U.S. DEPARTMENT OF COMMERCE
National Technical Information Service

PB-296 809

Vehicle Anti-Theft Security System Design. Volume II Technical Report

Arthur D. Little, Inc., Cambridge, MA

Prepared for

National Highway Traffic Safety Administration, Washington, DC

Dec 78

DOT HS-804 340

VEHICLE ANTI-THEFT SECURITY SYSTEM DESIGN
Volume II: Technical Report

John S. Howland

Arthur D. Little, Inc.
Acorn Park
Cambridge, Massachusetts 02140

Contract No. DOT HS-7-01723
Contract Amt: $121,280

December 1978
FINAL REPORT

This document is available to the U.S. public through the National Technical Information Service, Springfield, Virginia 22161

Prepared For
U.S. DEPARTMENT OF TRANSPORTATION
National Highway Traffic Safety Administration
Washington, D.C. 20590

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Re[cipient's Catalog No.]
DOT HS 804 340		PB296809

4. Title and Subtitle	5. Report Date
VEHICLE ANTI-THEFT SECURITY SYSTEM DESIGN Volume II: Technical Report	December 1978
	6. Performing Organization Code
7. Author(s) John S. Howland	8. Performing Organization Report No. C-81215
9. Performing Organization Name and Address Arthur D. Little, Inc. Acorn Park Cambridge, Mass. 02140	10. Work Unit No. (TRAIS) 11. Contract or Grant No. DOT-HS-7-01723
12. Sponsoring Agency Name and Address U.S. Department of Transportation National Highway Traffic Safety Administration Washington, D.C. 20590	13. Type of Report and Period Covered Final Report October 1977 to December 1978 14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

This report covers a comprehensive study of automobile theft and anti-theft system design. It is printed in two volumes: Volume I – Summary Report and Volume II – Technical Report. A vehicle theft survey was conducted consisting of a literature search and interview of a wide range of expert sources, including law enforcement officials, insurance personnel, automobile manufacturers, and automobile thieves. The data, which includes up-to-date statistics on theft rates, motives, methods, and costs, were analyzed to identify and rank the important performance criteria for anti-theft systems.

Based on these criteria, a conceptual design study was conducted to identify anti-theft system concepts. Several promising system concepts were found and a remote steering lock coded by means of a keyboard in the passenger compartment was selected as optimum for the test system. It was fabricated and installed in a test vehicle.

Prior to the installation of the improved system, the factory-equipped locked vehicle was mobilized by an amateur test subject in 50 seconds. The improved system resisted the efforts of a retired professional auto thief who gave up the effort after nearly 17 minutes. This was well beyond the design goal of 10 minutes.

The ultimate consumer price increase to cover the system is estimated to be between $17 and $36. This is well below the design goal of $50 which was based on the expected average savings in theft costs over the life of the vehicle.

As a result of the survey and the design program, a modified safety standard based on minimum time-to-defeat is recommended as the most straightforward and least design-restrictive approach. An alternative, based on limited accessibility of the vulnerable components, is also recommended if subjective compliance testing must be avoided. However, the latter alternative is inherently more design restrictive.

17. Key Words	18. Distribution Statement
Automobile Theft Anti-Theft Systems Auto Theft Costs Auto Theft Methods Safety Standard – Theft Protection	Document is Available to the U.S. Public through the National Technical Information Service, Springfield, VA 22161

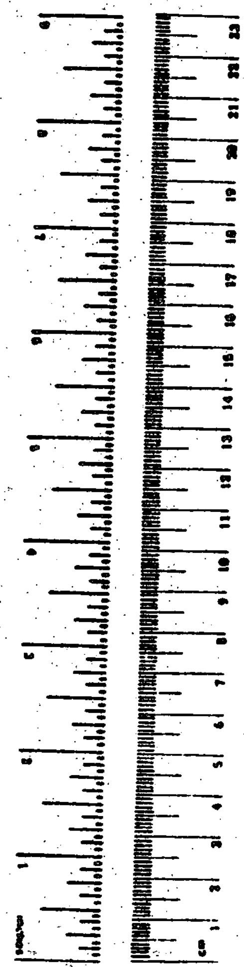
19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified		A08-A01

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

METRIC CONVERSION FACTORS

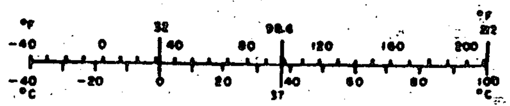
Approximate Conversions to Metric Measures

Symbol	When You Know	Multiply by	To Find	Symbol
	LENGTH			
in	inches	2.5	centimeters	cm
ft	feet	30	centimeters	cm
yd	yards	0.9	meters	m
mi	miles	1.6	kilometers	km
	AREA			
in^2	square inches	6.5	square centimeters	cm^2
ft^2	square feet	0.09	square meters	m^2
yd^2	square yards	0.8	square meters	m^2
mi^2	square miles	2.6	square kilometers	km^2
	acres	0.4	hectares	ha
	MASS (weight)			
oz	ounces	28	grams	g
lb	pounds	0.45	kilograms	kg
	short tons (2000 lb)	0.9	tonnes	t
	VOLUME			
tsp	teaspoons	5	milliliters	ml
Tbsp	tablespoons	15	milliliters	ml
fl oz	fluid ounces	30	milliliters	ml
c	cups	0.24	liters	l
pt	pints	0.47	liters	l
qt	quarts	0.95	liters	l
gal	gallons	3.8	liters	l
ft^3	cubic feet	0.03	cubic meters	m^3
yd^3	cubic yards	0.76	cubic meters	m^3
	TEMPERATURE (exact)			
°F	Fahrenheit temperature	5/9 (after subtracting 32)	Celsius temperature	°C



Approximate Conversions from Metric Measures

Symbol	When You Know	Multiply by	To Find	Symbol
	LENGTH			
mm	millimeters	0.04	inches	in
cm	centimeters	0.4	inches	in
m	meters	3.3	feet	ft
m	meters	1.1	yards	yd
km	kilometers	0.6	miles	mi
	AREA			
cm^2	square centimeters	0.16	square inches	in^2
m^2	square meters	1.2	square yards	yd^2
km^2	square kilometers	0.4	square miles	mi^2
ha	hectares (10,000 m^2)	2.5	acres	
	MASS (weight)			
g	grams	0.035	ounces	oz
kg	kilograms	2.2	pounds	lb
t	tonnes (1000 kg)	1.1	short tons	
	VOLUME			
ml	milliliters	0.03	fluid ounces	fl oz
l	liters	2.1	pints	pt
l	liters	1.06	quarts	qt
l	liters	0.26	gallons	gal
m^3	cubic meters	35	cubic feet	ft^3
m^3	cubic meters	1.3	cubic yards	yd^3
	TEMPERATURE (exact)			
°C	Celsius temperature	9/5 (then add 32)	Fahrenheit temperature	°F



PREFACE

The author would like to express his appreciation for the opportunity afforded by this program to extend and deepen his background and understanding of the technology of automobile theft. It has been interesting and rewarding work, being a subject containing elements of such diverse fields as engineering, law enforcement, safety technology, sociology, consumer affairs, and insurance. It is hoped that this work will contribute toward a creative, cooperative effort by Government and industry to reduce the burden of automobile theft — a burden borne by virtually every U.S. citizen.

Many individuals contributed to the successful conclusion of this program. Consultants included Mr. David Barry, who helped with his general knowledge of the problem and to marshal West Coast information sources for the survey, and Mr. Rufus "Tinker" Whittier, who contributed his unique talents as the test subject for the validation tests.

The theft survey would not have been possible without the generous help provided by the many sources of information listed in Appendix B of Volume II. In addition, the assistance of Lt. Courtney of the San Francisco County Jail and Mr. William Quealy at the Middlesex County House of Correction in obtaining the thief interviews was greatly appreciated.

The number of Arthur D. Little, Inc., people who applied their special talents to the program is too great for individual recognition and, thus, thanks must be tendered collectively. However, the design efforts of the principal contributors listed on the title page, the library assistance of Ms. Kathleen Long, the secretarial services of Ms. Donna Sullivan, and the editorial services of Mr. Dana Pierce deserve special acknowledgement.

Finally, but certainly not least, the author would like to thank Mr. Dennis Grieder of NHTSA, Contract Technical Manager, whose cooperation and contribution were essential to the successful completion of the project.

TABLE OF CONTENTS

Preceding page blank

TABLE OF CONTENTS (Continued)

TABLE OF CONTENTS (Continued)

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

Automobile theft in the United States has skyrocketed to monumental proportions in recent years. Annual vehicle thefts currently total about 1 million and total annual costs to the public are more than $2 billion. Thousands of injuries and hundreds of deaths can be attributed annually to accidents involving stolen vehicles.

One of the many reasons for the escalating theft rate, especially the 70% stolen by amateur thieves, is the ease with which most cars can be stolen. Despite evidence that the theft rate is related to the ease of theft, automobiles costing $10,000 and more are still equipped with anti-theft devices that can be defeated in 2 minutes or less by an amateur auto thief with little experience or skill.

Theft protection systems are currently specified by Federal Motor Vehicle Safety Standard (FMVSS) No. 114. This standard requires functional performance which prevents unauthorized use in the absence of attack on the anti-theft system itself. However, it provides no definition of attack resistance level. Thus, there is a clear need for the development and application of improved anti-theft systems and the standards against which they are measured.

The objectives of this program were threefold:

- The identification and selection of cost-effective, anti-theft performance criteria which can reduce the vehicle theft rate;
- The design, fabrication, and testing of an improved anti-theft system that complies with these criteria; and
- The development and recommendation of modifications to FMVSS No. 114 which reflect both the performance criteria and the technical realities imposed on the designer.

The program consisted of four major task areas:

- A vehicle theft survey in which a wide variety of information sources were tapped to obtain an up-to-date picture of theft experience and technology. These data were analyzed critically to provide a basis for the identification of performance criteria. The vehicle theft survey is reported in Chapter 3.
- Based on the survey results, important anti-theft performance criteria were identified and analyzed to determine their relative effectiveness and importance as bases for design goals and standard improvements. This work is covered in Chapter 4.
- Using the results of Chapter 4, a design study was conducted to identify and select design concepts for an improved anti-theft system. The selected concepts were then developed, fabricated in prototype form, and tested for effectiveness. These tasks are described in Chapters 5 and 6.
- Finally, based on the results of the performance criteria study, the experience gained, and the design program, existing anti-theft standards were studied and recommendations for improvements were developed. This study is covered in Chapter 7.

In Chapter 2, the approaches followed in conducting these tasks and the principal results and conclusions are summarized.

2. SUMMARY

VEHICLE THEFT SURVEY

The vehicle theft survey consisted of a thorough review of published literature concerning vehicle thefts, as well as interviews with a wide variety of expert sources — ranging from law enforcement officials to thieves — to obtain unpublished data and opinion.

The results of the survey were then sifted, correlated, and analyzed to isolate the critical data needed as a basis for the development of effective anti-theft performance data.

In addition to special surveys conducted on limited samples of the theft population, general theft data are compiled by the FBI and the National Automobile Theft Bureau (NATB), an insurance industry investigative organization. However, it should be noted that the NATB records cover only about 20% of all auto thefts and these emphasize the professional segment. Thus, general conclusions drawn from these data can be erroneous when applied to the general theft experience. Moreover, a tendency was noted in the literature to assume that amateur auto theft results in a low loss due to the fact that the car is recovered. In fact, the best available data show that amateur theft losses are significant and, when combined with the higher amateur theft rate, result in a greater total loss to the consumer than that due to professional operations.

Because the amateur is severely limited in his ability to apply costly theft methods, for example, a tow truck, this segment of the theft experience is the one in which improved anti-theft systems can have the greatest impact. Moreover, it is this segment which contributes the bulk of theft-related accidents.

The principal results and conclusions from the survey follow:

1. The average annual theft rate in the United States is 7.23 per 1000 vehicles, with a peak rate in Massachusetts of 25 per 1000.
2. The national theft rate for certain specialty auto models appears to be as high as 70 per 1000; the Massachusetts peak for one model was calculated at 198 per 1000.
3. Recovery rate data for the entire United States indicate that about 70% of all thefts are perpetrated by joy riders or small-time, non-professional strippers. The remaining 30% can be attributed to professional operations and insurance fraud.
4. The total cost of automobile theft in the United States is at least $2 billion annually. Accidents costs run to $60 million and criminal justice system costs to $200 million. The remainder are direct losses to the consumer.
5. Allocation of these costs by type of theft shows that the amateur joy rider and small-time stripper cost the U.S. consumer between $1.1 and 1.4 billion annually, while professional theft costs run between $0.7 and 1 billion.
6. The resulting cost of amateur auto theft alone is, thus, $10 to 13 per registered automobile per year, or $100 to 130 over a 10-year vehicle life.
7. Although a wide range of theft methods have been used, currently the most prevalent methods include the use of a "slim-jim" or wire against the doorlock mechanism, and a slide-hammer against the steering-column lock.

8. Nationally, about 13.6% of all thefts are accomplished with a key that has been left in the ignition.
9. The steering-column locks on most vehicles can be defeated in 30 seconds or less, the most difficult within 2 minutes. Although recent data indicate that the theft rate on specific vehicles can be significantly reduced by improving the lock, no changes have been made which appear to deter a theft beyond a few minutes.
10. It is generally agreed among thieves, law enforcement officials, and investigators that deterrence beyond 10 minutes will discourage most amateur thieves.

PERFORMANCE CRITERIA

Anti-theft system performance specification is unique in comparison with other automotive systems because the usual functional performance characteristics are trivial. The system designer must recognize that the imporant criteria relate to the ability of the system to resist attack by an intelligent, adaptive thief whose objective is to defeat the normal functional operation of the system. Thus, performance criteria were found to group logically into three classes —functional, attack resistance, and post-theft.

Post-theft criteria relate to measures which will diminish the value or market for stolen vehicles. These include identification of major parts and improved salvage titling and can have a significant effect on professional theft operations. However, they are generally outside the scope of FMVSS No. 114, and thus were not considered further in this program.

Functional and attack resistance criteria were identified in general terms and analyzed for their effects on theft deterrence, consumer acceptability, and cost.

The important functional criteria are either specified by the current FMVSS No. 114, or are commonly satisfied by current design practice. The only exception is that significantly improved theft deterrence would be provided by a criterion ensuring passive activation of the system so that a vehicle cannot be left unprotected.

Attack resistance criteria include:

- Time-to-defeat limits,
- Accessibility limits,
- Resistance to tools,
- Conspicuousness, and
- Complexity.

Resistance to tools and complexity were generally found to be overly design-limited or design-restrictive in their application. The only exception is that amateur theft can be deterred by systems designed only to resist man-portable tools.

Time-to-defeat was found to be the only important measure of theft resistance and can obviate the need for any other attack resistance criterion. However, if applied as a standard provision, time-to-defeat inherently requires compliance testing with a human subject.

Alternatively, several secondary attack resistance criteria can be used to specify performance level instead of the fundamental time-to-defeat limit. The most important of these were found to be those specifying accessibility limitations or tamper protection. The first would place specific limits on the location of the decoding and latching functions of the system. The second would specify a design that requires a time-consuming repair or reset if attacked forcibly. In addition, resistance to several other potential methods of attack would require specification. This alternative can be concluded to be significantly more design restrictive than the minimum time-to-defeat approach.

SYSTEM DESIGN

A conceptual design study was conducted. It included a systematic concept generation and evaluation process to identify as many promising anti-theft concepts as possible. This morphological approach included the identification of methods characteristic to each energy or signal transmission medium for code insertion, decoding, latching, and vehicle function lock. The study included both mobilization protection systems and sensor screen concepts. The latter class included both alarms and tamper protection systems. In addition, a number of improvements to entry protection systems were identified and evaluated.

Preliminary screening of the concepts identified two promising classes of code insertion/decoding systems:

- The non-remote decoder using a conventional key and protected by a sensor screen to prevent attack; and
- The remote decoder using a conventional key or keyboard and located, along with the latching mechanism, such that access by a thief will require excessive time delay.

The latter concept was selected for the test system of this program because it provided the highest degree of confidence that the design goals would be met in the initial trial, and that the least modification of existing vehicle systems on the test vehicle would be made necessary. Keyboard code insertion was selected for the test system to avoid developing a reader for a conventional key, or using expensive card or tape readers. It also inherently avoids providing an additional mechanism to ensure that the key is not left in the system.

Several possible vehicle functions are available for mobilization protection. However, for the test system, a steering lock was selected because it offered the most convenient option for packaging the electronic decoder circuitry in a relatively cool environment. This basis for selection applies primarily for a retrofit system, but other types of lock could be easily used for a production design.

The remote steering lock with keyboard code insertion was designed in detail for the test vehicle, a 1977 Dodge Colt, and two test units were fabricated. In addition, several modifications were made to the door lock system on the test vehicle and a commercial hoodlock was installed. These modifications were implemented primarily to benefit from the validation tests rather than with great hopes of substantially extending the time-to-defeat.

The increase in vehicle price due to the replacement of the existing steering column lock with remote steering lock of this type produced in very high volumes and factory-installed is estimated to fall between $17 and $36. This is well below the design limit of $50.

SYSTEM TESTING

Prior to the installation of the test system, a theft test on the factory-equipped vehicle was conducted. A "slim-jim" attack was used on the doorlock and a slide-hammer on the steering column lock. The author served as a test subject for this test which was his first attack on the Dodge Colt lock and on a steering column lock mounted in a vehicle.

In this trial, the door was unlocked in a few seconds and the steering column lock defeated in an additional 40 seconds. The total time from approach to the vehicle to the point where it was driven off was about 50 seconds.

After a series of functional and thermal bench tests, the remote steering lock was installed in the test vehicle, shaken down by road testing, and made ready for the validation test. An independent expert test subject, Mr. Rufus H. Whittier, was retained for the test. After a complete briefing on the principles and configuration of the test system, the validation time trial was conducted. The doorlock and hoodlock were defeated with a period of 2 minutes and 50 seconds. However, the remote steering lock could not be defeated within a period of 16 minutes and 40 seconds. The subject gave up the attack as fruitless at this point. In his opinion, this car would never be stolen on the street without a tow truck.

SAFETY STANDARD MODIFICATIONS

After studying existing anti-theft standards in the light of the performance criteria and the design program, it was concluded that the most direct — and least design-restrictive — method for specifying attack resistance is in terms of a minimum defeat time. However, this inherently carries with it a need to test compliance with a human test subject. It is felt that effective compliance test methods and expert technicians can be developed for this purpose.

If the time-to-defeat approach is found unacceptable, it is alternatively possible to specify attack resistance objectively in terms of limits on the method of housing and locating the vulnerable parts of the system. This alternative is inherently more design-restrictive and, in fact, is known to preclude certain promising anti-theft concepts.

Specimen modifications for FMVSS No. 114 following these two alternative approaches are provided in this report.

3. VEHICLE THEFT SURVEY

The vehicle theft survey consisted of a thorough review of the published literature concerning vehicle theft, as well as interviews with expert sources — ranging from law enforcement officials to car thieves — to obtain unpublished data and opinion.

The sources covered in the literature survey, along with a bibliography of the literature, including abstracts of the important citations, are provided in Appendix A. This bibliography stresses recent literature which has appeared since a comprehensive literature survey and bibliography were published by the Motor Vehicle Manufacturers Association[1].* In Appendix B, the various organizations and individuals contacted or interviewed for unpublished information are listed.

In this chapter, the information obtained is analyzed and discussed in the context of each major subject area addressed.

SOURCES OF THEFT DATA

There are only two basic sources of vehicle theft data; viz., local and state law enforcement organizations and the insurance industry.

The only general source of law enforcement statistics is the FBI Uniform Crime reports[2] in which vehicle theft data from virtually all U.S. jurisdictions are collected and analyzed to determine the theft rate per 100,000 inhabitants in each geographical subdivision of the United States. In addition, information concerning age, sex, race, and city-size is tabulated for all persons arrested for motor vehicle theft. In addition to the Uniform Crime reports, a number of special surveys have been conducted in recent years, based on law enforcement statistics or conducted by law enforcement officials.[3-8]

The only general source of insurance industry data appears to be the files of the National Automobile Theft Bureau (NATB) which is an industry-supported investigative organization. This organization only files thefts where there is no quick recovery, and receives statistics from member companies that insure 90 to 95% of the insured vehicles in the United States. For this reason, NATB statistics only represent 200,000 thefts per year of the total 1,000,000 that occur, and they tend to concentrate on the professional auto-theft segment where no "quick" recovery occurs.[9]

In addition, each insurance company maintains its own statistics on vehicle theft which usually is included in their general comprehensive coverage. The data available from this source consist of partial and total theft claim frequency and dollar losses.[10,11] Partial theft is defined as one where the vehicle is not moved from the site of initial entry. Although NATB files can provide vehicle model and year data for their particular segment of the theft experience, there do not appear to be any general insurance statistics available which break down theft occurrence or losses by model, year, method of theft, recovered versus unrecovered, or type of installed anti-theft device.[11,12]

---

*Numbers in parentheses refer to references listed at the end of this report.

Recently, the results of a special survey conducted by General Motors Corporation in cooperation with several insurance companies became available.[13] This survey, which was based on questionnaires completed by the insurance companies for a total of 16,619 thefts, provides valuable data on average losses by model year, recovery status, and model. It also provides some indication of the degree of stripping and the theft method used. However, it stresses partial theft over total theft and the Michigan-Illinois geographical area.

The only remaining source of data uncovered in this study was a sample of 178 thefts reported to the Massachusetts Division of the American Automobile Association (AAA). These data which have not been published are interesting since they not only indicate the theft experience by model and year, but also give some information on method used, anti-theft equipment installed, and the dollar losses associated with recovered vehicles including uninsured losses. This latter type of information is not available elsewhere.[14]

THEFT RATES

Overall Theft Rates

The number of national motor vehicle thefts in 1976 was 957,600 — down about 4.3% from the 1975 experience.[2] This corresponds to a per capita rate of 469.4 thefts per 100,000 inhabitants. The rate is higher in urban areas, with Boston reporting a rate of 1648.7 and New York, 1095 per 100,000 inhabitants. Of greater interest is the theft rate expressed in thefts per 1000 vehicles. This is, of course, a direct index of the probability that a vehicle will be stolen. Moreover, if sufficient theft and exposure data are available, thefts per 1000 can be used as a convenient comparison of the relative susceptibilities of various segments of the vehicle population.

Since there were approximately 140 million vehicles registered in the United States during 1976,[15] the national vehicle theft rate was 6.8 thefts per 1000. Some 83% of all vehicle thefts, or 794,808, involved automobiles. Since there were about 110 million automobiles registered during this period, the automobile theft rate was 7.23 thefts per 1000.

The Massachusetts state theft total for 1976 was 76,257[2] which, since the total registration is about 3 million,[16] translates into a rate of 25 thefts per 1000. This is likely the highest overall state theft rate.

Theft Rate by Manufacturer

Of particular interest in an equipment-oriented study are the manufacturers' theft rates. It might be expected that this would provide a comparison of the relative capability of several anti-theft system designs to resist theft. Of course, superimposed on theft resistance is the relative attractiveness of the various models to the thief population.

Unfortunately, the most recent survey in which thefts were differentiated by manufacturer, model, and model year, the General Motors Survey,[13] is useless for purposes of comparing theft rates, since the total registrations in the population from which the thefts were drawn are unknown.

However, by correlating police and registry data, Barry[13] determined the theft rate in Massachusetts during 1974 by vehicle model and year.[6] The rates for the major manufacturers are shown in Table 1 with a comparison (by year) between those models having a steering column lock and those without. Although the steering column lock category shows a lower rate for three of the manufacturers, the Ford data show a significantly higher rate for the later models. In fact, the rate for 1972 Lincolns was 198 per 1000. This trend was later verified with national statistics from Reference (3) in the LEAA study,[18] as shown in Table 2.

TABLE 1. THEFT RATE IN MASSACHUSETTS – JANUARY 1974
(No. of Thefts per 1000 Registrations)

Manufacturer	Average for Vehicles Equipped with Steering Column Locks	Average for Vehicles without Steering Column Locks
AMC	4	5
Chrysler	12	22
Ford	46	11
General Motors	11	17
Total	21	16

Notes: Averages shown are averages of rate by model year for each category.
Data from Reference (6).

TABLE 2. THEFT RATES* BY MANUFACTURER AND MODEL YEAR

Manufacturer	Model Years		
	1968 and Before	1969-1971	1972-1975
AMC	7	5	5
Chrysler	7	5	4
Ford	7	8	12
General Motors	13	5	6
Others	14	7	6

*Numbers of annual thefts per 1000 registrations.
Date from Reference (18).

Ford, however, improved the design of its steering column locks beginning with its 1976 models. Recent data compiled by Allstate Insurance Company from NATB and new registration statistics[11] show that the 1976 and 1977 Ford models, especially the higher priced models, experienced a significant drop in the theft rate index compared with the preceding year. The theft index is a relative measure of the theft rate for a given model compared with the overall rate for all cars. Because it is derived from NATB data, it stresses, as noted earlier, professional rather than amateur thefts. However, if this trend is verified as more complete data are obtained, it would support the value of improved anti-theft hardware in reducing theft.

Theft Rate by Model Year

There is no clear trend concerning theft rate by model year obvious from available statistics. The only overall U.S. data are those presented in Table 2 where the theft rate is shown in three separate model year groupings. Overall, these data do not show any major preference between old and new cars, but they do seem to indicate a significant preference by thieves for older General Motors and miscellaneous vehicles and new Ford products.

Regional data from California[17] and Massachusetts[6] are available, and have been analyzed to provide the information in Table 3. The Massachusetts data show a marked preference for new vehicles with a theft rate which is about 3½ times the national average and 5 times that of very old vehicles. Of course, there is no large variation among vehicles for the 10 model years preceding the date of the survey.

TABLE 3. THEFT RATE* BY YEAR IN CALIFORNIA AND MASSACHUSETTS
(California Oct. 23-29 1977; Massachusetts Jan.-June 1974)

Model Year	California Rate	Massachusetts Rate
1976	8.6	–
1975	8.6	–
1974	11.2	–
1973	8.6	–
1972	5.9	24
1971	6.9	20
1970	9.1	19
1969	9.2	19
1968	11.6	20
1967	11.0	17
1966	16.9	17
1965	20.9	13
1964	24.7	19
1963	28.0	16
1962 and Before	11.2	5

*Number of annual thefts per 1000 registrations.
Source data from References (6) and (17).

The California data show a much higher theft rate for older cars, a phenomenon only partly understood. The theft rate for the preceding 8 to 10 model years is near the national average, but then increases to 4 times the national average for 1963 vehicles before it again drops off for earlier models. The high 1963 model year theft rate can almost entirely be attributed to the theft of 1963 Chevrolets which occurred at a rate of 76 thefts per 1000.

Theft Rate by Vehicle Category

It has long been recognized by those studying automobile thefts that certain categories of automobiles are stolen more often than others. These are usually thought to be the luxury and specialty or sporty-type vehicles. However, the only data available which allow differentiating on a national scale among categories or models within the line of a given marque is that produced by the NATB.

NATB data for 1976 models stolen in 1976 were correlated to show the theft rate for several vehicle categories in Table 4. The NATB rate is, of course, lower than the national rate because it only covers 20% of the total thefts. The second column adjusts the NATB rate to reflect this situation. However, this presentation is not strictly valid, because NATB statistics stress professional theft, while a major proportion of the national theft experience is amateur. Thus, simple scaling of the rate would not accurately reflect preferences by category that the professional might have in comparison with the amateur.

TABLE 4. THEFT RATES[a] BY VEHICLE CATEGORY
(Calculated from NATB Data for 12/1/76 through 05/31/77)

Category	NATB Rate	Estimated Rate Adjusted to National Level
Compacts and Subcompacts	2.93	14.7
Intermediates	2.61	13.0
Full Size	2.65	13.3
Luxury Intermediates		
⊙ Mercedes	1.99	10.0
⊙ Seville	8.74	43.7
Specialty		
⊙ Corvette	13.87	69.4

[a] Number of annual thefts per 1000 registrations.

1. Data from Reference (11) for 1976 vehicles stolen in 1976.
2. Adjustment to national level simply made by multiplying the rate by 5 to compensate for the ratio between NATB thefts and the national experience.

However, the data of Table 4 indicate that, except for a few very specialized models, the theft rate is not significantly dependent upon vehicle size. In general, the theft rate is greater for higher priced models. For example, the adjusted theft rate for Cadillacs alone (except Seville) is 27.5 thefts per 1000; and for Lincolns, it is 38.5 thefts per 1000.

The 1976 leader was the Chevrolet Corvette followed by Cadillac Seville and Lincoln. In 1975, the leaders were Lincoln and Ford Thunderbird followed by the Corvette. The only foreign car that appears on the list of the 10 models with the highest theft rate is the Porsche.

Some regional preferences show up in local data. For example, the high rate for the 1963 Chevrolet in California has already been mentioned. Its rate is even higher than the national Corvette rate. The all-time high noted in any of the data that have been reduced by model was the Massachusetts rate for 1972 Lincolns stolen in 1974, viz., 198 thefts per 1000.

Recent California data show a marked preference for late-model pick-up trucks and vans. Several recent Ford models are stolen more often than all but 30 automobile models. These pick-up trucks are generally those which are not equipped with steering column locks.

THEFT MOTIVES

Cars are stolen for two general reasons: transportation for joy-riding or commission of another crime and profit by resale of vehicle or parts. There are no directly applicable statistics with which the theft for various motives can be separated.

The 1966 Department of Justice Survey of thieves[7] showed that only 8.1% stole for monetary gain. However, this figure is not reliable since thieves always list joy-riding as their motive when apprehended due to the lower penalties which usually apply.

Recovery rate is often used as an index of amateur versus professional auto theft. This was shown in the FBI survey[3] to be about 70% nationally with variation between 50% for New York, Baltimore and Philadelphia and 90% for Los Angeles. Recent California data indicate recovery data over 90%.[17]

However, many of the vehicles recovered have been stripped to some degree, presumably for profit. The FBI survey of recovered vehicles showed the breakdown of Table 5[3]. California data show about 20% not recovered, 31% stripped, and the remaining 49% intact or damaged.[8]

TABLE 5. ANALYSIS OF RECOVERED VEHICLES

Purpose of Theft	No. of Vehicles	Percentage
Transportation	3512	35.1%
Use in Crime	273	2.7
Stripping	3796	37.9
Resale	131	1.3
Unknown	2302	23.0

1. On the assumption that 70% of all thefts are recovered, this analysis shows that small-time theft for profit accounts for 27% of all thefts while transportation accounts for 43%.
2. Data from the 1974 FBI Survey of Reference (3).

The most recent analysis of recovered vehicles conducted as part of the General Motors survey[19] showed that parts were removed from 1232 out of 2089 recovered vehicles, or 58.9%. In this survey, the parts stolen from both these recovered total thefts and a large number of partial thefts were listed. By far, the most common items were wheel covers, wheels, tires, radios and other electronics, and batteries. Although it is not possible to separate total and partial thefts in this listing, and thus verify the conclusion, the data appear to indicate that major body parts and mechanical components are stolen in less than 16% of the cases where the vehicle is recovered. Thus, the small-time theft for profit can be estimated to be 84% of the recovered population which in this sample represents about 40% of the total thefts.

However, determining the actual motives for a given recovered vehicle is difficult and approximate at best. A well-known occurrence in major urban areas is the theft of a vehicle for joy-riding purposes, followed by stripping or re-stealing by an illegal junk dealer following its abandonment. Thus, the original purpose of theft was likely joy-riding in some unknown portion of the thefts reported "stripped." The best conclusion that can be reached is that the 70% of thefts nationally where the vehicle is recovered is almost entirely made up of some combination of theft for transportation and small-time theft for profit.

There are two types of highly professional car-theft enterprises. The first steals and strips cars for expensive body assemblies such as the front-end clip, doors, and the rear or "dog-house" assembly. The second involves the "replating" of late-model stolen cars with VIN plate and title from a junk car of the same model. The recovery rate from both of these types of operations is negligible. Thus, it is quite likely that the 30% of vehicles unrecovered contains these two populations, along with the many stolen for fraudulent insurance claims and for shipment overseas for resale.

Because most stolen vehicles involved in fraudulent insurance claims are not recovered, there are no hard data concerning their incidence. They are potentially important in this study because, in essence, they represent a portion of the thefts which can never be countered. Several professionals in the insurance investigation field indicated unofficially that between 5 and 10% of all automobile thefts are believed to be involved with fraudulent claims.

Taking all of this information together allows bracketing the major motives by percentage of the total theft population, as shown in Table 6.

TABLE 6. MAJOR THEFT MOTIVES

Motive	Percentage of All Thefts
Professional Car-Theft Operations	20 to 25
Fraudulent Insurance Claims	5 to 10
Small-Time Theft for Profit	20 to 30
Theft for Transportation	40 to 50

THEFT COSTS

Total Thefts

The only nationally reported cost for auto theft was that provided by former FBI Director Clarence Kelley in a recent speech; viz., an estimated $1.6 billion for 1976. It is presumably based on an estimated average loss paid by insurance in the case of "total" theft of $1600 times the 1,000,000 thefts which occurred in 1976. However, this estimate represents only an approximation for part of the total cost of automobile theft. It is of interest to examine all of the component costs in as much detail as possible with available statistics.

Recent data obtained from two of the largest automobile insurers in the United States indicate that the average paid losses for 1976 total $154,889,597 for 76,209 paid claims for total theft*.[10,11] Thus, the average covered loss was $2032 per theft. In a recent survey made in

*Total theft is defined as the case where the vehicle was moved from the site of the theft.

Massachusetts by the American Automobile Association, 107 owners, who were insured, reported an average loss of $240 per theft which was not covered by insurance.[14] While this may reflect the deductible amount which is not universally applied throughout the United States, it is probably accurate to state that the insurance payment seldom reflects the total loss experienced by the owner in case of theft.

Insurance administration losses are also a component of the loss to society due to theft. In 1975, the losses paid on private passenger vehicle insurance were only 83% of the premiums paid.[16] Thus, the actual cost of $2032 per covered loss was $2448. Adding this to the uninsured loss of $240 gives an estimate of $2688 as the average total direct loss per automobile theft. Since there were 794,808 automobile thefts in 1976, the total direct loss can be estimated at $2.14 billion. This estimate of direct loss is almost certainly an upper bound for that which was actually incurred. It is based on the average loss sustained by insured stolen cars, while the 794,808 thefts include many uninsured vehicles. The losses sustained by owners of the latter group are very likely lower on the average than those in the insured group. Thus, the total direct loss due to auto theft certainly lies in the range between $1.6 and 2.14 billion. In the case of the insured group, this cost is distributed among all insured owners. In the case of the self-insuring motorist, this loss is borne by each individual experiencing a theft.

Since there are about 110 million automobiles registered in the United States, the above direct loss estimates translate into a range of $14.50 to $19.50 per vehicle per year nationally. The losses, of course, are concentrated in areas with a high theft rate. For example, the total cost in Massachusetts in 1975 was estimated to be $115 million for 2.7 million registered vehicles, resulting in an average of $42.60 per vehicle.[19]

However, there are indirect costs to society which are not reflected in this direct loss. One of these is due to the extraordinarily high accident rate associated with stolen cars. This has been variously reported as 47 and 200 times the normal accident rate.[7,18] The LEAA study[18] reports that one out of every 350 accidents involves a stolen car. The National Safety Council reports a total cost for all motor vehicle accidents of $21.2 billion for 1976.[15] Thus, the total accident cost attributable to auto theft is $60.6 million.

The final indirect cost attributable to auto theft is its share of the cost of the criminal justice system. In 1974, the total cost of the criminal justice system including police, judicial, legal, and corrections for all jurisdictions was $14.9 billion.[16] The Uniform Crime reports provide a measure of the portion that is attributable to auto theft.[2] In 1976, the total arrests recorded by 10,119 law enforcement agencies was 7,881,050, while arrests for motor vehicle theft alone were 110,708. Thus, motor vehicle thefts account for about 1.4% of all arrests. Using this as an estimate of the proportion of criminal justice system costs attributable to motor vehicle theft provides an estimate of $208.6 million for these costs.

Combining direct costs with those due to accidents and the criminal justice system gives a range of $1.9 to $2.4 billion for the total annual cost of auto thefts.

The best available data which differentiate between theft costs or losses for recovered and unrecovered vehicles are found in the General Motors survey which covered 2089 total thefts.[13] The direct losses sustained for various model years are shown in Table 7. Despite the author's disclaimer, the losses by year follow the expected pattern. Also, as would be expected, the losses

TABLE 7. AVERAGE LOSS BY MODEL YEAR

Model Year	Total Theft/ Vehicle Recovered	Total Theft/ Vehicle Not Recovered
1977	$2,034	$6,748
1976	2,290	5,551
1975	1,836	4,253
1974	1,955	3,216
1973	1,351	2,565
1972 and Earlier	766	1,379
Overall Average	$1,522	$2,903

1. Data from Reference (13).
2. Authors suggest comparisons between years not valid without adjustment for exposure.

for recovered vehicles do not drop off so quickly as the unrecovered because they reflect damage and part replacement rather than total market value. However, the figures of greatest interest are the overall averages for the two categories. These can be used to assess the total direct losses experienced as a result of all thefts between these two major groups.

It has been stated that no anti-theft device will deter the professional. While this statement may be too strong, it is relatively meaningful. That is also true of the owner who files a fraudulent claim. These two components almost certainly make up the bulk of those thefts in which the vehicle is never recovered. Taking the average loss of $2903 per unrecovered automobile (Table 7) and multiplying it by the 1976 total of about 238,442 unrecovered automobiles gives a total direct loss of $0.692 billion for professional car theft and fraudulent claims.

However, the same rationale also shows that the 556,366 recovered automobiles with an average loss of $1522 resulted in a direct loss of $0.847 billion. This group of thieves is almost certainly made up largely of joy-riders and small-time strippers not equipped with compactors or other effective means for vehicle disposal. Moreover, this is the group that provides the bulk of the accident costs and criminal justice system costs associated with car theft.

The argument against improvement of anti-theft systems on automobiles most often advanced by manufacturers and others is based on an assumption that professional auto theft is the most costly component and that this will not be deterred by realistic improvements in anti-theft hardware. The underlying assumptions in this argument are fallacious. Not only do its proponents quote recovery percentages of 50% which are only typical of certain cities, such as New York and the NATB portion of the theft experience, but they also underestimate the losses associated with a theft in which a vehicle is recovered. In fact, as the above calculation shows, 55% of all direct losses due to automobile theft occur in thefts where the vehicle is recovered.

The comparison can be further refined by allocating the indirect theft costs between the two groups, as shown in Table 8. This calculation shows that about 60% of all theft costs can be

TABLE 8. TOTAL ESTIMATED THEFT COSTS FOR 1976
($ billions)

Cost Component	Vehicle Recovered	Vehicle Not Recovered
Direct Loss[1]	$0.88 to 1.18	$0.72 to 0.963
Accident Costs[2]	$0.06	
Arrest, Prosecution, & Correction Costs[3]	$0.19	$0.02
Totals	$1.13 to 1.43	$0.74 to 0.98

1. Calculated by applying 55/45% to total direct losses of $1.6 to 2.14 billion.
2. Calculated by assuming that all theft-related accidents are in the joy-riding/small-time stripper group.
3. Calculated by assuming that 90% of all criminal justice system costs are associated with the joy-rider/small-time stripper group.

attributed to thefts in which the automobile is recovered, largely made up of the joy-rider and small-time stripper components. This cost is estimated to fall between $1.13 and 1.43 billion. These costs average between $10 and $13 per registered automobile per year. A substantial reduction in the so-called amateur class of theft would be expected to provide a proportionate savings in this cost nationally, both directly and through a shift of criminal prosecution effort to other crime areas. The direct portion of the savings would, of course, be concentrated in the high-theft areas.

Partial Thefts

The direct losses discussed in the preceding section are all associated with total thefts, defined as those cases where the vehicle was taken away from the site of the theft by the thief. Another class of theft is that in which components and personal property are removed by a thief at the original site without moving the vehicle. This is usually termed partial theft.

Partial theft losses are of interest in this study only to the degree that they might be reduced due to improved anti-theft hardware designed to reduce total theft. For example, an important part of a total anti-theft system is the entry protection system. Improved entry protection systems would be expected to reduce losses due to property and components stolen from the passenger compartment. Likewise, improved hood-locking, systems combined with entry protection, would reduce losses due to engine compartment thefts.

In 1976, 22.3% of all larcenies consisted of motor vehicle accessories and 20.1% consisted of motor vehicle contents.(2) Since there were 6,270,800 larcenies, some 2,658,819 were partial motor vehicle thefts. The average loss for accessories was $134 and that for contents $216.(2) This is consistent with the value reported in the General Motors survey, viz., $200 for a partial theft.(13) Taking the average loss of $175, we estimate the total value of stolen goods to be $0.465 billion. The recovery rate for this type of property is about 10%.(2) Thus, the net direct loss due to partial vehicle theft can be estimated at $0.419 billion.

There are no accident costs related to partial theft, but a significant portion of the criminal justice system costs of $14.9 billion is related to larceny. Since 42.4% of all larcenies were partial vehicle thefts and there were 1,117,300 arrests for larceny in 1976,[3] then we can estimate that 473,735 arrests were for thefts of vehicle contents or accessories. Since the total arrest figure was 9,608,500 in 1976, 4.93% can be estimated to have been for partial vehicle theft. This corresponds to a cost of $0.735 billion if the total criminal justice system costs are allocated by arrests.

The preceding calculations indicate that the total annual direct and indirect cost of partial vehicle theft can be estimated to be $1.154 billion, which represents a cost per registered vehicle of $8.24 per year.

Safety Hazard of Vehicle Theft

Another cost to society due to vehicle theft is that of injury and death. The monetary cost of accident losses has already been included in the calculations of the preceding section. However, the intangible loss to life and limb should also be noted.

The FBI survey showed that, of 10,014 recovered vehicles, 429 were involved in traffic accidents in which 20 persons were injured and 2 were killed.[8] On the assumption of a national recovery rate of 70%, these vehicles correspond to 14,305 thefts. Thus, the 957,600 thefts in 1976 can be estimated to have caused about 1339 injuries and 134 deaths.

THEFT TECHNOLOGY

Existing Anti-Theft Systems

Modern automobiles are provided with two standard factory-installed anti-theft systems. Entry protection is provided by means of door and truck-lid locks and, in some cases, a hood-latch mechanism released from the interior of the vehicle. Prior to 1969, protection against setting the vehicle into operation was traditionally provided by a locking ignition switch. In addition, some models, notably Ford products in the late 1930's, also featured a device for locking the steering mechanism.

Beginning in 1969, General Motors vehicles incorporated a steering column lock which has been standard equipment on all models since. This lock prevents the steering of the vehicle as well as ignition and starting when intact and in the locked position. Beginning in 1970, Federal Motor Vehicle Safety Standard (FMVSS) No. 114 mandated the use of this type of system, or one which would prevent forward self-mobility of the vehicle, and thus the other manufacturers of vehicles sold in the United States followed suit with similar mechanisms.

Entry locks generally consist of a cylindrical lock with five or six tumblers. In the case of Chrysler and Ford, these are simple pin tumblers. General Motors and AMC, on the other hand, use disc tumblers which operate a side locking bar. When the correct key is inserted, the rotation of the cylinder actuates a linkage mechanism which unlocks the interior push-button lock and actuates the door latch, as does the interior door handle of an unlocked door. Truck-lid locks operate the same way, except that there is no interior push-button lock and the mechanism is somewhat simpler, since the latch is usually located immediately behind the cylinder.

The major U.S. manufacturers comply with FMVSS No. 114 by means of a steering column lock. This lock combines a bolt (latch in the case of Chrysler) which locks the rotation of the steering wheel, with the simultaneous locking of the mechanism which actuates the ignition and starting switch, unless the cylindrical lock is turned with the proper key. The types of cylindrical locks used are the same as those used for the entry locks, as described above, except that the body of the cylinder is usually heavier and the cylinder is retained in the steering collar housing by means of a pin or plate device.

In the case of General Motors and Ford, the ignition switch is located in a secure location near the base of the steering column and is operated by a rod attached to the steering bolt. In the case of Chrysler, the switch is located in the cavity under the steering wheel and is operated directly by the mechanism which operates the steering latch.

In all vehicles with column-mounted shift levers, the lock cannot be rotated to the locked position and the key removed unless the shift lever is in the "PARK" position, or if manual, in the reverse position. This is a safety provision to prevent locking the steering mechanism, while the vehicle is in motion. Exceptions are made for floor-shift vehicles where a separate button must be pushed to enable the locking action. Some floor-shift vehicles allow for the actuation of the steering lock when the key is pulled out.

FMVSS No. 114 also requires lock cylinders which provide 1000 (or more) different combinations and a warning device to remind the driver that the key has been left in the lock if the driver's door is opened while the key is in the "off" or "lock" position.

Optional factory-installed alarm systems have been offered for some vehicles. The LEAA study indicated that these were available in 1975 on all full-size cars from the three major manufacturers and for the smaller size Ford products.[18] However, recent interviews with the automobile manufacturers indicated that most of these options have been dropped due to lack of purchaser interest.[20,21,22]

In addition to factory-installed equipment, there are many systems available on the market for seller or owner installation. These are far too numerous to describe individually in this report. Many are listed and briefly described in Appendix D, excerpted from the Massachusetts H.O.T. Car Campaign Handbook.[23] Howland describes and rates many of these devices for purposes of establishing insurance discounts,[24] and Hunt presents the rationale behind the level of insurance discount allowed for the various systems listed in Appendix C.[25]

After-Market Systems

The after-market systems fall into several major classes, each of which is discussed below.

Alarms

Alarm systems sound a siren or a vehicle horn when illegal entry is attempted or the vehicle is jostled. Some of these systems are passively activated when the motor is turned off or the key removed. Only recently have any data concerning the effectiveness of alarms become available. The General Motors survey identified 362 automobile and truck thefts in which alarm systems had been installed and were definitely "on" at the time of the theft.[13] Because it is unknown how many alarms prevented thefts — and thus claims — in the population examined, the true deterrence of an alarm cannot be evaluated from the data. However, in cases where a theft claim was made, 60 alarms were defeated by the thief and 134 operated but did not prevent the theft. Of course, many of the latter group may have prevented total theft of the vehicle and limited the theft to partial theft of personal property.

Ignition Shut-Off Switches

There is a wide variety of these devices which generally operate in series or parallel with the ignition switch to prevent starting unless activated. Some incorporate elaborate anti-tampering features and some are passively engaged.

Fuel Shut-Off Valves

Solenoid valves cause the vehicle to stop several minutes after starting, unless deactivated.

Mechanical Devices

Mechanical devices include hood locks, steering wheel locks, armored sheaths which surround the steering column, and the like.

Theft Methods

There are many methods used to gain entry into a locked vehicle and then to disable the ignition lock system. The more important of these are described in this subsection.

Door Button Hook

One of the most common methods used to gain entry is that of using a bent wire to hook and raise the door button from outside. The wire is forced through the gasket at the edge of the window. In the case of older cars where the door button is close to the gasket, a thin blade or screwdriver can be used to open the door as fast as is possible with a key. One thief discussed the effectiveness of using a short length of rubber tubing at the end of a wire to raise the tapered-type buttons. The general method is prevalent in many areas. Because it often does not leave any marks on the door, it is often listed as a "no visible means" entry by investigators. However, the Michigan theft study[4] showed that 43% of all vehicles stolen were two-door hardtops and 7% four-door hardtops. This is felt to be due, at least in part, to the relative ease with which the door lock can be circumvented. The recent General Motors study indicates that 20% of the 5045 theft entries were effected by this method.[13] However, they also list another 38% as unknown, many of which probably used this method.

"Slim-Jim"

Another common method used to unlock doors involves use of a thin blade of spring steel with a hook or notch on one end. It is inserted between the window and frame at the appropriate location for the particular vehicle and used to unlock the button lock mechanism by pushing or pulling directly on the internal linkage. There are understandably no statistics for this method since it leaves no visible evidence. However, its use is common knowledge among thieves, investigators, and manufacturer security experts. The advent of the frameless or channel-less side window has made this method particularly effective. A wire with a hook on its end can also be employed as a "slim-jim" for many door lock mechanisms.

Window Breaking

Actual breaking of window glass is seldom used as a method of entry because it results in a conspicuous and suspicious condition. Also, the thief does not want to remain at the scene long enough to remove the pieces of glass from the seat and, thus, would be forced to sit on them. However, with older vehicles having vent or wing windows, a common entry method is to force the catch on the window and unlock the door from the inside. At this point, this method is more common in California where old cars are stolen more often than new cars. The combined total of broken glass and forced vent window comprised 18% of the entries in the General Motors study.[18]

Slide-Hammer

In the eastern and midwestern areas of the United States, the slide-hammer has become the prevalent method for forcing the steering column lock. However, it is also used to remove the lock cylinder from doorlocks, truck-lid locks, and the older type ignition locks. The method is the same in all cases. After removal of any decorative ring, the screw at the end of the slide-hammer is engaged into the key-slot or a notch at the edge of the lock cylinder. The sliding weight is then slammed back against its stop, producing a tensile impact on the lock. Several such blows are sufficient in most cases to pull the lock cylinder free, exposing the mechanism so that it can be unlocked from the outside, typically with a screwdriver. Barry[6] showed that the steering column lock on 1970-1975 Ford products was particularly susceptible to this type of attack. Theft data in Massachusetts showed that 70% of the 1972 through 1974 cars stolen in 1974 were Ford products. A recent AAA survey in Massachusetts showed that 60% of 178 stolen cars were Ford products.[14] Nationally, the FBI survey[3] showed that 50% of the recovered vehicles studied were Ford products, compared with their market share of only about 20%. Moreover, of the 43% having removed or forced ignition locks, 80 to 85% were Fords, and, of the 57% with intact ignition locks, only 27% were Fords. Recent data obtained following improvement of the Ford lock showed a reversal of this trend for the newer models.[11]

When used against the older ignition switches, the slide-hammer allows the manual operation of the switch with a dummy cylinder or screwdriver. In some cases the switch is hot-wired after it is pulled free of the dashboard.

The recent General Motors survey which was nationwide, but concentrated in Michigan and Illinois, showed that 37% of total thefts where the method could be defined were accomplished by pulling out the ignition lock cylinder.[18] Moreover, the same study showed that entry was accomplished by attack on the door lock cylinder in 6.5% of the cases.

Door-Lock Turning

The entire door lock receptacle is keyed by means of its mounting hole — located in the door in most models. A method of opening the door that has been described is to grasp or pry the lock outward to free the keying action and then turn the entire lock to unlock the mechanism. It is not known how often this method is actually used. The FBI study shows only 1% of recovered vehicles with a tampered doorlock.

Try-Out Keys

Try-out key sets consisting of 5 to 725 keys are obtainable. Each set approximates several of the 1000 combinations in use. Although any given key has been found to operate any given lock 6 to 7 out of 10 times, no specific evidence was uncovered to indicate the use of such try-out sets.[16] Public Law 90-560 prohibits the use of U.S. mails for advertising or delivering master keys or sets, and several states have enacted similar laws.[20] Of course, the use of a try-out set would leave no visible means of entry or ignition lock attack, and the FBI study shows this in 65% and 33% of thefts, respectively.[3] Likewise, the General Motors survey shows unknown method of entry in 38% of thefts and unknown method of mobilization in 38.6%.[18] Thus, the conclusion in the LEAA study[16] that this "tedious" approach is seldom used is questionable.

Torsional Attack

A common method of attack against the steering column lock has been to insert a blank key to raise the tumblers and then to twist the key to break the tumblers. This allows unlocking and starting the vehicle. This method is generally applicable to Ford and Chrysler locks of the major U.S. manufacturers, since GM and AMC use a lock cylinder with a sidebar.[10] The FBI survey indicated that torsional attack accounted for 18% of ignition lock thefts, 78% of which were Fords.[3] This was largely due to the use of brass tumblers which have since been replaced by steel tumblers. The more recent General Motors survey shows only 2.8% of ignition lock thefts due to torsional attack.[18]

Lock Picking

The lock cylinders used in various automobile locks are generally susceptible to the rake pick. The exceptions are the GM and AMC locks which have a sidebar to prevent rotation. Normally, a slight torque is placed on the barrel during rake picking to create a slight edge to hold each picked tumbler as it is raised to the correct level. There is no evidence from any source that manual lock picking, in the classical sense, is used against auto locks. However, a device called the rake or pick gun which provides a vibrating blade that is inserted into the lock is described by Brickell and Cole.[30]

Another type of crude pick consisting of a key blank filed with several circular lobes was described by California police as a method that is being used against late-model Fords. The blank is inserted and jiggled back and forth until it raises enough tumblers to allow the turning of the lock.[29] The California study report describes a similar device, reported to be used against trunk locks.

Lock Impressioning

Lock impressioning which involves use of a locksmith's tool to decode the lock has been reported as a common method of theft.[3] Typically, the door-lock cylinder is removed and taken away from the vehicle. A key is cut and the thief returns to steal the vehicle with a key. The tool is not felt to be in the general possession of a large number of thieves, but it is certainly a method that has been commonly used by professional thieves. The separate doorlocks used on post-1974 GM locks are designed to counter this method. Parenthetically, it might be noted that obtaining the lock code and cutting a key is currently reported to be a common method in California. Some Datsun models have the code on the outside face of the lock; others in the instruction book which is usually in the glove box. Some Volkswagen models have their code on the doorlock cylinder which can be read simply by removing one screw holding the outside cover of the door handle. Recent rules have been instituted in California requiring better identification for individuals requesting a replacement key with a code number.

Static Lock Cylinder Extraction

Static lock cylinder extractors have been recently reported as a theft method, particularly against GM steering column cylinders which are the most difficult to release with the dynamic slide-hammer. The split mandrel on the extractor is clamped onto the rim of the lock cylinder after removing the outer ring. The cylinder is then jacked out with a wrench, the extraction force being reacted against the steering column housing. There are no data on how prevalent this is as a theft method in the field.

Hot-Wiring

This method of theft was the prevalent method used prior to the advent of the steering column lock, and it is still used in the theft of older vehicles. It basically consists of electrically shorting the ignition switch and then shorting from a positive battery source to the starter solenoid to start the engine. In essence, the function of the ignition switch is duplicated by means of jumper wires. This can be accomplished behind the dashboard or under the hood. Many of the pre-1970 vehicles simply had a plug at the back of the ignition switch which could be unplugged and jumped with paper clips.

Drilling Out the Lock Cylinder

Theoretically, the lock cylinder can be drilled out. However, the hardened plate on the GM lock makes this extremely time-consuming. For reasonable theft times, even with the Ford die cast cylinder, a battery-powered electric drill would be required. There are no data which indicate that this method is applied with any frequency.

Attack on Lock Housing

At one time, before the slide-hammer came into common usage, the steering column lock was often destroyed to the point where the lock cylinder was freed and the mechanism could be operated without a key. The experienced thief could peel back a strip of the die casting to the retaining pin location with a cold chisel and remove the cylinder. This method is not frequently used now since the slide-hammer is a much faster and less conspicuous method. The General Motors survey indicates that the lock cylinder was broken out in 11% of the cases examined.[13]

Use of Owner's Key

The use of the owner's key to enter and/or mobilize an automobile is commonly reported as a major method of theft. Table 9 shows the results of the major stolen vehicle surveys concerning this method. An earlier survey by the Justice Department[9] showing that 40% of all thefts were accomplished with the owner's key has been omitted because its data came from thief interviews which are highly unreliable for this particular data, since this method tends to result in a lesser penalty for the thief.

TABLE 9. SUMMARY OF VEHICLES STOLEN WITH A KEY IN THE IGNITION LOCK

Survey Reference	Total Thefts	Thefts with Key in the Ignition Lock	Percent of Thefts with the Key
California[8]	411	193	47
Michigan Phase I[4]	2,466	167	6.7
Michigan Phase II[4]	135	42	31
FBI Special Survey[3]	10,014	1,695	17
FBI Survey[31]	116,409	15,434	13
General Motors Survey[13]	2,089	322	15
Totals	131,524	17,853	13.6%

The California survey showed 47% of the stolen cars were taken with factory keys. (Adding substitute keys raises this to 58.8%.) This correlates with the conclusion reached in this survey of experts which also indicates a major portion of the cars stolen in California are stolen with a key.

The two Michigan surveys show completely different results concerning the owners' keys being left in the ignition.[4] There is no explanation for the discrepancy. The FBI surveys cover the largest number of cars, and the results of the special survey of recovered vehicles and the survey of 116,409 theft reports show comparable results regarding thefts due to owners' keys being left in the vehicle.

Analysis of the FBI and Michigan data in the LEAA study[16] suggests that vehicles equipped with warning buzzers are left with the key in the ignition and subsequently stolen about as frequently as cars not equipped with a buzzer.

Survey of Manufacturers

Vehicle security specialists at the three major U.S. automobile manufacturers were interviewed to determine current and projected improvements in theft prevention equipment.[20,21,23] The major modifications that have been made recently or are being contemplated for the door lock system center around the design of the interior lock button. Ford has recently introduced a flush door button on some two-door models. The door is unlocked with the door handle from the inside. On four-door models, FMVSS No. 206 requires that, for children's safety, the rear doors cannot be unlocked by means of the door handle. Thus, the conventional mushroom door buttons are retained on the rear doors of four-door models. Ford also reports that it is developing no-button door locks, but no details were supplied concerning the design approach. Chrysler and GM have made no recent change in the door button design.

Chrysler has adopted the policy of providing tapered buttons through its dealers, and these can be used by the interested owner to improve theft resistance. GM has also retained the mushroom button as the optimum current design for child safety and the handicapped consumer who has reduced manual dexterity. However, both Ford and GM state that they are searching for or developing button design modifications which will improve theft resistance, while still allowing convenient operation by handicapped owners.

Baffles have been added in some cases to make actuation by the "slim-jim" more difficult. However, all three manufacturers state the opinion that a "slim-jim" can always be devised which will be capable of releasing the doorlock. Another design approach which has been applied is that of reversed linkage in which the free play provided for button actuation is contained in the lock mechanism rather than in the linkage system. This reportedly makes "slim-jim" attack more difficult, but has evidently not been used to any significant degree.

The major innovation in locking approach is the separate door and ignition combinations used on the post-1974 GM products. This effectively precludes the thief from making an ignition key by decoding the doorlock.

Both Ford and Chrysler described efforts to improve the retention of lock cylinders on door and trunk lid locks to improve their resistance to the slide-hammer. All manufacturers stressed the difficulty of improving the door-locks within the constraints imposed by the window operating mechanism, the required impact resistance, and the trend toward thinner doors imposed by vehicle weight limitations.

As a result of the vulnerability of the steering column lock to the slide-hammer, various improvements have been made or are in the development stage. Ford introduced a variety of changes, beginning in 1974. These include the addition of a snap-ring-retained steel washer and necked-down shaft on the lock cylinder such that removal with a slide-hammer requires more blows and, when the cylinder does break free, a portion is left in the mechanism. This makes actuation of the mechanism with a dummy cylinder or screwdriver more difficult.

As noted earlier, initial insurance statistics indicate that the theft rate for the 1976 and 1977 Ford products incorporating this change are comparable with other vehicles in the same price class. Other changes introduced by Ford include a steel anti-drill plate placed in front of the tumblers, better retention of the tumbler cap, use of stainless-steel tumblers for increased torque resistance, and the use of an enlarged retaining pin for the cylinder. Their performance criterion has been that the cylinder should resist 60 blows with a 15-lb slide-hammer, and they report that the current locks meet or exceed this requirement.

The other manufacturers have not made any major changes in their steering column locks, except that Chrysler replaced the cylinder retaining pin with a larger, steel pin several years ago. However, the 1978 Omni reportedly incorporates a roll pin retainer to improve the resistance of the steering column lock to the slide-hammer. Also GM reports that it will introduce an ignition lock improvement to increase slide-hammer resistance in its 1979 models.

None of the three manufacturers interviewed reported any planned change in the basic door or ignition locking system now used. Very preliminary planning appears to be under way in connection with the incorporation of security features into on-board microprocessor systems, the primary application of which will be the control of engine performance.[32] However, this is not likely to occur for 5 to 8 years and appears to be centered around the doorlock system for vehicles equipped with electrical doorlocks. The general reaction was that such a system would appear first on higher priced models to be followed later on lower priced models if consumer reaction were favorable.

Key-ejection and keyless systems have been considered, but no conclusions or plans concerning their adoption were provided. GM tested a keyboard system, designed to prevent the use of a vehicle by intoxicated drivers and report a lov degree of user acceptability.

All three manufacturers state that they do not have data on the cost or the portion of vehicle price attributable to existing security systems. If this cost could be separated from that of the other functions performed by the systems, it would be regarded as proprietary by each manufacturer.

Time Required to Defeat Existing Systems

Barry conducted a test program to establish the time required to remove the lock cylinder from steering column locks with a slide-hammer.[6,18] The times for the three major U.S. manufacturers' locks are summarized in Table 10. Assuming that the previously cited 60-blow performance criterion is achieved by the Ford locks for 1976 and later, the Ford time has almost certainly been increased to the 120-second range, not counting any additional time required to turn the mechanism with the piece of the cylinder remaining in the sector gear.

TABLE 10. MINIMUM TIME FOR REMOVAL OF IGNITION LOCK CYLINDER BY MEANS OF A SLIDE-HAMMER

Manufacturer	Minimum Removal Time (sec)
Ford (pre-1976)	10
Chrysler	30
General Motors°	120

°AMC locks are substantially the same as GM locks.
Adapted from References (6) and (18).

No source of data was uncovered concerning the time required to circumvent the existing door lock systems. The earlier hardtops with mushroom shaped buttons can be entered as quickly without a key as with one — a matter of 2 or 3 seconds. Likewise, many of the specific door mechanisms which are extremely vulnerable to the "slim-jim" can be circumvented in a few seconds.

Thief Profiles

The FBI reports that the most frequently apprehended motor vehicle thief is a male between the ages of 13 and 18. Males are arrested six times as often as females and 53% of all arrests are of individuals under the age of 18.[2]

Articles have appeared in the popular press describing car thieves who appear to be modern-day Edisons turned bad, armed with a formidable array of techniques for countering any imaginable anti-theft device.[33] While there are undoubtedly many such highly skilled and experienced car thieves, especially among the professional ranks, neither arrest statistics nor the proportion of thefts attributable to professionals indicates that this type of thief is typical. Rather, interviews with thieves by Barry,[6] as well as those conducted in this survey,* and with law enforcement officials also indicate that the great bulk of thefts are committed by juveniles or young men. Many of the professional auto-theft operations make use of these individuals for the actual theft since they are relatively immune from serious prosecution, if caught.

The general thief profile shows that the car thief often begins to steal cars between the ages of 13 and 15. Many appear to steal one or more cars every night for joy-riding purposes. These thieves often strip easily removed and marketed parts from the cars they steal and then abandon the vehicle. As they get older and in need of more lucrative endeavors, they often turn to other sources of income and abandon car theft, except as a means for acquiring transportation for the commission of another crime.

Most of the thieves interviewed showed little general mechanical aptitude or talent. More often, their methods are operation-oriented, i.e., they concentrate on a specific type of vehicle lock with which they have experimented and been successful. The knowledge and techniques used appear, in general, to be communicated directly from one thief to another, usually as a result of cooperative efforts during a number of thefts.

*See Appendix D.

Most of the thieves interviewed had little general knowledge of the mechanisms used in a variety of vehicles and could only identify hardware used in the type they liked to steal. Only one thief reported perfecting his technique by practicing on cars in a junk yard.

Thieves interviewed in the San Francisco jail all displayed an ignorance of the slide-hammer and of methods for defeating the steering column lock. This correlates with the theft rate by vehicle type and year discussed previously. On the other hand, all thieves interviewed in Massachusetts were familiar with and had used the slide-hammer.

Another regional difference noted from the interviews was the time allotted to the theft. California thieves characteristically cited 5 minutes as their normal theft time (1 minute was the minimum) and 10 minutes as the outside limit, after which they would normally abandon the attempt. Massachusetts thieves cited average normal theft times of 1½ minutes (30 seconds was the minimum), and 2 to 5 minutes as the outside limit. While testing by Barry (see Table 10) during this program suggests that 30 seconds may be a somewhat immodest claim for a locked car without a key, it is certainly possible for most types of cars.

The specific circumstances would, of course, affect the outside limit. Thieves indicated that in a remote, relatively safe location, they might risk exposure for a much longer time. Several indicated the strong sense of vulnerability felt during the pre-entry phase of the theft and their tendency to look for an unlocked vehicle and to avoid vehicles showing any evidence of an alarm system. None of the thieves interviewed mentioned breaking the glass as a means for entry and at least one indicated that he would never use this method because it was too obvious to the police and left glass fragments on the seat on which he would then have to sit.

4. ANTI-THEFT PERFORMANCE CRITERIA

The objective of this program is the improvement of FMVSS No. 114 in such a way that it mandates anti-theft performance level as well as function, but is not design-restrictive. This statement is, of course, somewhat contradictory in terms. The specification of any minimum level of performance or functional characteristics necessarily eliminates those designs incapable of achieving these levels. The intent, however, is to avoid standard provisions which preclude a range of different designs that are each capable of achieving the required level of theft deterrence. Moreover, it is important to eliminate provisions that are based on specific systems and the known attack methods used to defeat them. Such provisions inhibit the application of clever design which cannot only deter that specific attack method, but also other whole classes of potential methods.

The program also encompasses the design and development of a specific improved anti-theft system as described in Chapters 5 and 6. The first step in this process was, of course, the formulation of a fairly detailed list of design specifications.

The basic building blocks for both the development of a standard and the designer's list of specifications are the performance criteria for effective anti-theft performance. This chapter covers the identification, evaluation, and ranking of these performance criteria based upon the information gained in the theft survey of Chapter 3.

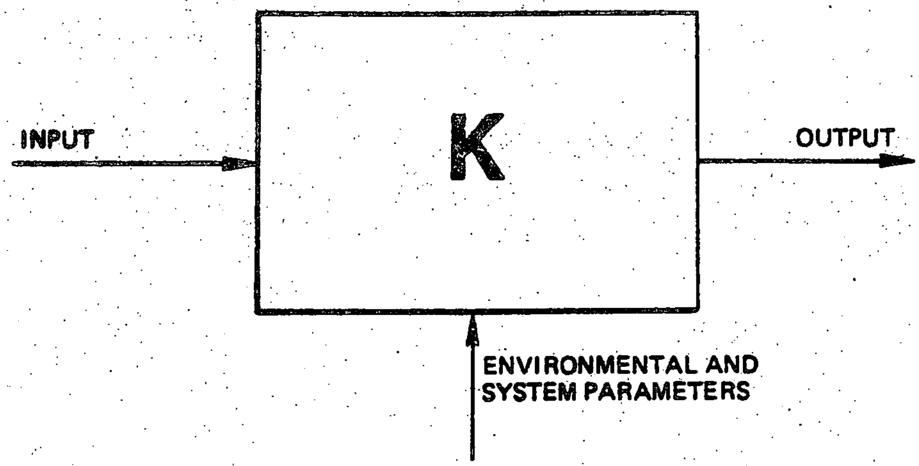
UNIQUE CHARACTER OF ANTI-THEFT PERFORMANCE

In terms of specifying performance, anti-theft systems are unique in comparison with other motor vehicle systems. This distinction must be understood at the outset. Otherwise, the formulation of an effective anti-theft performance standard is doomed to failure.

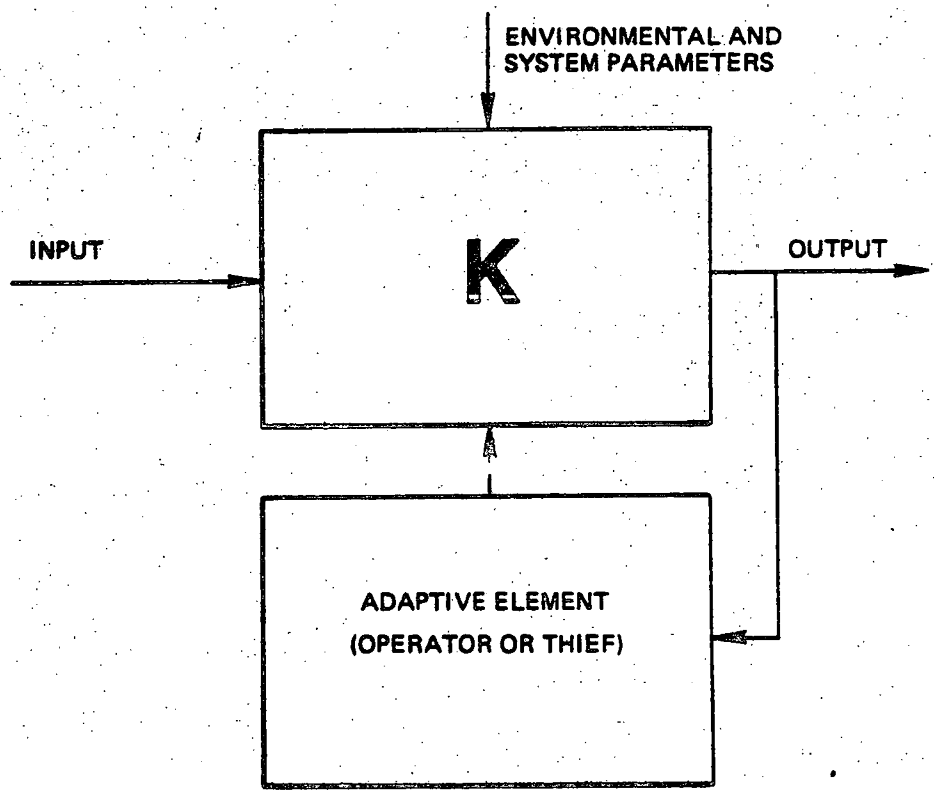
It is convenient to discuss the performance of a generalized motor vehicle system in terms used by the control engineer. As shown in Figure 1(a), the system can be represented by a transfer function, K, which relates the output to the input, as well as a number of environmental and system parameters. The transfer function, K, can, of course, be a function of time or frequency, depending on the nature of the input. Taking the hydraulic brake system as an example, the output could be stopping distance and the input a step force applied to the brake pedal. Typical environmental parameters are temperature, pavement type, and pavement condition, while system parameters would include the weight carried by the vehicle, the type of brake fluid used, etc.

In this case, if the parameters are all held constant, one would expect the stopping distance or performance for a given brake system to be a repeatable function of the applied force, within experimental error. The example would be carried further by realizing that there are predictable failure modes, such as the loss of a single pressure-carrying component which would result in a different transfer function, but would also provide repeatable performance for a given system.

Thus, for this example, a performance standard can easily be formulated which specifies the minimum performance level in terms of the output for a specified input. FMVSS No. 105 does this for the two conditions described above. This system and most of the others on an automobile can be termed passive because, once the operator's input is specified, the characteristics of the system and its response to the passive parameters do not change.



(a) PASSIVE OPEN-LOOP SYSTEM



(b) SYSTEM WITH ADAPTIVE FEEDBACK

FIGURE 1. GENERALIZED SYSTEM BLOCK DIAGRAMS.

The thief, however, can be viewed as an adaptive element. He views the output or results and varies his attack on the system to produce his desired result. He is capable of acting directly on the anti-theft system and changing its characteristics so that it no longer functions as designed.

Thus, the anti-theft system must be characterized by a block diagram of the type shown in Figure 1(b). The adaptive feedback element in this case represents the thief.

The essential difference between the anti-theft system and other automotive systems is that the open-loop performance of the anti-theft system without the inclusion of the thief is trivial. In general, the characterization of the system can only express the activation and deactivation operations of the system in response to the operator's input. It can never describe the fundamental performance of the anti-theft system, its resistance to intelligent attack. The trivial open-loop performance is what the current version of FMVSS No. 114 specifies. It does not concern itself with any form of attack, other than the relatively unimportant use of try-out keys.

This problem, of course, is much easier to identify than it is to solve. Because the system must include the intelligent, adaptable thief in order to express meaningful performance levels, the whole system is not within the control of the designer. It is, however, in this context that the task of identifying meaningful performance criteria must be approached.

GENERALIZED ANTI-THEFT SYSTEM

For reference in the discussion of this and subsequent chapters, it is convenient to define the major elements of a generalized anti-theft system. These are shown functionally in the block diagram of Figure 2. Virtually any anti-theft system designed to prevent the operation of a critical vehicle function or to sound an alarm, unless deactivated by an operator with the appropriate code, can be visualized in this way. Specific systems, of course, seldom encompass all of the generalized elements shown.

For example, the standard factory-equipped entry or steering column locks do not provide either a sensor screen or a sensor signal processor. The code insertion device in each case is a key and the decoders are lock cylinders. The bolt or latch mechanisms are incorporated into the doorlatch and steering column mechanisms for the mechanical locking functions. For the ignition and starting functions, the latching mechanism is a switch.

The various signals shown can, in general, be mechanical, electrical, hydraulic, or pneumatic. In the current standard systems, the coded signal is mechanical. The binary signal is mechanical in the case of the door lock and steering wheel lock, and is transduced from mechanical to electrical in the case of the ignition/starting switch.

The operating energy sources can also occur in any media. In the case of the existing locks, they are mechanical and both are supplied by the operator as he turns the key.

The sensor screen and sensor signal processor show, in general fashion, the function of any system designed to sense illegal entry or tampering. In general, this type of anti-theft system can sound an alarm, feed back a blocking signal to the decoder or latch mechanisms, or both. For example, the conventional alarm system, available as optional factory equipment or purchased as an aftermarket system, uses switches on all entry points as a sensor screen and sounds an alarm,

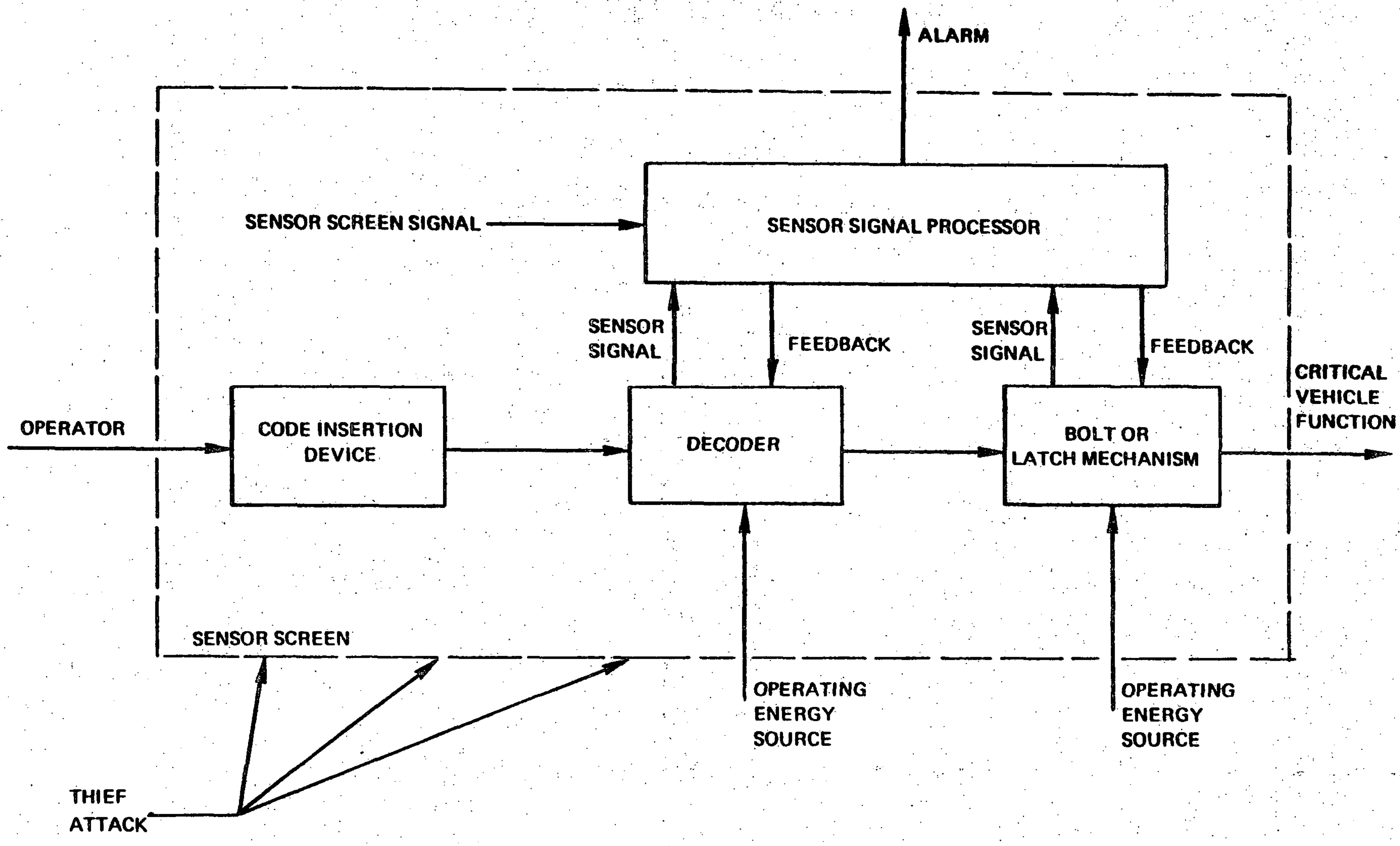


FIGURE 2. GENERALIZED ANTI-THEFT SYSTEM.

as well as feeding back a switch opening in the ignition circuit in case of illegal entry. No commercial system known to this author is currently available which incorporates a tampering sensor on either the decoder or latch mechanism. However, this is a feasible concept and has been proposed in several forms.

This picture of the anti-theft system is useful because it provides a framework within which any proposed system can be discussed. It also shows clearly where the major constituent functions occur and where the vulnerability lies. For example, a thief can quickly obtain access to the binary signal point by means of a slide-hammer or a "slim-jim." If he could only access the coded signal point quickly, he would have great difficulty deactivating the system because of the ease in providing thousands of possible coded signals.

PERFORMANCE CRITERIA CLASSES

Based upon the vehicle theft survey of Chapter 3 and the studies of this program, it is apparent that the various anti-theft system performance criteria can be logically grouped into three major classes, which are defined and discussed below.

Functional Criteria

Functional criteria merely state what the system must do to be effective. In this discussion, they are further restricted to define system function in the absence of attack by a thief. Thus, this class includes criteria related to the provisions of the current version of FMVSS No. 114 as well as a number of others. In general, functional criteria are concerned with the locking function, number of codes or combinations, safety provisions, anti-key retention, and passive activation. Functional criteria which specify either mobilization or entry protection systems can be defined.

Attack Resistance Criteria

These performance criteria are concerned with defining the capability of the system to withstand attack by a thief who does not possess the authorizing code or key. The various identified performance criteria falling into this class include:

- Time-to-defeat,
- Accessibility,
- Resistance to tools,
- Conspicuousness, and
- Complexity.

Time-to-Defeat

It has been generally stated by every source consulted in the theft survey that time-to-defeat is the only important measure of theft resistance. In fact, except for conspicuousness, the remaining attack resistance criteria all have, as a basic objective, the imposition of a minimum defeat time.

In fact, it is clear that the attack resistance class of criteria can be considered to be a two-tier hierarchy. The imposition of a minimum time-to-defeat obviates the need for any other attack resistance criterion. Moreover, the criterion is also inherently free of design restriction. The designer can use any possible system design so long as it is capable of resisting attack for the prescribed period. Finally, opinions on the length of time which is likely to be effective are very consistent, always being cited in the range of 5 to 10 minutes. As it happens, this is a fortuitous time range because its provision on a system by a performance criterion would not impose any undue maintenance burden in the case of a need for normal servicing of the system. For example, the standard time estimated for the removal and replacement of an ignition and starting switch on most current automobiles is 0.7 to 0.8 hour by a mechanic with moderate skills.(34) The major problems with using a minimum time-to-defeat as a performance criterion include:

- It requires performance testing with a human subject.
- Realistic time-to-defeat criteria will likely require some limitation on tools and equipment.
- Design of a system to meet such a criterion inherently requires that the designer be able to identify the methods which potential attackers will use against the system.

The first of these will likely prove the major obstacle to the use of this criterion as a basis for safety standard. It implies the need for a defined test with subject(s) having a specified skill level, and some method, statistical or otherwise, for judging the results. Limitation on tools or equipment will be required to allow realistic design without the need to deter uncommon or expensive methods of theft such as the use of a tow truck.

Identifying the potential methods of attack and, further, forming the methods to be those where the time-to-defeat can easily be predicted and estimated are part and parcel of an effective anti-theft system design. It is entirely analogous to the use of failure modes and effects analysis (FMEA) to design systems that are fail-safe, an accepted design procedure for consumer products. An effective set of performance criteria must require this design process. Thus, this problem is inherent.

Methods of estimating the time required to accomplish a given operation are well-defined in the industrial engineering literature, as are measurement techniques once a system has been designed and test models are available.(35)

In fact, the automobile industry currently assembles this type of data for purposes of establishing warranty allowance schedules for dealerships. This body of data is also used to compile the various published standard time guides.(34)

If time-to-defeat is ultimately found to be unacceptable as the attack resistance criterion in formulating the anti-theft safety standard, then it will be necessary to move down to the second tier of the hierarchy and replace time-to-defeat with one or more of the remaining criteria. It is important to note that, except for conspicuousness, each of the other criteria has, as a basic objective, the establishment of a minimum defeat time for a system. In each of these cases, the designer who wishes to predict or measure the quantitative effectiveness of his design will have to use defeat time as the measured quantity. Even conspicuousness is related to defeat time, since its basic objective is the reduction of the average time allowable to a thief for a successful theft.

Accessibility

The only advantage of the second-tier attack resistance criteria over time-to-defeat is that they can be expressed in objective terms related to the system itself, independent of a thief or a thief test subject. However, there is a penalty for this advantage. They are inherently more design-restrictive, and thus less adaptable to the application of clever design to achieve the basic objective.

For example, accessibility criteria are designed to impose a time penalty on the thief by ensuring that the vulnerable parts of the anti-theft system are located in a place which he cannot easily reach. These parts, as defined in Figure 2, are the decoder, bolt or latch, and sensor signal processor, if used. An accessibility criterion must be expressed in terms of specific locations in the vehicle. For example, the criterion could specify that the vulnerable parts be located:

- remote from the passenger compartment;
- in a locked engine compartment; or
- such that they can be reached only from under the vehicle.

As such, accessibility criteria inherently impose some degree of design restriction. Each of these criteria would effectively preclude the current type of mechanical lock cylinder decoder, unless a complex — and likely impractical — method of transmitting the coded mechanical signal to the remote decoder were used. In fact, the criteria tend to mandate the use of electrical or electronic decoders for ease in transmitting the coded signal. Thus, even if a designer were to produce an exceptionally secure mechanical lock for the passenger compartment capable of meeting a reasonable defeat-time criterion, it would likely be forbidden by an accessibility criterion effectively worded for general application.

Resistance to Tools

Resistance to specific tools is another type of criterion widely proposed in the past for attack resistance. To avoid subjective wording in terms of time, these generally require specification of the type of tool and a limitation on force level, energy level, number of blows, etc. As such, they are inherently design-restrictive when used as the basis for a general performance standard. To be effective, they must anticipate both the design used for the anti-theft system and the method of attack at which they are aimed. Thus, a vast list of tools and specified limitations would be required to provide a complete coverage of conceivable anti-theft system designs. Moreover, thieves have been clever in the past at designing or adapting new tools to attack new systems, and there is no reason to believe that this capability will not continue. Thus, tool resistance criteria are likely to be of only transient use.

Conspicuousness

The value of conspicuousness in thwarting auto theft was stressed by a number of sources in the vehicle theft survey. Thieves will, in general, not break window glass because it represents a suspicious condition that often leads to apprehension by a police officer. One thief stressed the vulnerability felt by the thief during the entry phase of the theft when he is exposed. This stresses the potential benefits of improved door locks. A major flaw in the steering column lock is that a thief can gain access to the operating mechanism by lying on the front seat where he cannot be easily seen from the outside. Many sources have pointed out that if the lock were rotated 90 degrees on the steering column, the thief would be visible as he worked on it.

Conspicuousness can be provided by either aural or visual means, and thus criteria can be objectively worded to specify the level or nature of the signals produced. However, the provision of aural conspicuousness implies an alarm system. Likewise visual conspicuousness requires either an alarm system (e.g., with flashing lights) or, at minimum, a defined degree of visibility for any effective method of attack. The latter is closely related to an accessibility criterion and would impose a location limitation on the vulnerable parts of the system. Thus conspicuousness criteria used as a basis for a performance standard are inherently design-restrictive.

Moreover, the quantitative effectiveness of conspicuousness as a theft deterrent cannot be accurately predicted. There is no question that a vehicle which is equipped with an alarm system now stands a lower chance of being stolen relative to the remaining population not so equipped. However, the alarm system does not inherently delay the theft. Many cars equipped with alarm systems have been stolen. This occurrence would likely increase greatly if all vehicles were so equipped.

Complexity

The final type of second-tier attack resistance criterion is some defined degree of system complexity. This has been proposed by many previous investigators as a general means of increasing theft deterrence and is, of course, related to several of the other criteria. For example, complexity can increase the time-to-defeat by increasing the number of operations required to mobilize the vehicle. It can impose the requirement for special defeat tools which are either expensive or difficult to improvise. Finally, it can impose the need for a level of knowledge on the thief which is beyond that typically at his disposal. As such, there is no question that complexity can be a valuable tool for the designer in developing an effective anti-theft system. However, unless it is expressed in terms of the subjective time-to-defeat measure, complexity can only be expressed in terms of the specific characteristics of the system. For example, number of moving parts, number of redundant locking functions, number of electronic components, etc., would be typical expressions of complexity. These are, of course, all inherently design-restrictive.

A complexity criterion would tend to preclude a very simple design which effectively reduces the potential attack on the system to a single well-defined method and extends the time required for this method to beyond the 10-minute range. Many designers, including this author, feel that this approach is one of the most promising ones for achieving effective anti-theft designs.

Post-Theft Criteria

An important theft deterrent is provided by any factor which diminishes the value of the vehicle for the thieves' purposes. There is little that can be done to a vehicle for this purpose in the case of the joy-riding thief or the small-time stripper who removes accessories, tires, battery, or body parts for his own use or that of his friends. However, professional car thefts constitute 20 to 25% of all thefts and direct losses of close to $1 billion per year.

Virtually all professional auto theft is done with the objective of removing and selling major body and drivetrain components or reselling the vehicle. Currently, auto theft investigators are hamstrung by the fact that most major parts are not identified with the original vehicle identification number (VIN), and the titles and VIN plates from junk vehicles can easily be transferred to a stolen vehicle of the same year and model.

Thus, two anti-theft performance criteria for a complete system of vehicle theft deterrence are the following:

- Requirement that all major body and drivetrain components be marked by stamping the original VIN on them, and
- Requirement that salvage titles be separate and distinct from normal titles and not convertible without careful inspection of the vehicle to ensure that the VIN plate and other identification have not been transferred from a different vehicle.

Both of these criteria go somewhat beyond the scope of FMVSS No. 114. Further use of the VIN for theft deterrence would be a logical extension of FMVSS No. 115 and titling laws are generally within time perview of the individual states. Thus, while they are mentioned here for completeness, this class of deterrent criteria will not be carried further in the analysis and ranking of performance criteria.

Parenthetically, it might be noted that the title and remains of most "totally-wrecked" late model vehicles become, at some point, the property of the insurance company which insured the owner. Thus, the objectives of the salvage title law could be easily achieved within the insurance industry itself by effective control over the titles and resale of its wrecked vehicles. Of course, such measures would have the effect of decreasing the junk value of these vehicles in the interest of decreasing later theft claims for vehicles that have been stolen and replated with the VIN plate from the junk vehicle.

INDICES OF PERFORMANCE

In subsequent sections of this chapter, various and specific performance criteria in the functional and attack resistance classes will be ranked according to their importance on overall system performance and acceptability. As discussed in the preceding section, any anti-theft system must reflect both functional and attack resistance criteria to be effective. The functional criteria define what the system must do in the absence of attack to prevent the use of the vehicle by unauthorized persons. The attack resistance criteria, on the other hand, define the required capability of the system to resist the forcible by-passing of its functional features.

It is felt that these two classes should be ranked separately to avoid confusion. However, both should be judged against the same important indices of performance as follows:

Theft Deterrence

Theft deterrence potential can be evaluated quantitatively by estimating the total theft incidence or costs that can be saved if systems are applied which reflect the criterion in question. This estimate must be based upon that proportion of thefts or theft costs at which the criterion is aimed times its estimated effectiveness in reducing the number of thefts.

For reference, the theft cost data of Chapter 3 are broken down in greater detail among the various major theft types in Table 11. A similar breakdown of the number of thefts in 1976 among the various types is shown in Table 12.

TABLE 11. SUMMARY OF ESTIMATED AUTO-THEFT COSTS BY TYPE OF THEFT
($ billions)

Costs	Vehicle Unrecovered		Vehicle Recovered		
	Frauds[1]	Professional Theft Operations[2]	Small-Time Theft for Profit[3]	Transportation Thefts[4]	Totals
Direct losses[5]	$0.116	$0.576	$0.302	$0.545	$1.54
Accident costs[6]			0.021	0.039	0.06
Arrest, prosecution, & correction costs[7]	—	0.021	0.067	0.021	0.21
Subtotals	0.116	0.597	0.390	0.705	1.81
Costs for theft by means of key left in vehicle[8]		0.081	0.053	0.095	0.25

Notes:

(1) Assumes 5% of all thefts are frauds – see Table 6.
(2) Assumes 25% of all thefts are by professionals – see Table 6.
(3) Assumes 25% of all thefts are by small-time thieves for profit – see Table 6.
(4) Assumes 45% of all thefts are for joy-riding or transportation – see Table 6.
(5) Average losses for unrecovered and recovered vehicles are $1522 and $2903, respectively, from Ref. (13) – see Table 7. Total automobile thefts were 794,808 for 1976.
(6) Data from Refs. (15) and (18) – assumed all in amateur category.
(7) Date from Refs. (2) and (16) – 90% of total allocated to recovered vehicle categories and 10% allocated to professional category.
(8) Based on Table 9, 13.6% of each category, except frauds, is assumed to have occurred by this method.

TABLE 12. SUMMARY OF AUTOMOBILE THEFT INCIDENCE IN 1976 BY TYPE OF THEFT

Type of Theft	Number of Thefts
Professional theft operations(2)	198,702
Fraudulent insurance claims(1)	39,740
Small-time theft for profit(3)	198,702
Transportation(4)	357,664
Total	794,808
Number of thefts by means of key left in vehicle(5)	102,689

Notes:

(1) Assumes 5% of all thefts are frauds – see Table 6.
(2) Assumes 25% of all thefts are by professionals – see Table 6.
(3) Assumes 25% of all thefts are by small-time thieves for profit – see Table 6.
(4) Assumes 45% of all thefts are for joy-riding or transportation – see Table 6.
(5) Average losses for unrecovered and recovered vehicles are $1522 and $2903, respectively, from Ref. (13) – see Table 7. Total automobile thefts were 794,808 for 1976.

Consumer Acceptability

Many performance criteria that impose obstacles in the path of a thief will also put constraints on the authorized user of the vehicle. If these are sufficiently annoying, many drivers will not use the system or, if it is passive, disable it. Thus, the system will become ineffective for theft protection. The proper balance between effectiveness and consumer acceptability must be found.

In advance of extensive testing, perhaps in the marketplace, the potential consumer acceptability of a performance criterion or system design must be a judgmental factor. The basis for this judgment is the degree of change imposed on the driver's habits. If, for example, a performance criterion would impose additional time-consuming steps on the process of mobilizing the vehicle, it would suffer from low acceptability. Likewise, if it imposed difficulty on customary operations, such as parking lot or valet services or getting back into a car after locking a key in, it would be less acceptable to the consumer as well.

Cost

A proposed performance criterion alone does not have a characteristic cost. It is required that the criterion be implemented with an actual system design to the point where a great deal of detailed technical visibility has been gained before costs can be estimated with any accuracy.

However, the cost of any system resulting from a performance criterion is an important rating factor. Aside from the pain and suffering experienced by accident victims, auto theft is primarily an economic problem. The latter is the only factor in the great bulk of thefts. Thus, the cost of anti-theft equipment must be consistent with the savings produced.

The various manufacturers claim that they cannot estimate the separated costs for the systems that have been installed on U.S. automobiles for the past seven years.[20,21,22] However, an independent firm has performed such a cost study for entire compact and intermediate vehicles under Government sponsorship.[86,87] Although the breakdown of parts was not detailed enough in each case to separate the anti-theft parts from the overall system in which they are contained, the data of Table 13 are included here for reference.

In ranking performance criteria, cost can only be assessed on the basis of engineering judgment concerning the probable relative cost necessary to implement the various proposed criteria.

Safety, Reliability, and Maintainability

These are extremely important performance indices for evaluating a system concept. However, at the performance criteria level, sufficient technical visibility of the specific methods necessary or possible for implementing each criterion is not available for any realistic comparison of these characteristics. It is felt, at this level, that their inclusion would only confuse the issue and diffuse the impact of the other ratings which can be more accurately visualized. Thus, except for comment in any unusual case where safety, reliability, or maintainability are clearly related to the basic criterion under consideration, these factors should be deferred to the system concept level. General statements that can be made are that all anti-theft systems must meet the important safety criteria including:

a) ensuring that no vehicle function critical to safety can be inadvertently compromised while the vehicle is in motion;

b) ensuring that the occupants can open the doors from inside, if necessary; and

c) providing for interior door locks consistent with child safety.

Maintainability and theft deterrence are inherently conflicting requirements and require a trade-off. However, in general, defeat times that are consistent with theft deterrence are well within the normal repair times associated with maintaining a vehicle. Thus, it appears that this trade-off can be successfully achieved.

RANKING OF FUNCTIONAL CRITERIA

Although virtually all of the performance criteria which fall into the two major classes — functional and attack-resistance — can be evaluated for their effects on theft deterrence, consumer acceptability, and cost, these classes should be ranked separately. Each system must meet criteria in both classes, and specification for what the system should do must not be confused with specifications on how well it must resist attack. To compare them in a single rank list would be tantamount to violating the well-known precept against comparing "apples and oranges."

With the exception of safety criteria of the type listed at the end of the preceding section, the various general functional criteria are listed and defined as follows:

1. *Mobilization-Protection* — This type of criterion specifies that the system must prevent activation of at least one automobile function necessary for its mobilization, unless it is deactivated with the authorized code or code insertion device. The current standard, of course, specifies at least two critical automobile functions, but

TABLE 13. CONSUMER COSTS FOR ANTI-THEFT EQUIPMENT AND RELATED HARDWARE

Component	Remarks	Consumer Cost-Dollars	
		1975 Ford Pinto	1975 Chevrolet Malibu
Rear deck lock cylinder and mounting hardware	Latch mechanism not included because required in any case	0.67	0.67
Front door latch and lock mechanism	Latching function required in any case, two required per vehicle	5.75	6.10
Front door lock cylinder	Two required	0.95	1.00
Lock control rod and plastic pushbutton	Two required	.057	0.65
Steering column	Does not include steering wheel, gear shift control, turn switch, or horns. However, steering functions are required in any case	21.72	41.22
Cable hood-release assembly	For information only — now not an effective anti-theft device		0.72

this was a reaction to the earlier ease in hot-wiring. In fact, the resulting systems ended up less effective in some ways than earlier systems. Thus, there is no fundamental advantage in redundancy. The important characteristic is attack resistance which is covered in the other criteria class.

2. *Mobilization-Passive Activation* — This type of criterion specifies requirements for the automatic activation of the protection system under some conditions intended to define the point when the operator leaves the vehicle. The intent is to keep him from leaving the vehicle unprotected against theft. The current standard accomplishes this, in part, by ensuring that the system is activated whenever the key is removed.
3. *Entry-Protection* — This type of criterion specifies that, when activated, the system would prevent all points of entry to the vehicle unless deactivated by the proper code or code insertion device.
4. *Entry-Passive Activation* — This type of criterion specifies that the entry protection system be activated automatically whenever the operator leaves the vehicle.
5. *Number of Codes* — This type of criterion specifies an effective minimum on the number of different authorizing codes for the mobilization protection, entry protection, or both systems.
6. *Anti-Key Retention* — This type of criterion specifies that the system must not be capable of retaining the authorizing code or code insertion device when the operator leaves the vehicle.
7. *Key-Retention Warning* — This type of criterion specifies that the system remind the operator to remove the code or code insertion device when leaving the vehicle.
8. *Mobilization Warning* — This type of criterion specifies that the system remind the operator to activate mobilization protection when leaving the vehicle.
9. *Entry Warning* — This type of criterion specifies that the system remind the operator to lock the doors when leaving the vehicle.

The above nine criteria are rated in Table 14 for their theft deterrence potential with the aid of the data summarized in Tables 11 and 12. The rationale and judgment exercised in the process of estimating the potential savings are summarized as follows:

- It is estimated that the combination of criteria 1 and 2 with sufficient attack resistance could deter up to 80% of all amateur (vehicle recovered) thefts and 20% of the professional category. In each case, these percentages should be applied after subtracting those thefts effected when the key was left in the vehicle. The savings in the professional category accounts for those cases in which the car is stolen by small-time thieves and sold to the professional operation. The resulting savings are then separated 80%/20% between criteria 1 and 2 to account for an estimated 20% of drivers who will leave the system deactivated if they have the choice.
- Because many means of entry leave no visible evidence, it is not known how many stolen cars were left with unlocked doors. Thus, it is difficult to estimate savings which would result from improved entry protection. Ultimately a window can always be quickly broken. Thus it is estimated that the combination of criteria 3 and 4, at best, could result in saving 10% of the transportation category alone, with further separation of 80%/20% between criteria 3 and 4 to account for drivers who would leave the door unlocked if they had the choice.

TABLE 14. THEFT DETERRENCE RATING – FUNCTIONAL CRITERIA

Criterion	Estimated Potential Annual Savings or Benefit		Rating on a Relative Scale from 0 to 10
	Costs ($ billions)	Number of Thefts	
1. Mobilization – Protection	0.689	273,587	10
2. Mobilization – Passive Activation	0.172	68,396	2.5
3. Entry – Protection	0.049	28,613	1.0
4. Entry – Passive Activation	0.012	7,153	0.3
5. Number of Codes°	0.293	130,476	4.8
6. Anti-Key Retention	0.133	68,099	2.5
7. Key-Retention Warning	0.030	15,133	0.6
8. Mobilization Warning	0.034	13,679	0.5
9. Entry Warning	0.002	1,431	0.1

°Current benefit rather than savings since now in common practice.

- Criterion 5 is now in universal practice to a degree that is probably sufficient. Thus, its benefit must be estimated rather than savings. If there were a substantially fewer number of combinations, says 10 instead of 1000, there undoubtedly would be more thefts. It is questionable, however, whether anyone really wants to steal a car is deterred by the number of combinations. The relative importance, of course, increases as other methods are made more difficult. Thus, it is felt that a factor of 20% should be attached to this criterion for all classes except fraud to accurately represent its importance.
- Criterion 7 is now in universal practice, and available statistical evidence indicates that it has had little effect on the incidence of thefts by means of a key left in the vehicle. However, the variability in the data would allow the potential benefit to be of the order of 20% of the key thefts, so this value is assigned.
- Criterion 8 can only provide a portion of the benefit estimated for criterion 2. This portion is arbitrarily estimated at 20%. Likewise criterion 9 is estimated at 20% of criterion 4.

It is of interest, at this point, to rank the nine functional criteria in order of decreasing theft deterrence as shown in Table 15 before bringing in the more subjective judgment associated with consumer acceptability and cost.

It can be seen that the top six criteria, with the exception of anti-key retention, are implemented to some degree in current automobile design practice. However, the current method of passively activating the mobilization protection system requires that the driver remove the key. Thus, this would not satisfy a true passive activation criterion which is designed to ensure that the system is activated when the vehicle is left. Thus, this analysis suggests that significant

TABLE 15. FUNCTIONAL CRITERIA RANKED IN ORDER OF DECREASING THEFT DETERRENCE

Mobilization - Protection
Number of Codes
Mobilization - Passive Activation
Anti-Key Retention
Entry Protection
Key-Retention Warning
Mobilization Warning
Entry - Passive Activation Entry Warning

improvement in theft deterrence can be achieved by applying a functional criterion which leads to a system that automatically activates mobilization protection without driver option when the vehicle is parked.

The nine functional criteria can only be rated by arbitrary judgment for consumer acceptability. However, for purposes of this quantitative ranking task, this judgment has been expressed in terms of the relative ratings shown in Table 16. The rationale is as follows:

- Criterion 1 can be implemented in many ways which will cause no change or impact on the driver's habits. Thus, it is given the highest rating.
- Criterion 2 will likely require some change in habits for effective implementation, for example, the reinsertion of a code or a key that cannot be retained each time the vehicle is started or mobilized. In that sense, it is similar in effect to criterion 6, and both are given a relative rating of 5.
- Criterion 3 represents no change from current practice. Improved attack resistance, which will be rated later, may have an impact when the key is locked inside. A rating of 10 is assigned here.
- Criterion 4, however, will have a substantial effect on the consumer. He would have to unlock the doors each time he wished to reenter the vehicle after having closed the door. This would be expected to have a very low degree of consumer acceptability and is assigned a rating of 1.
- Criterion 5 has no impact on the consumer beyond current practice.
- Momentary warnings, such as required for criteria 7, 8, and 9, have little annoyance value to the driver. Criterion 7 is, of course, now in practice. They are all arbitrarily assigned a rating of 8.

In a similar fashion, these criteria can only be rated for their potential cost impact at this stage on the basis of engineering judgment concerning the relative costs likely to implement them. The ratings are shown in Table 17 and the rationale is as follows:

- Criterion 1, without any specification of attack resistance, will impose no cost burden beyond that now in practice. Thus, a rating of 10 is assigned.

TABLE 16. CONSUMER ACCEPTABILITY RATING – FUNCTIONAL CRITERIA

Criterion	Rating on a Relative Scale from 0 to 10
1. Mobilization – Protection	10
2. Mobilization – Passive Activation	5
3. Entry – Protection	10
4. Entry – Passive Activation	1
5. Number of Codes	10
6. Anti-Key Retention	5
7. Key-Retention Warning	8
8. Mobilization Warning	8
9. Entry Warning	8

TABLE 17. COST RATING – FUNCTIONAL CRITERIA

Criterion	Rating on a Relative Scale from 0 to 10
1. Mobilization – Protection	10
2. Mobilization – Passive Activation	6
3. Entry – Protection	10
4. Entry – Passive Activation	10
5. Number of Codes	10
6. Anti-Key Retention	8
7. Key-Retention Warning	10
8. Mobilization Warning	7
9. Entry Warning	7

- Criterion 2 depends upon the degree of automatic or passive activation used. However, measures beyond the current key activation when the engine is turned off will impose some cost penalty. A rating of 6 is assigned arbitrarily, because a means of activating energy will be required.
- Criterion 3 is in current practice and has been assigned a rating of 10.
- Criterion 4 could be implemented by minor changes in the door latch mechanism which would not be expected to significantly alter its cost.
- Criterion 5 is now in practice and will not impose any significant cost burden on any system which has been visualized.

- Criterion 6 would require minor cost increase in the lock cylinder, if a cylinder lock were used to achieve its objectives. If innovative systems are used to meet other criteria, the anti-key retention objectives are not likely to increase their complexity significantly. Thus, a rating of 8 has been assigned.
- Criterion 7 is now in practice and would not require additional costs.
- Criterion 8 and 9 would each require additional switches or circuitry to provide the warning signals, but these would not be high cost items. Ratings of 7 have been assigned because, it is predicted that the costs will fall between those for criteria 2 and 6.

The ranking of each of the functional criteria with respect to the three individual performance indices can be seen from Tables 15, 16, and 17. In general, the ratings could then be weighted as to importance and the weighted ratings added to give an overall rating. At this point, however, there is no rational basis for assigning relative weight among the three performance indices. Thus, the three ratings for each criterion have simply been added and tabulated in Table 18, where the criteria have been rearranged in the order of decreasing overall rating.

TABLE 18. OVERALL RATING – FUNCTIONAL CRITERIA
(Ranked in Decreasing Order)

Criteria		Overall Rating on a Relative Scale from 0 to 30
No.	Title	
1.	Mobilization – Protection	30
5.	Number of Codes	24.8
3.	Entry Protection	21
7.	Key-Retention Warning	18.6
6.	Anti-Key Retention	15.5
8.	Mobilization Warning	15.5
9.	Entry Warning	15.1
2.	Mobilization – Passive Activation	13.5
4.	Entry – Passive Activation	11.3

By comparing Tables 15 and 18, it can be seen that the addition of consumer acceptability and cost ratings have caused the mobilization-passive activation and the anti-key retention criteria to drop to a lower rank. In fact, now the top four criteria are represented in current design practice. This is not surprising since consumer acceptability and cost have been of primary concern in arriving at current practice.

It is important, however, to point out that if significant improvement in theft deterrence is to be achieved by functional criteria alone, this will require provisions for bringing about passive activation of the system, and/or preventing the retention of key or code in the system when the vehicle is left.

RANKING OF ATTACK RESISTANCE CRITERIA

In the previous discussion of the attack resistance class of performance criteria, it was concluded that the performance level of an anti-theft system could best be specified simply in terms of time-to-defeat. This is the basic measure of performance, and such a performance criterion would obviate the need for any other. Most important, it would impose no inherent design restriction on the type of system selected to meet the various functional criteria.

Time-to-defeat criteria can always be used by the individual designer as the design goal. However, their use as a basis for a performance standard suffers from the inherent problem that a test subject and data interpretation method must be specified. This problem may ultimately render an effective time-to-defeat criterion unacceptable as a basis for the safety standard.

If so, then attack resistance must be defined by several second-tier performance criteria which can, in general, include accessibility limitations, defined levels of conspicuousness, resistance to specific tools, defined levels of complexity, and possibly resistance to several specific attack methods not covered by the more general criteria. The use of these second-tier attack resistance criteria will undoubtedly prove to be more cumbersome and design-restrictive than the simpler time-to-defeat. However, because this approach may prove necessary, they will be rated comparatively for theft deterrence, consumer acceptability, and cost.

As noted in previous discussions, resistance to specific tools and defined system complexity are felt to be both overly design-restrictive and generally ineffective. Thus, criteria falling into these categories will not be considered further. The identified forms of the others are listed and defined as follows:

1. *Mobilization-Accessibility* — This type of criterion specifies that the decoder, latching mechanism, and associated hardware carrying the binary locking signal must be located in vehicle locations with specified limited accessibility. Possible alternatives include restricting these elements to locations other than the passenger compartment, to the engine compartment, or to the locations accessible only from underneath the vehicle.
2. *Entry-Accessibility* — This type of criterion limits the exposure of any binary element of the door latch system from outside the vehicle. However, to be practical, access by breaking the window glass would have to be excepted from the criterion. Likewise, the criterion would have to allow access by cutting or deforming the door panel or forcibly removing the lock cylinder or decoder.
3. *Conspicuousness-Visual* — This type of criterion imposes a specified level of visibility on any attack method feasible against the vulnerable elements of the mobilization protection system.
4. *Conspicuousness-Alarm* — This type of criterion specifies that a sensor screen (see Figure 2) be provided to sense illegal entry or attack on either the entry protection or mobilization protection systems and also control an aural or visual alarm.
5. *Tamper Detector* — This type of criterion specifies that the critical components of the mobilization protection system be designed in such a way that effective forcible attack result in disabling the system in the locked state. It is conceivable that this could either be achieved passively with suitable design or actively using a sensor screen and feedback system.

6. *Dual Codes* — This type of criterion requires the use of a mobilization protection code or combination which differs from that used on exterior entry protection systems. It is effective only where the latter uses conventional lock cylinders or other devices that can be decoded from outside the vehicle.
7. *Code Restrictions* — This type of criterion forbids certain combinations of code elements which are unusually vulnerable to decoding or lock forcing. They would be effective only in the case of conventional mechanical locks.
8. *Visible Codes* — This type of criterion prohibits the visible recording of a code on the vehicle.
9. *Power Restriction* — This type of criterion forbids the use of a system that requires an uninterrupted source of power or energy to remain locked.

These nine criteria are rated in Table 19 for their theft-deterrence potential with the aid of the data summarized in Tables 11 and 12. Reference is also made to the functional criteria ratings of Table 14. The rationale and judgment exercised in the process of estimating the potential savings or benefits are summarized as follows:

- If time-to-defeat cannot be used as an expressed criterion, then theft-deterrence can only result from criteria which are either designed to produce sufficient time for defeat or to reduce the allowable time. The two methods visualized for extending time-to-defeat are effective limits on accessibility for the vulnerable elements, or protection of accessible elements by an effective tamper detector which obviates all rapid methods of attack. Both of these general criteria, it is felt, can lead to effective methods of theft deterrence. It is estimated that up to 80% of all amateur thefts without the key could be deterred and 20% of the professional category. This figure is used in Table 19 for criteria 1 and 5, although even greater savings would likely be possible if the system were, in addition, passive.
- The functional entry protection criterion would require an accessibility criterion to achieve the level of theft deterrence assigned in Table 14. Thus, criterion 2 is given this same rating.
- Visual conspicuousness, without an alarm, is expected to deter some amateur thefts, but not a large percentage. A value of 10% of amateur thefts without a key is assigned to this criterion.
- Conspicuousness by an attention-producing alarm, it is felt, would be more effective. However, it is not believed that the consumer would ever accept a passive alarm. There is some evidence that alarms are activated by the driver less than 50% of the time and that they, in turn, only prevent theft in a fraction of cases when they are activated. Thus, 20% of amateur thefts without the key is used as our estimate of the deterrent value.
- The use of the door lock to determine the mobilization code is a known method of theft. However, purportedly, it is only in common use by professionals, and the universal use of dual codes will likely only force the professional to adopt another method to get the cars he desires. Thus, no deterrent value is assigned to criterion 6.
- Criterion 7 can have a small effect on amateur theft and a value of 10 was assigned to it.

TABLE 19. THEFT-DETERRENCE RATING — ATTACK-RESISTANCE CRITERIA

Criterion	Estimated Potential Annual Savings or Benefit: Costs ($ billions)	Number of Thefts	Rating on a Relative Scale from 0 to 10
1. Mobilization — Accessibility	0.689	273,587	10
2. Entry — Accessibility	0.049	28,613	1
3. Conspicuousness — Visual	0.095	48,070	1.8
4. Conspicuousness — Alarm	0.190	96,140	3.5
5. Tamper Detector	0.689	273,587	10
6. Dual Codes			0
7. Code Restrictions	0.095	48,070	1.8
8. Visible Codes°	0.095	48,070	1.8
9. Power Restriction°	0.095	48,070	1.8

°Current benefit rather than savings since now in common practice.

- Likewise, criterion 8, which is now essentially in universal use, likely inhibits some amateur thefts so a value of 10 was assigned to it.
- Finally, the requirement that the system be independent of a power source which is true for all existing systems forecloses anticipated methods of attack which, although cumbersome, might increase amateur theft. Thus, a value of 10 was assigned to this criterion.

Table 19 shows that the resulting ranking of attack resistance criteria for theft deterrence shows mobilization and tamper detection in a strong first place. Both are capable of imposing significant theft times. These are followed by the alarm criterion. The remainder of the attack resistance criteria are felt to have very low deterrent values.

Like the functional criteria, attack resistance criteria can be rated for consumer acceptability based on inherent inconvenience or change in driver habits that they would impose. Relative ratings have been assigned in Table 20 according to the following rationale.

- Criteria 1 can be implemented in many ways which would not have any impact on driver habits. It is even possible to obtain the benefits of effective accessibility requirements and use a key which appears identical to those now used. Thus, a value of 10 has been assigned.
- Criterion 2, however, is perceived as causing some driver inconvenience when the key is accidentally locked into the vehicle, because effective accessibility limits would preclude the current methods of entry without the key. Thus, a value of 5 has been assigned.
- Visual conspicuousness, criterion 3, has no real impact on the user and has been assigned a 10 rating.

TABLE 20. CONSUMER ACCEPTABILITY RATING — ATTACK RESISTANCE CRITERIA

Criterion	Rating on a Relative Scale from 0 to 10
1. Mobilization — Accessibility	10
2. Entry — Accessibility	5
3. Conspicuousness — Visual	10
4. Conspicuousness — Alarm	5
5. Tamper Detector	10
6. Dual Codes	7
7. Code Restrictions	10
8. Visible Codes	10
9. Power Restriction	10

- The alarm, however, is known to be an annoyance to the owner, especially when implemented in a passive or automatic fashion, and has been assigned a 5 rating.
- Criterion 5 can be implemented in ways which will be imperceptible to the driver, and thus is given a 10 rating.
- Criterion 6 is in use now by one major manufacturer and is known to cause some mild annoyance to the driver. However, this is not felt to be as unacceptable to the driver as criteria 2 and 4, so it has been assigned a 7 rating.
- The remaining criteria can all be implemented in ways which cause no perceivable effect on the driver. Thus, ratings of 10 were assigned.

Each of these criteria can be rated for cost impact through the use of engineering judgment concerning the likely complexity and cost of hardware required for their implementation. It is important to note that only increases in cost above that consistent with the current types of protective systems are considered in this judgment. The ratings are shown in Table 21 according to the following rationale:

- Criteria 1, 4, and 5 all imply the most complex level of additional equipment on the list. At this point, there is no basis to assume that there are relative differences among them, so a rating of 3 has been assigned in each case. Criteria 1 and 4 each require some type of central signal processor which presumably would be remote from the passenger compartment. In the case of criterion 1, signals would be transmitted to this unit from a code insertion device. In the case of criterion 4, signals would be transmitted from a sensor screen. If criterion 5 is implemented in an active way with sensors and a remote signal processor, it is entirely comparable to an alarm system. It is conceivable that it could be implemented passively; for example, as an added feature on the existing type of steering column lock. Although in this case it would likely be less costly, it would also be less effective,

TABLE 21. COST RATING – ATTACK RESISTANCE CRITERIA

Criterion	Rating on a Relative Scale from 0 to 10
1. Mobilization – Accessibility	3
2. Entry – Accessibility	8
3. Conspicuousness – Visual	10
4. Conspicuousness – Alarm	3
5. Tamper Detector	3
6. Dual Codes	10
7. Code Restrictions	10
8. Visible Codes	10
9. Power Restriction	10

being vulnerable to direct mechanical attack in the passenger compartment. In Table 21, it has been given the same rating as criteria 1 and 4 to be consistent with the potential theft-deterrence rating assigned in Table 19.

- Criterion 2 requires the addition of protective shields or the redesign of the door latch mechanism. This, it is felt, can be implemented with relatively little cost impact beyond current hardware so it has been assigned a value of 8.
- The remaining criteria can each be implemented with virtually no increase in complexity over the hardware now in common use, and thus have been assigned ratings of 10. For example, criterion 3 requires, at most, a configurational change, and this may be inherent in a relocation to obtain inaccessibility. Criterion 6 can be achieved merely by using the trunk or glovebox code for the doors as well. Criteria 7 and 8 are in common practice now and criterion 9 merely would impose some design restriction on the nature of any system designed to implement the mobilization protection function. It is, of course, in effect with the current types of steering column locks. It is also significant to note that a likely safety criterion applied to the design would restrict the use of a system that requires power to remain unlocked, assuming that the vehicle function locked is required for safe operation.

Combining the ratings for the three indices, as before, without the relative weighting, results in the ranked list of Table 22. While the numerical ratings here are somewhat arbitrary, the relative importance is felt to be significant. The conclusions are that, if the important time-to-defeat cannot be used as a performance criterion, the most important attack resistance criteria become limitations on the accessibility of the vulnerable elements of the system as covered by criteria 1 and 5. This is true in spite of inherently higher costs associated with these criteria. The next group members achieve their relatively high ratings by virtue of the fact that they are cheap and unobtrusive rather than effective. Finally, the last two are low on all three counts.

TABLE 22. OVERALL RATING – ATTACK RESISTANCE CRITERIA
(Ranked in Decreasing Order)

Criteria No.	Criteria Title	Overall Rating on a Relative Scale from 0 to 30
1.	Mobilization – Accessibility	23
5.	Tamper Detector	23
3.	Conspicuousness – Visual	21.8
7.	Code Restrictions	21.8
9.	Power Restriction	21.8
8.	Visible Codes	21.8
6.	Dual Codes	17
2.	Entry Accessibility	14
4.	Conspicuousness – Alarm	11.5

EFFECT OF THIEF ADAPTABILITY

The theft deterrence ratings of Tables 14 and 19 were based on estimates of the potential reduction in theft in terms of the current incidence of theft methods as determined in the vehicle theft survey of Chapter 3. However, it is very important to consider the adaptability of the thief, when designing a new anti-theft system which will see widespread application, or writing a new anti-theft standard. Recent history demonstrated that the widespread implementation of a very effective method for countering hot-wiring simply resulted in the adaptation of the thief population to different methods of attack.

If the ruling performance criterion is stated in terms of time-to-defeat — regardless of the method — then the designer must visualize every possible method of theft and design his system accordingly. If he overlooks some method of attack, then his system will not meet the criterion. However, if attack resistance is specified by some combination of the second-tier criteria, such as those listed in Table 19, then the situation is not so straightforward. Suppose, for example, that criterion 1 or criterion 5 is implemented very effectively and universally so that forcible attack on the decoder or latch mechanisms becomes much to time-consuming or conspicuous for the bulk of thieves. Then, the thief population would carefully scrutinize the system for another weakness. Now suppose, in addition, that conventional keys are still employed in a given system and the same code is used in the door lock as in the mobilization lock. In this case, it would be expected that the method known as door-lock impressioning (see Chapter 3) would come into much more widespread use than is currently the case. This would raise the relative importance of criterion 6 — dual codes — from that based on the current incidence of this type of theft.

This line of reasoning illustrates the importance of covering each significant type of attack with a deterrent criterion when using second-tier criteria. The net result is that both the system designer and the standard writer must visualize all of the general methods of attack and counter them with effective design goals or standard provisions.

It is interesting and significant to note that the time-to-defeat criterion does not place the burden on the standard-writer, only the designer. In payment for this burden, however, the designer is granted much less design restriction.

In quantitative terms, this means that, assuming one of the most deterrent criteria, such as attack resistance — criterion 1 or 5, has been implemented, those having a lower current deterrence will become much more important. This must be recognized by the standard writer if the resulting standard is to have more than a transient value.

SUMMARY

The discussion in this chapter shows that effective anti-theft system design requires that the anti-theft standard and design practice reflect two classes of performance criteria — functional and attack resistance.

The most important functional criteria, however, are already covered by the current standard (FMVSS No. 114) or are in current general practice. The only significant improvement in theft deterrence suggested by the analysis is a higher degree of passive or automatic activation of the mobilization lock, and this would carry a significant penalty in consumer resistance and cost.

It was shown generally that a time-to-defeat requirement is the most effective attack resistance criterion and that its use would effectively obviate the need for any other. It also would inherently impose the least design restriction of the attack resistance criteria.

However, it was recognized that practical problems of implementation may preclude the use of a time-to-defeat requirement in a revised safety standard. In this event, it would be necessary to specify attack resistance in terms of a number of second-tier criteria which impose limits on accessibility, levels of conspicuousness, and resistance to specific types of attack.

The most important of these second-tier criteria were found to be those specifying accessibility limitations or tamper protection. The first would place specific limits on the location of the decoding and latching functions of the mobilization protection system. The second would specify a design that requires a time-consuming repair or reset for any effective forcible attack on the system.

However, it was recognized that if such criteria were implemented, the thief would likely resort to one of several methods which are now rarely used. This would require additional criteria concerning the use of differing codes for doorlocks and mobilization locks, restrictions on certain combinations, restrictions on the visible recording of codes on the vehicle, and restriction to a system that requires no power source to remain locked.

When universally applied, it is predicted that a criterion which specifies limits on entry lock accessibility will have little theft-deterrent value. It does have high consumer acceptability and low cost.

Alarm systems, while providing moderate theft protection, will suffer from low consumer acceptability when automatically activated and also because of their high relative cost.

5. SYSTEM DESIGN

A major portion of the effort in this program has been devoted to the design and fabrication of an improved anti-theft system based upon the performance criteria identified in the earlier tasks. The design stage of this task is described in this chapter.

DESIGN GOALS AND SPECIFICATIONS

The first stage in the design process is the conceptual design. At the outset of this stage, it is necessary to identify the performance goals and specification, where possible, that the system is intended to satisfy. The performance criteria identified and ranked in the preceding chapter provide the basis for these goals and specifications. The designer must select and refine the particular set toward which he will design. This is accomplished, along with the addition of safety, cost, maintainability, and reliability goals in this section.

Functional

Based on the evaluation presented in Chapter 4, the important anti-theft functional performance goals selected for the improved system were as follows:

(1) *Mobilization — Protection* — The anti-theft system is to prevent at least one automobile function necessary for its self-mobilization, unless deactivated with the proper code;

(2) *Number of Codes* — The system is to be capable of being coded with at least 1,000 different combinations;

(3) *Entry Protection* — The system is to incorporate locks requiring the proper code or key on all entry points, including the engine compartment hood;

(4) *Anti-Key Retention* — The system is to incorporate a design feature that will ensure that the driver will not leave the mobilization protection system deactivated; and

(5) *Passive Activation* — The system is to incorporate a design feature that will ensure that the mobilization protection function will be activated when the driver leaves the vehicle.

Goals (4) and (5) were selected as desirable design goals, even though they were ranked below the various warning features in the ranking of Table 18. This selection was based upon the theft deterrence ranking of Table 15, and the fact that the purpose of this design is to produce an *improved* anti-theft system. The only *functional* improvements of any importance are visualized to be anti-key retention and passive activation features.

Attack Resistance

The fundamental attack resistance goal to be satisfied by the improved anti-theft system is that it be capable of resisting forcible deactivation for at least 10 minutes. However, this has been translated into a design approach as follows:

(1) *Mobilization* — The vulnerable elements of the mobilization protection system will be contained either in a secure housing located in the engine compartment in a

Preceding page blank

relatively inaccessible place such that all conceivable methods of attack will take at least 10 minutes; or the mobilization protection system will incorporate a tamper detector which will cause the system to disable in the locked state when forcibly attacked in such a way that a 10-minute restoring period is ensured.

(2) *Entry* — The vulnerable elements in the entry protection system will not be accessible from outside the vehicle except by breaking the window, cutting or deforming the door panel, or forcibly extracting the doorlock cylinder.

(3) *Conspicuousness* — The mobilization protection system will be arranged such that the action of the thief will be visible for effective methods of attack.

(4) *Codes* — The system will be capable of codes which will effectively preclude trial-and-error and the decoding of the door-lock combination to obtain the mobilization combination. The code will not be marked on the vehicle.

(5) *Power restriction* — The system will not require any power source to remain in its locked state.

It can be seen that this list of design goals effectively incorporates all of the first eight ranked criteria of Table 22. It was felt worthwhile to include an entry accessibility goal, despite its poor overall rating, in order to benefit from the design experience and testing on the prototype system.

Safety

(1) When the vehicle is in motion, the system will be designed to prevent the inadvertent activation of a lock on any vehicle function which could compromise safety.

(2) The system will not require the reinsertion of a code, or code insertion device, in order to restart a stalled engine.

(3) The entry locks will be capable of being manually unlocked from inside the vehicle.

Cost

The design of the system will be consistent with an increase in consumer price of $50 or less in very large production quantities. This is well within the anticipated cost savings which can result as determined by the theft survey, even if less than half the number of current thefts is deterred.

Maintainability

The design of the system will be consistent with disassembly, part replacement, and reassembly in a time period of about one hour. This is comparable to the servicing times for current designs. The possible requirement that the vehicle be towed to a service facility in the case of an unsuccessful attack is felt to be a reasonable tradeoff, in view of the fact that the owner would still have his or her vehicle.

Reliability

After development, the design of the system will be consistent for high-volume production, with reliability levels comparable to those of existing automotive mechanisms and electrical components.

Conceptual Design

Following the selection of the general design goals, the next step was the identification of design concepts and a preliminary screening to determine the most promising. Because of the preoccupation of the American public with the automobile, the sharp increase in vehicle theft in recent years, and the Yankee ingenuity of Americans, there are a vast number of existing and proposed anti-theft concepts in circulation. For those actively involved in the anti-theft problem, barely a week goes by without the appearance of a "new" device or system description.

As noted in Chapter 3, the great majority of these systems involve combinations of alarms, ignition shut-off switches, fuel shut-off valves, and additional locking devices. Many of these systems would suffer greatly in effectiveness, were they to become factory equipment and well-known and understood by the potential thief. However, many ideas generated in the past have potential for application in effective factory-installed anti-theft systems.

The approach taken for the conceptual design task followed the generalized anti-theft system described in Chapter 4. Various means of accomplishing each of the major component functions of Figure 2 were generated. For this purpose, sessions were organized that included specialists in a variety of technical disciplines. The identified concepts, along with those provided by previous investigators and designers, were than classified morphologically and are discussed in this report in the context of this classification. This approach helps to avoid overlooking promising concepts or classes of concepts. It also provides some economy in selecting the most promising or appropriate classes of concept for further more detailed evaluation and preliminary design.

Mobilization Protection Concepts

Table 23 lists morphologically all of the mobilization protection concepts identified. The concepts are organized according to function (code insertion, decoding, latching, vehicle function locked) and the principal energy or signal transmission medium. In general, one could employ various cross-combinations of concepts to accomplish the four functions. However, code insertion and decoding must be considered together since these elements are inherently mated. Moreover, the optimum latch is primarily determined by the vehicle function to be locked.

These concepts are discussed briefly in this section to evaluate their promise in general and to screen out those obviously unsuitable for the test system to be constructed in this program. The more promising concepts are then evaluated in more detail in the next section.

Vehicle Functions

As listed in Table 23, virtually any vehicle function critical to the operation of the vehicle is a candidate for the protection system. Control of the ignition primary is traditional and offers a convenient method of accomplishing the engine activation and deactivation requirements embodied in the current standard. Ignition timing could also be locked in a condition which would preclude engine operation, but this would not be a desirable way to shut off the engine, since unfavorable combustion conditions would occur as the engine shut down and damage could result.

Another family of engine functions that could be used, either in addition to or instead of ignition primary switching, include the interruption of air, fuel, or mixture flow to the engine. These methods, in general, would be implemented with a valve. Depending upon where it is

TABLE 23

MATRIX OF MOBILIZATION PROTECTION CONCEPTS

Functions / Media	Code Insertion	Decoder	Latch	Vehicle Function Locked
Mechanical	Conventional Key Improvements Medeco Lock Ace Lock Keso Lock Bura Lock Strengthening against Removal Armoring the Housing Button Combination Lock Dial Combination Lock	Lock Cylinder	Bolt Switch	Brakes Steering Shift Lever Transmission Ignition Primary Ignition Timing Fuel Flow Mixture Flow Air Flow Starting Motor ↓
Pneumatic	Conventional Key Keyboard	Pneumatic Cylinder Fluidic Logic	Bolt Switch	↓
Hydraulic	Conventional Key Keyboard Electrical Keyboard	Hydraulic Cylinder Rotary Spool Valve (Electro-mechanical)	Bolt Switch Combined with Decoder	↓
Electrical	Magnetic Key Passive Electrical Key Active Electronic Key Keyboard	Magnetic Circuit Remote Electronic Circuit	Solenoid Relay ↓	↓
Optical	Punched Hole Key Conventional Key (Tritsch Patent) Character Recognition Fingerprint Recognition	Remote Electronic Circuit ↓	↓	↓
Acoustic	Voice Recognition Tone Burst	↓	↓	↓

accomplished, fuel flow interruption is vulnerable to the substitution of an alternative supply by the thief. Ultimately, this might force him to replace the carburetor. Mixture or airflow can be interrupted by a gate or plate valve incorporated into the intake manifold, and this concept could result in an extremely effective mobilization protection system. However, for purposes of a retrofitted test system, it is not promising because it would involve an external, and thus vulnerable, valve which would alter the flow geometry in the critical intake flow path.

Another approach to the interruption of mixture flow could be implemented by deactivating the valves already present in the engine. Such a scheme has been proposed for achieving a variable displacement engine[38]. Solenoid actuators are used to activate or deactivate cylinders in response to load demand. This type of system could be used for anti-theft protection if it were already installed in a vehicle for achieving fuel economy. However, it would be far too costly for anti-theft alone.

In principle, either the service or parking brake system could be locked by the anti-theft system. However, conventional parking brake linkages and hydraulic brake lines are vulnerable to being cut by the thief. Moreover, in the case of the service brake system, effective attack by a thief is likely to produce a number of vehicles on the road being operated without brakes, thus creating a safety hazard.

Steering is the currently conventional second locking function and it remains a strong contender. It can be effectively accomplished by a latch or bolt at any point ahead of the pitman arm or output of the steering box. Beyond this point the linkages are vulnerable to mechanical attack. Moreover, the force levels which a thief can apply with the steering wheel are very high on the output shaft and linkages making locking very difficult.

The shift lever is currently used as an interlock on the steering column lock. However, the linkages can be disconnected and the transmission manually shifted to drive within the engine compartment. With increased protection of the linkages or a floor shifter, this method could be used as an effective locking system.

Even more promising, however, is the transmission itself. Locking, along with decoding, can be accomplished within the transmission casing. Two general concepts are the use of the current "PARK" interlock used to lock the rear wheels, or the addition of a hydraulic by-pass valve which could interrupt torque transmission when the system was activated.

Locking the operation of the starting motor is an effective anti-theft concept for a vehicle with an automatic transmission. This is currently being implemented in well over 90% of U.S. automobiles in production.

In summary, in addition to ignition primary, the most effective mobilization protection concepts include the locking of steering, transmission output motion, torque transmission, or mixture/air flow. All of these are also candidates for the test system to be constructed in this program, although mixture/air flow valving is somewhat inconvenient to implement as a retrofit system since it involves a custom inlet mainfold. Likewise, modifications within the automatic transmission would involve envelope restrictions and difficulties as retrofit concepts which would not be the case for original equipment.

Code Insertion and Decoding Concepts

The baseline mechanical code/decode system is, of course, the conventional key and lock cylinder and it must remain as a promising device due to its simplicity, low-cost, and user familiarity. Its major vulnerabilities — removal and picking — can be decreased somewhat and more detailed discussion of concepts for these purposes will be presented in succeeding sections of this report. However, its basic disadvantage, the proximity of the decoder to the code insertion point is inherent. This proximity means that a thief can use mechanical attack on the housing to get to the functions which are protected by the lock while in the passenger compartment.

Table 23 shows that virtually every media offers the possibility of an analog to the conventional removable key and an analog to the combination lock; i.e., a keyboard system. There is a basic design trade-off question between the use of a removable key, on the one hand, with a proven user acceptability, and a keyboard which precludes the key being left in the vehicle, and thus prevents some 13.5% of current thefts.

Of course, other methods can be used to prevent leaving the key in the vehicle. Also, the use of remote — and thus less accessible — decoding can be accomplished with any one of many removable key concepts. Thus, the selection between key and keyboard should be left to each designer or manufacturer, provided the system meets minimum functional and performance requirements.

The use of conventional mechanical combination locks for this application has questionable merit. This type of lock, typically, is considerably more costly than a key lock. Moreover, the decoder remains in close proximity to the code insertion location and, thus, is vulnerable to direct attack or removal.

Pneumatic code signal insertion and decoding are technologically feasible. In an automobile, such a procedure would typically make use of the manifold vacuum as the energy source in a fashion similar to the many other control functions now performed in this fashion in the automobile. However, since the engine is off when the system is being deactivated, a vacuum storage device would be inherently required and this could prove unreliable due to potential leaks. Moreover, the fluidic logic — to provide 1000 combinations — would require many switches since these combinations typically are binary. Thus, the device would require the development of multilevel resolvers, or require a large number of simple switches, and this would be considerably more complex than the current air conditioning and ventilation control system. The hydraulic analog would be similarly complex with the added disadvantage that there is no source of hydraulic energy at non-atmospheric pressure convenient for code signal transmission.

However, an electro-hydraulic system in which the end function locked is the flow of pressurization of the hydraulic fluid in the transmission remains a promising concept.

Various electrical, electronic, or magnetic removable keys have been identified as promising methods for coding an "unpickable" or remote decoder. The following list does not pretend to exhaust all possibilities, but provides a representative sampling:

- Conventional key with several magnetized buttons which operate bistable tumblers in the mating lock cylinder;

- Plastic laminate key card which contains a recorded permanent magnet code which is "read" by the decoder, much as the tape is read by a recorder;
- Conventional key or plastic card containing coded spots of magnetically permeable or electrically conducting material which complete magnetic or electrical circuits in the decoder, respectively;
- Key or card containing resistive, capacitive, or inductive elements which complete a circuit in the decoder to inactivate the system;
- Active electronic key circuit which transmits a signal to a remote receiver, thereby avoiding a key slot or location for tampering.

All of these components are feasible and can provide convenient coding for an anti-theft system. Most of them are inherently more costly than a conventional key, but they offer the advantage that electrical signals can be more easily transmitted to a remote decoder than can mechanical signals.

However, the alternative code-insertion device is the electrical keyboard which, of course, precludes the leaving of the key in the vehicle. Since keyboards are now being used in great quantity for a wide variety of consumer products, such as calculators and even in automotive applications, they are available at low cost. A keyboard system with a remote decoding circuit in an inaccessible location at the point where the vehicle function locking is performed is perhaps the most straightforward low-cost concept capable of easily being retrofitted to an existing test vehicle.

Various optical coding and decoding concepts have been proposed. They include:

- A plastic card punched with a coded hole pattern that is read by masked photocells;
- A decoder which incorporates "tumblers" that respond to a conventional key to produce coded light paths that are then transduced to a coded electrical signal and decoded remotely (Tritsch, U.S. Patent No. 3,639,906);
- Signature or fingerprint recognition systems which would allow vehicle operation only by authorized users.

All of these concepts are inherently more costly than their electrical counterparts and, in general, do not appear to offer any basic advantages. Signature or fingerprint recognition is a developing technology which is probably not ready for automotive application. It also makes multi-user operation difficult, unless the required computer contains sufficient memory for storing the required number of different characters.

The same comments can be applied to voice recognition systems. Tone burst coding could conceivably be used to activate a remote decoder, but there is no good reason to use it in this application. Its primary advantage lies in the remote keying of devices through a voice transmission path, such as a telephone line or a radio link. For this application, the code-insertion device can use multi-conductor cables or simple unmodulated pulse sequences to actuate a remote decoder.

Sensor Screen Concepts

The sensor screen class of anti-theft concepts contains systems which sense the incursion of a thief into the automobile or his tampering with the main mobilization protection system. The system then either sounds an alarm or operates on the protection system to render the attack fruitless, or both. Table 24 lists the various identified concepts for this purpose morphologically.

Alarm systems form the best-known class of sensor screens and, thus, deserve major discussion at this point. The major component in the alarm system is the processor which is a simple circuit designed to respond to the closing of any one of several switches and turn on an alarm, such as a siren, bell, or the vehicle's horn. Usually two time delays are provided, one to allow the operator to get out of the vehicle after activating the system without setting it off, and another to allow him to shut it off after he reenters the vehicle. Often, the alarm, itself, is placed on a timer so that it ceases and resets after a period of several minutes.

Specific alarm circuits will not be described in this report. They are well developed and covered in the popular electronic literature[39,40] and many variations and improvements are possible, limited only by the ingenuity of the designer.

For purposes of this program, however, several factors of importance should be mentioned:

- Unless the alarm system feeds back to lock out critical functions, it is inherently incapable of delaying a theft itself. It only makes the theft more conspicuous. In a remote or unpatrolled area, the thief can steal the car and ignore the alarm until he gets to a safe location.
- Unless the engine compartment is locked or the alarm sounding device is placed in an inaccessible location, the thief can use the time delay provided to disable the sounding device and then proceed with the theft as if the system were not there.
- Although a tilt-switch alarm is the only known method to effectively protect a vehicle against theft by towing, it suffers from a major weakness due to the ease with which it can be set off. The thief merely sets it off repeatedly until the owner leaves it shut off. The thief then steals the vehicle in normal fashion.
- Tilt switch and other alarms are already causing significant annoyance in densely populated areas. This could be expected to become prohibitive if all cars had alarm systems.
- The retail cost of effective alarm systems now ranges between $50 and $150. Produced in volume sufficient for installation in every car, the manufacturing cost would undoubtedly drop, but it is questionable whether it would be low enough, when combined with that of improved basic protection systems, to meet the $50 price goal for this program.

In general, it may be concluded that the marketplace has probably already selected the appropriate application for alarm systems — additional protection for the individual owner who desires it and finds its cost acceptable. Moreover, as more and more alarms are installed, it is likely that local restrictions will be applied concerning tilt-switch actuation, acceptable sound levels, and shut-off time limits.

TABLE 24

MATRIX OF SENSOR SCREEN CONCEPTS

Media \ Function	Sensor	Processor	Feedback	Alarm
Mechanical	Presence of Lock Cylinder	None	1. Freezes the Normal Lock Mechanism 2. Opens the Mechanical Connection & Covers Access Hole	None Required
Electrical	Door & Entry Switches Switch to Sense Presence of Lock Cylinder Tilt Switches	Alarm Switching Processor	Can be Used to Lock Out Critical Vehicle Functions	Usually Vehicle Horn or a Siren Can be Flashing Lights
Optical	Photoelectric Cells to Sense Incursion or Thief's Presence			
Acoustic	Ultrasonic Source & Sensors Detect Thief's Presence			
Hydraulic	Pressure Switch Senses Presence of Lock Cylinder	None Required	Opens Starting Motor Circuit or Other Critical Circuit	None Required

Optical and acoustic sensors are commonly applied in area security systems where there are a large number of possible incursion paths and switching would be expensive. In the case of an automobile, there are typically only six entries of interest and four of these already have usable switches. Thus, there is little advantage to these concepts which are inherently more costly.

The other major classes of sensor screen concepts are those in which tampering with the main protective system is sensed rather than vehicle entry. The class of mechanical concepts designed to respond to the forced removal of a lock cylinder to ensure that this action does the thief no good is one of the most promising methods of improving the current steering column lock. However, it carries with it the necessity of improving the resistance of most lock cylinders to picking. Both of these subjects will be covered in more detail in a succeeding section.

An electrical sensor could also be placed in the steering column lock to detect the forced removal of the lock cylinder, but the knowledgable thief would likely be able to readily by-pass such protection, unless the latching device were buried in an extremely inaccessible location. In this case, a sophisticated device is being applied only to guard against one form of attack. It would appear to be fundamentally more advantageous to couple this latching device to an effective code-insertion and decoding system and use it as the main mobilization protection system.

Another type of sensor that has been proposed to sense forced removal of a lock cylinder is a closed pressurized hydraulic line which holds closed a pressure switch in the starter primary circuit. When the lock cylinder is removed, the fluid begins to leak, thereby disabling the starter. This system can be simply defeated by the thief who alters the order of attack steps. He can first wire the ignition and starter circuits to start the engine and then extract the steering column lock cylinder to allow steering and shifting.

Entry Protection Concepts

When studying current door lock designs, it is difficult to avoid the conclusion that they have been designed for rapid entry in the event that the owner inadvertently locks his keys in the car. This, of course, produces no penalty, time delay, or otherwise on the thief. However, the vehicle theft survey indicated that the door entry phase can be an effective theft deterrent. The thief feels exposed and vulnerable to detection during this phase and will readily abandon the theft if he encounters any significant difficulty. Of course, if all cars had effective door lock systems, the delay imposed would inherently never exceed the time it takes to break the window. It is important to note that this act in itself is conspicuous and would lead to detection in many cases, either at the site or by alert police patrols.

It is possible to conceive very elaborate entry protection concepts combining effective main protection systems and sophisticated sensor screens to detect tampering. For example, if the main mobilization protection system incorporates an electrical code insertion device and a remote decoder, the code insertion device (key or keyboard) entry can be on the outside of the vehicle. Then, the decoder would not only inactivate the mobilization protection device, but unlock the doors by means of solenoid-operated latches or bolts. A system of this type is well-within the current state-of-the-art. Since the code insertion would be electrical, mechanical attack on the code insertion point would be ineffective. The thief would then be outside the vehicle with no means of entry, if the doorlatches were well-protected, unless he broke a window. If he did so, he could then enter the car, but would have no way to mobilize it. Presumably, the decoder would be located in an engine compartment which is also protected by a latch operated by the decoder. Thus, attack on the decoder would require forcing the hood lock and then performing extensive (i.e., 10 minutes or greater) disassembly under the hood. A separate means of operating the hood latch would be required to access the decoder for repair if it should fail, but this could be made time-consuming and to require a lift.

This type of centralized entry protection system where entry protection and mobilization protection are unified into one overall system, although currently feasible, may be considered a likely direction for security system design in the future. Certainly, electric door locks will be required and this is now an option found only on the more expensive models.

Table 25 lists identified door lock concepts in several basic groups. In the vehicle theft survey, we determined that current door lock systems have three primary vulnerabilities:

- The mechanism inside the door is vulnerable to actuation by means of tools inserted between the glass and window frame;
- The inside lock release devices can be actuated by means of tools inserted between the window and its frame or gasket seal, or through the opening created by prying the door slightly;
- Vent window latches can be readily forced through the crack at the edge of the window or broken.

Thus, in addition to basic changes in the method of code insertion and decoding for the door lock system, the important concept classes are the introduction of barriers to prevent attack on the locking linkages, modification of interior lock releases, and modification of the basic lock linkage system.

Probably, the most effective concept of the latter type would involve the relocation of the lock and latching mechanism to the door-post from the door. The only access would then be by removal of the lock cylinder.

Interior door lock releases are an inherent vulnerability. For safety reasons, the passengers must always be able to unlock and open the doors from the inside. However, the use of round knobs, relocation of the release to a shielded location, or the elimination of the release button or lever and the shielding of the interior handle can all be used to place a significant time penalty on the thief who is not willing to break a window.

For this program, where an existing vehicle will be modified for test, the most promising concepts are to replace the interior lock releases with devices that are difficult to operate with a wire or blade from outside and to shield the interior linkages from actuation through the window frame.

TABLE 25

MATRIX OF DOOR LOCK CONCEPTS

Concept Class	Concept	Remarks
General	Eliminate Vent Windows	Too Easy to Force without Breaking Glass
Modification of Interior Lock Releases	1. Flush Door Buttons	Can only be used on two door models because rear doors cannot be allowed to open with door handles to ensure child safety. Requires shielding interior door handle.
	2. No Lock Release – Automatic or Key Locking	Same as above – Key locking undesirable because owner will not take time to do it.
	3. Tapered Buttons	Difficult, but not impossible, to raise from outside.
	4. Rotary Lock Release with Round Knob	Very difficult to operate from outside.
Modification of Lock Linkages	1. Put the Entire Mechanism in the Door Post	Provides least access from outside for attack.
	2. Design Unlocking Mechanism to be Rotary Rather than Linear	Makes operation by pushing or pulling through window frame impossible.
	3. Design Unlocking Linkages to Come Apart when Pushed or Pulled	Possible for connecting links between interior release & door latch. However, door latch itself would still require enclosure.
"Slim-Jim" Barriers	1. Seal Bottom of Window against Outer Sill	Earlier window designs where window was supported in a metal channel across entire bottom edge essentially achieved this. The newer window mechanisms eliminated this advantage.
	2. Enclose Unlocking Linkage & the Latch Assembly so that it cannot be Reached on the outside of the Glass	Appears to be generally possible using sheet metal baffles, even with current mechanism design.
Code Insertion/Decoder Modifications	1. Combination Locks	These are generally more difficult to pick but would have low user acceptability – pushbotton types most practical.
	2. Pick-Resistant Lock Cylinders	There are many types of cylinders that are virtually impossible to pick. This method will become more important as the rest of the system is improved.
	3. Strengthen Cylinder against Forcible Removal	In the case of door locks this can be effectively accomplished by spreading the load out over a large area on the door panel. Several manufacturers now report changes in this direction. The weak point then becomes the inner barrel of the cylinder.
	4. Electrical Code Insertion with Remote Decoder & Electric Door Locks	Can be integrated with the mobilization protection system – only effective attack would be electrical attack on the solenoid and this should be easily protected (for example by potting connections & leads).
Sensor Screens	1. Wire in Window Glass – Either Sounds Alarm or Locks out Electrical Mobilization of Entry Protection Systems	Only Concept which can effectively resist window breaking.
	2. Tamper Detector on Door Lock Cylinder	If interior button attack, "Slim-Jim" attack, and lock picking are eliminated, the only way the entry locks can be breached is by attacking the lock cylinder. This can be sensed by switches which would sound alarm or lock out the protection systems.

Code Insertion and Decoding

The preliminary screening of the preceding section identified two promising classes of code insertion/decoding systems:

- The non-remote decoder using a conventional key and protected by a sensor screen to prevent attack; and
- The remote decoder using a conventional key or keyboard and located, along with the latching mechanism, such that access by a thief will require excessive time delay.

Both of these classes are felt to be feasible and potentially effective. In the following subsections, they are discussed in more detail to provide a basis for the selection of the test system for this program.

Conventional Mechanical Key System

The basic characteristic of the conventional key/lock cylinder system is that, unless complex mechanical signal transmission devices are used between the code-insertion point and the decoding cylinder, the cylinder must be located at a point which is accessible from the passenger compartment.

Thus, for theft resistance, the design strategy becomes one of protecting the decoder output or latching mechanism from attack and making the lock cylinder unpickable within reasonable time periods.

Two types of forcible attack on the lock cylinder have been prevalent — torsional failure of the tumblers and forcible extraction of the entire cylinder or its central plug.

Torsional failure can be prevented by strengthening the tumblers, providing disk tumblers, or by locking the cylinder barrel with a side-bar. In principle, it is only necessary to provide sufficient shear area to resist the maximum torque that can be applied by a key or key-like element that will fit into the key slot. This should always be possible with appropriate design.

Although forcible extraction of the cylinder can be deterred for significant periods of time by strengthening the means of retention, no such effort has extended the slide-hammer method beyond 10 minutes, to this author's knowledge. While this might be possible using extraordinary measures, such as assembling the lock cylinder from the inside behind a hardened insert in the steering column casting, it would require substantial experimental development with test housings using various extraction tools. This is beyond the scope of this design program.

Another method of deterring extraction is the use of a design which senses extraction and responds by rendering the internal mechanism inoperative or inaccessible. This is discussed later in this section under Sensor Screen Concepts.

All of these methods would require strengthening of the steering column housing in areas where direct cutting attack could expose the protective devices or the locking mechanism.

Assuming that a combination of these measures is capable of extending the defeat time beyond 10 minutes, the critical weakness then becomes pick resistance. Although most automobile thieves do not now pick locks, it should be expected that this will become an important method of attack if all others are foreclosed. Appendix E illustrates the method of picking the simple pin-tumbler lock and describes a number of pick-resistant locks. The conclusion reached is that, with moderate cost increase, lock-picking can likely be made sufficiently time-consuming to satisfy the performance criteria. However, an improved key lock system should not make use of the simple pin-tumbler lock.

Remote Electronic Decoding

The remote electronic decoder can be coded by a removable key with an appropriate transducer and transmitter located at the point of code insertion (usually the passenger compartment) or by a keyboard. For purposes of this program, the keyboard concept is felt to be the optimum system because it offers the following advantages:

- It eliminates the need for providing a mechanism that ensures that the removable key is not left in the system, and
- It eliminates the need to develop a transducer to read a conventional key or to use relatively expensive card or tape-reading devices.

Low-cost keyboards are currently available on the market which, in large-volume production typical for automobile applications, would cost less than $1.00.

The keyboard concept requires two basic electronic circuits: a transmitter at the keyboard location, and a receiver/driver to perform the decoding function at the remote location and to drive the latching mechanism.

If a keyboard system is to conveniently replace the current type of key lock, it should also incorporate the following subsidiary functions:

- it should complete the primary ignition circuit for the vehicle, when coded, and should provide a switch for turning off the engine;
- it should complete the starter circuit, when coded, and provide a switch for starting the engine; and
- it must contain an interlock to prevent the inadvertent locking of a critical vehicle function while the vehicle is in motion.

A block diagram of a remote electronic decoder and keyboard system to perform these functions is shown in Figure 3. In this diagram, a door switch is shown as a convenient method for interlocking the function lock. In this case, the driver must sequentially shut off the engine and open the door before the function lock actuates.

Selection

While both the preceding concepts are capable of meeting the functional design goals and can, it is felt, be designed to meet the theft-resistance goals, the mechanical concept would require considerable modification to the existing steering column lock. Not only would the

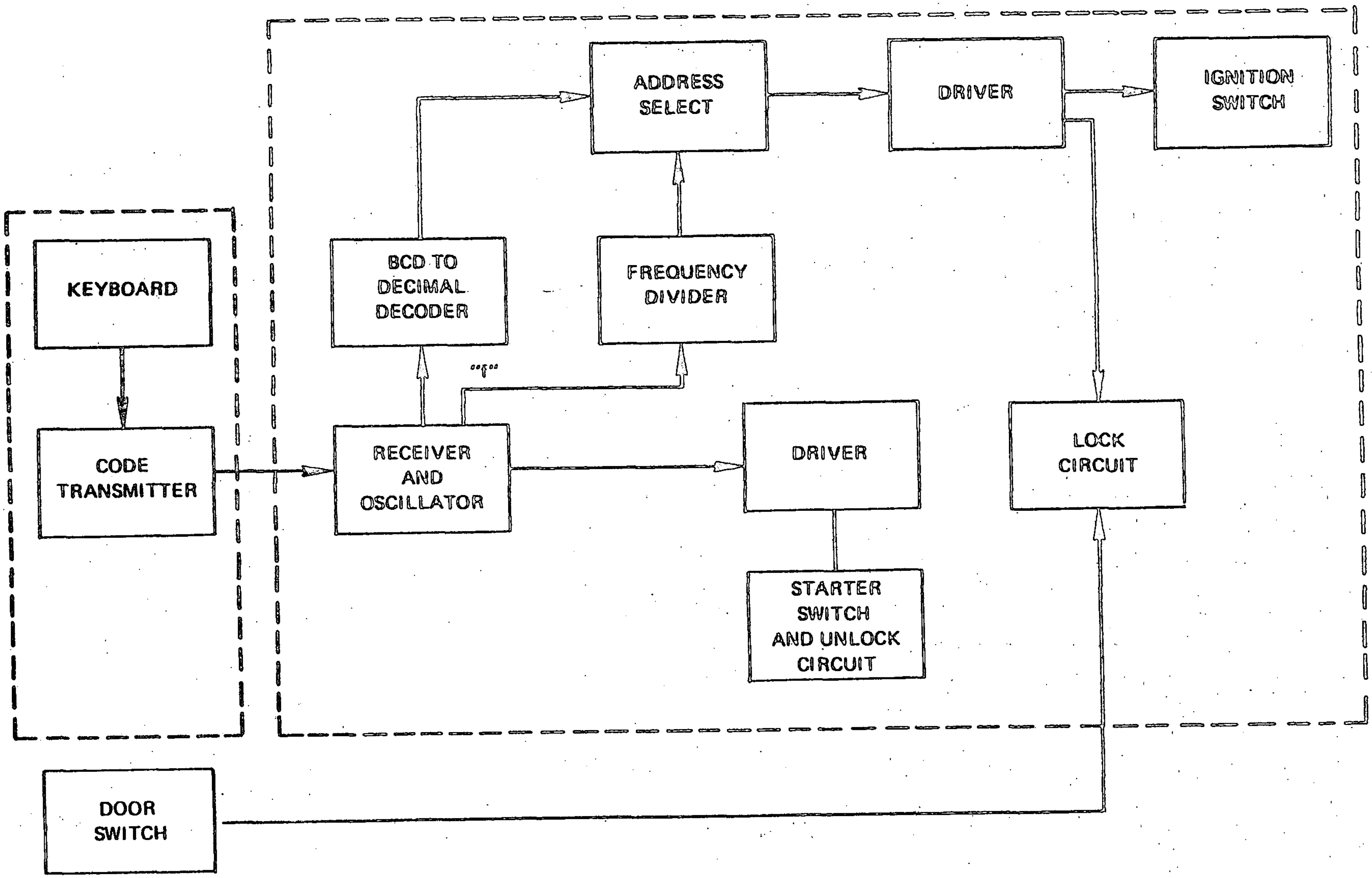


FIGURE 3. BLOCK DIAGRAM OF KEYBOARD/ELECTRONIC DECODER SYSTEM.

housing require strengthening, but a protective sensor screen mechanism would likely have to be added within the current envelope and the lock cylinder would have to be replaced by a pick-resistant lock. This degree of modification makes retrofitting the system to an existing vehicle difficult and its success at meeting the defeat time requirement questionable. To be confident of the latter, the designer should redesign the entire system with that goal in mind.

The electronic system, on the other hand, can be easily retrofitted to an existing vehicle and its defeat time made arbitrarily long simply by selecting the optimum remote vehicle function to be latched and providing the required hardened enclosure and disassembly difficulty.

Thus, for the purposes of this program, the optimum code insertion/decoding system is felt to be the keyboard electronic system operating on any one of several critical vehicle functions as the secondary protective means.

Vehicle Function and Latch Design

As described previously, there are several promising critical vehicle functions for mobilization protection available if a remote decoder/latch system is used. For the purpose of a test system in this program, these are evaluated as follows:

Mixture Flow Valve

While this function remains promising for a production design, it would require considerable modification of the intake manifold for retrofit to an existing vehicle. If it were incorporated into the carburetor, it would be vulnerable to simple replacement of the carburetor, possibly within the 10-minute time goal.

Transmission Function

Two promising methods of implementing this function exist. The first would be an electromechanical device to prevent taking the vehicle out of "PARK," unless the correct code had been inserted. This could easily be incorporated in a new transmission design and is only limited by the available space in most existing designs.

The second method is the interruption of hydraulic flow in the torque converter or bypassing the flow of the pump to prevent the required pressure level. The valve would be controlled by a decoder. The first of these options has been reduced to practice in a development model using an electromechanical decoder.[43] In this system, a stepping motor, controlled by a keyboard and electronic logic circuit, sequentially positions a rotary valve until its ports are aligned and flow can occur.

However, the concept requires the use of a decoder which can survive in the transmission environment which can reach 300°F temperature levels. Thus, a mechanical decoder, in this case incorporated in the valve design, is required. An electronic decoder is typically not capable of surviving these temperatures. Thus, it would require packaging in a cool, but still secure, location where no access would be provided to the signal which operates the transmission valve.

For this reason, the use of transmission function as the protected system is not felt to be promising in combination with an electronic decoder for the test system in this program.

Starting Motor

An extremely simple mobilization protection system is conceptually possible by using the electronic decoder to interrupt the starting motor circuit unless the correct code has been inserted. However, the temperatures that result in the starting motor housing after protracted cranking has occurred (for example, if the engine has been difficult to start) would exceed the survivability limit of the electronic circuit.

Thus, the feasibility of the concept would require packaging of the electronics in a separate location connected electrically to the starting motor by a secure path. While this might be easily provided in an original design (for example, from the flywheel housing), it would be extremely difficult as a retrofit design.

Steering

The steering gearbox itself can be locked at its input shaft by a device conceptually similar to that commonly used on the other end of the steering column, but operated by a remote electronic decoder enclosed with the lock.

In a production system, this would be incorporated into the gear-box housing which is strong enough to resist direct attack. Its location in the engine compartment, which can be locked, is generally awkward, and the design of the gearbox mounting can be arranged to preclude substitution within the specified time period.

Finally, the temperature of the steering gearbox remains close to ambient. Thus the electronic package can be included in the housing for maximum security.

A preliminary design for a steering lock of this type that can be retrofitted to an existing vehicle is shown in Figure 4. The housing would mate with a collar welded onto the existing steering gearbox. A notched wheel surface would be added to the steering column lower universal joint. This notched wheel could be locked by a pawl which is actuated positively in both directions by solenoids controlled hy the enclosed electronic decoder circuitry.

The pawl, when locked into engagement with the notched wheel, could prevent withdrawal toward the left of the housing, even though the housing bolts were removed. The dowel pin would prevent rotation of the housing when the housing bolts were removed, if it were withdrawn. Thus, the lock could be readily disassembled for adjustment of the steering box bearing preload, but only if unlocked.

Operation of the lock occurs as follows. When the lock coil is pulsed by the decoder, the armature moves to the position shown. The torsion spring puts a downward force on the pawl, and, if it is aligned with a notch, it enters the notch, locking the steering input shaft. If not aligned, it remains under the influence of the downward force and enters whenever the steering wheel is turned, and alignment occurs.

When the release coil is pulsed by the decoder, the armature moves into contact with the core of the release coil, and the pawl then experiences an upward force. If there is little torque on the steering column, the pawl disengages, unlocking the shaft. If the column has a high torque (arising from tire friction), disengagement will occur when the operator relieves the torque.

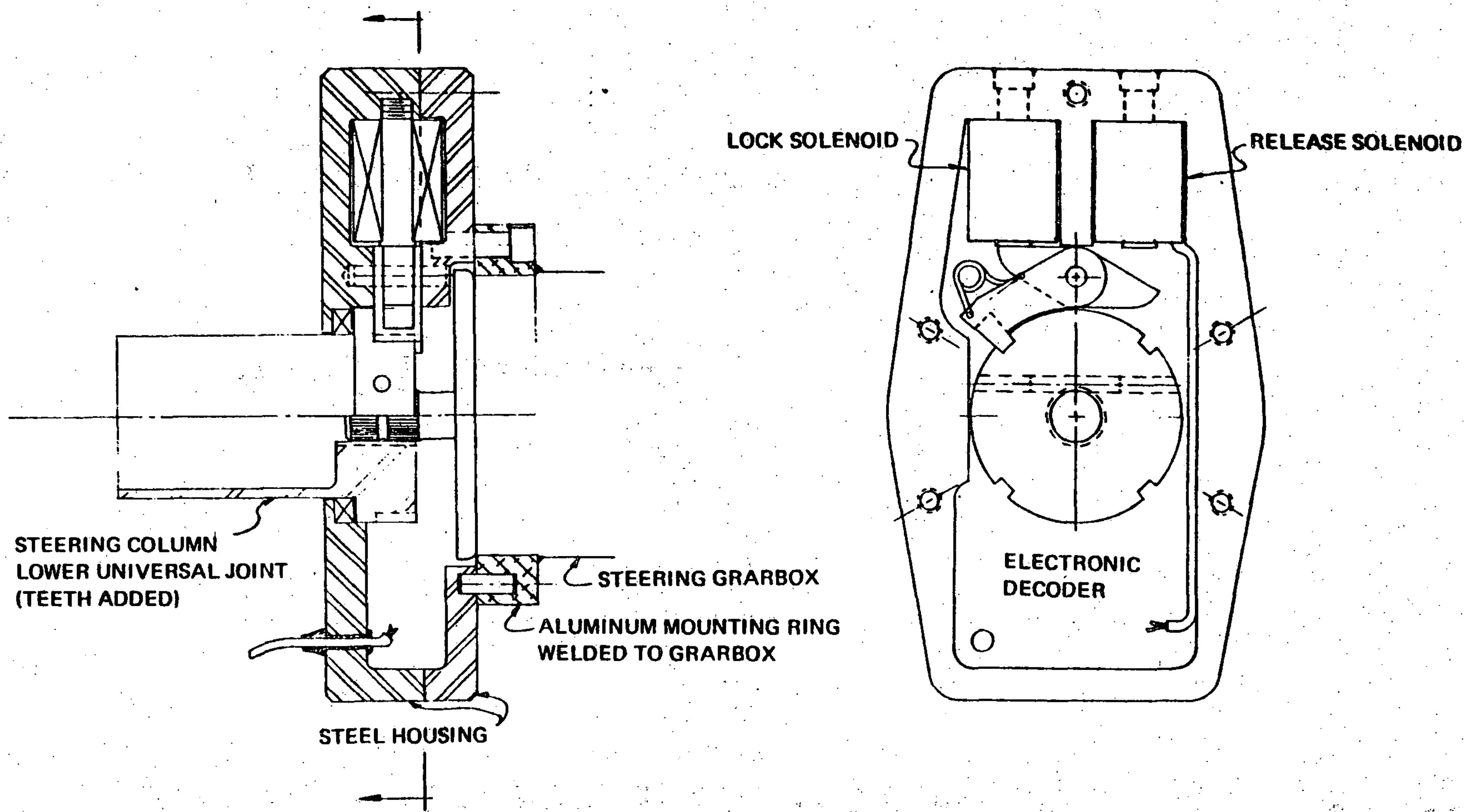


FIGURE 4. PRELIMINARY DESIGN OF A REMOTE STEERING LOCK.

The armature is supported at its center of mass, so that it will not change position in response to bumps and other accelerations of the vehicle. The bistable armature requires no power to remain in either position. Interruption of power will neither lock or unlock it. Locking actuation can be interlocked to the gear selector in the case of an automatic transmission vehicle, or a door switch in the case of a manual transmission.

It should be noted at this point that the precise type of locking mechanism used to engage the notched wheel can vary widely. The toggle mechanism shown in Figure 4 was selected at the preliminary stage when the proposed test vehicle was a 1975 Plymouth Valiant. Later, when a 1977 Dodge Colt was selected as the test vehicle, an entirely different mechanism was chosen to implement the concept, as will be described in the Detailed Design section of this report.

Entry Protection

It will be recalled that, in Chapter 4, attack resistance performance criteria for the entry protection system were ranked near the bottom of the list (Table 22). This suggests that little emphasis should be placed on the improvement of existing entry locks. However, because thieves often cite the entry phase of the theft as critical, and to benefit from the validation test results, it was decided to make incremental improvements to the existing entry locks on the test vehicle.

The improvements selected were as follows:

- Shielding the active lock elements from tampering through the clearance space between the window and its frame;
- Replacing the interior lock buttons with round knobs; and
- Pinning vent windows closed, if present.

The door latch mechanism for all of the models of interest consists of an assembly of stamped metal linkages and springs mounted on a stamped metal bracket which is, in turn, mounted inside the door frame. When locked, this mechanism can be unlocked by tripping any one of the following linkages:

- the lever operated by the lock cylinder,
- the crank arm on the lock cylinder itself,
- the lever operated by the inside lock button,
- connecting links between the inside lock button and the latch mechanism,
- the inside lock button or lever.

To protect the system against "Slim-jim" attack, all of the interior linkages must be shielded if they can be reached from outside the glass. In general, this would require sheet metal barriers of the type shown in Figures 5 and 6 for a doorlock system typical of a 1975 Colt. These schematic diagrams are not meant to show the precise shape for the optimum barrier, but rather only typical shapes. The optimum shape can best be developed as a model with the actual mechanism and then reproduced in sheet metal. Figure 6 also shows the replacement of the interior unlocking lever, which can easily be actuated from outside with a wire hook, by a round knob which cannot.

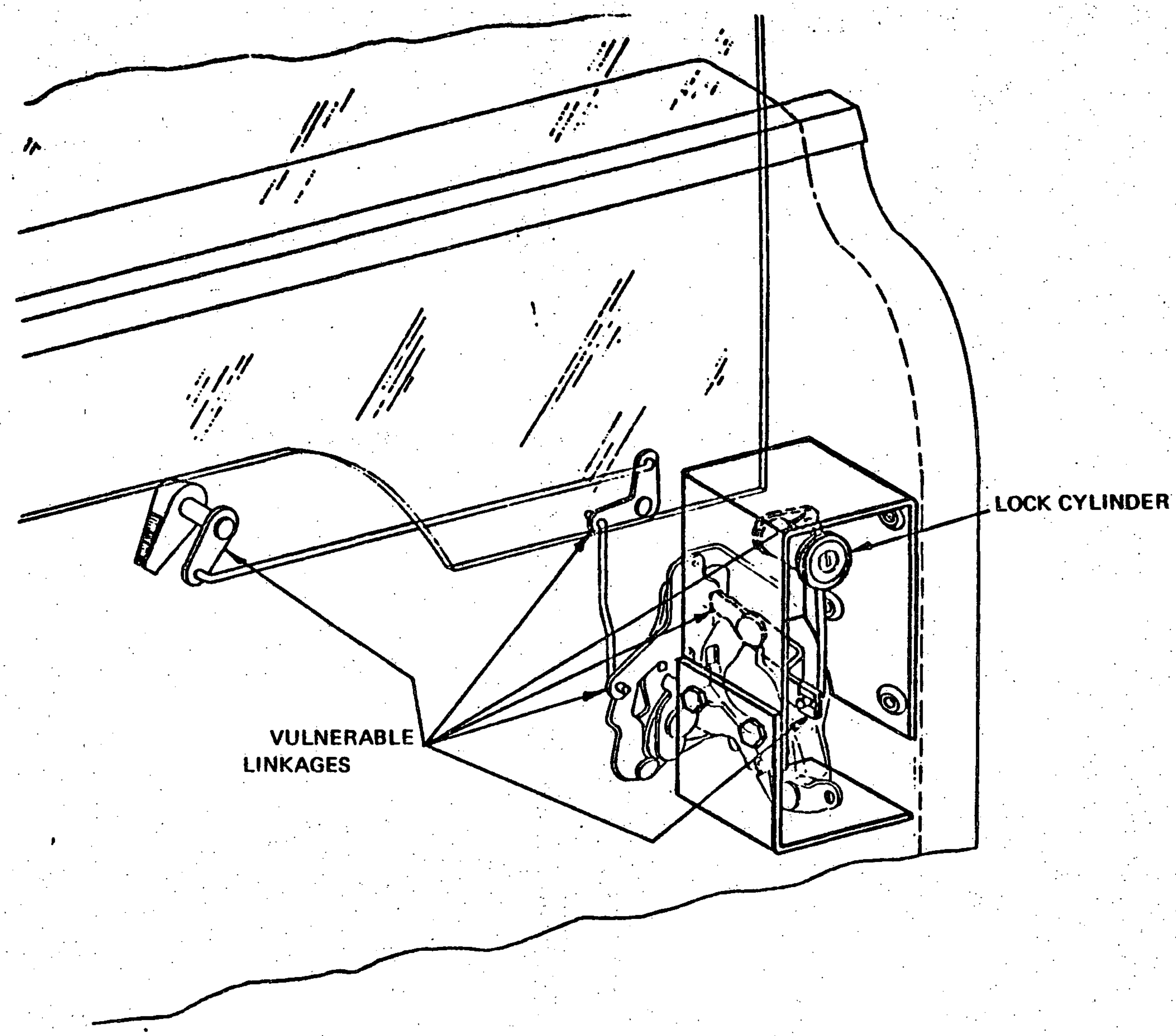


FIGURE 5. DOOR LOCK SYSTEM – BARRIER MOUNTED ON OUTSIDE OF GLASS.

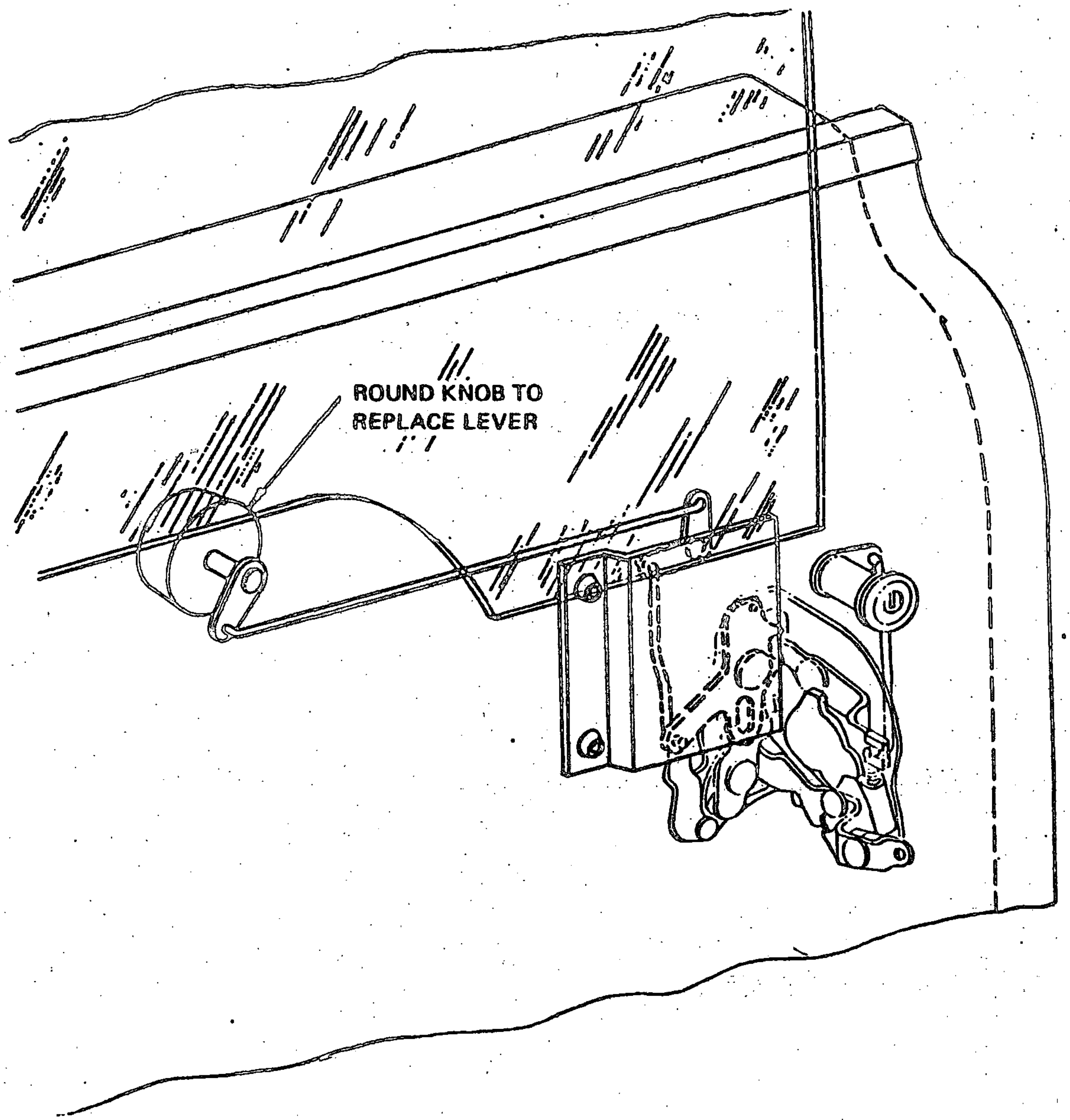


FIGURE 6. DOOR LOCK SYSTEM – BARRIER MOUNTED ON INSIDE OF GLASS.

Sensor Screen Concepts

Two sensor screen concepts were identified in the Concept Design section as having significant importance as theft deterrents. These are evaluated for potential in this program as steering column lock and entry protection, each of which is discussed below.

Steering Column Lock

Several concepts have been identified for protecting the conventional system against methods of forcibly removing the lock cylinder to gain access to the unlocking mechanism. Two of these are illustrated in Figures 7 and 8.

Figure 7, which was adapted from a previous study by this author,[41] shows a modification to the type of steering column lock used on Ford automobiles. It is designed to respond to the forcible withdrawal of the lock cylinder by pulling a pin into a blind hole in the bolt which locks both the steering and the ignition switch. This would enforce time-consuming disassembly to free the pin. With this concept, it would also be required to strengthen the housing casting, at least in the region of the lock retaining pin so that the knowledgeable thief would not be able to cut away the housing in this area and disable the protective mechanism in a short period of time.

Another similar approach is shown in Figure 8 for a steering column lock of the type used by Chrysler. Here, a hardened spring-loaded baffle is added which, upon the forcible removal of the lock cylinder, would move into place and shield the mechanism from actuation.

While it is believed that this general concept, coupled with other measures to strengthen the steering column lock, represents a promising approach to the development of a 10-minute lock, it has already been concluded that it is not the optimum approach for the test system in this program.

Entry Protection

The usual sensor screen envisioned as part of the entry protection system is an alarm system triggered by door switches. Previous analysis has pointed out that such a system has a relatively low deterrent value, unless it causes the locking of a critical vehicle function in a hardened inaccessible location. In this case, the code insertion that allows use of the car has simply been moved out to the doors rather than contained in the passenger compartment.

This concept is extremely promising and is felt by this author to be the logical extension of the electronically coded remote lock. However, to eliminate the susceptibility to direct mechanical attack on a cylinder lock, an effective system would require a keyboard on the outside of the door or an electronic key or card reader. It would also imply the use of electrical door locks which are now used only on the higher price models. As such, it was not felt suitable for the test vehicle on this program. However, it should be viewed as a likely concept for overall vehicle security on the automobiles of the future.

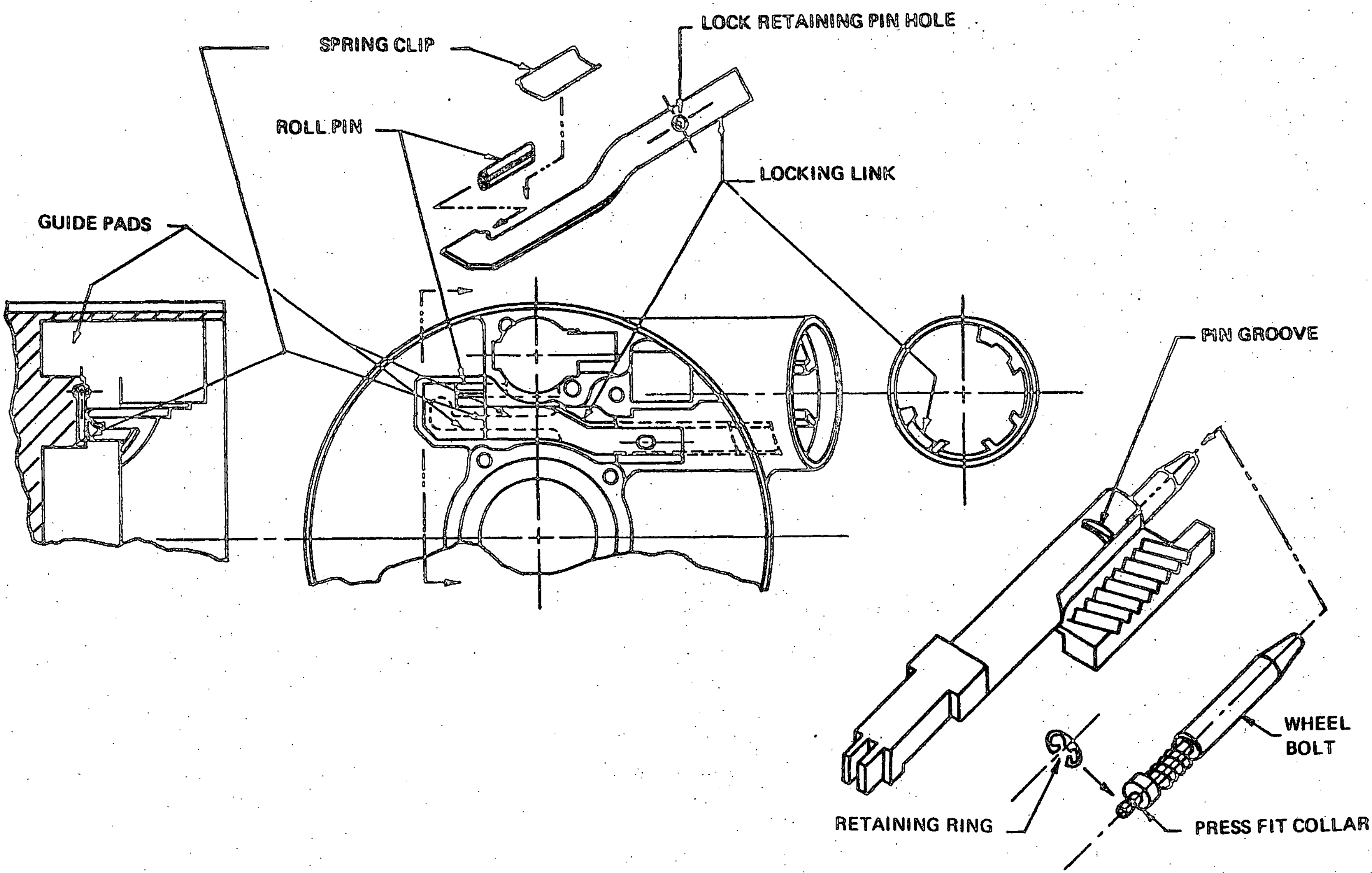


FIGURE 7. LOCK CYLINDER REMOVAL PROTECTION CONCEPT FOR THE FORD STEERING COLUMN LOCK.

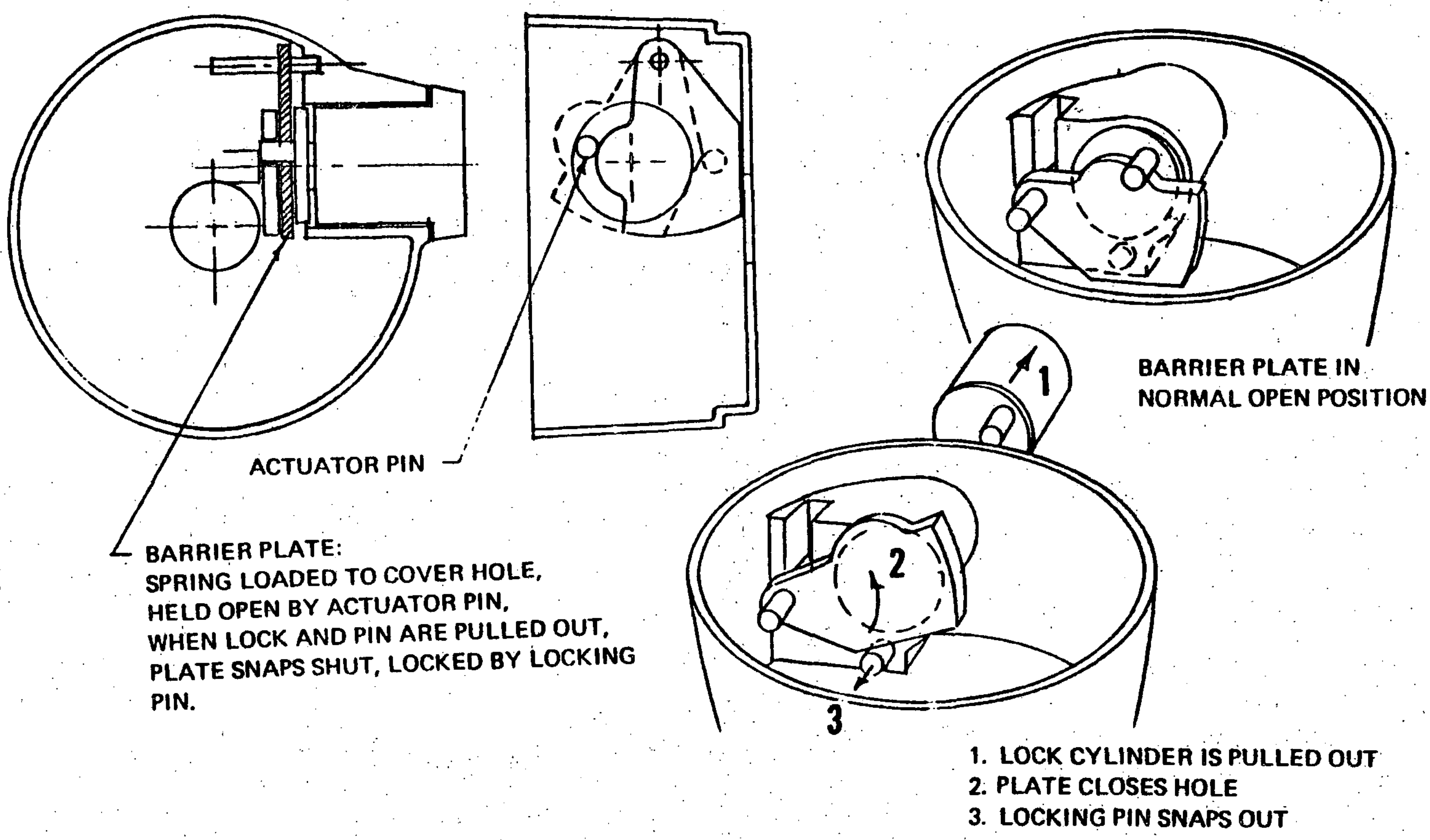


FIGURE 8. BARRIER PLATE MODIFICATION FOR THE CHRYSLER STEERING COLUMN LOCK

DETAILED DESIGN

As concluded in the preceding section, the optimum mobilization protection system for use as the test system in this program is a remote steering lock with a keyboard code insertion device located in the passenger compartment. This system concept was found to be optimum because:

- it meets the accessibility criterion and is believed easily capable, with suitable design, of meeting the defeat time criterion;
- it provides secure and cool packaging of the remote electronics without vehicle modifications which would be costly for a retrofitted device; and
- it is the shortest development path to a system which would preclude leaving a key in the vehicle.

All of the remaining criteria and design goals can be met with suitable design.

In the following subsections, the detailed electronic and mechanical design for the remote steering lock is described. Finally, the entry lock modifications are illustrated.

The vehicle selected and supplied by the Government for the validation testing was a 1977 Dodge Colt two-door sedan with a manual four-speed transmission. Thus, the test system was designed specifically to fit this vehicle. However, the relevant components and layout of this vehicle are entirely typical of most other cars on the U.S. market. By altering the physical layout, the system concept could be implemented for any automobile.

Electronic Subsystem

A schematic diagram of both the passenger compartment unit and the remote receiver/driver unit is shown in Figure 9. Drawings of the P/C board, component layout, and a parts list have been supplied separately to the Government.

Specifications for the test system are listed in Table 26. For convenience in mating the electronic driver to the locking mechanism, it was decided to use relays for the switch closure. A production version would make use of electronic switching in place of the relays to improve reliability and lower the cost.

Because the test unit had to make use of available integrated circuits, the temperature range was limited to 0°C to + 60°C. For high-volume production, custom large-scale integrated (LSI) circuits would be developed. This should allow extension of the low temperature limit down to −30°C which would be necessary for automotive application. Low temperature limits of −30°C and even −55°C are commonly specified for solid-state devices meeting military specifications and are within the state-of-the-art.

The standby current chain of 10 mA represents no significant problem. However, this would also likely be reduced somewhat for a production unit using customized LSI.

The test system is configured around an LSI designed for television remote control applications. The S2600 transmitter IC interfaces directly with the 12-button keyboard and produces an on/off keyed 40-kHz carrier. Each button causes a 76.8-ms message to be transmitted. A

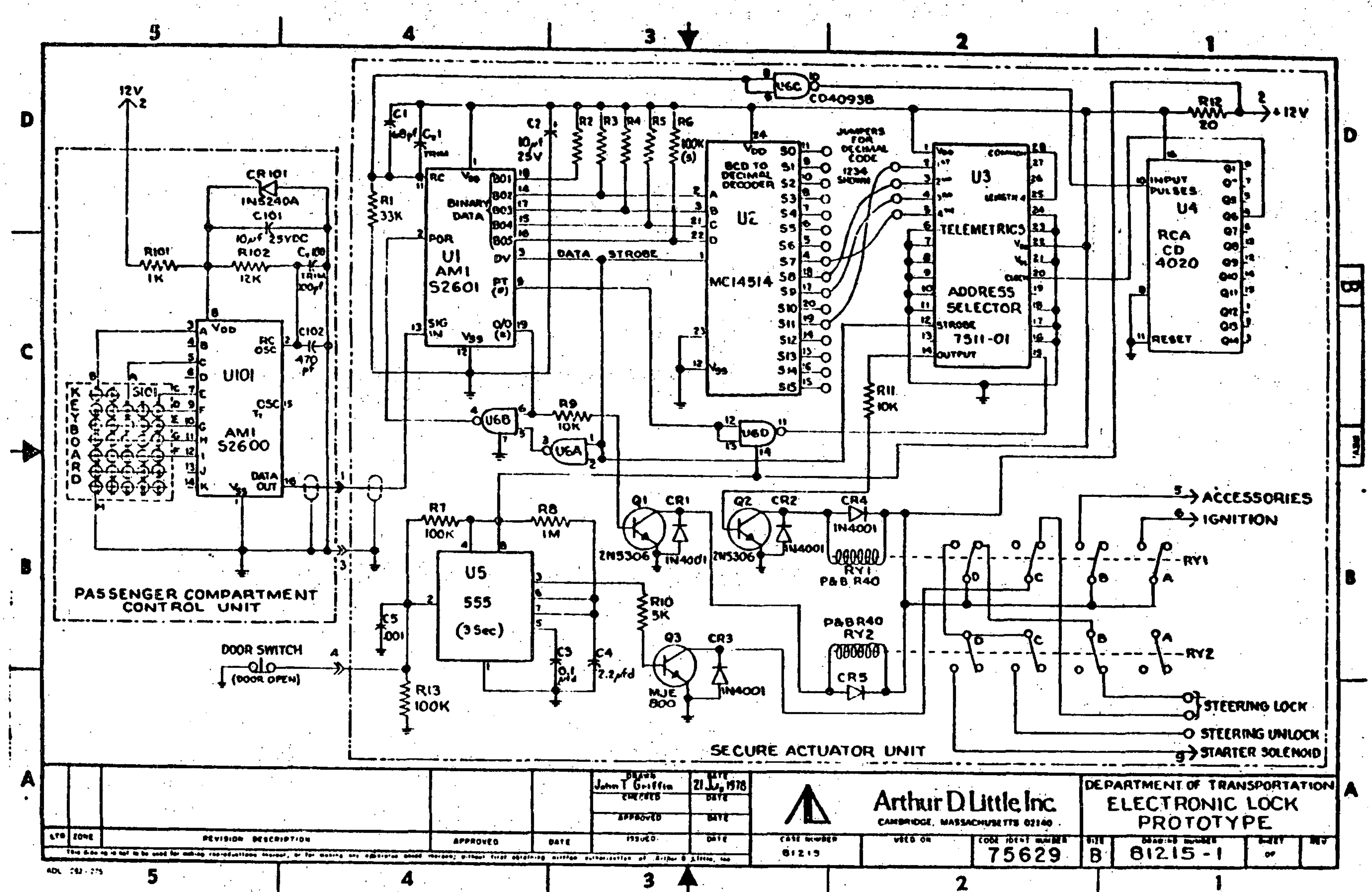


FIGURE 9. REMOTE STEERING LOCK ELECTRONICS.

TABLE 26. ELECTRONIC SYSTEM SPECIFICATIONS

Combinations:	10,000 (four sequential digits)
Power Supply:	12 VDC, negative ground (9-16 VDC)
Noise Immunity:	1/2 of power supply
Decoding Time:	Less than one second after last digit
Minimum Coding Time:	Reading time for 10,000 combinations should be greater than 20 minutes
Maximum Cable Length:	25 feet of #22 copper wire
Standby Current Drain:	Less than 10 mA
Environmental:	0°C to +60°C
Output:	Switch closures to enable the ignition primary, the starter circuit, and the locking circuit. Switch closure to operate the unlocking circuit.
Controls:	10-digit keyboard start button ignition shut-off button doorswitch locking control

message consists of two redundant frames of 12 bits per frame. A frame, in turn, consists of a start bit, a 5-bit preamble (mask programmed into the chip), 5 bits of data, and a stop bit. Each bit is 3.2-ms wide. A message is not validated at the output of the S2601 receiver IC, unless the 5-bit preamble matches and two successive frames are received.

Four of the five possible data bits from the S2601 are presented to a BCD-to-decimal converter resulting in a unique output from the converter corresponding to one of the 10 numeric keys. These outputs are selectively strapped (to set the code) to a Telenetics address recognizer (7511-01) configured to provide an output only after receiving four sequential inputs in the correct order.

The output of the Telenetics IC latches after the correct code is entered and can be reset by actuating one of the non-numeric keys at the operator's console, corresponding to the "LOCK" position of a conventional ignition switch. A second non-numeric key is used to engage the starter. It would be possible with additional switching to provide selection of "ignition/accessory" or "accessory only" following the code insertion.

The preamble is analogous to the use of various keyways in a mechanical lock. It can take on any one of 50 different combinations. Assuming that a thief had this preamble code and a device that could sequentially generate all 10^4 different combinations, the electronics can only read at a rate of 0.3 second per four-digit combination. Thus, the minimum reading time for 10^4 combinations would be 50 minutes and the average theft time would be 25.0 minutes with such a code generator.

However, in a production unit using customized LSI's, it would be possible to further increase the difficulty by:

- increasing the number of code digits from five to six;
- changing the preamble code frequently among the production units; or
- including logic in the receiver to sense insertions of the incorrect code and cause a delay in this case.

One of the commonly stated objections to the keyboard system is the inconvenience presented to the driver who wishes to leave his car with a parking lot attendant, valet service, or service station. For this purpose, the design of custom electronics could provide the option to insert and store part of the code so that the service personnel could start and drive the car with, for example, one code digit. The stored partial combination would then be cleared by the driver when he retrieved his car. Such a system would greatly improve the security of parking lots and service facilities which are now a major source from which thieves can obtain keys to an automobile.

Another design feature that could be included in customized electronics is the ability for the owner to reprogram the code at will. Although this would require programmable memories and would increase the cost of the electronics somewhat, such a feature would add significantly to the security of the device. Whenever the owner suspected that his combination had been compromised, he would simply change it.

Mechanical Subsystem

Mechanical subsystem assembly is shown in Figure 10. A full set of engineering drawings has been supplied to the Government. The following description is keyed to the part numbers of Figure 10.

As is normally the case with a retrofitted device, the overall shape reflects the need to fit the system into the available space around the input shaft of the steering gearbox. This carries the advantage in the present case of limiting accessibility to the device. One side is very close to the inside of the left front fenderwell. The other side is very close to the side of the motor. The remainder of the housing is between the firewall and the steering box. Since the power brake cylinder and other components are located above the system, the only accessibility is beneath the vehicle and this is limited severely by the frame. This is ideal for an anti-theft system.

The housing (2) is machined from stainless-steel for the test system. In a production design, the system would be integrated with the steering box in a cast-iron housing. However, to obtain high strength and torch-attack resistance within the envelope available for retrofit, it was decided to use stainless-steel.

The housing is mounted on a collar threaded onto the input shaft boss of the steering gearbox, and is retained by a screw (15) inside the electronics cavity and two pins (18) on the collar.

The locking wheel (4) is made from 4140 steel and engages the input spline on the gearbox. The lower half of the standard steering column universal joint is welded to this ring.

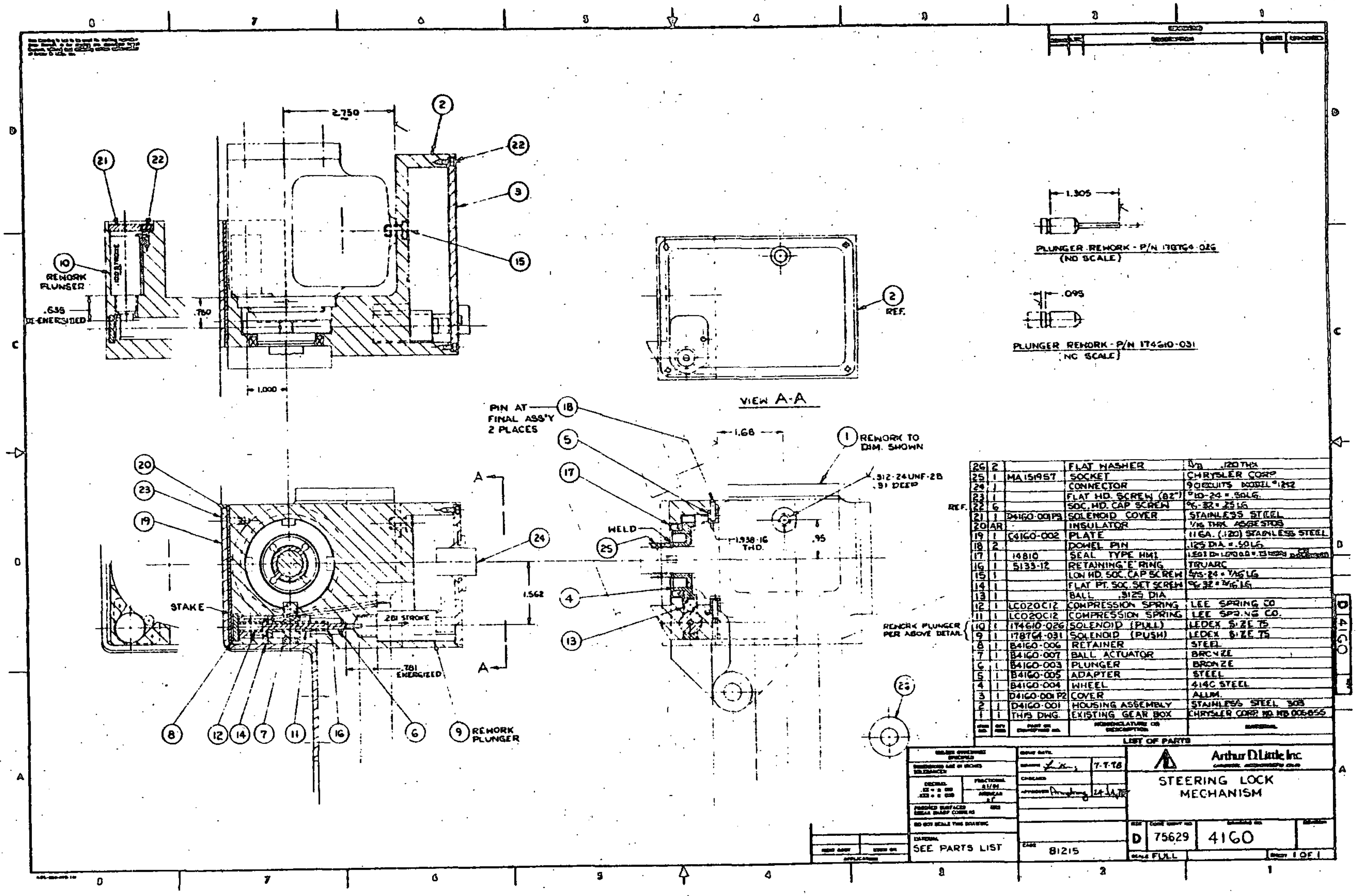


FIGURE 10. MECHANICAL LAYOUT

The steering gear is locked by means of a ball (13) which engages the notches on the wheel (4). The plunger (6) is forced to the left on signal by a solenoid (9). This stores the unlocking energy in a spring (12) as the plunger (6) is latched by the unlocking solenoid (10). As the plunger (6) moves to the left, it compresses a spring (11) which bears on a ball actuator (7). If the ball and notch are aligned, the ball is forced into the notch by the ball actuator and the steering is locked. If the notch is not in position, the locking energy is stored in the spring (11) until the steering wheel is next rotated to the point where the notch lines up and locking occurs.

When the unlocking signal is received, the solenoid (10) retracts, unlatching the plunger (6) which then moves slightly to the right so that the solenoid (10) will not relatch when the signal pulse ceases. Then, as soon as the sideload is removed from the ball by turning the wheel slightly, a spring (12) forces the plunger (6) and ball actuator (7) to the right so that the ball can move back to the unlocked position.

The rectangular cavity under the cover (3) is provided for the remote electronic unit. The entire unit including the cover, screw holes (22), and solenoid (10) with its leads is potted in epoxy after assembling.

An asbestos insulator (20) and a plate (19) were provided to increase the resistance of the unit to torch attack through the fenderwell. This protection would not be required in a production unit.

A photograph of the remote steering lock unit mounted on the steering gearbox is shown in Figure 11, and the keyboard is shown mounted in the vehicle in Figure 12.

Entry Lock Modifications

The actual doorlock system on the 1977 Dodge Colt test vehicle was fitted with the type of protective baffles illustrated schematically in Figures 5 and 6. This was accomplished by removing the interior door panels and the lock mechanisms. Appropriately shaped baffles were then fitted in place by trial and error and fabricated from sheet metal. The objective was simple — to shield each element of the mechanism which can be used to unlock the door from access by a tool inserted through the window slot.

The resulting baffles are shown in the photographs of Figure 13. In addition, a small crank arm was added inside the door and the factory button release was replaced with a simple round knob, as illustrated in Figure 6.

No engineering drawings were prepared for these modifications for the following reasons:

- They are appropriate in detail only for this particular test vehicle. Any other vehicle would require, in general, baffles with entirely different shapes.
- The validation test showed that, while the modifications do indeed slow down the entry phase of a theft, they have a low deterrent effect in comparison with an effective mobilization lock, and thus should not be mandated.

In addition to the doorlock modifications, the test vehicle was fitted with a locking hoodlatch manufactured by Continental Auto Co., St. Charles, Illinois. This device is simply a spring-loaded bolt operated from the passenger compartment through a push-pull cable. A simple

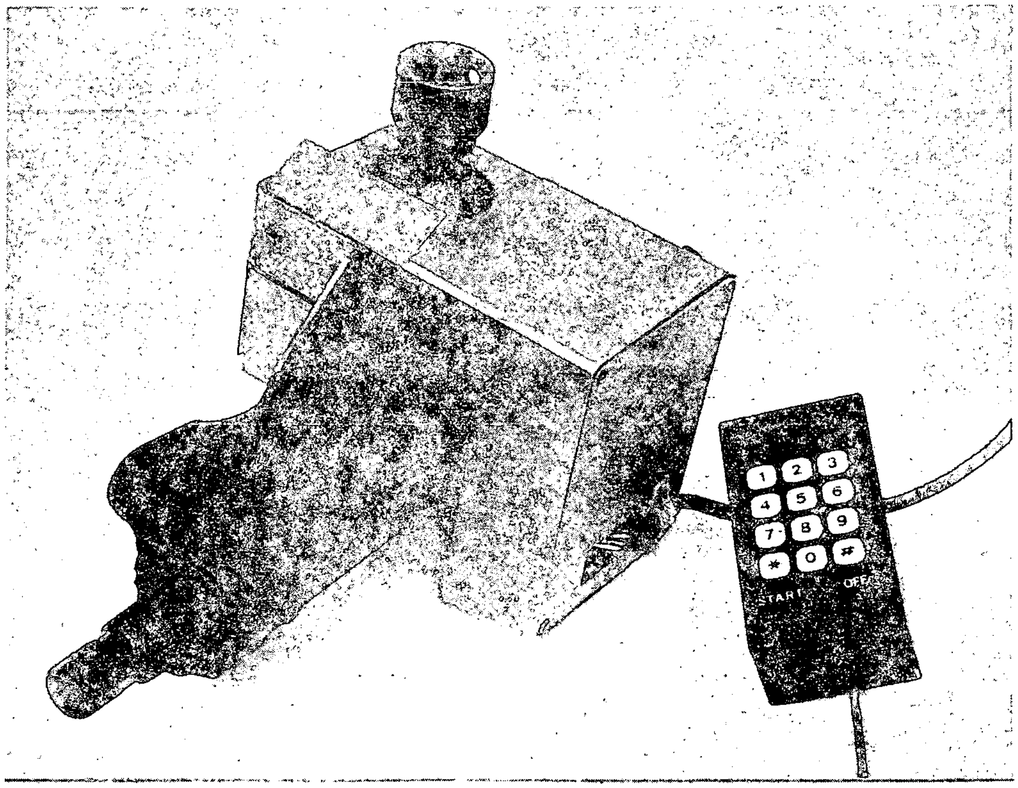


FIGURE 11. REMOTE STEERING LOCK UNIT MOUNTED ON STEERING GEARBOX.

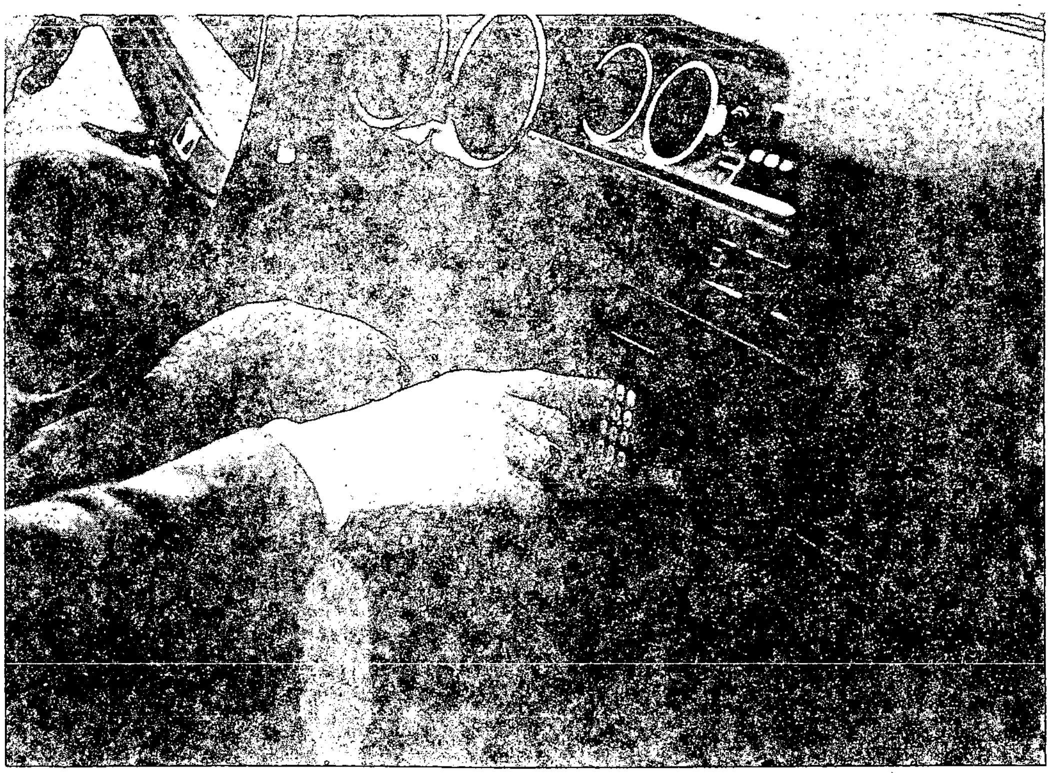
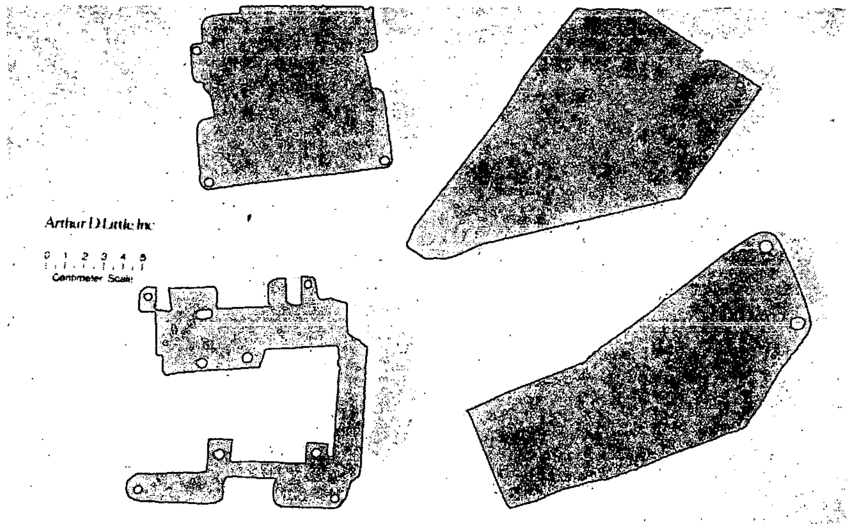
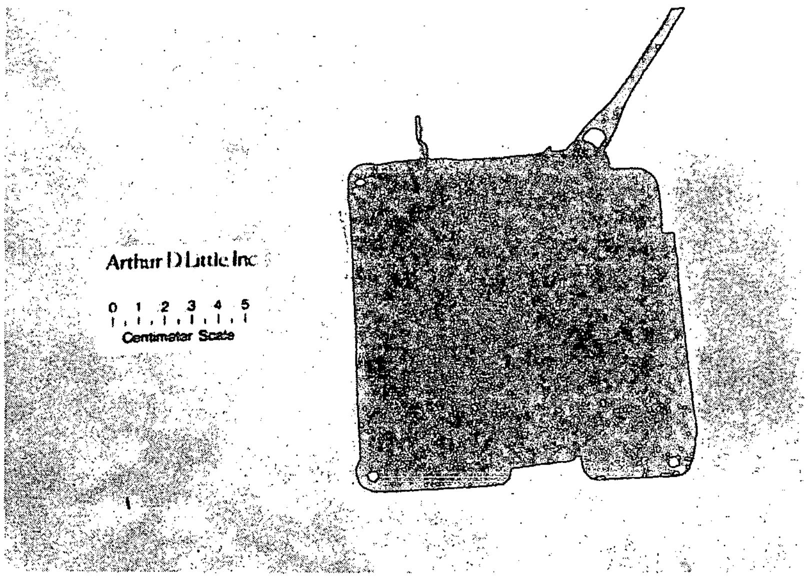


FIGURE 12. KEYBOARD SHOWN MOUNTED ON VEHICLE DASHBOARD;





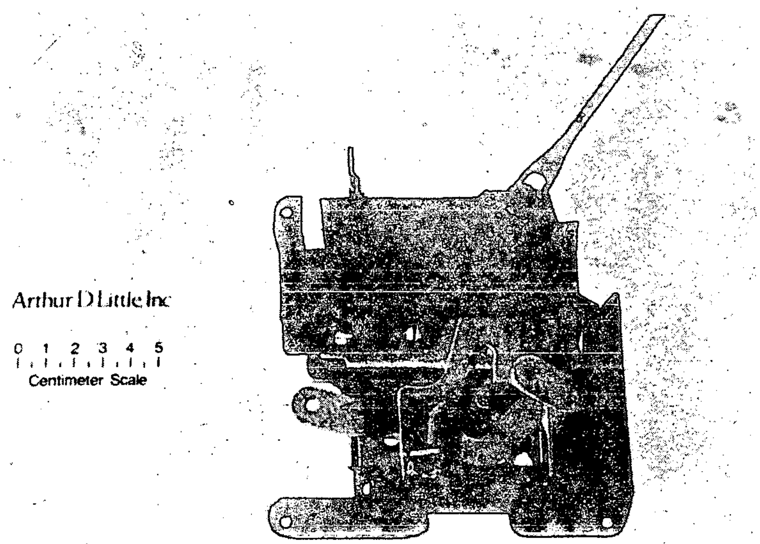


FIGURE 13. PROTECTIVE DOORLOCK BAFFLES INSTALLED ON TEST VEHICLE.

cylindrical lock is used in the passenger compartment to lock and operate the cable. The device includes a built-in ignition kill switch which was not used on the test vehicle.

Again, the testing showed that, on this particular vehicle, the hood lock imposed only a short delay on the theft.

Reliability and Maintainability

The availability of the automobile is dependent upon the reliable operation of the anti-theft system. Thus, reliability is of prime importance. Without extensive performance and life-testing of a large number of production units, or extensive failure data on the individual components which will be used in a production unit, accurate prediction of reliability cannot be made. However, at this stage the general characteristics of a production version of the remote electronic steering lock can be visualized and reliability can be discussed qualitatively relative to current hardware.

Assuming that the electromechanical relays were replaced with solid-state devices and that all microcircuitry were designed and developed for the automotive environment, the electronic circuit should be entirely comparable to the many other solid-state units that are being increasingly applied by the automobile industry. Many of these, such as ignition and fuel-mixture controls, also directly affect the availability of the vehicle. Thus, the industry apparently has evaluated and accepted the reliability of solid-state microcircuitry.

The latching device, itself, is entirely analogous to those currently used for the steering column lock. Thus, with appropriate design, this portion of the system should be no less reliable than those which have been proven over many years of application.

The keyboard used in the test system was developed especially for telecommunications systems and other consumer applications where reliability and long life is of paramount concern. Finally, the electromechanical solenoids required to transduce the electronic control output to the mechanical latch operation are rugged, long-life units which have been used for automotive applications for many years. Thus, it is expected that a production version of the concept will easily be capable of meeting the reliability requirements for automotive application.

Maintainability refers to the ease of repair in case of failure and is important for automobiles because it directly affects repair costs. The keyboard unit, of course, can be mounted in such a way that it can be removed and replaced in a few minutes. Thus, it presents no maintainability problem.

The remote unit, however, was designed purposely to be time-consuming to remove and replace. For the test unit, the design increases the normal time somewhat beyond that required for a stock gearbox due to the requirement that the steering column universal joint must be disassembled in place. Moreover, the engine mounts must be unbolted and the engine moved slightly to remove and reinstall the unit. This procedure was found to require a minimum of about 45 minutes by an experienced mechanic.

This removal and replacement time, while not excessive in comparison to the 0.8 hour allowed for many current ignition switches, is longer than it need be for a production unit. Depending upon the final design used for coupling the unit to the steering column and mounting the gearbox on the frame, the time could probably be reduced to a half hour or less. It is only necessary to ensure that it is takes longer than 10 minutes for effective theft deterrence.

It is anticipated that the production electronics package would be replaced as a unit. The steering lock should be designed such that this unit cannot be removed and replaced without first removing the steering gearbox from the vehicle.

Cost Analysis

A prime objective of this program is to develop cost-effective improvements to the safety standard. Accordingly, the goal of the design tasks has been a system which is consistent with an increase in consumer price of $50 or less in very large production quantities. This figure was selected as a conservative measure of the potential theft cost savings from the data gathered in the vehicle theft survey of Chapter 3.

Subsequent testing, reported in Chapter 6, determined that the value of entry lock improvements and hoodlocks is dubious. Thus, it is concluded that these should not be mandated by the standard, and no further effort was devoted to performing a production cost analysis on these subsystems.

However, the remote steering lock has been studied to estimate its production cost in quantity and the increase in vehicle price which would likely result from its use in a typical U.S. production vehicle.

This study requires not only a consideration of the design changes to the remote steering lock which would be made to implement its use as a production device, but also an estimate of those elements in the current anti-theft systems that would no longer be required. It is the difference between these that is significant for assessing the net cost impact.

Table 27 lists the estimated reductions in cost possible from the elimination of the current type of steering column lock. The resulting total manufacturing savings of $2.41 can only be regarded as an approximation of the possible savings from the elimination of the various steering column lock designs in use by the several U.S. manufacturers. However, it is believed that this is a conservative estimate since simplifications in wiring and a number of miscellaneous small parts and fasteners were ignored in the assessment.

The additions required for the improved remote steering lock design of this chapter are, of course, better defined. For this assessment, it has been assumed that the lock and the remote electronics would be housed in a redesigned steering gearbox. The lock would be assembled into the input end of the gearbox through the cover prior to the assembly of the gears. Thus, no new seals would be required. Table 28 details the estimated manufacturing costs for the mechanical subassembly of the remote steering lock. The resulting total is $2.97. Thus, the net increase in manufacturing cost for the mechanical assembly alone is $0.56.

To this must be added the estimated manufacturing cost of the electronic assemblies. There are, of course, no electronics in the current steering column lock to offset the addition of the passenger compartment keyboard unit and the remote decoder/driver circuit.

TABLE 27. ESTIMATED MANUFACTURING COST REDUCTIONS DUE TO ELIMINATION OF CURRENT STEERING COLUMN LOCK

Component	Change	Basis of Estimate	Cost Savings
1. Steering Column Housing	Simplification of the Housing Casting	Savings of 6 oz. of Zinc @ $0.40/lb.	$0.15
2. Lock Cylinder	Delete	Refs. (36) & (37)	1.00
3. Internal Bolt or Latch Assembly	Delete	Manufacturing Estimate (3 to 5 Simple Parts)	0.17
4. Ignition/Starting Switch	Delete	Manufacturing Estimate (4-position switch)	0.75
5. Wiring Harness	Simplify	No Cost Credit Taken	–
6. Warning Buzzer Switch	Delete	Manufacturing Estimate	0.08
7. Notched Sector Wheel	Delete	Manufacturing Estimate	0.05
8. Assembly and Test	Delete	Labor to Assemble and Function Test the Deleted Parts Estimated as 50 secs. at $15/hr.	0.21
		Total Savings	$2.41

TABLE 28. ESTIMATED MANUFACTURING COSTS FOR THE REMOTE STEERING LOCK MECHANICAL ASSEMBLY

Component	Remarks	Basis of Estimate	Cost
1. Steering Gearbox Housing	Larger and more Complex	4 lb. Cast Iron @ $0.15/lb.	$0.60
		Additional Machining	0.15
2. Gearbox Input Shaft	Larger Diameter for Lock — Possibly Welding Lock Wheel	Manufacturing Estimate	0.08
		Additional Machining	0.16
3. Plungers	Two Required from Rod	Screw Machine Parts	0.10
4. Springs	Two Compression Springs Required		0.06
5. Solenoids	Two Required	Estimated from Discussion with Manufacturer	1.00
6. Ball Activator	Molding or Die Casting		0.005
7. Notched Wheel	Should be 4140 Steel		0.08
8. Cover for Electronics Cavity	Cast Iron or Stamped Metal		0.10
9. Miscellaneous Hardware			0.05
10. Assembly	Estimated as a Total of 80 secs. Labor at $15/hr.		0.33
11. Functional Test at End of Assembly Line	Estimated as 60 secs. Labor at $15/hr.		0.25
		Total Cost	$2.97

Table 29 lists the various manufacturing cost elements estimated for the test prototype design produced in large quantities. If the resulting $25.44 is added to the $0.56 net charge for the mechanical assembly, the total manufacturing cost becomes $26. References (36) and (37) indicate that the markup between total manufacturing and tooling costs and final consumer price averages about 30 to 38% for an entire vehicle. Thus, the above would be expected to produce a maximum price increase of $36.

However, the estimate of Table 29 is based on the design for which no real production or value engineering has been performed. It would be expected that much of the decoder circuitry could be highly integrated into a single chip. The PC card, if necessary, could be a much lower cost unit. The keyboard would probably be cheaper in the 10^6 quantities required for automotive use. Several of the manufacturers contacted, including Chromerics, could not provide an accurate estimate for these quantities. Alternatively, a cheaper keyboard such as those used on low-cost calculators could be used. Finally, the very expensive relays could probably be replaced by solid-state switching or at least reduced to one in a production unit. The net impact of these various changes are estimated to provide a potential $13.77 manufacturing cost reduction from the current design. This would reduce the maximum price increase to $17.

Thus, the vehicle price increase resulting from the replacement, in production, of the current type of U.S. steering column lock with a remote unit of the type designed in this program is estimated to fall between $17 and $36.

TABLE 29. ESTIMATED MANUFACTURING COSTS FOR THE ELECTRONIC SUBASSEMBLIES

Component	Part No.	Basis of Estimate	Cost
Integrated Circuit	AMI 52600	Manufacturer's Estimate	$ 2.25
Integrated Circuit	AMI 52601	Manufacturer's Estimate	2.25
Integrated Circuit	Telaris 7511-01	Manufacturer's Estimate	1.45
Integrated Circuit	Motorola MC14514BCP	Manufacturer's Estimate	0.88
Integrated Circuit	Signetic 555	Manufacturer's Estimate	0.55
Integrated Circuit	RCA CD4020BE	Manufacturer's Estimate	0.43
Integrated Circuit	RCA CD4093BE	Manufacturer's Estimate	0.21
Transistor	GE 2N5306A	Manufacturer's Estimate 2 Required	0.19
Transistor	Motorola MJE800	Manufacturer's Estimate	0.24
Diode	Motorola 1N4001	Manufacturer's Estimate 5 Required	0.175
Zener	Motorola 1N5240A		0.048
Resistors	Miscellaneous	15 Required	0.15
Capacitors	Miscellaneous	9 Required	2.27
Keyboard	Chromerics ER-21623	Manufacturer's Estimate	2.50
Connectors	Miscellaneous	Manufacturer's Estimate	0.10
PC Card	ADL Drawing	Manufacturer's Estimate	4.00
Relays	P.B. R40-E3-X4-V200	Manufacturer's Estimate 2 Required, 10,000 Quantity	7.40
PC Assembly & Testing	Automation Assumed for Component Insertion and Test		0.10
Keyboard Unit Assembly			0.25
		Total Cost	$25.44

6. SYSTEM TESTS

FABRICATION AND ASSEMBLY

Two complete test systems were fabricated and assembled from the design described in the preceding chapter and the drawings submitted separately. The remote steering column locks were assembled on two spare steering gearboxes purchased for the 1977 Dodge Colt test vehicle. Neither the mechanical nor electronic units of the steering column lock presented any unusual fabrication problems. The special P/C boards were photoscreened from the drawing and the components mounted in the laboratory. Fabrication of the mechanical unit involved only straightforward machining. Assembly of the entire unit was simple and straightforward.

After bench testing and the theft test on the factory-equipped vehicle, the remote steering lock was installed in the vehicle. As noted previously, this is a relatively time-consuming process because the steering-column universal joint must be assembled in place and the engine moved slightly while the unit is being placed in the vehicle. However, the installation is straightforward and no special techniques are required.

The doorlock baffles were fabricated in preliminary fashion from sheet metal as described in the preceding chapter. These were then fitted, with slight modifications, into the doors. The placement of parts inside the door is complex and, without detailed drawings of the door, the only practical method for installing this type of baffle is by customized fitting. If this modification were made in production, of course, the exact shape of the various baffles could be established.

The locking hoodlatch was simply assembled in the vehicle between the bottom of the dashboard and the bulkhead in front of the radiator in accordance with the manufacturer's instructions.

BENCH TESTS

Prior to installation in the vehicle, the mechanical and electronic units were tested separately and assembled together to ensure that the system functioned as designed. No major problems were found as a result of these bench tests.

A slight modification of one dimension on the mechanical unit was found necessary to ensure that it would unlatch in the event that the ball and notch were not aligned when the unlocking pulse was received.

The electronic units were cycled in a thermal test chamber to test their operation over the desired temperature range. The unit was found to operate down to -10°C which is below the specified limit. Elevated temperatures as high as 32°C presented no problem. The units were cycled and tested several times over this temperature range.

VEHICLE TESTS

Factory Equipment

Prior to the installation of the test system and doorlock modifications, a theft test was conducted on the factory-equipped vehicle. The author served as test subject for this test. After studying and experimenting with the doorlock system, it was decided to use a "slim-jim" attack on the linkages through the window slot. A slide-hammer was chosen for defeating the steering column lock.

A single trial was conducted to defeat the protective systems and mobilize the vehicle. This trial was recorded on motion picture film with a visible clock showing the elapsed time. The test subject unlocked the door in a few seconds and defeated the steering column lock in an additional 40 seconds. The total time from approach to the vehicle to the point where it was driven off was about 50 seconds.

It is worth noting that this trial represented the first time that the test subject ever attacked a Dodge Colt steering lock or, for that matter, any steering lock mounted in a vehicle. An experienced thief would likely be somewhat faster, probably closer to 30 seconds.

Road Testing

The test system was then installed on the vehicle and subjected to about 100 miles of road testing on all types of pavement. The purpose of this test was to shake down the unit, especially the electronics, before final potting in preparation for the validation test.

The only problem experienced during these tests was a periodic tendency for the malfunction of the door interlock circuit which did not appear during bench tests. When installed in an actual vehicle, the opening of the ignition circuit relay occasionally caused arcing and a false signal on the door interlock. This resulted in the immediate locking of the steering upon shutting off the engine before the door was opened. Since this characteristic defeated the safety provision of the door interlock, the circuit was later modified to eliminate this behavior. After road testing, the test unit was removed and potted with epoxy resin. It was then reinstalled in preparation for validation testing.

Validation Test

The validation test on the prototype improved anti-theft system consisted of a defeat time trial against the combined system, including the doorlock, hoodlock, and remote steering lock. An independent expert test subject, Mr. Rufus H. Whittier, was retained for the tests. Mr. Whittier serves as a consultant to law enforcement agencies, insurance companies, and anti-theft equipment manufacturers. He is a nationally known authority on automobile theft. Prior to his retirement as a professional auto thief, Mr. Whittier estimates that he stole more than 8000 cars of all types. Since that time he has conducted many demonstrations and tests of all types of anti-theft equipment, including factory-installed systems and retrofitted systems.

During the week prior to the test, which was held on 9 November 1978, the test subject was fully briefed on the systems installed in the test vehicle. This briefing included:

- removal of the interior door panel to allow a study of the interior lock mechanism and baffling,
- study of the remote steering lock and hoodlock as mounted on the vehicle,
- study of the disassembled steering lock on the bench and its method of operation,
- study of all drawings of the device, and
- a question and answer period concerning the principles of operation for the devices and the mechanism.

The only groundrule applied to the test itself was that only man-portable tools would be allowed. We felt that this would conservatively simulate the practical theft situation in which the theft was not carried out with a tow truck. Amateur theft, which is the principal target of the improved anti-theft system, does not conventionally involve a tow truck.

After planning his attack following the interviewing period, the test subject was prepared with his own set of equipment to carry out the validation test on the scheduled day.

The time trial was witnessed by Government observers from the National Highway Traffic Safety Administration and by various Arthur D. Little personnel. A backup steering lock system was available for a second trial to obtain learning curve information in the event that the initial system was defeated in a marginal time period.

The time trial was recorded on motion picture film and still photographs with a visible clock showing elapsed time. The times were also recorded as the test proceeded.

The test subject first attacked the door lock system (Figure 14). Having become convinced by studying the system that a "slim-jim" attack was impossible, he pried the door away from its frame and worked an interior doorlock knob into its unlocked position using a welding rod with a chisel shape ground onto one end. The doorlock was defeated in 1 minute and 20 seconds.

He then moved under the car and reached up into the engine compartment to cut the plastic sheath and operate the hood lock cable with diagonal cutters. The hood lock was defeated in an additional 1 minute and 30 seconds, or an elapsed time of 2 minutes 50 seconds after the start of the trial.

The test subject then attacked the remote steering lock from under the vehicle (Figure 15). As a result of his study of the system, he was convinced that mechanical attack on the housing was not practical because of the limited access and working space and the time which would be required. Thus, he elected to probe the electrical circuitry which was accessible on the test version through a hole in the cover and interfaces between the steering box and the lock housing. None of these possible access points would exist in a production version of the device. The test subject applied 12 volts from a hot-wire to various elements of the circuit in an attempt to find an electrical path to the unlocking solenoid. All of these measures were unsuccessful and, in fact, only served to destroy part of the electronic circuit and ensure that the device would remain in the locked state. The test subject gave the attack up as fruitless after an elapsed period of 16 minutes and 40 seconds or 13 minutes 50 seconds work on the steering lock alone.

This test subject stated that he would never attempt to steal a car equipped in this fashion on the street without a tow truck. He believes that it can only be stolen in that manner.

Conclusions

The principal conclusion reached as a result of the validation test is that it is quite feasible to design and produce a cost-effective mobilization protection system which will deter most thieves well beyond the 10-minute goal applied in this program. In fact, the experience gained in this program indicates that effectively designed remote locking systems will, in general, force the use of a tow truck to steal the vehicle. This would effectively eliminate amateur auto theft and provides the opportunity, through local control and licensing of tow vehicles, to make professional operations more hazardous.

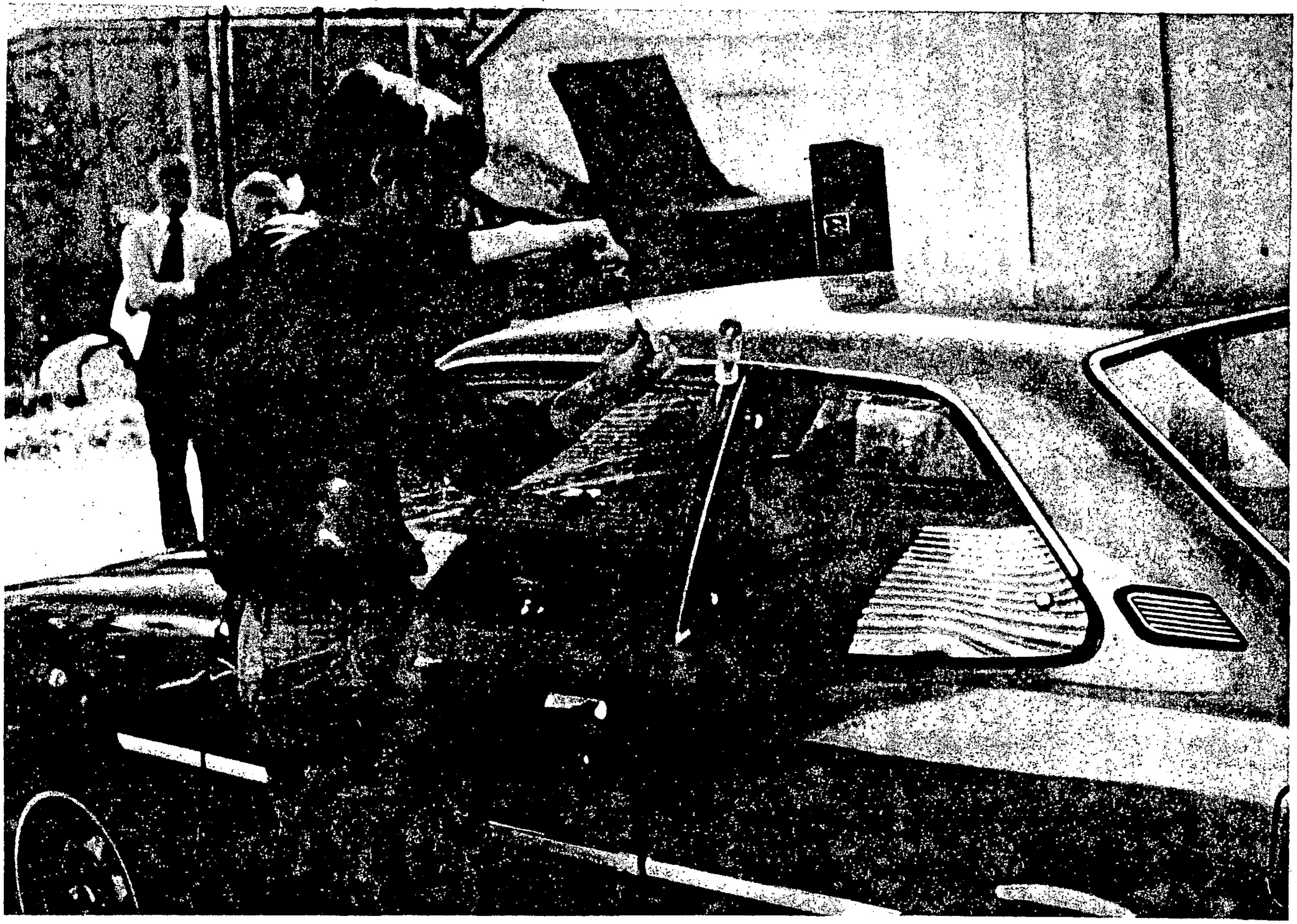


FIGURE 14. DOOR LOCK SYSTEM BEING ATTACKED DURING TEST.

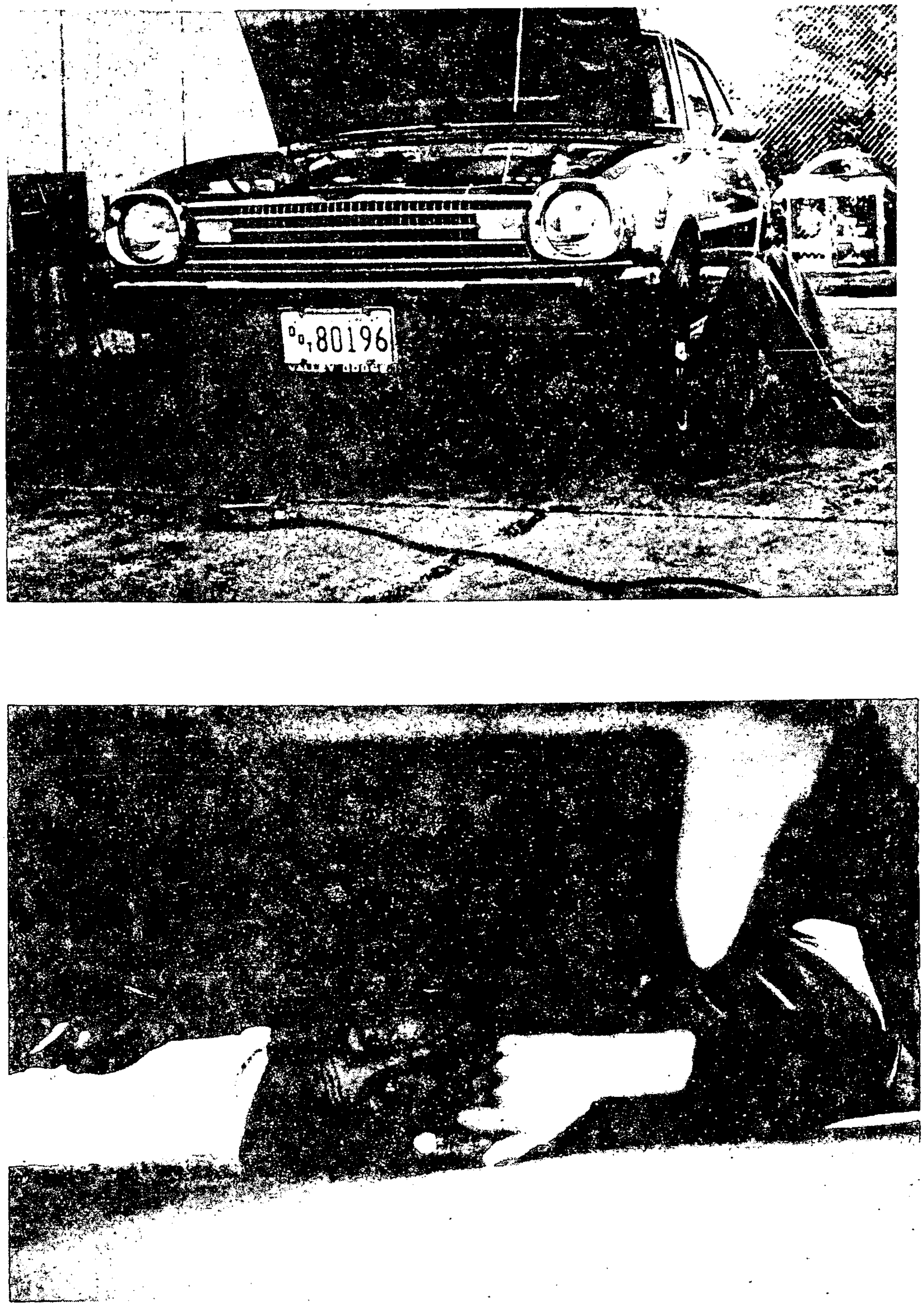


FIGURE 15. REMOTE STEERING LOCK UNDER ATTACK FROM BENEATH VEHICLE.

The key to achieving the required defeat time is to locate the vulnerable elements of the system, the decoder and the latch, in an extremely inaccessible location in the vehicle. In addition, these elements have to be housed and the housing mounted in such a manner that access to or replacement of the vulnerable elements will require more than 10 minutes — with a high degree of confidence. There are many conceptually possible ways to achieve this level of security in the automobile.

The only general design restrictiveness imposed by this approach is that it implies the use of electrical code transmission from the passenger compartment to the remote lock. Keyboard code insertion was found to be the simplest method of achieving this status, and it offered no significant inconvenience in the prototype system. The potential problem arising when it is desired to allow someone other than the owners to drive the car could easily be solved using enhanced decoder circuitry in a production version. It is also possible, of course, to implement the system with a key or card reader as the code insertion device. The comparative advantage of the keyboard is that it is fully passive or automatic and eliminates the possibility of the driver leaving the car with the key in it.

The doorlock modifications demonstrated that it is possible to achieve substantial increases in defeat time over the systems used in most current production vehicles. However, the resulting times do not offer a major deterrent to the skilled and dedicated thief and do present an inconvenience to the owner who locks his key into the vehicle. Since the amateur thief can ultimately break the window to steal the vehicle, if necessary, it is believed that doorlock improvements are not the optimum way to achieve mandated improvements in theft deterrence.

Likewise, a locking hoodlatch achieves a significant level of deterrence and, in some vehicles, may provide an important method to attain the required degree of protection for the remote locking system. However, in many vehicles, such as the test vehicle in this program, the hood lock only provides a short delay to the skilled thief. Thus, its effectiveness as a mandated feature is questionable.

7. ANTI-THEFT STANDARD DEVELOPMENT

The ultimate objective of this program was to develop and recommend modifications to FMVSS No. 114, *Theft Protection — Passenger Cars,* which will improve anti-theft system performance. This chapter presents a detailed comparison of the two existing anti-theft standards, FMVSS No. 114 which is provided in Appendix F and its European counterpart, E.C.E. Regulation No. 18 given in Appendix G.

One of the objectives of this program was the development of standard provisions that specify minimum performance in a way which is not design-restrictive. In studying the existing standards, it became clear that there are three important characteristics of this type that can be attributed to a given standard provision. These characteristics are defined as follows for the purposes of the discussion contained in this report:

Unrestrictive — Any provision which neither specifies nor presumes a particular design or class of designs for the anti-theft system or protective device;

Design-Limited — Any provision which presumes that a particular design or class of design may be used to meet unrestrictive requirements and applies only to such systems or devices;

Design-Restrictive — Any provision that specifies the use of a particular design or class of designs.

Then, based upon the vehicle theft survey of Chapter 3, the development of performance criteria of Chapter 4, and the design and test work of Chapters 5 and 6, alternate standard provisions were developed and modifications to the standard were recommended.

COMPARISON OF EXISTING STANDARDS

In general, ECE Regulation No. 18 is considerably longer and more detailed in presentation than is FMVSS No. 114. Thus, it is convenient to follow the paragraphs of Regulation No. 18, bringing in the FMVSS No. 114 provisions for comparison at the appropriate point. Each of these comparisons is then followed immediately by a comment relating to the importance of the provisions and any improvements suggested by the vehicle theft survey and other work in the program to date.

Purpose, Scope, and Application

Paragraph 1.1 of ECE No. 18 simply states that the regulation applies to devices that can prevent unauthorized use of power-driven vehicles having at least three wheels. The related provisions of FMVSS No. 114 are covered in Paragraphs S1 and S2, where the purpose is stated to be the specification of requirements for theft protection to reduce the incidence of accidents resulting from unauthorized use, and the applicability is stated to be for passenger cars.

Comment: *The inclusion of accident prevention in the purpose is appropriate for FMVSS No. 114. However, the applicability to ECE No. 18 is broader, since it includes all powered vehicles with three or more wheels, while FMVSS No. 114 only covers passenger cars. In fact, ECE No. 18 could be considered too broad in that it extends coverage to heavy trucks and buses. The vehicle theft survey, however, identified the importance of protection against the theft of* *light trucks and multi-purpose passenger vehicles which are among the most frequently stolen late-model vehicles in the western states. Thus, it is concluded that FMVSS No. 114 should be extended to these vehicle classes.*

Definitions

Paragraph 2 of ECE No. 18 contains part of the basic functional requirement specified by the regulation, since it defined the "protective device" as a system to prevent the unauthorized normal activation of the engine in combination with at least one other system which prevents the effective movement of the vehicle. This is somewhat redundant with the later requirements specified by Paragraph 5. The comparison with FMVSS No. 114 will be drawn with the latter. This paragraph also defines the boundaries of the steering system and defines "combination" and "key." The latter two terms are defined in exactly the same way as they are in Paragraph S3 of the FMVSS No. 114 which contains no other definitions.

Comment: *This section of the standard should rightfully contain the definition of any term used in later provisions which is not otherwise clear.*

Functional Specifications

Paragraph 5.1 of ECE No. 18 requires that the protective device prevent normal starting of the engine and steering or forward self-mobility, unless the device is put out of action. Paragraph S4.1 of FMVSS No. 114 provides for exactly the same function, except that it states that it should be a key-locking system and it does not allow for the ineffectiveness of the system if it is put out of action.

Comment: *The broad definition of "key" in both standards allows the use of virtually any code-insertion device, including removable keys and keyboards. However, Paragraph S4.1 of FMVSS No. 114 presumes a key that can be removed and is, thus, design-restrictive. Although Paragraph S4.1 does not make provision for the ineffectiveness of the system if it is put out of action, that must be presumed and is, of course, true for all systems used to meet the standard. It should be noted that the ranking of performance criteria of Chapter 4 suggests that it is only necessary to lock one critical vehicle function, if this locking function is also covered by an effective attack-resistance specification.*

Single Key and Supplementaray Devices

Paragraph 5.2 of ECE No. 18 requires that the functional specifications be accomplished by the action of a single "key." FMVSS No. 114 has no such explicit provision, but implies this by activating the system when "the key is removed." Paragraph 5.2.1 allows supplementary devices using separate keys.

Comment: *FMVSS No. 114 is design restrictive in this sense, because there is no inherent need to require a removable key for an effective system. Note that the single key provision of ECE No. 18 has no effect on doorlocks. A separate key is explicitly allowed by Paragraph 5.2.1 for that purpose.*

Passive Activation

Paragraph 5.3 of ECE No. 18 requires that the anti-theft system be activated in order for the key to be removed. This is also mandated by S4.1 of FMVSS No. 114.

Comment: *Fully passive activation of the system must take place whenever the driver shuts off the engine and/or leaves the vehicle. Both standards allow systems where a key can be left in the vehicle, a situation that results in approximately 13.6% of all thefts.*

Attack Resistance

Paragraph 5.4 of ECE No. 18 requires that the system not be capable of rapid, inconspicuous defeat by low-cost, easily concealed and readily available tools. FMVSS No. 114 has no such requirement.

Comment: *This performance definition in ECE No. 18 is one of the major distinctions between the two standards and is the basic fault usually attributed to FMVSS No. 114. The weakness of the ECE No. 18 provision is that it does not define the attack-resistance characteristics — defeat time, accessibility, conspicuousness, or resistance to tools — in specific terms. Thus, although many objective critics would conclude that no U.S. system meets this requirement, it is subject to argument. To be effective, each of these performance characteristics should be defined in a way which clearly states the required performance level. This can be done in an unrestrictive way for defeat-time and conspicuousness. Accessibility limitations, however, imply some degree of design restrictiveness since they, in effect, specify one or more acceptable locations and may force the designer to use a given type of signal transmission. Similarly, definition of resistance to specific tools is inherently design-limited, since it can only reflect the ability of the author to visualize the systems that will be used to meet the standard. Moreover, as new systems are developed, such a requirement is likely to become ineffective, because new tools will be adapted by the thief to overcome the system. Thus, it appears that an attack-resistance specification should not provide any restriction to the tools used or, alternatively, should make only a very broad restriction, such as allowing only hand-powered tools.*

Disassembly

Paragraph 5.5 of ECE No. 18 requires that the device be original equipment and restricts its design to one which cannot be defeated by removal of its housing or disassembly without destroying part of the protective device or cutting non-removable fasteners. FMVSS No. 114 has no such provision.

Comment: *Current systems would not meet this requirement since they can be defeated by removal of their housing. Moreover, the requirement for covered or non-removable fasteners is design-restrictive. It would appear that this type of requirement would be superfluous if the preceding one were worded in a clear and effective fashion.*

Number of Combinations

Both Paragraph 5.6 of ECE No. 18 and Paragraph S4.3 of FMVSS No. 114 require more than 1,000 combinations for the device if the manufacturer's production is greater than 1,000 (annual production is specified by ECE No. 18). However, ECE No. 18 requires that the actual frequency of occurrence of one combination be 1 per 1,000 in vehicles of one type.

Comment: *Here ECE No. 18 is potentially much more effective than FMVSS No. 114, since merely providing 1,000 different combinations does not guarantee their random use unless the frequency of occurrence is specified. The provision is unrestrictive, since every anti-theft system has a combination of some sort.*

No Visible Code

Paragraph 5.7 of ECE No. 18 requires that neither key nor lock shall be visibly coded. There is no such requirement in FMVSS No. 114.

Comment: *Lock combinations stamped on lock cylinders, or on plates, in a vehicle have been used by thieves to obtain keys and steal vehicles. The requirement would be more broadly effective if it forbade the recording of the system combination anywhere on the vehicle.*

Torque Requirement

Paragraph 5.8 of ECE No. 18 requires that the lock cylinder shall resist turning under a torque less than 0.25 m-kg, except with the mating key. FMVSS No. 114 has no such requirement.

Comment: *This requirement applies only to conventional lock cylinders, and thus can be considered design-limited. It is aimed at a method of defeat commonly used, viz., the breaking of the lock tumblers. However, the specified torque appears to be much too low to be effective since 0.25 m-kg. (21 in.-lb) can be easily applied with a pair of pliers or a small wrench. The minimum torque to failure should be 15 or 20 times this level and the key-slot should be small enough to preclude the insertion of blank keys of high-strength steel large enough to sustain the torque required to break the tumblers.*

Lock Design

Paragraphs 5.8.1 and 5.8.2 of ECE No. 18 forbid certain combinations of identical tumblers. FMVSS No. 114 has no such requirement.

Comment: *This requirement applies only to conventional lock cylinders and is aimed at preventing torsional forcing with a small number of try-out keys. It is design-limited and appears to be somewhat redundant with the torque requirement. It could, however, be accomplished in a very general, non-design-limited way by stating that no combination with more than two identical code values or levels would be acceptable.*

Safety

Paragraph 5.9 of ECE No. 18 requires that it not be possible to activate the system accidentally, while the vehicle is in motion, and further requires that it shall not be activated by an uninterrupted continuation of stopping the engine, or by key withdrawal of less than 5 mm, unless a separate interlock is provided to prevent accidental withdrawal of the key. Paragraph S4.2 of FMVSS No. 114 provides only that the prime means for deactivating the engine not activate the device.

Comment: *FMVSS No. 114 does not preclude activation of a steering lock while the vehicle is in motion, and thus, conceivably could allow an unsafe condition to occur.*

Power Assistance

Paragraph 5.10 of ECE No. 18 provides that, once locked, the anti-theft system must remain in place without power assistance. Thus, cutting the electric or other power to the system must not unlock it. FMVSS No. 114 has no such requirement.

Comment: *Although no current system relies on power assistance to hold the lock in its activated state, it is conceivable that one could be designed in such a manner. It would be susceptible to attack by means of cutting the battery cable or shorting out the electrical system.*

Anti-Starting

Paragraph 5.11 of ECE No. 18 requires that normal starting of the motive power (engine) shall not be possible until the protective device has been deactivated. This appears to be completely redundant with Paragraph 5.1.1 and is the same as Paragraph S4.1 (a) of FMVSS No. 114.

Comment: *This provision is design-restrictive since it mandates that an otherwise effective anti-theft system must be augmented by a device to prevent starting the engine. Although this may be desirable in all cases from a practical viewpoint, it is of dubious importance to theft resistance.*

Particular Specifications

Paragraph 6 of ECE No. 18 imposes a number of specifications on several alternative classes of the device required in Paragraph 5.1. FMVSS No. 114 contains none of these specifications. In summary they are:

(a) Steering locks are required to positively engage once set, meet a specified wear or life test, and resist a 20 m-kg torque about the steering wheel axis.

(b) Transmission locks are required to prevent rotation of the driving wheels.

(c) Gearshift locks are required to prevent change of gear and lock only in reverse, neutral, or park.

Acoustic or Visual Warning Devices

Paragraphs 10.1 and 10.2 of ECE No. 18 allow (but do not require) the device to be equipped with an alarm that sounds the horn or flashes the passing lights for up to 30 seconds. Presumably, although not specified, this would occur only if the device were attacked by a thief. FMVSS No. 114 has no provision.

Anti-Key Retention Warning

Paragraph 10.3 of ECE No. 18 allows (but does not require) a warning device if the driver's door is opened, unless the key has been removed and the protective device activated. This is similar to Paragraph S4.4 of FMVSS No. 114 which *requires* such a warning.

Comment: *However, the warning required by FMVSS No. 114 need not operate if the key is withdrawn partially, or if it is in the "on" or "start" position, or after it has been inserted and before it has been turned. Thus, there appear to be a variety of ways to leave one's key in the car without setting off the warning. Moreover, the warning can cease as soon as the door is closed.*

DEVELOPMENT OF ALTERNATIVE PROVISIONS

The ranking of the performance criteria of Chapter 4 and the results of the subsequent development of an improved anti-theft system, based on the important conclusions of Chapter 4, provide the basis for identification of improvements to the safety standard.

The major issue remains the attack-resistance requirements. The most direct way to specify attack resistance is in terms of time-to-defeat which requires a subjective test for compliance. The alternative is to attempt to obtain an equivalent attack resistance by means of objectively worded provisions that can be tested for compliance without a subjective test. It has been shown that the second approach is inherently more design-restrictive than the former.

The conclusion reached in this study is that this is an issue that must be resolved by the rulemaker rather than the researcher. While a simple time-to-defeat is much more direct and definitive, it is recognized that it presents problems in testing compliance. Thus, coherent and consistent alternative standards are recommended in the next section of this report. The rationale leading to the major provisions of these recommended standards is discussed as follows:

Functional Requirements

It is important to recognize that the standard must be worded so as to ensure certain functional characteristics in addition to attack resistance. The most important of these are mobilization protection and the number of codes allowed by the system.

Although entry protection was found to have significant deterrent value, the studies and test results of this program suggest that it is preferable to put increased cost into the mobilization lock rather than the door or hood lock. Thus, it has been concluded that the safety standard should not mandate improvements in the entry lock system. Manufacturers will continue to provide systems comparable to the current type because the consumer expects and demands it.

The only other controversial functional requirement area is that centering around the problem of ensuring that the owner does not leave a key in the car. The best way to achieve this is through passive activation of the mobilization lock and/or the use of a design which precludes the retention of a key by the system. The current steering column lock cannot be made fully passive without introducing a safety problem. If retention of the key is prevented in the "Lock" position, the driver can leave the key in the vehicle in the "OFF" position. If it is designed to eject in the "OFF" position, locking the wheel, it violates the safety provision which prevents inadvertent locking of the steering while the vehicle is in motion.

It will be recalled from Chapter 4 that fully passive activation is important for theft deterrence, but was rated relatively low for consumer acceptability and cost. However, it is very clear that, if a keyless system were used, fully passive locking with safety interlock is the only rational approach from a security standpoint. Otherwise, the system allows the equivalent of the simple toggle switch ignition. This would return to the simple switch feature used on the 1964 and earlier Chevrolets. These vehicles have always been and continue to be among the leaders in theft rate.

For these reasons, it is concluded that the best compromise between adequate security and lack of design restrictiveness is to require either a fully passive system, or one where a "key" remains in the system while it is inactivated and is incapable of being retained in the system in the locked or activated state.

Defeat Time Requirements

The defeat-time requirement can simply specify that the mobilization protection system cannot be defeated within a period of 10 minutes. However, some means of measuring this must also be implied and this is where the controversy lies.

The only standard currently in use which, like FMVSS No. 114, applies to a design where an attack may be expected on the system is the Poison Prevention Packaging Standard administered by the Consumer Product Safety Commission.[44] This regulation specified a test on each applicable package design by 200 children to ensure a statistical measure of its effectiveness.

Studies in this program indicate that the minimum test sample which would provide any degree of statistical confidence would require about 20 different test subjects. However, a very important factor to consider with the anti-theft system is that failure to deter for 10 minutes with even a single subject is an indication of a fatal weakness in the system. This indicates that a fast method of attack exists which will quickly be communicated and learned by the whole thief population. Thus, it may be concluded that statistical test results are not meaningful, and that compliance testing should be used to attempt to determine the minimum possible defeat time. In practice, this could probably be best achieved through the use of one or more expert anti-theft technicians employed or contracted by NHTSA to test all systems for compliance. A single failure indicates that a system is not good enough. If this scenario is not acceptable, then a standard based on defeat time is probably not practical.

Alternative Attack-Resistance Requirements

The results of Chapter 4 and the design and test program of Chapter 5 and 6 clearly demonstrated the importance of limited accessibility as an alternative to defeat-time. In a standard provision, this must take the form of specifying that the vulnerable decoder and latch elements be housed and located in a defined way.

In Chapter 4 visual conspicuousness was also found to be important. However, there is no simple, objective way of requiring this in a standard. Conspicuousness can best be achieved objectively by judiciously choosing the way in which accessibility is defined.

The tamper-detector approach found promising in the previous discussion presents a problem for the standard writer. Without defining a specific design, there is no way to define its ability to resist attack objectively. Thus, it is concluded that it remains a promising design approach, but only in response to a standard which specifies minimum defeat-time. This is a graphic illustration of the fact that a defeat-time standard is less design-restrictive.

If the standard protects the vulnerable elements of the system from attack by limiting accessibility, the only remaining methods of theft, other than the tow truck, become the various possible methods for obtaining the code. Thus, requirements against identical codes in the doorlock and recording codes on the vehicle become important. Moreover, since inaccessibility implies a remote lock, electrical signal transmission and actuation become likely, and a restriction against the need for a source of power to hold the system in its locked state becomes important.

RECOMMENDED SAFETY STANDARDS

Based on the discussion of the preceding sections, two alternative recommended safety standards are provided as follows.

Alternative A — Minimum Defeat Time

1. Purpose and Scope

This standard specifies requirements for theft protection to reduce the incidence of accidents resulting from unauthorized use.

2. Application

This standard applies to passenger cars, light trucks, and multi-purpose passenger vehicles.

3. Definitions

"Authorizing Code" means a combination of numbers or signals manually applied to or stored on a code-insertion device which permits deactivation of the theft-protection system.

"Critical function" means a vehicle function necessary to the control of the vehicle while in motion.

4. Requirements

4.1 Each vehicle shall have a theft-protection system that, when activated, will prevent —

(a) controlled self-mobilization of the vehicle, and

(b) defeat by a test subject, without advance knowledge of the authorizing code, within a period of 10 minutes using tools that are man-portable to the attack scene.

4.2 The theft-protection system required by 4.1 shall activate automatically when the driver shuts off the engine and leaves the vehicle in such a way that no function critical to safe operation can be locked inadvertently while the vehicle is in motion.

4.3 If a removable code-insertion device is used, the system required by 4.1 shall not be capable of retaining the device in the "OFF" or "LOCKED" state.

4.4 The number of different authorizing codes for the system required by 4.1 of each manufacturer shall be at least 1000, each with a frequency of occurrence of approximately 1 per 1000 vehicles.

Alternative B — Limited Accessibility

1. Purpose and Scope

This standard specifies requirements for theft protection to reduce the incidence of accidents resulting from unauthorized use.

2. Application

This standard applies to passenger cars, light trucks, and multi-purpose passenger vehicles.

3. Definitions

"Authorizing Code" means a combination of numbers or signals manually applied to or stored on a code-insertion device which permits deactivation of the theft-protection system.

"Critical Function" means a vehicle function necessary to the control of the vehicle while in motion.

"Decoder" means a device which responds to the authorizing code to deactivate the theft-protection system.

"Latch" means a locking device which prevents some vehicle function critical to controlled self-mobilization of the vehicle, unless deactivated by the decoder.

4. Requirements

4.1 Each vehicle shall have a theft-protection system that, when activated, will prevent controlled self-mobilization of the vehicle by a person without the authorizing code.

4.2 The vulnerable elements in the system required by 4.1, including the decoder, latch, and any signal path carrying a simple lock-unlock signal, shall be located —

(a) in a major engine, drivetrain, or control system housing, and

(b) in such a place as to be accessible for mechanical attack or disassembly only from underneath the vehicle.

4.3 The standard time allowed for warranty removal and replacement of the housing of 4.2(a) shall be 10 minutes or more.

4.4 The theft-protection system required by 4.1 shall activate automatically when the driver shuts off the engine and leaves the vehicle in such a way that no function critical to safe operation can be locked inadvertently while the vehicle is in motion.

4.5 If a removable code-insertion device is used, the system required by 4.1 shall not be capable of retaining the device in the "OFF" or "LOCKED" state.

4.6 The number of different authorizing codes for the system required by 4.1 of each manufacturer shall be at least 1000, each with a frequency of occurrence of approximately 1 per 1000 vehicles.

4.7 The authorizing code for the system of 4.1 shall be different from any code used for the doorlocks or other locks on the same vehicle and no code shall be recorded anywhere on the vehicle.

4.8 Once activated, the system of 4.1 shall remain passively activated independent of any power source.

8. CONCLUSIONS

The salient technical conclusion that can be drawn from the results of this program is that cost-effective anti-theft systems, which can be expected to drastically reduce the number of automobile thefts, are entirely feasible as factory-installed devices. At least one such design concept has been shown to result in a consumer price increase which is well below the vehicle's share of theft costs over its lifetime.

However, to mandate the result by safety standard requires the inclusion of effective attack-resistance criteria in the standard. The most direct, and least design-restrictive way to accomplish this is to specify a minimum defeat time. This, of course, results in compliance testing problems. Unfortunately, the only alternative is to specify objective requirements concerning packaging and accessibility of the vulnerable elements of the system. This alternative is inherently more design-restrictive.

This program was wide-ranging. It included a vehicle-theft survey; a study of performance criteria and anti-theft standard provisions; and the design, development, and testing of an improved anti-theft system. The principal conclusions that can be drawn from each of the major task areas follow.

VEHICLE THEFT SURVEY

1. The average annual theft rate in the United States is 7.23 per 1000 vehicles, with a peak rate in Massachusetts of 25 per 1000.

2. The national theft rate for certain specialty models appears to be as high as 70 per 1000, and the Massachusetts peak for one model was calculated to be 198 per 1000.

3. Recovery rate data for the entire United States indicate that about 70% of all thefts are committed by joy-riders or small-time, non-professional strippers. The remaining 30% involves professional operations and insurance fraud.

4. The total cost of automobile theft is at least $2 billion annually. Accident costs amount to $60 million and criminal justice system costs amount to $200 million. The remainder represent direct losses to the consumer.

5. Allocation of these costs by type of theft shows that the amateur joy-rider and small-time stripper cost the U.S. consumer between $1.1 and 1.4 billion annually, while professional thefts cost between $0.7 and 1 billion.

6. Thus, the resulting cost of *amateur* auto theft alone is $10 to 13 per registered automobile per year, or $100 to 130 over a 10-year vehicle life.

7. Although a wide range of theft methods have been used, the most prevalent current methods include the use of a slim-jim or wire against the doorlock mechanism and a slide-hammer against the steering-column lock. Nationally, about 13.6% of all thefts are accomplished with a key that has been left in the ignition.

8. The steering-column locks on most vehicles can be defeated in 30 seconds or less, the most difficult within 2 minutes. Although recent data indicate that the theft rate on specific vehicles can be significantly reduced by improving the lock, no changes have been made which appear to deter a theft beyond a few minutes.

9. It is generally agreed among thieves, law enforcement officials, and investigators that deterrence beyond 10 minutes will discourage most amateur thieves.

PERFORMANCE CRITERIA

1. Anti-theft system performance can be specified in terms of functional, attack resistance, and post-theft criteria.

2. The most important functional criteria are either specified in the current FMVSS No. 114, or are satisfied by current design practice. The exception is a suitable combination of anti-key retention and/or passive activation requirements to ensure that the vehicle will not be left unprotected.

3. Time-to-defeat alone can provide sufficient attack resistance, and no other criteria would be required. This would impose no restriction at all on the design used to achieve the required defeat-time.

4. If time-to-defeat is found unacceptable as a performance criterion upon which to base the safety standard, the same result must be achieved through the specification of accessibility limits for vulnerable components and a number of other specific objective requirements. This approach is inherently more design-restrictive.

5. Post-theft criteria which diminish the value of the stolen vehicle represent a promising approach to reducing professional theft. They would effectively reduce the market for stolen vehicles. However, these criteria can best be implemented by improvements in FMVSS No. 115 and local titling laws.

6. Improved attack resistance could also be effective in reducing professional theft if combined with improved local regulation of towing operations.

SYSTEM DESIGN

1. Effective theft deterrence can be accomplished by locking virtually any vehicle function critical to the controlled mobilization of the vehicle.

2. The key to achieving effective performance is to make the vulnerable components of the system inaccessible to the thief. These include the decoder, latch, and any other elements which process the simple lock-unlock signal.

3. This can best be done by locating these components in an inaccessible hardened location, such as a major vehicle housing, which can only be reached from underneath the vehicle or by lengthy disassembly.

4. Following this design approach, a remote steering lock, located in the steering gearbox, was found to resist theft successfully by a former professional auto thief fully briefed in

its method of operation for a period well beyond 10 minutes. This test subject's opinion is that a car equipped in this manner would never be stolen on the street without a tow truck.

5. The remote lock approach implies the use of electronic code transmission between the passenger compartment and the remote location.

6. A keyboard code-insertion device can be a convenient alternative to a removable key and will effectively prevent theft with the owner's key.

7. An alternative to the remote lock is a tamper detector which will respond to attack on an otherwise vulnerable lock by disabling a vehicle function in such a way that lengthy repair time is required to restore it.

8. A remote function lock using a keyboard code-insertion device can be manufactured in high-volume production at a cost which will limit the vehicle price increase to between $17 and $36. This is well below the possible savings in average amateur theft costs to the consumer over the life of the vehicle.

9. Doors are inherently so vulnerable to attack that improvements in doorlocks are not concluded to be a cost-effective approach to theft deterrence.

ANTI-THEFT STANDARD

1. The current U.S. anti-theft standard specifies only functional criteria and not attack-resistance criteria. Thus, it effectively specifies only performance in the absence of attack by a thief. Of course, this is a paradox since the only purpose of an anti-theft system is to resist attack.

2. The current European standard specifies attack resistance in very general qualitative terms which are useless for purposes of testing compliance.

3. The most direct — and least design-restrictive — method for specifying attack resistance is in terms of a minimum defeat-time. This allows a simple straightforward anti-theft standard.

4. However, the time-to-defeat standard inherently carries with it the need for test compliance using a test subject.

5. Objective specification of attack resistance requires definition of general limits on the method of housing and locating the vulnerable parts of the system. This approach is inherently more design-restrictive and, in fact, can be shown to preclude certain promising anti-theft design concepts.

6. Assuming that the objective accessibility limits are effectively defined, there is no technical basis for choosing between these two approaches to the standard. Instead, it is a matter that must be resolved between the rulemaker and the industry. Each must be able to agree on a suitable method for measuring or testing compliance. There is no doubt that meaningful compliance test methods and expert technicians could be developed for this purpose.

9. RECOMMENDATIONS

One objective of this program was, of course, the recommendation of improvements for FMVSS No. 114. These have been made in Chapter 7 of this report. However, the research and development work also suggests a number of specific areas where further work is desirable in order to improve anti-theft technology and the standard against which anti-theft systems are measured. Recommendations for the general direction of this work are included as follows.

DEVELOPMENT TESTING

The fabrication and test tasks of this program were limited in scope to two prototype systems and a single validation test. As described in earlier chapters, this was conducted very conservatively to ensure that the level of deterrence achieved and the defeat time trial would be meaningful. However, it would be desirable to carry the development of the remote lock to the next step of a production prototype packaged as a production unit would be. A number of units should then be fabricated and tested rigorously using every possible method of attack to establish the minimum defeat times.

For the remote steering lock, the methods of attack can be easily identified. They are:

- Mechanical attack on the housing to expose the leads to the unlocking solenoid and actuation with a live wire, followed by hot wiring to start and operate the engine.
- Mechanical attack on the housing, followed by mechanical attack on the latch itself to force it to the unlocked position, followed again by hot wiring the starter and ignition.
- Removal of the entire locked steering gearbox and replacement with an unlocked gearbox or one with a known combination.

It is expected that development testing of this type would allow the identification and removal of any weaknesses in the system. It would also provide general information on the design features that should be included on remote protection systems of this type.

FIELD TESTING

After a production prototype unit has been tested and developed to correct any weaknesses found, the next logical step to establish the capabilities of the system is actual field testing.

With an anti-theft system, however, a field test program must be approached properly to provide any meaningful results. It is well-known that thieves, like a stream, follow the path of least resistance. Thus, if they encounter a car with an unusual anti-theft system, they are likely to move on to one which does not. Even after the general appearance of a new system, a period of learning of perhaps a year is necessary.

For this reason, it is not clear how meaningful results could be obtained from a field test. It is known from a single sample of 4033 successful total thefts and 260 unsuccessful attempts reported in the recent GM survey[18] that the success rate of thieves against the current steering column lock is about 94%.

Preceding page blank

However, if a large fleet of cars were equipped with a production prototype remote lock and field-tested in a high theft rate area, a control against which to measure the results would be difficult. Assuming that the measured success rate were well below the levels which apply to the current designs, it would not be known whether this was due to its invulnerability or simply the fact that the thief population had insufficient exposure to the device to learn its weaknesses.

Another problem is the number of vehicles needed to ensure that a sufficient number of attempts will be made. Even in high theft areas, the average rate is only about 25 thefts per 1000 vehicles per year.

Finally, there would be a need to ensure that every vehicle stolen could be recovered in order that it could be studied to determine the method of theft. For example, if the device forces all successful thefts to be accomplished by tow truck, it would have accomplished its goal.

Thus, it is recommended that any field test program of improved anti-theft devices be conducted in phases. The initial phase should constitute a careful planning program to design the experiment in such a way that adequate control testing is included to ensure that meaningful conclusions can be drawn from the results.

If the results of this initial study are negative, funds would be better spent if channelled into an exhaustive laboratory test program to determine the vulnerability of a proposed design.

DEVELOPMENT OF A TAMPER DETECTOR

The conceptual design analysis of this program indicated that the tamper detector approach, combined with the existing steering column lock and a pick-resistant lock cylinder, is a promising approach. One of its advantages is that it can be implemented with no change perceptible to the consumer.

If this concept requires a remote lock activated by a sensor in the steering column, then there is little to be gained in comparison with the remote lock developed in this program or a similar one.

However, the design concepts illustrated in Figures 7 and 8 hold the promise that such a system could be implemented with minor mechanical changes in the steering column lock itself. This could provide an improved lock with a much lower price increase than a remote electronically coded lock.

For this reason, it is recommended that a design, fabrication, and test program be conducted to develop a prototype of this type of system and test it for vulnerability.

The approach recommended is to select one or more standard U.S. designs for modification. A design study would then be conducted to select the optimum type of modification for each steering column lock. A prototype would be designed and several test steering columns fabricated.

DEVELOPMENT OF DEFEAT TIME COMPLIANCE TESTING

This program has shown the fundamental importance of defeat time as a measure of theft deterrence and noted the relative difficulty in determining compliance with a minimum time-to-defeat standard.

However, the time-to-defeat standard provides a substantial advantage over any alternative because it applies no restriction on the use of clever design.

For this reason, it is recommended that a study be conducted to develop the information necessary to evaluate defeat-time compliance testing of anti-theft equipment. This study should include not only the technical aspects of the testing itself and the test subject, but should also include an initial survey of Government personnel charged with determining compliance, industry personnel responsible for qualifying systems, and any other interested sources of information or opinion. This approach, it is felt, holds the best prospect of finding an acceptable method of assessing compliance which allows the important benefits of a minimum defeat-time standard.

LIST OF REFERENCES

1. Kingsbury, A., *Motor Vehicle Theft, A Bibliography,* Motor Vehicle Manufacturers Association, Vehicular Security Committee, 1974, Available from NTIS as No. PB 241-687.

2. *Crime in the United States — 1976,* Uniform Crime Reports, FBI, Washington, D.C., 1975.

3. *A Special Motor Vehicle Theft Survey Report,* September—October 1974, FBI, Washington, D.C., 1975.

4. *Michigan Motor Vehicle Theft Study,* Michigan State Police, East Lansing, Michigan, Phase I-1974, Phase II-1975.

5. Frese, R., and Heller, N.B., *Measuring Auto Theft and the Effectiveness of Auto Theft Control Programs,* paper presented at the 38th National Meeting of the Operations Research Society of America, Detroit, Michigan, 28-30 Oct. 1970.

6. Barry D., *Report on the Causes and Prevention of Auto Theft in Massachusetts,* Mass. Consumers Council, Boston, Mass., Oct. 1974.

7. U.S. Department of Justice, *Survey on Auto Theft,* Washington, D.C., 1967.

8. *Vehicle Theft Control Project Evaluation Report,* California, Oct. 1976.

9. Personal interview of Mr. Paul W. Gilliland, Vice President of NATB, Jericho, N.Y.

10. Information supplied by Mr. Gene Gardner, State Form Insurance Companies, Bloomington, Il.

11. Information supplied by Mr. Darrell W. Ehlert, Allstate Insurance Companies, Northbrook, Il.

12. Information supplied by Mr. Brian O'Neill, Vice President — Research, Insurance Institute for Highway Safety, Washington, D.C.

13. Boak, R.W., et al., *Summary of the Automotive Theft Survey,* General Motors Corp., Environmental Activities Staff, Warren, Michigan, March 1978.

14. Information supplied by Mr. Richard Hoover, Mass. AAA, Chestnut Hill, Mass.

15. Accident Facts — 1976 Edition, National Safety Council, Chicago, Il., 1976.

16. *Statistical Abstract of the U.S. — 1976,* U.S. Dept. of Commerce, Bureau of the Census, Washington, D.C., 1977.

17. Data supplied by Sgt. Richard Ledbetter, California Highway Patrol, Sacramento, Cal.

Preceding page blank

18. Barry D., et al., *Preliminary Study of the Effectiveness of Auto Anti-Theft Devices*, U.S. Dept. of Justice, Washington, D.C., Oct. 1975.

19. Data supplied by James H. Hunt, Massachusetts State Rating Bureau.

20. Personal interview with Mr. Donald Wolfslayer, Chrysler Corporation.

21. Personal interview with Mr. G.R. Williams, Ford Motor Co.

22. Personal interview with Mr. James Doto, General Motors Corp.

23. *H.O.T. (Hands Off This) Car Campaign Handbook*, Mass. H.O.T. Car Campaign, 1977.

24. Howland, J.S., *Engineering Study of Anti-Theft System Effectiveness*, Foster-Miller Assoc. Inc., Waltham, Mass., December 1976. (Report submitted to Massachusetts Consumers' Council.)

25. Hunt, J.H., *Recommendations of the Hearing Officer Relative to Discounts on Comprehensive Coverage Premium Rates for Motor Vehicles Equipped with Anti-Theft Devices*, Mass. State Rating Bureau, January 20, 1977.

26. Personal interview with the San Francisco Police Dept. Auto Theft Squad.

27. Personal interview with Mr. Lee S. Cole, Auto Theft Ignition.

28. Personal interview with NATB, Pacific Division, Investigators.

29. Personal interviews with five California auto thieves.

30. Brickell, D., and Cole, L.S., *Vehicle Theft Investigation*, Davis Publishing Co. Inc., Santa Cruz, Cal., 1975.

31. *Motor Vehicle Thefts — A Uniform Crime Reporting Survey*, FBI Law Enforcement Bulletin, August 1975.

32. Jones, T.O., et al., *Application of Microprocessors to the Automobile*, SAE Paper 750432, June 1976.

33. Snedaker, K., *The Steal-to-Order Biz: Is Your Car Next?*, Car and Driver, April 1977.

34. *Motor's Parts & Time Guide*, published annually by Motor, 250 West 55th St., New York, N.Y.

35. *Industrial Engineering Handbook*, Maynard, H.B., ed., Second Edition, McGraw-Hill Book Co., New York, 1963.

36. Harvey, M.R., and Chupinski, D.J., *Development of a Motor Vehicle Materials Historical, High-Volume Industrial Processing Rates Cost Data Bank (Compact Type Car)*, Pioneer Engineering and Manufacturing Co., Warren, Michigan, October 1976, Report on Contract DOT-HS-5-01153, DOT Report No. HS-802066, NTIS PB-262-118.

37. Harvey, M.R., and Chupinski, D.J., *Development of a Motor Vehicle Materials Historical, High-Volume Industrial Processing Rates Cost Data Bank (Intermediate Type Car)*, Pioneer Engineering and Manufacturing Co., Warren, Michigan, May 1976, Report on Contract DOT-HS-5-01081, DOT Report No. HS-801-923.

38. Givens, L., *A New Approach to Variable Displacement*, Automotive Engineering, Volume 85, No. 5, May 1977.

39. Mentler, S., *An Improved Vehicular Intrusion Alarm*, Electronics World, August 1971.

40. Marston, R.M., *Anti-Theft Devices — Part II*, Radio-Electronics, December 1976.

41. Howland, J.S., *Conceptual Design Study for the Improvement of Anti-Theft Automobile Ignition Locks*, Foster-Miller Associates, Inc., Waltham, Mass., June 1976 (Report submitted to the Massachusetts Consumer's Council).

42. Bura, M.C., *Increasing the Pick Resistance of the Pin-Tumbler Cylinder Lock*, S.B. Thesis, Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, Mass., June 1975.

43. Personal interview with Mr. James Poole and Mr. William Hunt of Vanderpoole Industries, Inc., Charlotte, N.C.

44. Poison Prevention Packaging, Part 1700, Title 16, Code of Federal Regulations dated July 31, 1973.

APPENDICES

APPENDIX A

LITERATURE SURVEY AND BIBLIOGRAPHY

As part of the vehicle theft survey, a comprehensive literature survey was carried out to uncover information on all aspects of the auto-theft problem including methods used, thief profiles, costs and anti-theft devices.

Early in the literature search, a comprehensive bibliography compiled in an earlier literature search by Kingsbury (1) was supplied by the Motor Vehicle Manufacturers Association. This bibliography is available from the NTIS and contains a comprehensive list of vehicle theft references up to its publication date in 1974. Thus, this literature search was concentrated on obtaining more recent information published between 1974 and the present.

Sources Consulted

The sources consulted in this literature search are listed below. These sources were searched both manually and by computer, wherever possible, to assure maximum coverage.

- Applied Science and Technology Index, 1965 - present
- Best's Insurance Reports: Property and Liability, 1977
- Business Periodicals Index, 1965 - present
- Engineering Index, 1965 - present
- FBI Uniform Crime Reports, 1977
- Insurance Periodicals Index, 1968 - 1976
- NTIS Government Index, 1964 - present
- PAIS (Public Affairs Information Service), 1965 - present
- Psychological Abstracts, 1967 - present
- SAE Abstracts (Society of Automotive Engineers), 1970 - present
- Sociological Abstracts, 1963 - present

Bibliography and Abstracts

1. "Autodiebstahl: Stueckgewinne bis zu 13000 DM." Wirtwoche 26: 44+, October 20, 1972. Discusses auto theft in West Germany.

2. "Auto Thefts Add Up to Billions." National Underwriter p. 63, April 15, 1977. Trade journal article on the costs of auto theft as reported at the 1977 NATB annual convention.

3. Barry D., Report on the Causes and Prevention of Auto Theft in Massachusetts. Boston, Mass.: Massachusetts Consumer Council, Oct. 1974. Study including analysis of theft data to determine rate by model, testing of ignition locks, and interviews of car thieves to characterize the theft problem in Massachusetts.

4. Biles, G.W., Design Study for Decreased Automobile Theft/Intrusion Vulnerability. San Francisco State University, Dec. 1976. Study summarizing proposed auto theft modifications for automobiles.

5. Boak, R.W., et al., Summary of the Automotive Theft Survey. Warren, Mich.: General Motors Corporation, March 1978. Report summarizes the results of a joint project between General Motors and several automotive insurance companies to obtain data on theft by year, make, model; condition of recovered vehicles and dollar losses, theft methods, etc. Survey stresses partial rather than total theft (12,033 out of 16,594 cases) and the Michigan and Illinois area (5857 out of 16,594 cases with rest scattered).

6. Brickell, D., and Cole, L.S., Vehicle Theft Investigations. Santa Cruz, Calif.: Davis Publishing Co., 1975. This book serves as a textbook for training vehicle theft investigators and presents considerable information on vehicle identification and theft methods.

7. California Highway Patrol. Vehicle Theft Control Project Evaluation Study. Sacramento, Calif.: October, 1976. Final summary report of a three-year project aimed at reducing car theft. The report includes a definition of the problem and information on data systems, titling, training and investigation. Considerable information is given on specific techniques, and the report contains the Special Vehicle Theft Arrest Survey (June 1976) which presents data associated with the 646 offenses including offender profile, criminal history, vehicle profile and court disposition.

8. "Car Theft: The 'Pros' Are Taking Over." U.S. News and World Report 81: 45, Oct. 4, 1976.

9. Ferretti, F. "Low Risks Combined with High Returns Helping to Make Car Stealing a Rapid Growth Venture." New York Times p. 29, Feb. 14, 1977. Newspaper article outlining the car theft problems of New York City, especially professional cutting plant operations. Reportedly the source for recent cost estimates for theft given by the Director of the FBI.

10. "Fooling the Car Thief: A Selection of Inventions for Baffling Evilly Disposed Persons." The Autocar p. 386-87, Feb. 28, 1920. Part of a series on car theft which appeared in this British journal. It shows the origins of some of our current anti-theft devices.

11. Frese, R.C., Generating Automobile Theft Control Strategies Via Mathematical Programming. Report to the Missouri Law Enforcement Assistance Council, August, 1972. Study to identify the optimum law enforcement method to reduce the costs of auto theft and expedite vehicle recovery.

12. Frese, R.C., and Heller, N.B., Measuring Auto Theft and the Effectiveness of Auto Theft Control Programs. Paper presented at the 38th National Meeting of the Operations Research Society of America, Detroit, Mich., Oct. 28-30, 1970. Develops a multi-dimensional measure of the aggregate cost of auto theft to a city. Method is illustrated with data on 7278 auto thefts occuring in St. Louis in 1967.

13. Grundy, Gary L., "Engine Staller Thwarts Car Thieves." Electronics 49#26:71-72, Dec. 23, 1976. Article which discusses an anti-theft circuit that simulates engine malfunction.

14. Howland, J.S., Conceptual Design Study for the Improvement of Anti-Theft Automobile Ignition Locks. Waltham, Mass.: Foster Miller Associates, Inc., June, 1976. Study of auto theft methods in Massachusetts indicate that the primary method is the extraction of the ignition lock cylinder with a slide-hammer. Two specific design concepts are presented to thwart this theft method. Also, several specific recommendations are made for strengthening MVSS #114.

15. Howland, J.S., Engineering Study of Anti-Theft System Effectiveness. Waltham, Mass.: Foster Miller Associates, Inc., December, 1976. Study of a number of after-market anti-theft devices to determine their effectiveness for purposes of aiding in determining insurance premium discounts.

16. Hunt, J.H., Recommendations of the Hearing Officer Relative to Discounts on Comprehensive Coverage Premium Rates for Motor Vehicles Equipped with Anti-Theft Devices. Massachusetts State Rating Bureau, Jan. 20, 1977. Discussion of auto-theft in Massachusetts and nationally as it applies to recommended premium discount schedules.

17. Jones, T.O., et al., "Application of Microprocessors to the Automobile." SAE Paper 750432, June, 1976. Paper outlines the potential uses of on-board microprocessors including their application to vehicle security.

18. Kingsbury, Arthur, Motor Vehicle Theft: A Bibliography, Detroit, Mich.: Motor Vehicle Manufacturers Association, 1974 (PB241687). A comprehensive chronological bibliography on all aspects of automobile theft from the late 1800's to the present. The bulk of the work deals with locks of various types and purposes.

19. Marston, R.M., "Anti-Theft Devices, Parts I & II." Radio Electronics 47:56-8, Nov. 1976; 47:68-70, Dec. 1976. Description of several electronic circuits for use in anti-theft systems.

20. Mentler, S., "An Improved Vehicular Intrusion Alarm." Electronics World, August, 1971. This article presents a design for a simple manually activated and deactivated horn alarm circuit that operates from the door jam and other switches.

21. Michigan State Police. Michigan Motor Vehicle Theft Study - August-September - October, 1974. East Lansing, Mich., 1974. Study of the condition of 4784 reported stolen vehicles in Michigan, including analysis of the condition of over 3000 recovered vehicles.

22. Michigan State Police. Michigan Motor Vehicle Theft Study - Phase II - 1975. East Lansing, Mich., 1975. Detailed study of the method used to steal 135 recovered vehicles in Michigan.

23. "Motor Vehicle Theft - A Uniform Crime Reporting Survey," FBI Law Enforcement Bulletin 44, #8, August, 1975. Brief summary of the results of the Sept.-Oct., 1974 FBI auto theft study.

24. Panko, G., and Marshek, K.M., Vehicle Anti-Theft Devices and Systems, University of Connecticut Report, June, 1973. This report presents a summary of specific anti-theft devices obtained from a literature and patent search. These are used to synthesize seven anti-theft systems that are compared in the following reference.

25. Panko, G., and Marshek, K.M., "Comparative Analysis of Vehicle Anti-Theft Systems." ASME Paper 73-ICI-67, Sept. 1973. A decision matrix is used to evaluate and compare seven proposed anti-theft systems.

26. A Report on World Motor Vehicle Theft and Vehicle Security Considerations, U.S. Delegation to ISO/TC22/SC20, Subcommittee on the Identification of Vehicles.

27. Scalzo, J., "Merry Christmas Police - the World of the Car Thief." Car Life p. 34-37, 1969. Discusses car theft by both amateurs and professionals.

28. Serrans Gomez, Alfonso, "Estudio sociologico en la sustraccion en vehiculos." (A sociological study of motor vehicle theft) Revista Espanola de la Opinion Publica 26:129-58, Oct. - Dec. 1971. Study of the age and profile of car thieves in Spain concludes that the problem is primarily due to offenders in the age group from 15 to 20. It reports 98 or 99% of the vehicles are recovered.

29. Snedaker, K., "The Steal-to-Order Biz: Is Your Car Next?" Car and Driver, April 1977. Article based on conversations with a professional car thief concerning methods and disposition of vehicles.

30. U.S. Congress House Committee on Government Operations. Activities of the Interagency Committee on Auto Theft Prevention. Hearing before a subcommittee. 94th Congress. 2nd Session. August 4, 1976. Washington: Government Printing Office, 1976.

31. U.S. Dept. of Commerce National Bureau of Standards. Report of Tests of Automobile Ignition Lock Assemblies - Preliminary Draft. Washington, D.C., June 23, 1976. Tensile and torsional test results for five types of automotive ignition lock assemblies to measure the forces and torques required to remove the lock cylinders or operate the lock without a key.

32. U.S. Dept. Of Justice, Survey on Auto Theft, Washington, D.C., 1967. Survey of theft methods and motivations of 1659 auto thieves covering experience relative to 4077 offenses including the one for which they had been convicted.

33. U.S. Dept. of Justice. Federal Bureau of Investigation. A Special Motor Vehicle Theft Survey Report, Sept. - Oct. 1974. Washington, D.C.: Government Printing Office, March, 1975. This is a survey of the conditions of theft of 10,014 cars recovered during the period of the study.

34. U.S. Dept. of Justice. Federal Bureau of Investigation. Uniform Crime Reports for the United States, 1976. Washington, D.C.: Government Printing Office, Sept. 28, 1977. Summary of crime statistics including auto theft, compiled by the FBI from uniform crime reports obtained from virtually all U.S. jurisdictions.

35. U.S. Dept. Of Justice. Law Enforcement Assistance Administration. National Institute of Law Enforcement and Criminal Justice. Preliminary Study of the Effectiveness of Auto-Theft Devices, by David Barry et al., Washington, D.C.: Government Printing Office, Oct. 1975. Study of effectiveness of the steering column lock provided by the automobile manufacturers for compliance with MVSS 114. Also, presents summary of various auto-theft studies.

36. Wallenga, J.V., "A Study of Adolescent Auto Theft." Journal of the American Academy of Child Psychiatry 3: 14-28, Jan. 1964. Report of group sessions aimed at understanding the motivations and causes for seven juvenile auto thieves.

37. Wolfslayer, D.R. A Status Report on Vehicle Theft and Security. Detroit, Mich.: Chrysler Corporation, July 1976. Summary of various automobile theft data and the effectiveness of Chrysler anti-theft systems.

38. Zadig, E.A. Anti Car Theft Devices Competition. Popular Science p. 83, Sept. 1969. Summary of several patents issued on anti-theft devices.

APPENDIX B

INFORMATION SOURCES CONSULTED

During the vehicle theft survey, the following individuals were contacted or interviewed as potential sources of theft information and data.

1. Automobile Manufacturers

   Chrysler Corporation - Donald R. Wolfslayer
   Ford Motor Company - G. R. Williams
   General Motors Corporation - James R. Doto, William McLean, Thomas Terry
   Motor Vehicle Manufacturers Association - Thomas Carr

2. Automobile Theft Investigation

   National Automobile Theft Bureau - Paul Gilliland, Robert Sattler, Fred Douglas, William O'Donnell
   Independent - Lee S. Cole

3. Law Enforcement Organizations

   Boston Police Department - Sgt. Robert Scobie
   California Highway Patrol - Robert Berg, Sgt. Richard Ledbetter
   Detroit Police Department - Lt. Lordon Snow, Sgt. Richard Clayton
   Michigan State Police - Sgt. Richard Kill
   San Francisco Police Department - Lt. Genna, Inspectors Weatherman and Whitman

4. Insurance Companies

   Allstate Insurance Company - John Trees, Darrell Ehlert, Donald Kosta
   State Farm Insurance Company - Gene Gardner

5. Insurance Organizations

   American Mutual Insurance Alliance - Thomas Whelton
   Highway Loss Data Institute - Dr. William Haddon, John Trees
   Insurance Institute for Highway Safety - Dr. William Haddon
   Insurance Information Institute - John O'Connor
   Insurance Services Office - William J. McCormick

6. Insurance Regulation

   Massachusetts State Rating Bureau - James Hunt

7. Auto Thieves

California - "Ron", "Clyde", "Paul", "Frank", and "Rich". Massachusetts - "Rick", "Mike", "John", "Bruce", "Red", "Peter", and "Manny".

8. Other

Automobile Association of America - Richard Hoover
Massachusetts Consumers' Council - Bruce Singal
Massachusetts HOT Car Campaign - Jerry Swerling

APPENDIX C

LIST OF TYPICAL AFTERMARKET ANTI-THEFT DEVICES

(Adapted from Reference 23)

MANUFACTURER	BRAND NAME	MODEL NO. or SERIAL NO.	COMMENTS
Universal Security Instruments, Inc.	Standard Siren Alarm System	SA-1RCP	Intrusion of vehicle sets off alarm.
		SA-1R	Externally operated.
	Heavy Duty Siren Alarm	SA-1D	Same
	Loud Mouth Electronic Whooper Vehicle Siren Alarm System	ES 250 ES 250S	Same
	Vehicle Sensor Siren	SA-3S SA-3SCP	Same
	Loud Mouth European Sound Alarm System with Sensor	ES-200X ES-200SX	Same
Booth Securities Systems, Inc.	A.M.S. Anti-theft Vehicle Alarm	HA 9000-B	Alarm triggered by any sudden change in voltage caused by a drain on the battery. (e.g. Any light, brakes, horn, etc.)
Digi-Start Corp.	Digi-start		A key controls alarm triggering system for doors, etc. This is external; then key placed in ignition and set of digits must be properly recorded to start car.
Distributed by Ellis, The Rim Man	Deweko Auto Theft		An ignition cut-off switch having armored tubing leading from switch to engine compartment. Must insert a plug that has approximately 18 prongs on it.
Steering Column Security Locks	Big Jim Ignition Lock		Steel locking unit fitted over ignition. Can't get to ignition without removing lock. Also prevents steering of auto.
E & R Advertising	Auto Guard	AG-100	Partially kills ignition, therefore, engine cannot be started. Must be used in combination with tapered door lock buttons.
Alarm Shack	Guardian 1		Alarm sounded when entry made into trunk, hood or any door.
Alarm Shack	Guardian 2		Alarm sounded when entry made into trunk, hood or any door. Will qualify for 10% discount if automatic ignition cut-off device is added.
CAHS, Inc.	Fuel Lock	K-100	Blocks fuel line when hidden switch is tripped.
Whitney Catalog	Fuel Cut-off Device	12-2171T	Blocks fuel line when hidden switch is tripped.
Identicar Corp. of America	Identicar		Computer coded system permanently engraved on all car glass. (By means of sandblasting.)
Tracer Kode, Inc.	Tracer Kode		Same as Identicar.
Trionyx Electronics	Auto Security Alarm	CA-30	Alarm system connected to vehicle with wiring under dash-board. Opening any door activates alarm. Alarm must connect to hood.
Harcor International, Inc.	Auto Security System	3001	System is triggered when any light is turned on. Therefore, hood must be equipped with light. If triggered, horn beeps intermittently for 2½ minutes.
CAHS, Inc.		K-300	Ignition cut-off switch which operates automatically off the ignition.
Alarm Alert Systems	Alarm Alert	Auto-1	Intermittent horn blast activated by entry through any door, hood or trunk.
Car Secure	Car Secure		Permanently attached tempered steel collar covers ignition, and prevents steering.
Security Auto Lock, Inc.	Security Auto Lock		An oversized padlock clamps onto the steering column over the ignition and prevents access to it, and prevents steering.
Universal Security	Universal Siren Alarm	SA-3S	Alarm or siren activated by entry of doors, hood or trunk. External operation.
Selective Shopper	Gard-A-Car		It stalls engine after it has been operating for a few seconds. (Must be used in combination with tapered door lock buttons.)
Sears	Hi Lo Electronic Auto Burglar Alarm		Externally operated alarm activated by opening any door, hood or trunk.
Sears	Deluxe Hi Lo Electronic Auto Burglar Alarm		Same

MANUFACTURER	BRAND NAME	MODEL NO. or SERIAL NO.	COMMENTS
The General Automotive Specialty Co., Inc.	The General with Klaxon Sound	7103	Klaxon Siren activated by entry thru doors, hood or trunk. Internally operated.
	General with Klaxon Sound, Panic Switch & 3 minute exit delay.	7105	Same as above
	General with 3 minute exit delay & Panic Switch	7102	Same as above
	Klaxon Sound with Panic Switch	7107	Same as above
Auto. Device Mfg. Co.	Sensor Alarm	209	Voltage sensing alarm device. External operation.
American Muffler	Redex Alarms	3100	Voltage sensing alarm device, with external operation.
	Redex Alarms	3000	Same as above
Radio Shack	Auto Siren System		External operation. Activated by any door, hood or trunk.
RPI, Inc.	Ignition Kill System	IK277A	Passive kill switch.
	Ignition Kill Switch & Tapered Door lock butt.		Cuts ignition and helps prevent easy opening of the car doors.
Monroe Timer Co., Inc.	Sensomatic Autoshield	S12KL	Internally operated alarm triggered by opening doors, hood or trunk. It is a voltage sensing device.
Petrolock Corp.	Petrolock		Blocks gas flow automatically. Open valve by pressing switch.
Vantwood, Inc.	Fail Safe II Auto Alarm		Siren activated by entry thru doors, hood or trunk. Has automatic ignition cut-off. Activated by turning ignition key.
Sonaguard Div. of Microguard, Inc.	Sonaguard	512-S	System that emits loud pulsating horn sounds. Sets off siren & flashing headlights. Cuts off ignition automatically upon entry of doors, hood or trunk.
Clad Metals Corp.	Good Lock Car Collar		Steel collar permanently attached to steering wheel which prevents steering wheel from turning. Shackles attach to collar and fit between spokes of the steering lock. It is then locked.
RPI, Inc.	Autolarm	AL 576A	Intermittent horn blast activated by entry through any door, hood or trunk.
Jubilee Mfg. Co.	Jubilee Burglar	219	Alarm activated by entry into door, hood or trunk. Also cuts out ignition.
Safety Controls, Inc.	Sav-Car	SC-1	This device is a kill switch designed to resist tampering. It is a fully armored electrical auto starting lock. Activated by key in cylinder lock.
Chapman	Chapman Total Protection Alarm System	TP 3104 MD-8 MD	Includes alarm, Kar Lok, motion detector and detect alarm. Internal control.
Boston Investment Group, Inc.	Thugbuster		Electric hood lock, electronic key connector and key are in passenger compartment. All other parts are located in the engine compartment. Insertion of other than the electronic key incites alarm.
CAHS, Inc.	Automatic Fuel Lock	K-200	Blocks fuel line and also cuts off ignition.
Alarm Research & Mfg. Co., Inc.	Protector II Auto Theft Alarm		Alarm activated when doors, hood or trunk are opened. It is a passive alarm with automatic ignition cut-off. Qualifies only if auto has interior hood lock.
Automotive Security Devices, Inc.	Auto Paralyzer		Electronic device permits engine to start only when a 3 digit code is set on 3 dials. It includes a set of 42 identical wires. (1700 possible combinations.)
Chapman Industries Corp.	Kar Lok	KL-2004-8	Automatically locks hood and cuts off ignition system from within hood by pressing button. Hood lock is armored.
General Automotive Specialty Co., Inc.		7109 w/7802 Ign. cut-off kit	Voltage sensing causes siren to sound when light is turned on. Has automatic ignition cut-off.
Clad Metals Corp.	Guardex	1	A case-hardened steel protective cap which fits over the ignition lock to prevent extraction of the ignition lock cyl.
RPI, Inc.	Autolarm Total Protection System	ATPS-1	Alarm activated when doors, hood or trunk are opened. It is passive w/automatic ignition cut-off. Qualifies only if auto has interior hood lock.
Monroe Timer Co., Inc.	Passive Automatic Autoshield	S12KLP	Alarm activated when doors, hood or trunk are opened. It is a passive alarm with automatic ignition cut-off. Qualifies only if auto has interior hood lock.
Introl Corp.	Ambusher	AL-1	Passes delayed ign. cut-off sys. activated by engine speed.

APPENDIX D

CAR THIEF INTERVIEWS

As part of the vehicle theft survey, a number of admitted or convicted thieves were interviewed. This appendix summarizes the information obtained from five thieves interviewed at the San Francisco County Jail in San Bruno, California and seven thieves interviewed at the Middlesex County House of Correction in Billerica, Massachusetts.

The information obtained in this survey was consistent with that of earlier studies by Barry (6). The thieves usually start at an early age and move on to more lucrative enterprises or jail by their early 20's. None of the thieves interviewed were closely tied to organized auto theft rings although they occasionally may have supplied rings with cars or parts. They normally have buyers for parts lined up before the theft.

They all state that cars in which entry is not easy are a deterrent as are alarms. None of the California thieves was familiar with effective methods to attack steering column locks, while all Massachusetts thieves were familiar with most of the known methods. This correlates entirely with the differences in the theft data between California and other areas of the country.

None of the thieves interviewed relied on car theft as a primary means of income. They each learned the techniques they used from friends, but did not often compare techniques with other thieves once they began.

The salient information obtained in each interview is summarized in the following paragraphs with a nickname or pseudonym used for identification. In addition, the characteristic theft times and limits were obtained from most of the thieves and these are summarized in the discussion in the main body of the report.

California Thief Interviews

CLYDE

Clyde is 30 and serving a term for an offense other than car theft. However, he has stolen many cars, starting very early in his teens.

He stated that he had stolen cars for selling parts and resale of the car. He was familiar with replating the VIN.

He described the use of jiggle keys (on ca. 1968 GM cars), combination pick and prybars as typical methods. When he was very young, he often searched for a car with a key in it. He listed his theft time as 5 minutes. If it took 10 to 15 minutes, he would begin to worry. He stressed the vulnerability associated with the time before he could get the door open. He never broke window glass to get in.

He did not appear to be familiar with the slide-hammer, nor had he had very much experience with steering column locks since he has been in jail most of the time that they have been used on automobiles.

FRANK

Frank is 42 years old and is currently serving a four-month term for burglary. He estimates he has stolen 200 to 300 cars, beginning when he was 11 years old. He has not stolen a car for 15 years. His only arrest for car theft was when he was young, and he was caught primarily because he was driving erratically.

Frank started stealing at an early age, and his first car theft was at age 11, which was a 1928 Buick. Thereafter he stole cars primarily for his own use. He occasionally fixed up the cars and parked them several blocks from home for convenient access. He estimates he has stripped only about 10 cars. He said in all cases it was necessary to have the buyer lined up ahead of time.

Frank stopped stealing cars when he could afford to buy one of his own. The primary reason for stealing cars was to have a means of getting around town. For him, the car was "power, a space ship, my ride to the moon".

The method of theft was finding cars with keys in the ignition primarily.

Frank is primarily a burglar and armed robber. For these jobs, he says, it is not advisable to use a stolen car. He estimates he has participated in 300 armed robberies and 300 burglaries. He has spent 19 out of the last 24 years in prison for armed robbery.

Frank had only one experience dealing with organized car theft. A friend asked him if he would be interested in stealing cars for sale to a body shop. Frank drove with a friend to Oakland from San Francisco and dropped off a car and watched his friend be paid $500. He saw seven or eight young men working in the operation. Because it did not feel safe for him, he turned down the offer.

Frank is trained as a practical nurse, and in between his stays in prison that is his part-time occupation.

PAUL

Paul is 27 and currently doing a one-year sentence for auto burglary. He has stolen 15 or 20 cars in his career, but mostly these were taken during a period approximately nine years ago.

Paul stole cars mostly to impress his friends and for entertainment. Except for the occasional prank, there was no harm done to the car. At that time, he used no drugs which he could not easily afford. Since the period of theft was up to and including 1968, none of the cars had steering column locks. His basic theft method was to hot wire the cars.

Paul stole cars which were unlocked, or which were locked and had either a small vent window or rubber stripping between the front and back side windows. He could not get into cars in which the windows fit into slots in the door. When he had to defeat a door lock post with a tapered aluminum shaft rather than the usual mushroom shaft, he used a coat hanger over which surgical tubing had been pushed. He then put a crook midway in the surgical tubing and placed this over the door post and got sufficient friction to lift the door post up.

Paul has virtually no knowledge of how to break the steering column lock in the newer cars. He said that he knew a thief who could use a crescent wrench to break the wings (probably on a Ford) lock. He said he had tried one or two himself, but had trouble with them.

Paul never discussed techniques with other thieves. He gained his knowledge from experimentation. Part of his understanding of cars comes from working in a wrecking yard. Paul has good mechanical intuition, and explains his techniques articulately.

Paul says there are two types of auto alarms used on cars. One involves a small metal pendulum which hangs inside a small metal ring. Any motion of the car will cause the pendulum to touch the ring, activating an alarm circuit. To test whether a car has this type of alarm, all the thief has to do is shove the car, and see if the alarm is activated. If the alarm does not go off, then it is probably one which is activated by turning on the dome light or the light under the hood.

Paul has no experience in defeating the motion-sensing alarms. To deal with the second alarms, Paul has climbed in through the window to start the car and drive it away. Once it is in a safe location, he deliberately sets off the alarm and then goes under the hood to cut the appropriate wires. However, he has only had one or two encounters with sirens, and avoids them when he can.

Paul has had very little experience selling parts from cars, and has never sold an entire car. He says that it is necessary to have the buyer lined up ahead of time for a specific part. On one occasion, Paul obtained a part specifically for a buyer. He says that there is too much risk in selling the entire car.

Paul has been out of car theft since he was approximately 18, but landed in jail again when he was caught stealing from cars to support his heroin habit. To pay for his heroin, he has stolen parts from cars, without stealing the car. C.B. radios are the best item for resale.

RICH

Rich is 21 and currently doing six months for an auto theft arrest. He estimates he has stolen between 75 and 100 cars since age 17. He learned the techniques from watching friends at school.

Rich mostly stole the cars for the parts. In all cases, he had buyers lined up ahead of time. Many times, he stole engines from cars for sale to buyers who would drive down in trucks from Sonoma County, California. He charged between $200 and $400, depending on what the buyer could afford. These buyers were switching engines for resale to others.

Rich first stole cars for his own use and to impress his dates. Once, he bought a derelict Volkswagen for $30 in a junkyard. He pulled off the VIN and placed it on a stolen VW. He was stopped by the police for an equipment violation and the police found that the car was stolen. However, charges against Rich were dropped when it was discovered that he had taken steps to register the car in his own name. Rich could have recovered the car, but decided not to for fear that he would be discovered.

Rich has training as a sheet metal worker, and has worked in that field for five years in a union. He says he is giving up car stealing, because it has become only a pastime to him which, upon reflection, seems petty. The guys he knows who steal cars are all between 18 and 24. He does not feel there is very much money in car theft, and hopes to get his contractor's license.

Rich never stole any cars which had a steering column lock. He does not really know how, although a friend once showed him how to remove a lock without using any force. The friend somehow twisted the head of the lock off.

Rich's primary method with the older cars is to break the ignition lock with a screw driver or to hot wire the car. He always checked for sirens in order to avoid them.

Rich would only steal cars in which he could enter the car easily. Otherwise, broken windows would be a sign to a policeman. Thus, he relied on cars which were unlocked, or in which there was a small vent window, or where there was rubber stripping between the front and rear side windows.

RON

Ron is 22 and serving a term for auto theft. He estimates that he has stolen 40 to 50 cars and has been doing it since age 15. Most of his thefts were for transportation although he has sold some parts.

He usually steals older cars and listed the 1964 Chevrolet as a favorite. The usual method is hot-wiring. On occasion, he has stolen the key and had one made for his own use.

He does not try to steal cars with a steering column lock and stated that to use brute force on this type of lock takes too much time. He estimated that his time limit is about one minute to steal a car.

He is unaware of the slide-hammer or other measures effective against the steering column lock.

Massachusetts Thief Interviews

RICK

Rick is 22 and has a long record of car theft. He began at age 9 in a group, where he learned the techniques, and claims to have stolen 3000 cars. His ability to avoid capture does not appear to be as high as his theft capability.

His technical capability is high for the cars in which he specialized, Chrysler products with emphasis on the high-performance models. He uses the dent-puller for steering column locks and hot wires the older models. He is not familiar with the slim-jim and uses the vent window or a wire to pop the interior button to gain entry.

He does not damage the cars or strip them except for occasional tape decks or C.B. radios. He is not in the parts or vehicle resale business.

MIKE

Mike is 27 and began stealing cars at age 14. He often works alone and claims to have learned by himself. He estimates that he has stolen 1000 cars but this is probably a low estimate considering other remarks he made about his career.

His technical capability is extremely high and he knows the specific method of attack best used on every type of vehicle. He also exhibited familiarity with many methods not commonly used in Massachusetts and has stolen cars all over the U.S.

His motives were sometimes transportation and sometimes sale of parts for profit. His customers in the latter enterprise were usually body shops or dealerships. Sometimes he would deliver whole cars to order (price ~$500) and sometimes major body parts. At one time, he supplied VW's on order which he claimed ultimately became rental cars or dune buggies. Five or six thefts a night were not unusual for these cases.

JOHN

John is 26 and has been stealing cars since he was 15. He started in a group and then worked alone.

His motive was always transportation and he claimed he often kept the car five or six months. As would be expected, he was caught with several of these which had long been reported as stolen. He estimates he has stolen 25 vehicles.

He is a mechanic and would often improve the car while he was driving it. His technical capability is high and he is familiar with several methods of attack.

However, he often steals cars in parking lots or garages with the key in them. He also stated that 70% of the cars he has stolen were unlocked. He is aware of the common methods of unlocking the door but not the slim-jim.

He was never in the parts or vehicle resale business.

BRUCE

Bruce is 22 and began stealing cars in Maine at age 14. He estimates he has stolen 40 vehicles.

However, his technical capability does not appear significant and, unlike most Massachusetts thieves, he usually steals cars which have keys in them. He claims he does not know how to overcome the steering column lock.

Most of his experience is in small Maine cities instead of Boston and this may account for the number of vehicles left with keys in them.

His sole motive was transportation.

RED

Red is 18 and began stealing cars when he was 15 in a group. He estimates that he has stolen 25 vehicles and says he always steals Ford Grand Torinos. His usual method was to pop the ignition lock out with screwdrivers rather than a dent-puller although he was familiar with the latter.

He said that the dent-puller is not comfortable to carry while running.

His only motive was transportation although occasionally he removed and sold the wheels and tires.

PETER

Peter is 20 and began stealing cars when he was 16. He stated that he often stole 5 a night but did not have an estimate for the total.

He was familiar with the dent-puller and the normal methods for using screw-drivers on various models. His methods of entry were standard and he did not appear familiar with the slim-jim.

His sole motive was joy-riding.

MANNY

Manny is age 21 and began at age 14 with a friend. He estimates he has stolen about a hundred cars.

He was quite familiar with the common theft methods and the vehicles on which they can be used. He normally pops the button up, working through the window gasket, in order to gain entry and did not mention the slim-jim.

His sole motive was transportation and he is not familiar with the parts or vehicle resale business.

APPENDIX E

LOCK PICKING AND PICK-RESISTANCE LOCKS

The conventional automobile key lock can be improved to resist defeat within a prescribed time period by direct attack on the lock cylinder or its housing. This will, in general, require a combination of strengthening certain components and packaging to eliminate access to the latch after the vulnerable elements are forced. If this were accomplished, it is expected that a significant number of automobile thieves would turn to lock-picking, a method seldom used currently for car theft.

Two of the major U.S. manufacturers use simple pin-tumbler locks, such as that shown schematically in Figure E-1. This type of lock is picked very simply and quickly using the method illustrated in Figure E-2. Torsion is applied to the barrel by means of a moment-applying tool. The pick is then used to determine which pin is taking the torsional load as shown in Figure E-3(a) and this pin is forced upward until the load is released and the upper pin rests on the shelf as shown in Figure E-3(b). The pick is then used to find the next pin taking the moment and the action repeated until all five or six pins are at the release point and the barrel turns. In practice, this can be done by a skillful lock picker in a few seconds for the simple pin-tumbler lock.

There are many lock designs which can make picking so time-consuming that it becomes impractical. For example, Bura[42] simply machined a number of grooves in the pins. These grooves give false release signals, as the pin is forced upward, as illustrated in Figure E-4. Thus, the thief never knows whether he has reached the correct point with a given pin set. A prototype of this lock resisted picking by several locksmiths.

Other pick resistance lock concepts include the sidebar principle used in the General Motors cylinders as shown in Figure E-5, the Medeco lock of Figure E-6, and the Ace lock of Figure E-7, and the Keso lock of Figure E-8.

In the GM lock, the sidebar which has a very high torsional or shear strength does not drop until all six plate tumblers are in the correct location and there is virtually no pick signal available from one tumbler. The Medeco lock uses tumblers with two degrees of freedom, height and angle, and the latter does not provide a convenient pick signal. The Ace lock incorporates 7 axial pin sets which, in essence, require that it be picked several times to rotate the barrel through one revolution. The Keso lock provides a large number of pin-tumblers acting in four different directions which makes the picking action much more difficult and time-consuming.

Preceding page blank

It can be concluded that much of the gain resulting from improvement of the key locking system would be quickly lost if the simple pin-tumbler lock were retained in a large proportion of automobiles. However, there are many types of pick-resistant locks known within the state-of-the-art which can likely extend the pick time sufficiently at a moderate cost.

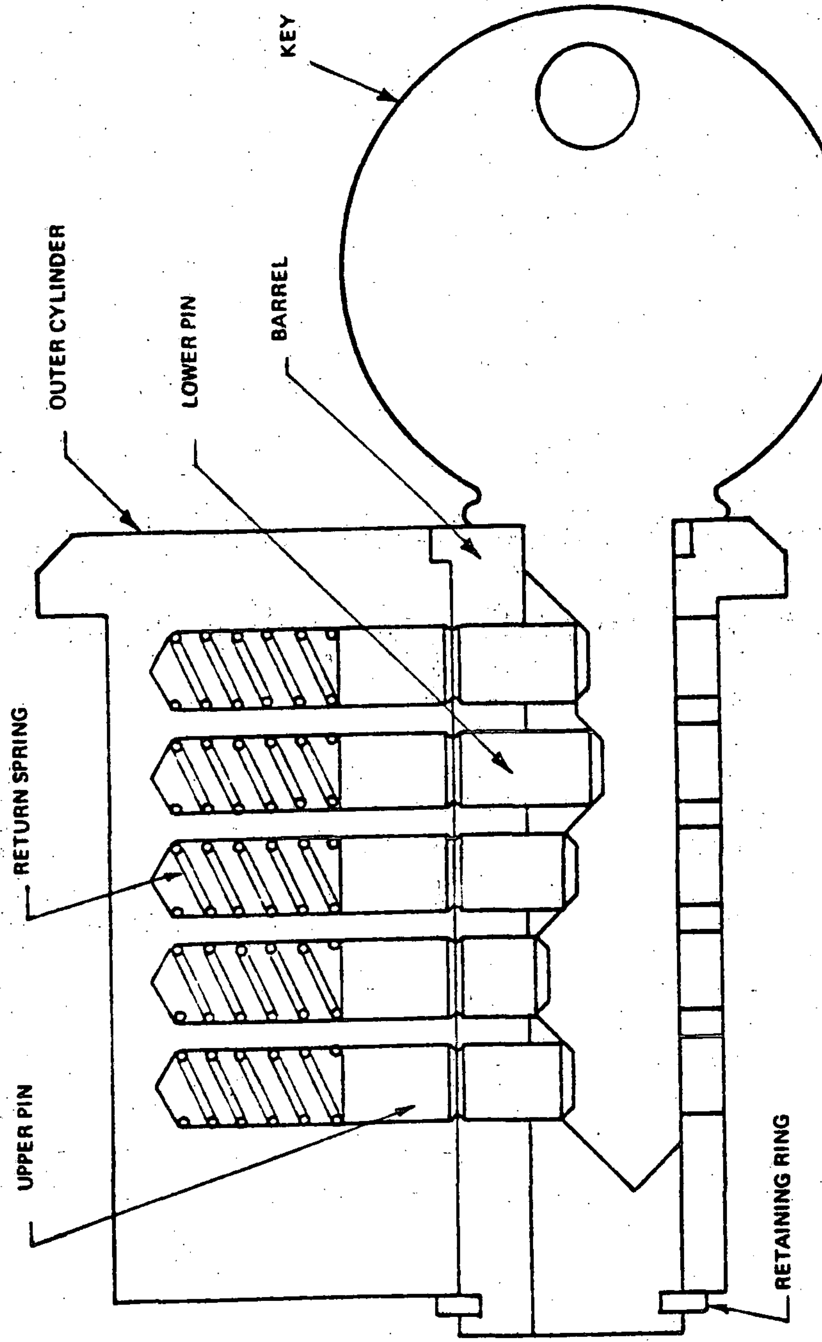


FIGURE E–1. SIMPLE PIN-TUMBLER CYLINDER LOCK.

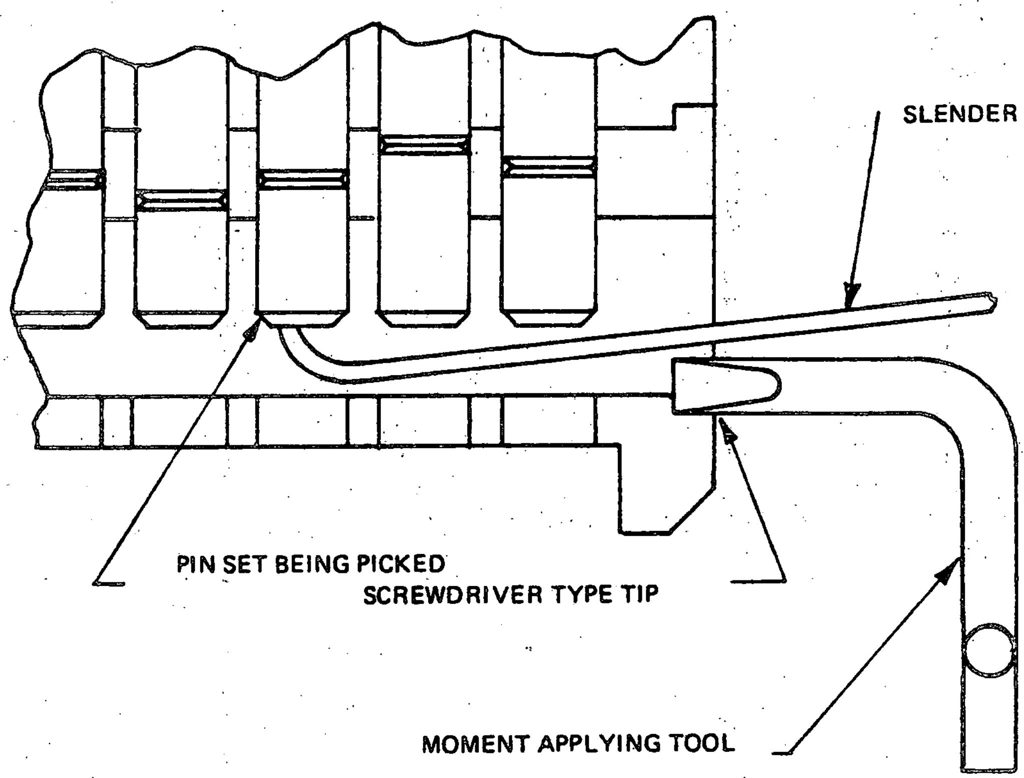
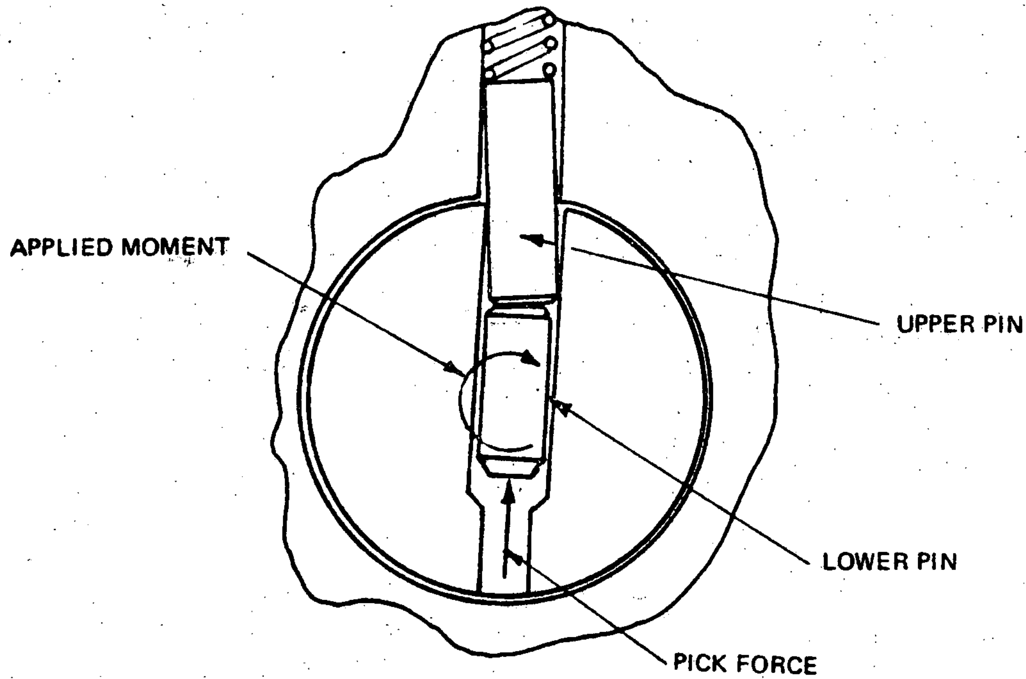
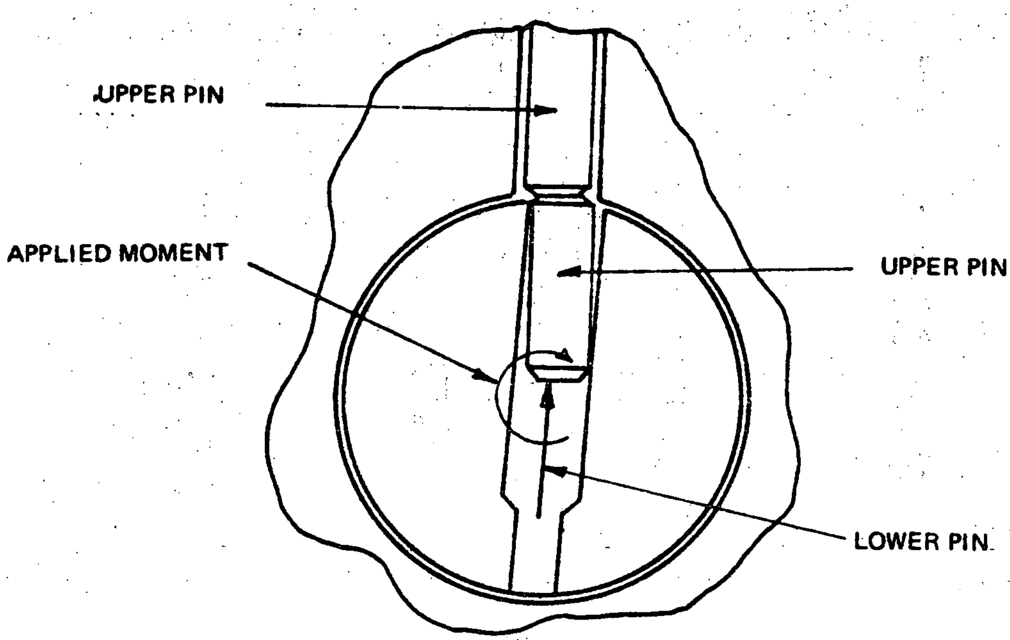


FIGURE E–2. PICKING THE PIN-TUMBLER CYLINDER LOCK



(a) PIN SET TAILING THE MOMENT



(b) PIN SET AFTER PICKING TO RELEASE POINT

FIGURE E–3. PICKING ACTION ON A SINGLE PIN SET.

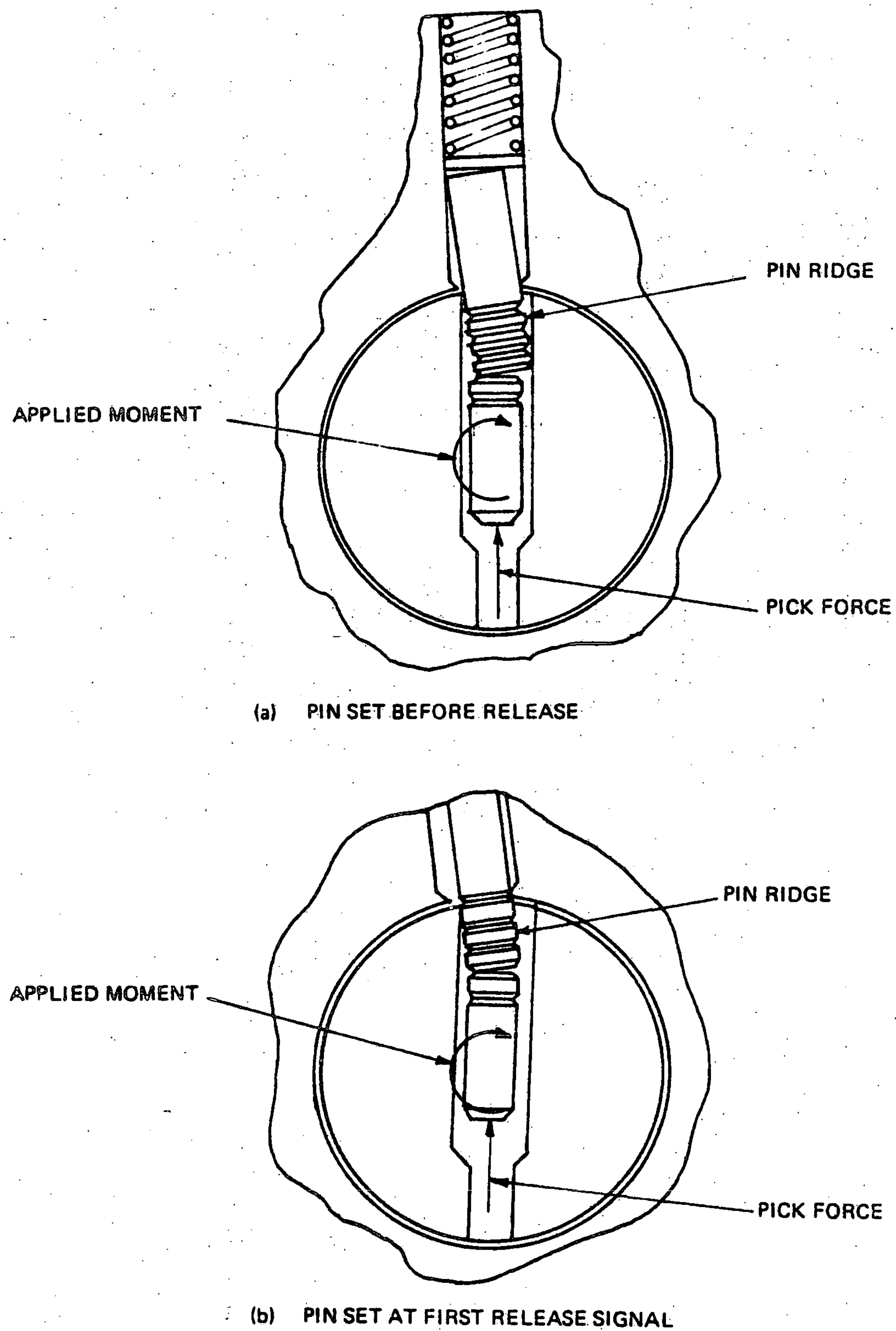


FIGURE E–4. BURA PICK RESISTANT LOCK.

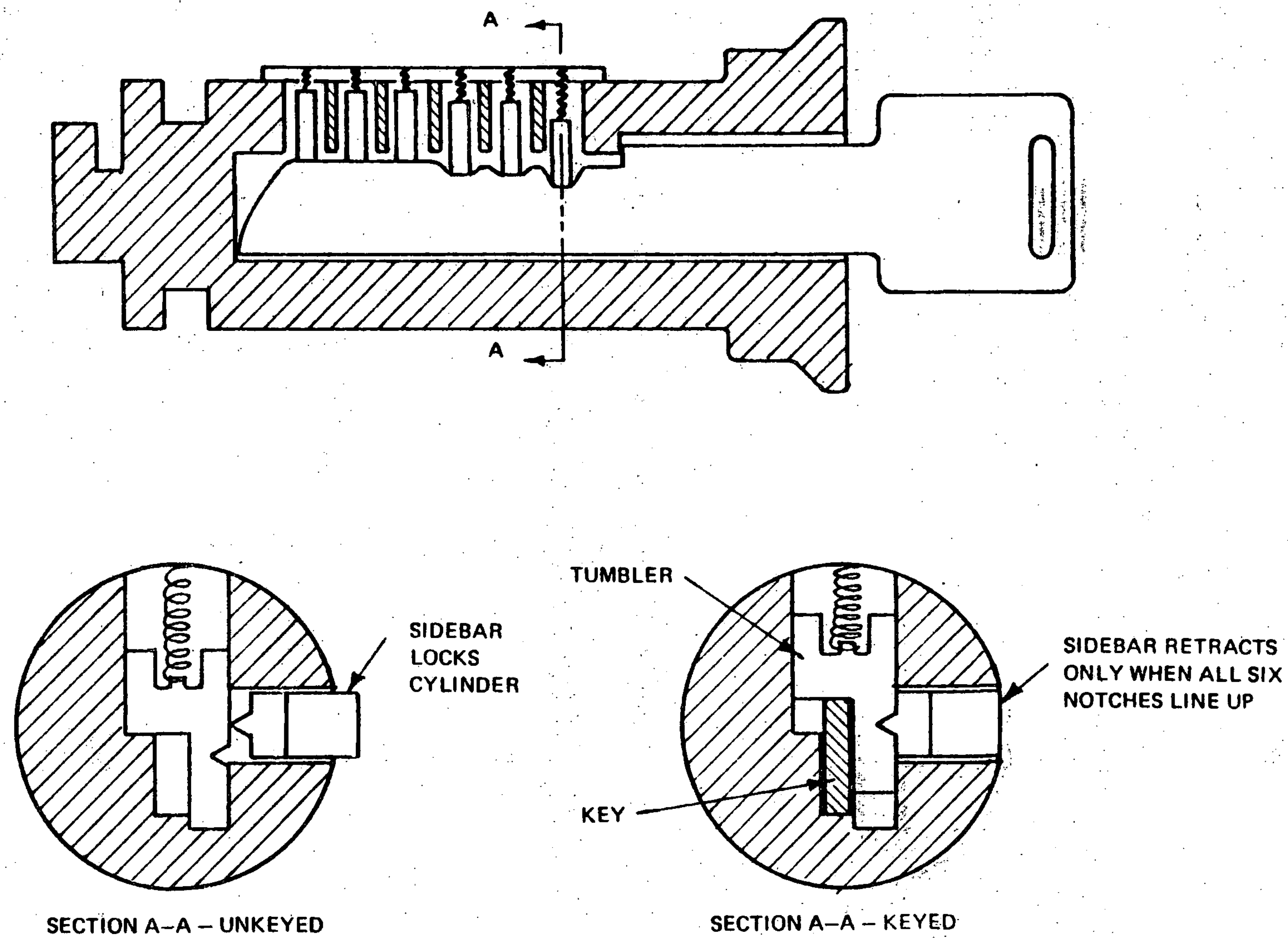


FIGURE E–5. SCHEMATIC DIAGRAM OF THE SIDEBAR LOCK.

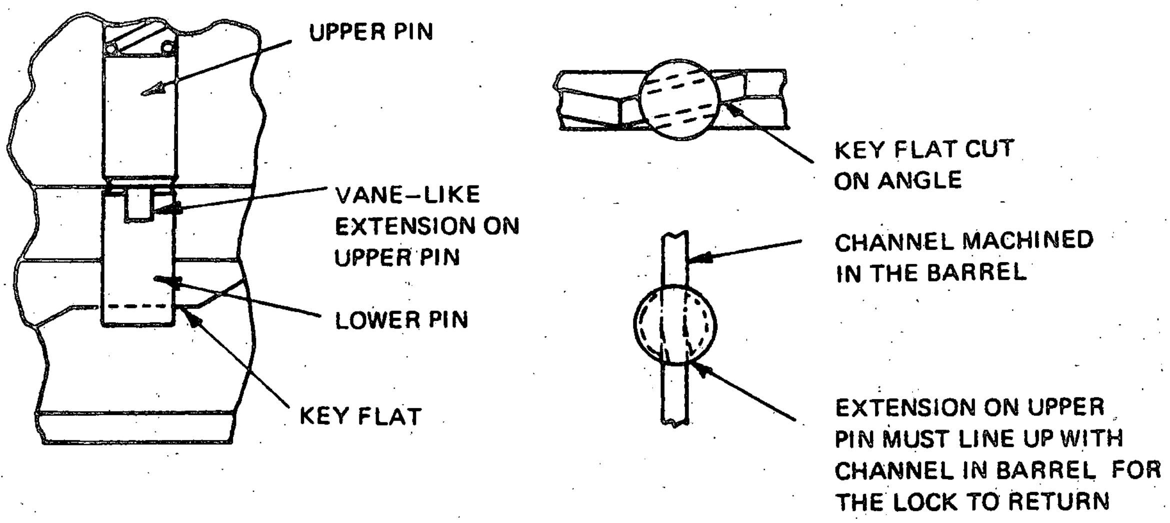


FIGURE E–6. SCHEMATIC DIAGRAM OF MEDECO PIN SET.

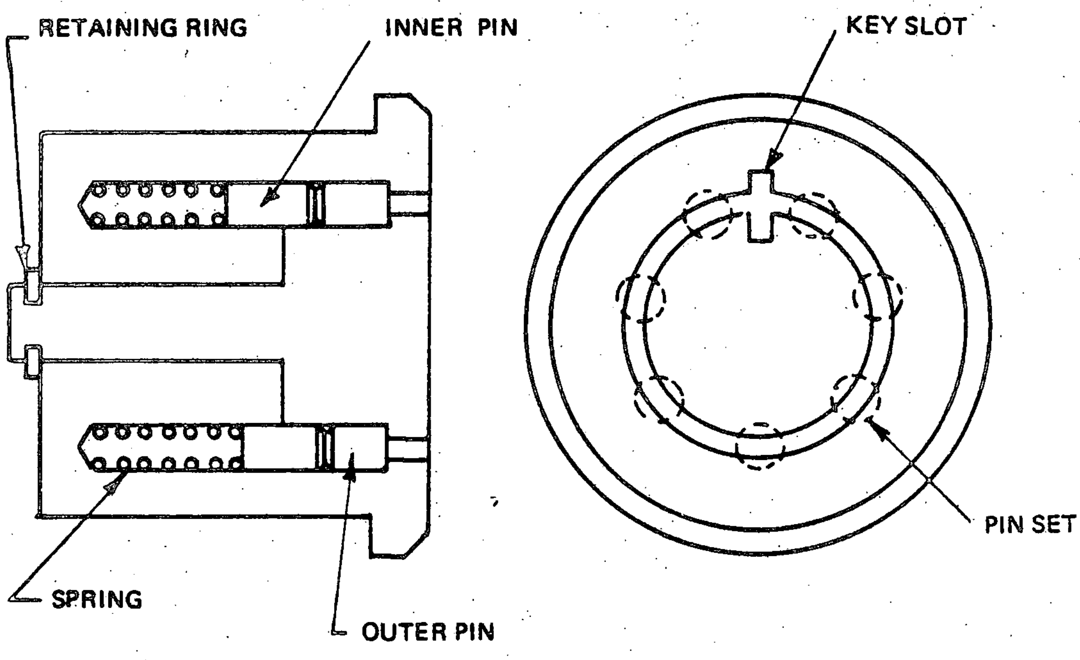


FIGURE E–7. SCHEMATIC DIAGRAM OF THE ACE PIN–TUMBLER LOCK.

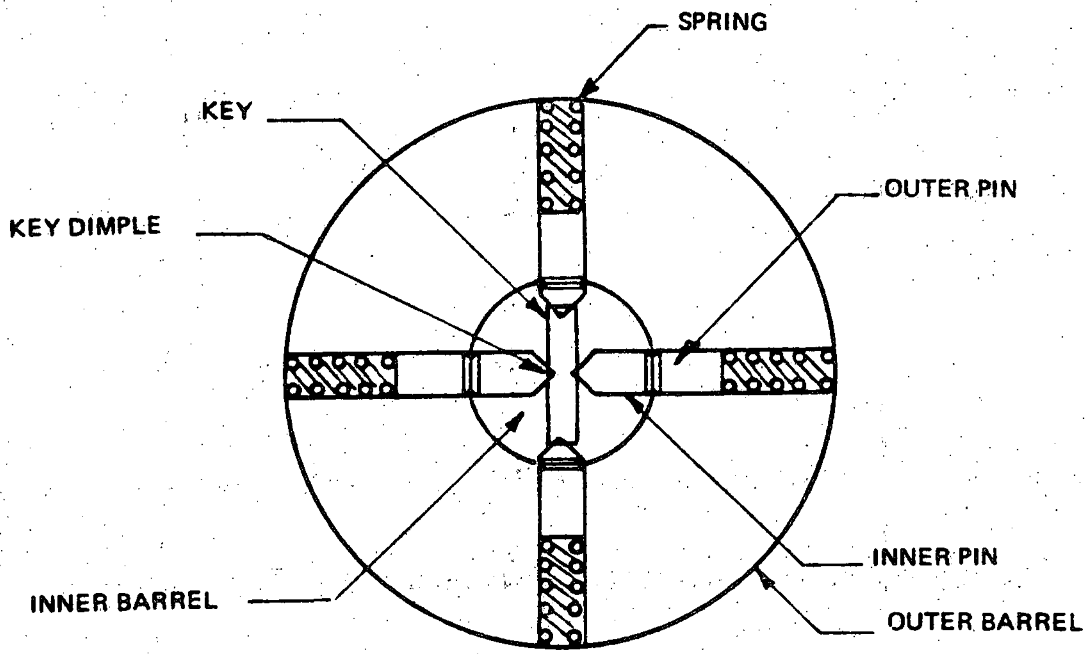


FIGURE E–8. SCHEMATIC DIAGRAM OF FOUR PIN SETS OF THE KESO PIN TUMBLER LOCK.

APPENDIX F

MOTOR VEHICLE SAFETY STANDARD NO. 114

Theft Protection - Passenger Cars

S1. Purpose and scope. This standard specifies requirements for theft protection to reduce the incidence of accidents resulting from unauthorized use.

S2. Application. This standard applies to passenger cars.

S3. Definitions. "Combination" means one of the specifically planned and constructed variations of a locking system which, when properly actuated, permits operation of the locking system.

"Key" includes any other device designed and constructed to provide a method for operating a locking system which is designed and constructed to be operated by that device.

S.4 Requirements.

S4.1 Each passenger car shall have a key-locking system that, whenever the key is removed, will prevent -

(a) Normal activation of the car's engine or other main source of motive power; and

(b) Either steering or forward self-mobility of the car, or both.

S4.2 The prime means for deactivating the car's engine or other main source of motive power shall not activate the deterrent required by S4.1(b).

S4.3 The number of different combinations of the key locking systems required by S4.1 of each manufacturer shall be at least 1,000, or a number equal to the number of passenger cars manufactured by such manufacturer, whichever is less.

S4.4 A warning to the driver shall be activated whenever the key required by S4.1 has been left in the locking system and the driver's door is opened. The warning to the driver need not operate -

(a) After the key has been manually withdrawn to a position from which it may not be turned;

(b) When the key-locking system is in the ON or START position, or

(c) After the key has been inserted in the locking system and before it has been turned.

APPENDIX G

ECONOMIC COMMISSION OF EUROPE REGULATION NO. 18*

Uniform Provisions Concerning the Approval of Power-Driven Vehicles with Regard to their Protection against Unauthorized Use

1. Scope

1.1 This Regulation applies to protective devices designed to prevent the unauthorized use of power-driven vehicles having at least three wheels.

2. Definitions

2.3 "Protective device" means a system designed to prevent unauthorized normal activation of the engine or other source of main engine power of the vehicle in combination with at least one system which: locks the steering; or locks the transmission; or locks the gear-shift control; or any system within the art which effectively prevents the unauthorized movement of the vehicle;

2.4 "Steering" means the steering control, the steering column and its accessory cladding, the steering shaft, the steering gearbox and all other components which directly affect the effectiveness of the protective device;

2.5 "Combination" means one of the specifically planned and constructed variations of a locking system which, when properly activated, permits operation of the locking system;

2.6 "Key" means any device designed and constructed to provide a method of operating a locking system which is designed and constructed to be operated by that device.

5. General Specifications

5.1 The protective device shall be so designed that it is necessary to put it out of action in order to enable:

5.1.1 The engine to be started by means of the normal control; and

5.1.2 The vehicle to be steered, driven or moved forward under its own power.

5.2 The requirements of paragraph 5.1 shall be met by the single application of one key.

*As presented in the Federal Register, Vol. 41, No. 44, p. 9375, Thursday, March 4, 1976.

5.2.1 The optional fitting of supplementary devices to prevent unauthorized use of the vehicle shall be permitted, even if they require a separate means of activation.

5.3 A system operated with a key inserted in a lock shall not permit removal of the key before the protective device referred to in paragraph 5.1 has come into action or has been set to act.

5.4 The protective device referred to in paragraph 5.1 above, and the vehicle components on which it operates, shall be so designed, that it cannot, rapidly and without attracting attention, be opened, rendered ineffective, or destroyed by the use of low cost easily concealed tools, equipment or fabrications readily available to the public at large.

5.5 The protective device shall be mounted on the vehicle as an item of original equipment, (i.e. equipment installed by the vehicle manufacturer prior to first retail sale). It shall be fitted in such a way that even after removal of its housing it cannot, when in the blocked condition, be dismantled otherwise than with special tools. If it would be possible to render the protective device ineffective by the removal of screws, the screws shall, unless they are non-removable screws, be covered by parts of the blocked protective device.

5.6 The key locking system shall provide at least 1,000 different key combinations or a number equal to the total number of vehicles manufactured annually if less than 1,000. In vehicles of one type the frequency of occurrence of each combination shall be roughly 1 per 1,000.

5.7 The key and lock shall not be visibly coded.

5.8 The lock shall be so designed, constructed and fitted that turning of the lock cylinder, when in the locked position, with a torque of less than 0.25 m.kg is not possible with anything other than the mating key, and

5.8.1 For lock cylinders with pin tumblers no more than 2 identical tumblers operating in the same direction shall be positioned adjacent to each other, and in a lock there shall not be more than 60 percent identical tumblers.

5.8.2 For lock cylinders with disc tumblers no more than 2 identical tumblers operating in the same direction shall be positioned adjacent to each other, and in a lock there shall not be more than 50 percent identical tumblers.

5.9 Protective devices shall be such as to exclude any risk, while the vehicle is in motion of accidental blockage likely to compromise safety in particular.

5.9.1 It shall not be possible to activate protective devices acting on the steering, transmission or gearshift control without first stopping the engine and then performing an action which is not an uninterrupted continuation of stopping the engine.

5.9.2 In the case of devices acting on the steering transmission or gearshift control the action of key withdrawal shall either necessitate a minimum movement of 5 mm before activation of the device or incorporate an override facility to prevent accidental removal or partial withdrawal of the key.

5.10 Power assistance may be used only to activate the locking and, or unlocking action of the protective device. The device shall be kept in its operating position by mechanical means only.

5.11 It shall not be possible to activate the motive power of the vehicle by normal means until the protective device has been deactivated.

6. Particular Specifications

In addition to the general specifications prescribed in paragraph 5, the protective device shall comply with the particular conditions prescribed below:

6.1 Protective Devices Acting on the Steering

6.1.1 A protective device acting on the steering shall block the steering.

6.1.2 When the protective device is set to act, it shall not be possible to prevent the device from functioning.

6.1.3 The protective device must continue to meet the paragraphs 5.9, 6.1.1, 6.1.2 and 6.1.4 after it has undergone 5,000 locking cycles of the wear producing test specified in annex 3 (attached).

6.1.4 The protective device shall, in its activated position, be strong enough to withstand, without damage to the steering stand, without damage to the steering mechanism likely to compromise safety, the application of a torque of 19.6 ndaN (20mkgf) about the axis of the steering shaft in both directions under static conditions.

6.2 Protective Devices Acting on the Transmission. A protective device acting on the transmission shall prevent the rotation of the vehicle's driving wheels.

6.3 Protective Devices Acting on the Gearshift Control.

6.3.1 A protective device acting on the gearshift control shall be capable of preventing any change of gear.

6.3.2 In the case of manual gearboxes it must be possible to lock the gearshift lever in reverse only; in addition, locking in neutral shall be permitted.

6.3.3 In the case of automatic gearboxes provided with a "parking" position it must be possible to lock the mechanism in the parking position only; in addition, locking in neutral and/or reverse shall be permitted.

6.3.4 In the case of automatic gearboxes not provided with a "parking" position it must be possible to lock the mechanism in neutral and/or reverse.

10. Acoustic or Visual Warning Devices Provided Additionally.

10.1 A protective device may be additionally equipped with an acoustic or visual warning device.

10.2 If the protective device is additionally equipped with an external acoustic and/or visual warning device, the signals emitted by the warning device shall be brief and shall end automatically after not more than 30 seconds; they shall recommence only if the device is actuated again. In addition,

10.2.1 If the signal is acoustic, it may be emitted by the audible warning device normally fitted to the vehicle;

10.2.2 If the signal is visual, it shall be produced solely by flashing of the vehicle's passing lights.

10.3 If the protective system is equipped with a driver warning feature, it shall be activated, unless the protective device has been activated and any key removed by the operator, when the operator opens the driver's side door.

ANNEX 3

(TO THE REGULATION)

WEAR PRODUCING TEST PROCEDURE FOR PROTECTIVE DEVICES ACTING ON THE STEERING

1. Test Sample and Test Equipment.

1.1 Shall consist of a fixture suitable for mounting the sample steering shaft relative to the protective device.

1.2 A means for activating and deactivating the protective device;

1.3 A means for rotating the steering shaft relative to the protective device.

2. Test Method. One cycle of the test procedure shall consist of the following operations during which the torque on the steering shaft shall not exceed 0.575 m.kg.

2.1 Start Position-The protective device shall be deactivated and the steering shaft shall be rotated to a position which prevents engagement of the protective device, unless it is of the type which permits locking in any position of the steering.

2.2 Set to Activate-The protective device shall be moved from the deactivated to the activated position, using the normal means of activation, for example by turning or withdrawing the key.

2.3[1] Activated-The steering shaft shall be rotated at a speed not exceeding the equivalent of 1 r.p.s. until the protective device locks the shaft.

2.4 Deactivated-The protective device shall be deactivated by the normal means, where necessary the shaft shall be rotated to facilitate disengagement.

2.5[1] Return-The steering shaft shall be rotated at a speed not exceeding the equivalent of 1 r.p.s. to a position which prevents engagement of the protective device.

2.6 Opposite Rotation-Repeat 2.2, 2.3, 2.4 and 2.5, but in the opposite direction of rotation of the steering shaft.

[FR Doc.76-6107 Filed 3-3-76;8:45 am]