The task at hand was obtaining smart gun technology requirements from the officers. Some requirements were found in validating the problem and other research methods, but the primary source for requirements was a survey designed to determine officer's attitudes. The goal was to find a set of requirements that would be the ideal smart gun technology, even if the set was impractical or contradictory. This would be a list of the officer's wants, which would probably be more

than they really need. From this list a search for the perfect technology could be started.

Officers want their firearm to operate predictably: the firearm must remain reliable in all the environments and circumstances that an officer may encounter. To achieve the acceptance of the law enforcement community the addition of a smart gun technology must not noticeably degrade any of the capabilities that exist in firearms today. It should be able to be used by fellow officers, and it should be able to be fired by either hand. The characteristic properties of size, weight, and shape should not noticeably change. It should remain easy to operate and maintain. Officers like the idea of the smart gun technology being able to fail and still allowing the firearm to fire, even though anyone could fire it.

A difficult set of requirements resulted from the wide ranging opinions of officers. While all the "wants" listed by the officers may not ultimately be met, their needs must be met. Listing requirements in this fashion allows individual technologists the latitude to develop products that meet the needs of officers, as well as create a market niche by incorporating additional features.

Evaluating Technologies

The wide ranging opinions of officers created a difficult set of requirements. The next step is to find a technology that can be used in a system to meet their requirements. With the assistance of existing quality techniques, the officer's qualitative requirements were transformed into a set of quantitative engineering requirements. In this way the individual technologies could be evaluated.

Fifteen implementations of fourteen technologies were taken through the entire ranking process. Each technology was assigned a score for each requirement as to the currently available capabilities of that technology. Each technology had characteristics that scored high in individual categories. Mechanical technologies ranked high for low power consumption and being less expensive. Electronic technologies scored high for their ability to discriminate digital codes. Biometric technologies scored high for being unique as a key. However, the evaluation revealed that no technology met all the officer's idealistic requirements. All technologies can use more dedicated development to tailor their attributes to a smart gun application.

Demonstration Models

It is easier to obtain comments from people when they have something in their hands that they can touch. Five demonstration models were developed to show conceptual operation of smart gun technologies. The technologies were selected to show how a particular implementation of a technology would operate, and how other technologies with similar characteristics might operate. The models were designed to highlight strengths and weaknesses of the technologies so that officer's comments could be obtained. The normal manner for models to be demonstrated was at a conference.

Officers gave comments about each technology after being educated about the operation of the models. In general officers liked the particular characteristics of each of the technologies that ranked high in the evaluations. The problem being there is not a single system that currently can combine only the best parts of each technology. Officers had concerns about anything that could perceivably go wrong at a time that it needed to operate. This list included: batteries, electronic circuits, and mechanical linkages. This generally covers all possible items. What has to be remembered is that, while it is true that the models displayed these weaknesses, it was the model's job to bring out these complaints so that some measure of importance between these various items could be obtained. More information on what is, and is not, important to officers can always be used.

Final Conclusions

Officers are, by the nature of their job, often very skeptical. When it comes to smart gun

technologies they are skeptical of the technology itself. Many are also skeptical of a takeaway ever occurring the themselves, it's the other officer's problem. The general consensus among law enforcement officers is that a smart gun is a good idea and could be very beneficial to their job, if...

The "if" can be summarized in one item: reliability. Since officers are more likely to use their firearms to defend themselves or others, than for it to be used against them, the firearm must operate every time they pull the trigger. The addition of any item to a firearm will generally make it less reliable.

Developing a smart gun that meets law enforcement officer's idealistic requirements is a very difficult problem. Fortunately the officer's actual needs are less than their wants. There are many opinions among officers, but there are few statistically definable facts about what they will ultimately accept. It may take a generation of smart gun systems to come and go before a smart gun is not only common but is favored over a non-smart gun; this is much as it is with other new technologies. It is suspected that if officers can be shown a firearm that recognizes them and it can be proved to them that it is reliable, then it will not much matter what else it does or does not do. Any other features will only be enhancements -- gadgets. First it has to work.

APPENDICES

Appendix A

Operational Environments

This appendix describes the requirements listed in the existing firearm standards, and from other sources such as firearm manufacturers. The requirements are not separated from the text, but should be obvious to the reader. Due to the severe conditions that could be encountered, both by law enforcement personnel and the handguns that they possess, any smart gun technology must be rugged. The technology may not meet the requirements individually, but must be able to meet them when incorporated into a smart gun system.

There are many standards available for firearms. The National Institute of Justice has standards[32,33] which establish performance requirements and test methods for firearms to be used by law enforcement officers. The Sporting Arms and Ammunition Manufacturers' Institute, Inc. also has voluntary industry performance standards[34] to provide the firearm designer and manufacturer with recommendations for methods to simulate certain conditions where the firearm is subjected to abusive mishandling. Individual companies typically develop their own internal quality procedures to meet and exceed these standards[35]. When government organizations need to develop a firearm they will develop their own specifications for its design and testing[24]. All of these specifications are different and the following requirements were selected based on these current standards. Since the following is an aggregate set of these requirements, references will not be individually listed.

Rough Handling and Dropping Shock

Police service weapons are occasionally dropped or handled roughly. At these times it is critical that the firearm does not discharge. Generally weapons fall as they are drawn from the holster or returned to the holster. Usually a weapon will be ready to be fired when it is dropped, and generally it is dropped on hard surfaces such as roads, walkways, and inside buildings. The smart gun technology must also survive these drops. The minimum drop test requirement for the smart gun technology is for the firearm to remain fully functional after a shock pulse type, duration, and magnitude such that the conditions emulate those that would be encountered if a fully loaded firearm were dropped on a 0.5 inch thick steel plate backed by concrete from a height of 4.0 feet. The drop test shock shall occur on each of seven axes, which are defined in Figure A-1, and each shock shall be repeated at hot (160 ° F), ambient (70 ° F), and cold (-60 ° F) temperatures.

Firing Shock

A separate shock environment is associated with the firing of live ammunition from the firearm. The smart gun technology shall be fully functional after the smart gun has been subjected to the operating shock environment. The operating shock axes are defined below in Figure A-2. On each axis the firearm shall be exposed to an acceleration signal with a frequency and amplitude content consistent with the firing of live ammunition. The number of test cycles shall be consistent with the service life of the firearm, however, the number of test cycles need not necessarily be equivalent.

Accelerations on the order of 950 g can be expected during the firing of live ammunition in test set-ups using fixtured firearms[36].

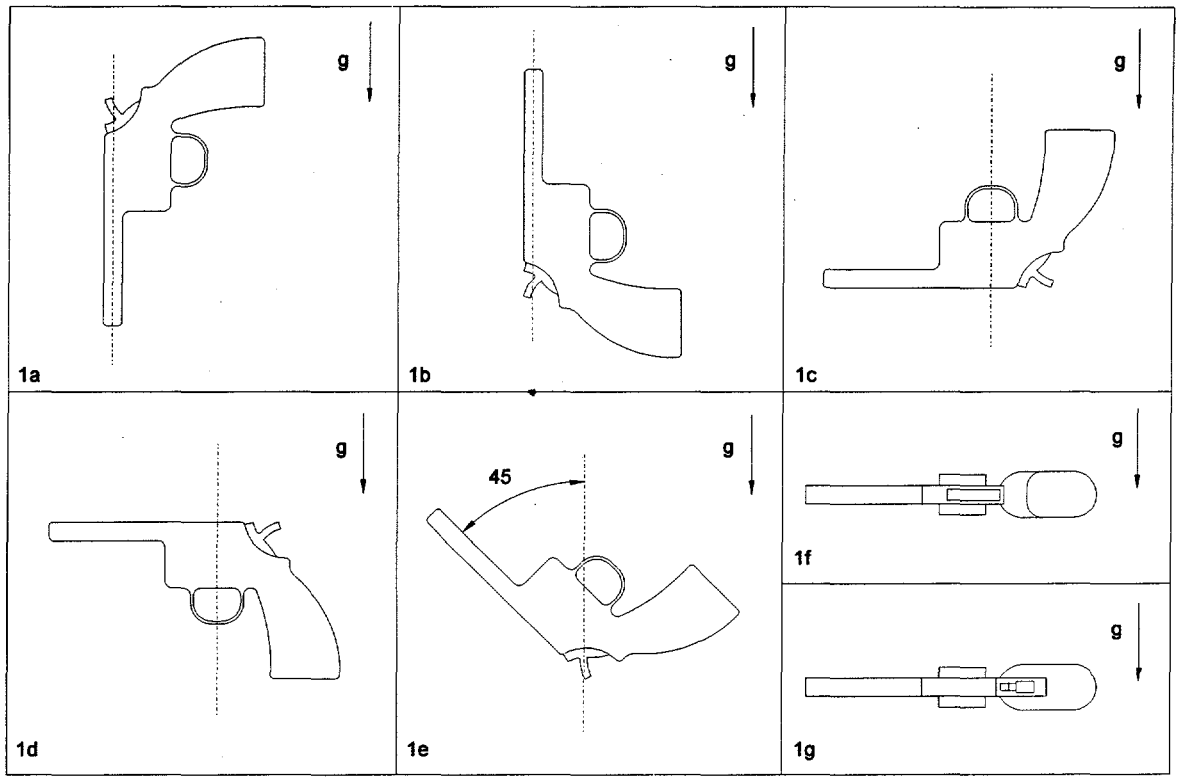


Figure A-1. Dropping Shock Axes

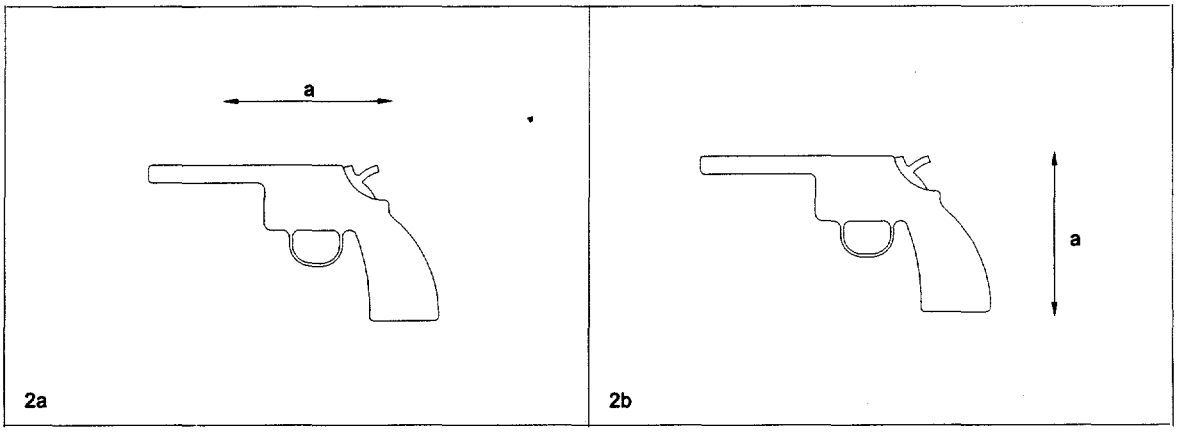


Figure A-2. Operating Shock Axis

Service Life

The number of live rounds that a firearm must survive varies with the way it will be used. The service life for a military firearm may reach 30,000 rounds. The NIJ only specifies a total of 600 rounds in their testing because they are looking for mechanical failures of the firearm that they have determined usually occur in the first 200 rounds of use. Manufacturers will test a firearm to 5000 rounds during development, while the useful life is expected to be between 10,000 and 15,000 rounds. The smart gun technology must have a service life that meets or exceeds the 10,000 live round capability of the firearm itself. For dry cycle testing the smart gun technology shall be able to authorize the firing mechanism greater or equal to 100,000 times.

Temperature

The firearm that the officer in hot and humid Florida carries is the same type of firearm that the officer in Alaska uses. Temperatures vary greatly around North America. The highest temperature recorded in North America, 134 °F, was in Death Valley, California the lowest temperature, recorded in Canada, was -81 °F.[37] While these are the extremes, it shows the wide range of operating temperatures that can exist in North America. Typical military electronic requirements list -55 °F to 165 °F, and electronics certified to operate during these levels are available. We see by comparison to the record temperatures that the military temperature requirements are not unrealistic. It is also possible the firearm will self heat given that enough rounds are fired. The smart gun technologies shall be fully functional when the temperature throughout the smart gun system is between -50 °F and 160 °F.

Noise Environments

Officers will often work in noisy environments. Some of the noise environments that must be dealt with include rock concerts, barrooms, and gun fights. Two examples of noise environment levels are heavy trucks which produce 90 dB at 50 feet, and freight trains that produce 75 dB at 50 feet.[38] The smart gun technology must operate during intermittent and constant noise environments up to and including a person's threshold of pain (approximately 130 dB).

Chemical Compatibility

The following is a list of substances taken from a specialized military handgun specification. It is included only as a reference list of substances that could come into contact with a firearm.

1. Water
2. Lubricant, cleaner and preservative for weapons and weapon systems, MIL-L-63460D (CLP)
3. Lubricant, semi-fluid (automatic weapons), MIL-L-46000C (LSA)
4. Lubricating oil, weapons, low temperature, MIL-L-14107C (LAW)
5. Lubricating oil, general purpose, preservative (water displacing, low temperature), VV-L-800C (PL-S)
6. Aerosol lubricant
7. Cleaning compound, solvent (for bore of small arms and automatic aircraft weapons), MIL-C-372C (RBC)
8. Dry-cleaning and degreasing solvents, P-D-680A, type 1
9. Insect repellent, NSN 6840-00-558-0918
10. Carbon-removing compound, P-C-111D, type 11
11. Trichlorethane solvent

12. Hydraulic fluid
13. Antifreeze (ethylene glycol)
14. Salt water (20% NaCl)
15. Gasoline
16. Kerosene
17. Diesel fuel
18. Jet fuel, JP-4
19. Decontaminating agent, STB, MIL-D-12468C (MU)
20. Decontaminating agent, DS2, MIL-D-50030H

Miscellaneous Environments

The following is a list of other environments taken from a specialized military handgun specification. It is included only as a reference list of environments that a firearm may experience.

Waterproof Capabilities

Capable of functioning after a two hour submersion of the smart gun in sea water at a pressure of 2 atmospheres (depth of 66 feet).

Salt Fog

Fully functional after the smart gun has been placed in a salt fog environment for 10 days. The salt fog solution shall be prepared in accordance with MIL-STD-810E (method 509.1).

Sand and Dust

Capable of operation during exposure of the smart gun to a sand and dust environment. Fully functional after the smart gun has been subjected to 96 hours of continuous exposure to a sand and dust environment.

Mud

Fully functional after the smart gun has been subjected to 96 hours of continuous exposure to a mud environment with only hand cleaning and wiping of the smart gun.

Surf Environment

Fully functional after the smart gun has been subjected to 96 hours of continuous exposure to a surf environment. The test chamber shall emulate conditions encountered in a surf environment: salt water and a sand and dust mixture.

Icing

Fully functional after the smart gun has been subjected to an icing environment until 1/8 to 1/4 inches of ice has accumulated on its exterior, and after removal of the ice using only tools normally available in the field.

Solar Radiation

Fully functional after the smart gun has been exposed to solar radiation for a period of ten 24 hour cycles.

Appendix B

Smart Gun Technologies Questionnaire

Smart Gun Technologies Questionnaire
For Law Enforcement Officers

The National Institute of Justice (NIJ) is concerned by the FBI Uniform Crime Report study citing that 14% of the officers killed between 1981 and 1990 were killed with their own weapon. That means 1 out of every 7 officers who are killed in the line of duty are killed with their own weapon. In it's effort to help law enforcement officers, the NIJ has asked Sandia National Laboratories to research the requirements for a Smart Gun. The most important requirements come from the law enforcement officers, and other people who would use a Smart Gun.

Please help us determine the correct requirements and features a Smart Gun would contain. We request that you assist us by completing this 10 minute questionnaire and return it in the post paid envelope attached. As appropriate, please fill in the blank, or circle the response that indicates the extent that you agree or disagree with the statements. Please provide any other information or comments you feel would be useful to us in this pursuit. While it is not required that you answer all of the questions, we appreciate and value your responses.

What is a Smart Gun? A Smart Gun is a firearm that uses a technology to determine if the person shooting has authorization to use the firearm. In this way the firing of a gun can be limited to the authorized person, such as a law officer. This could eliminate the possibility that an officer's gun is used against him or her. There are many ways that this can be accomplished. To find out what you want in a Smart Gun, we need your input.

SMART GUN FEATURES	**Strongly Disagree**	**Disagree**	**Neither**	**Agree**	**Strongly Agree**
1. A Smart Gun should look just like existing guns.	1	2	3	4	5
2. An indicator is needed to show that the Smart Gun can identify me as an authorized user.	1	2	3	4	5
3. An indicator is needed to show if the gun is safe or enabled.	1	2	3	4	5
4. I would want to be able to install the Smart Gun device in my existing gun.	1	2	3	4	5
5. A Smart Gun has to work if I am wearing gloves.	1	2	3	4	5
6. A Smart Gun has to work with my off-hand.	1	2	3	4	5
7. My partner, or other authorized people, have to be able to use my gun.	1	2	3	4	5
8. I would be willing to wear something such as a ring, or wristband, that my gun would recognize.	1	2	3	4	5
9. I would be willing to do something (like press a button on my uniform) to disable my gun if it was taken from me.	1	2	3	4	5
10. It is OK to have batteries in my gun.	1	2	3	4	5
11. The Smart Gun's identification feature should replace my gun's existing safety mechanisms.	1	2	3	4	5
MISCELLANEOUS QUESTIONS					
12. I think it would be valuable to have a gun that only fires for an authorized person, such as a law officer.	1	2	3	4	5
13. If a Smart Gun was available I would be interested in trying one.	1	2	3	4	5

14. My two main concerns about a Smart Gun are:

    1. _____

    2. _____

15. What are two ways a Smart gun could cause you problems?

1. _____

2. _____

FAMILIARITY WITH THE CONCEPT

16. Have you previously heard of a gun that limits it's use to authorized people?
    - __ Yes
    - __ No (If No, go to number 18)

17. What have you heard or seen?
    - __ Magnetic ring
    - __ Remote control
    - __ Capacitive sensors
    - __ Fingerprint
    - __ Voice Activated
    - __ Other: _____

USE SITUATIONS

18. Has a suspect ever taken, or attempted to take, your gun?
    - __ Yes
    - __ No (If No, go to number 20)

19. My response to someone taking my gun was based mostly on: (Circle the appropriate number)

Survival			Training	
1	2	3	4	5

DEMOGRAPHIC INFORMATION (OPTIONAL)

20. City: _____

21. State: _____

22. Your position/title/rank/job function: _____

23. Service weapon: _____
    (Brand-Model-Caliber)

24. Number of years in Law Enforcement work: _____

25. Name: _____

26. Department: _____

27. Daytime phone: _____

FOLLOW-UP QUESTIONS

28. I am interested in being further involved in this project in the following way(s):
    (If you are interested please complete your name and phone number above.)
    - __ Face to face interview
    - __ Telephone interview
    - __ Test and evaluation
    - __ Other: _____

29. Additional comments may be written below if desired.

RETURN TO: Douglas R. Weiss, Sandia National Laboratories, P.O. Box 5800, Albuquerque, NM 87185-0537, Phone:(505) 845-9134, Fax: (505) 845-9888, Email: drweiss@sandia.gov.

Appendix C

Summary of Preliminary Requirements for a Smart Gun Technology

The following are the identical requirements as found in the text. They are rearranged in this appendix in a topical order. The section of the report that describes the requirement is listed in parenthesis.

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. (Characteristics)

1.1.2 The smart gun technology should not affect the carrying of firearms in existing holsters. (Characteristics)

1.1.3 The smart gun technology must not affect the existing trigger pull standards. (Characteristics)

1.1.4 Addition of batteries should not greatly change the characteristics of the firearm, i.e., size, weight... (Power Failure)

1.2 APPEARANCE

1.2.1 The smart gun must have the general appearance of an existing firearm. (Characteristics)

1.2.2 The addition of smart gun technologies cannot add appendages which would appreciably increase snagging compared to an existing firearm. (Characteristics)

1.2.3 Any external device should have optional methods for attachment to the person, i.e., multiple fingers; fingers or wrists; implantable... (External Devices)

1.2.4 Ideally external devices can be attached to existing items, i.e., rings, watches, badges... (External Devices)

1.3 MISCELLANEOUS CHARACTERISTICS

1.3.1 The addition of a smart gun technology to a firearm should be operationally transparent to the user. (Simplicity)

1.3.2 The smart gun technology must be applicable to multiple types and brands of firearms. (Multi-Users)

1.3.3 The technology should also be applicable for use on multi-user weapons. i.e., shotguns. (Multi-Users)

1.3.4 Ideally no external devices are needed to operate the smart gun technology. (External Devices)

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... (External Devices)

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. (Environment and Circumstances)

2.1.2 The ideal smart gun technology operates without action by the officer. (Unconscious or Incapacitated Officer)

2.1.3 The smart gun technology should become enabled or disabled without action by the officer. (Passive Technologies)

2.1.4 A smart gun technology must operate within the capabilities of an officer in a highly stressful situation. (Works Under Stress)

2.1.5 A smart gun technology must be capable of ambidextrous one-handed operation. (Off Hand)

2.1.6 The smart gun technology must operate while wearing gloves typically worn by officers. (Gloves)

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. (Speed of Operation)

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. (Fail Armed)

2.1.9 The addition of a smart gun technology must not complicate the use of the firearm. (Simplicity)

2.1.10 Smart gun technologies must not be alignment critical. (External Devices)

2.1.11 Proper documentation for operational use must be supplied. (Maintenance)

2.1.12 The smart gun technology should only be operational while in the officer's hand. (Passive Technologies)

2.1.13 The operational range of any external device must be consistent with other requirements. (External Devices)

2.1.14 Smart gun technologies should be capable of being used by an off duty officer. (Off Duty)

2.2 RECOGNITION

2.2.1 The smart gun technology must properly recognize, and limit the use of the firearm, to the authorized user. (Proper Recognition)

2.2.2 The smart gun technology should be capable of being used by multiple users. (Multi-Users)

2.2.3 The technology must operate for a single individual on multiple firearms. (Multi-Users)

2.2.4 The smart gun technology must operate on the first verification attempt. (Proper Recognition)

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. (Proper Recognition)

2.2.6 For applicable recognition technologies, a method of adjusting the recognition threshold by a qualified person is recommended. (Proper Recognition)

2.3 POWER REQUIRMENTS

2.3.1 Ideally the smart gun technology would not require the use of batteries. (Power Failure)

2.3.2 A low power indicator must be supplied if batteries are used in a smart gun system. (Power Failure)

2.3.3 If batteries are used, they must be easily obtained, and factored into the cost of maintaining the equipment. (Power Failure)

2.3.4 Ideally a battery used in a smart gun system would last longer than 1 year. (Power Failure)

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. (Power Failure)

2.4 INDICATORS

2.4.1 A simple test to confirm that the smart gun technology is functioning properly must be available. (Indicator)

2.4.2 An indicator cannot be distracting to the officer. (Indicator)

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. (Environment and Circumstances)

2.6 SAFETY

2.6.1 The addition of smart technologies should not affect existing gun safety rules. (Safety)

2.6.2 Smart gun technologies must meet the existing law enforcement standards. (Safety)

2.6.3 The addition of smart technologies cannot act as a second trigger. (Safety)

2.6.4 Smart gun technologies and external devices should not cause medical side effects. (External Devices)

2.7 RELIABILITY

2.7.1 The smart gun technology must operate in a predictable manner. (Acceptance by Officers)

2.7.2 The addition of a smart gun technology must not significantly reduce the reliability of the firearm system compared to existing firearms. (Reliability)

2.7.3 The addition of a smart gun technology must not effect the primary use of firing the weapon by the authorized user. (Simplicity)

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. (Maintenance)

2.8 SECURITY

2.8.1 A smart gun technology must not be easily disabled by an adversary. (Fail Armed)

2.8.2 The technology must be such that even with full knowledge of how the system operates it cannot be easily defeated. (Adversarial Compromise of Technology)

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. (Adversarial Compromise of Technology)

2.9 COMPATIBILITY

2.9.1 The smart gun, compared to existing firearms, should not cause a loss of capabilities. (Loss of Capability)

2.9.2 The ideal smart gun technology could be installed in existing firearms without reducing the existing firearms capabilities. (Retrofit)

2.9.3 Smart gun technologies must meet existing applicable firearm standards. (Meets Law Enforcement 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. (Training)

2.10.2 Smart gun technologies must enhance and not eliminate weapon retention training. (Training)

2.10.3 Smart gun technologies training must extend beyond the use of technologies and include training for armorers and others as appropriate. (Training)

2.11 MAINTAINABILITY

2.11.1 Maintenance requirements for smart gun technologies must be held to a level that the average officer will do. (Maintenance)

2.11.2 There must be a method for armorers and manufacturers to test the smart gun technology. (Multi-Users)

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. (Multi-Users)

2.11.4 The smart gun must be capable of repeated maintenance without damage or a decrease in performance. (Maintenance)

2.11.5 Department's armorer or trained personnel should be able to perform most diagnostic tests and repairs. (Maintenance)

2.11.6 The technology should be upgradable when the next incremental version of the technology is introduced. (Maintenance)

2.11.7 Batteries should be easily replaceable, even in the field. (Power Failure)

3.0 ENVIRONMENTAL

3.0.1 The smart gun technology must operate in all likely environmental conditions. (Environment and Circumstances)

3.0.2 The remainder of the Environmental requirements are found in Appendix A.

4.0 EXTERNAL EQUIPEMENT

4.0.1 Ancillary equipment needed must be identified. (Control and Infrastructure)

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. (Cost)

5.0.2 Any additional costs associated with the use of smart gun technologies should be minimized. (Cost)

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. (False Security)

5.0.4 Recommendation of special procedures must be listed. (Control and Infrastructure)

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. (Proven Thorough Testing)

Appendix D

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 anoperator 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 see04682435)
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 actuable 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 fire arm 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 l.
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.

References

1 Commission on peace officer standards and training, *California peace officers killed in the line of duty 1987-1988-1989*, State of California, August 1992, pg. 27.

2 Commission on peace officer standards and training, *California Peace Officers Killed in the Line of Duty December 1986*, State of California, December 1986.

3 Sandia Capabilities, Sandia National Laboratories, Oct. 1993, pp. 2-3.

4 U.S. Department of Justice, FBI Uniform Crime Reports, *Law Enforcement Officers Killed and Assaulted, 1991*, Washington DC: U.S. Department of Justice, 1991, p. 38.

5 U.S. Department of Justice, FBI Uniform Crime Reports, *Law Enforcement Officers Killed and Assaulted, 1990*, Washington DC: U.S. Department of Justice, 1990, p. 26.

6 Safariland, *1994 Duty Gear Product Guide*, Safariland, Ontario, California. 1994.

7 Commission on peace officer standards and training, *California Peace Officers Killed in the Line of Duty December 1986*, State of California, December 1986.

8 Commission on peace officer standards and training, *Guidelines for Law Enforcement Officer Safety, Resulting from the Study of California Peace Officers Killed in the Line of Duty*, State of California, 1987.

9 Commission on peace officer standards and training, *California Peace Officers Killed in the Line of Duty 1987-1988-1989*, State of California, August 1992, pp. 12, 27, 54.

10 U.S. Department of Justice. *Killed in the Line of Duty, A Study of Selected Felonious Killings of Law Enforcement Officers*, Washington, DC: U.S. Department of Justice, September, 1992, p. 40.

11 Information received during a telephone interview with Officer Frank McKee of the San Francisco Police Academy. October 28, 1994.

12 U.S. Department of Justice. *Killed in the Line of Duty, A Study of Selected Felonious Killings of Law Enforcement Officers*. Washington, DC: U.S. Department of Justice, September, 1992, p. 12.

13 U.S. Department of Justice. *Uniform Crime Reports, Crime in the United States, 1988*, Washington, DC: U.S. Department of Justice, August, 1989, p. 232.

14 U.S. Department of Justice. *Uniform Crime Reports, Crime in the United States, 1988*, Washington, DC: U.S. Department of Justice, August, 1989, p. 234.

15 Commission on peace officer standards and training, *California peace officers killed in the line of duty 1987-1988-1989*, State of California, August 1992, pg. 27.

16 U.S. Department of Justice. *Uniform Crime Reports, Crime in the United States, 1988*, Washington, DC: U.S. Department of Justice, August, 1989, p. 237.

[17] U.S. Department of Justice. *Killed in the Line of Duty, A Study of Selected Felonious Killings of Law Enforcement Officers*, Washington, DC: U.S. Department of Justice, September, 1992, p. 14.

[18] U.S. Department of Justice. *Killed in the Line of Duty, A Study of Selected Felonious Killings of Law Enforcement Officers*, Washington, DC: U.S. Department of Justice, September, 1992, p. 29-30.

[19] U.S. Department of Justice. *Killed in the Line of Duty, A Study of Selected Felonious Killings of Law Enforcement Officers*, Washington, DC: U.S. Department of Justice, September, 1992, p. 31.

[20] U.S. Department of Justice. *Killed in the Line of Duty, A Study of Selected Felonious Killings of Law Enforcement Officers*, Washington, DC: U.S. Department of Justice, September, 1992, p. 4.

[21] Human Factors and Systems Planning, Bell Laboratories Kelly Education & Training Center, AT&T, 1991.

[22] Measuring Customer Satisfaction, Bob E. Hayes, ASQC Quality Press, 1992, p 57.

[23] U.S. Department of Justice. *Killed in the Line of Duty, A Study of Selected Felonious Killings of Law Enforcement Officers*, Washington, DC: U.S. Department of Justice, September, 1992, p. 30.

[24] Information received from Colt's Manufacturing Company, Inc., *HYBRID PERFORMANCE SPECIFICATION For Research and Development of an Offensive Handgun Weapons System "Special Operations Peculiar"*; Naval Weapons Support Center; Crane, Indiana 47522-5020; Approved 2-5-91, p. 1-13.

[25] U.S. Department of Justice, National Institute of Justice, Technology Assessment Program, *38/357 Caliber Revolvers NIJ Standard-0109.00*, Washington, DC: U.S. Department of Justice, July, 1983, p. 4.

[26] U.S. Department of Justice, National Institute of Justice, Technology Assessment Program, *9mm/45 Caliber Autoloading Pistols NIJ Standard-0112.01*, Washington, DC: U.S. Department of Justice, May, 1989, p. 6.

[27] U.S. Department of Justice, FBI Uniform Crime Reports, *Law Enforcement Officers Killed and Assaulted, 1990*, Washington DC: U.S. Department of Justice, 1991, p. 49.

[28] Information presented by David Boyd, Director, Science and Technology, National Institute of Justice, at the Law Enforcement Technology for the 21st Century conference, Washington D.C., June 20-22, 1994.

[29] U.S. Department of Justice, National Institute of Justice, Technology Assessment Program, *Equipment Performance Report: 9mm and .45 Caliber Autoloading Pistol Test Results*, Washington, DC: U.S. Department of Justice, August 1987, p. 10.

[30] James P. Holmes, Larry J. Wright, Russell L. Maxwell, *A Performance Evaluation of Biometric Identification Devices SAND91-0276*, Sandia National Laboratories, Albuquerque, New Mexico, June, 1991, p. 7.

[31] Information from Smith & Wesson Academy training materials, received July 11, 1994.

32 U.S. Department of Justice, National Institute of Justice, Technology Assessment Program, *38/357 Caliber Revolvers NIJ Standard-0109.00*, Washington, DC: U.S. Department of Justice, July, 1983.

33 U.S. Department of Justice, National Institute of Justice, Technology Assessment Program, *9mm/45 Caliber Autoloading Pistols NIJ Standard-0112.01*, Washington, DC: U.S. Department of Justice, May, 1989.

34 Sporting Arms & Ammunition Manufacturers' Institute, Inc., *American National Standard Voluntary Industry Performance Standards, Criteria for Evaluation of New Firearms Designs Under Conditions of Abusive Mishandling for the Use of Commercial Manufacturing*; ANSI/SAAMI Z299.5-1990; American National Standards Institute; New York, New York 10018, 1990.

35 Information from Smith & Wesson, *QP-07*, received July 11, 1994.

36 Extracted from test data received from Colt's Manufacturing Company, Inc., on November 11, 1994.

37 The New Grolier Multimedia Encyclopedia, Release 6, *Weather Variation and Extremes*, Grolier Electronic Publishing, Inc. 1993.

38 The New Grolier Multimedia Encyclopedia, Release 6, *Pollution, Environmental*, Grolier Electronic Publishing, Inc. 1993.

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 Rayliegh-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. Rodriquez, 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.

Distribution:

3	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
2	MS0762	D Spencer, 5861 (one for Criminal Justice library)
1	MS0782	F Bouchier, 5848
1	MS0759	P Bortniak, 5845
1	MS2643	D Plummer, 2643
2	MS2643	K Tweet, 2643
1	MS0509	D Williams, 2300
1	MS0537	M Mundt, 2314
2	MS0537	D Brandt, 2314
3	MS0537	D Weiss, 2314