2013-12

Securing public safety vehicles: reducing vulnerabilities by leveraging smart technology and design strategies

Johansmeyer, Michael

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SECURING PUBLIC SAFETY VEHICLES: REDUCING VULNERABILITIES BY LEVERAGING SMART TECHNOLOGY AND DESIGN STRATEGIES

by

Michael Johansmeyer

December 2013

Thesis Co-Advisors: Nadav Morag
Richard Bergin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE SECURING PUBLIC SAFETY VEHICLES: REDUCING VULNERABILITIES BY LEVERAGING SMART TECHNOLOGY AND DESIGN STRATEGIES			**5. FUNDING NUMBERS**
6. AUTHOR(S) Michael Johansmeyer			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The threat of public safety vehicles being used by criminals or terrorists to commit violent acts is real. The problem is public safety vehicles are vulnerable to criminal activity and terrorist use because they do not routinely utilize security technology measures involving three core aspects: theft prevention, authentication to specific operators (authorized use), and ability to track and recover public safety vehicles that get into the wrong hands. Consequences from such acts create great risk for the public's safety, including significant injury and loss of human life, as well as exposure to financial liabilities in the form of lost equipment, damage to property, and lawsuit settlements.

This thesis provides a model solution to agencies for securing emergency response vehicles with engineering (SERVE). The SERVE model was developed by the author and provides a framework for implementing public safety vehicle security enhancements taking the complex interaction between technological fusion, vehicle system integration and end user interface design into account. Tier I—Theft Prevention, Tier II—Authorized Use, Tier III—Tracking and Recovery can be implemented in stages, allowing agencies to utilize the technologies based on budgetary restraints and allocation of resources. Lastly, Tier IV—Human Machine Interface emphasizes the importance of the human machine interface by taking into account how technologies and operators communicate to ensure critical task proficiency is not disrupted.

14. SUBJECT TERMS Vehicle security, theft prevention technology, anthropometrics, eVID, authentication, unauthorized, engineering, public safety, SERVE model, vehicle theft prevention			**15. NUMBER OF PAGES** 95
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

SECURING PUBLIC SAFETY VEHICLES: REDUCING VULNERABILITIES BY LEVERAGING SMART TECHNOLOGY AND DESIGN STRATEGIES

Michael Johansmeyer
Division Chief, Seminole County Department of Public Safety
B.S., University of Central Florida, 2009

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2013

Author: Michael Johansmeyer

Approved by: Nadav Morag
Thesis Co-Advisor

Richard Bergin
Thesis Co-Advisor

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The threat of public safety vehicles being used by criminals or terrorists to commit violent acts is real. The problem is public safety vehicles are vulnerable to criminal activity and terrorist use because they do not routinely utilize security technology measures involving three core aspects: theft prevention, authentication to specific operators (authorized use), and ability to track and recover public safety vehicles that get into the wrong hands. Consequences from such acts create great risk for the public's safety, including significant injury and loss of human life, as well as exposure to financial liabilities in the form of lost equipment, damage to property, and lawsuit settlements.

This thesis provides a model solution to agencies for securing emergency response vehicles with engineering (SERVE). The SERVE model was developed by the author and provides a framework for implementing public safety vehicle security enhancements taking the complex interaction between technological fusion, vehicle system integration and end user interface design into account. Tier I—Theft Prevention, Tier II—Authorized Use, Tier III—Tracking and Recovery can be implemented in stages, allowing agencies to utilize the technologies based on budgetary restraints and allocation of resources. Lastly, Tier IV—Human Machine Interface emphasizes the importance of the human machine interface by taking into account how technologies and operators communicate to ensure critical task proficiency is not disrupted.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AASHTO	American Association of State Highway and Transportation Officials
AEI	automatic equipment identification
ASIC	application-specific integrated circuit
CFR	Code of Federal Regulations
CVISN	commercial vehicle information systems and networks
CVSA	Commercial Vehicle Safety Alliance
DAT	driver authentication technology
eVID	electronic vehicle immobilization device
FMCSA	Federal Motor Carrier Safety Administration
FOT	field operational test
FTA	Federal Transit Administration
FPGA	field programmable gate array
GPRS	global packet radio service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IoT	internet of things
IRRIS	intelligent road/rail information server
ITS JPO	Intelligent Transportation Systems Joint Program Office
MMS	multimedia messaging system
NHTSA	National Highway Traffic Safety Administration
OBD	on-board diagnostic port
PHMSA	Pipeline and Hazardous Materials Safety Administration
PSRC	Public Sector Reporting Center
RFID	radio-frequency identification
SDDCTEA	Surface Deployment and Distribution Command
TSA	Transportation Security Administration
USDOT	United States Department of Transportation
WAP	wireless access points

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The threat of criminals or terrorists using public safety vehicles to commit violent acts is real. Vulnerabilities, which result from the lack of security measures, make public safety vehicles prone to criminal activity and ideal instruments for use in the execution of violent acts. Consequences from such acts create great risk to the public's safety, including significant injury and loss of human life, as well as exposure to financial liabilities in the form of lost equipment, damage to property, and lawsuit settlements.

Many public safety vehicles, such as fire engines, do not contain controlled access mechanisms, such as door locks, keys, or an electronic key fob. If vehicle access mechanisms exist, they are not routinely authenticated to an approved individual. In the event vehicles are operated improperly, tracking and recovery devices to inform agency officials are rarely used. Public safety vehicles are frequently left running and/or unattended (e.g., emergency scenes, in staging parking lots and apparatus bays, and at hospitals during patient transport transfers as part of cultural norms within operating practices). Police cars, fire trucks, and ambulances do not draw the same suspicion as unmarked vehicles when parked next to buildings or in emergency locations.

The use of a public safety vehicle by an unauthorized operator (a criminal or a terrorist) can be prevented by use of technologies. There do not appear to be any standards, across the homeland security environment, with regard to the prevention of the use of public safety vehicles in dangerous or other unauthorized ways. The problem is public safety vehicles are vulnerable to criminal activity and terrorist use because agencies do not routinely utilize security technology measures involving three core aspects: theft prevention, authentication to specific operators (authorized use), and ability to track and recover public safety vehicle in the wrong hands.

The use of a universal symbol of help by criminals/terrorists has far reaching impacts to national security and public safety at all levels of government. There are clearly many examples of stolen and misused public safety vehicles across the United States and overseas, including successful use of police cars, fire engines, and ambulances

in terrorist acts. Additionally, there is a delay from the time a vehicle is stolen to notification of appropriate personnel in many incidents. This provides unauthorized users an opportunity to utilize these vehicles freely. The profile for unauthorized users is diverse as are their motives, including the mentally ill, intoxicated, mischievous, or malicious.

The *Hazardous Material Safety and Security Field Operational Test* conducted by U.S. Department of Transportation's Federal Motor Carrier Safety Administration (FMCSA), which partnered with the U.S. Department of Transportation (DOT's) Intelligent Transportation System Joint Program Office (JPO) offered real-world knowledge and scientific data supporting vehicle security technologies and the ability to categorize them based on capability.[1] Additionally, the study provided insight into how technologies that create inconveniences to the end user may prove to be less effective. This led to the human-machine interface study of design and two case studies involving anthropometrics.

Anthropometrics is the study of a person's (or group) physical measurements applied to a task(s) form and function.[2] This will assist the reader in understanding the importance of human interaction with security technologies with regard to design and engineering to ensure successful implementation outcomes. The two studies that are helpful in this are: *Field Quantification of Physical Exposure of Police Officers in Vehicle Operation*[3] and *Sizing Firefighters and Fire Apparatus: Safe by Design*.[4] The

[1] Science Applications International Corporation, *Hazardous Materials Safety and Security Technology Field Operational Test, Volume I: Evaluation Final Report Executive Summary*, 2004, Federal Motor Carrier Safety Administration, accessed February 20, 2013, http://www.fmcsa.dot.gov/documents/hazmat/fot/FINAL-Volume-I-Executive-Summary-11-10-04.pdf; Science Applications International Corporation, *Hazardous Materials Safety and Security Technology Field Operational Test Volume II: Evaluation Final Report Synthesis* (Washington, DC: U.S. Department of Transportation, 2004)

[2] "Workplace Safety and Health Topics: Anthropometry," Center for Disease Control and Prevention and National Institute for Occupational Safety and Health, accessed October 14, 2013, http://www.cdc.gov/niosh/topics/anthropometry/.

[3] Colin D. McKinnon, Jack P. Callaghan and Clark R. Dickerson, "Field Quantification of Physical Exposures of Police Officers in Vehicle Operation," *International Journal of Occupational Safety and Ergonomics-JOSE* 17, no. 1 (2011), 61.

knowledge gained supported the importance of human-machine interaction considerations at design and implementation phases of public safety vehicle technologies.

Technologies outlined in the case study were used as primary data when developing Tier I–VI categories and sub categories. Knowledge gained from industry reports supplemented the case study. Additional smart practices, such as common sense measures, were not emphasized in the findings of the case study; however, these are described as the simplest and most cost effective way to secure a vehicle by law enforcement agencies and insurance leaders alike.[5]

The securing emergency response vehicles with engineering (SERVE)[6] model (see Figure 1) provides a framework for implementing security technology within the public safety industry. Although specific interest in developing the SERVE model applies to securing emergency vehicles, SERVE may prove useful to other industries as well. Figure 1 simply provides a schematic representation of the complex interaction between technological fusion, vehicle system integration, and end user interface design. The three tiers of technology implementation and one tier of human-machine interface considerations are below.

A. TIER I—THEFT PREVENTION

These devices interrupt on board mechanical and electronic systems (e.g., parking brake [air or electronic], electronic ignition and power to starter). These devices include common sense measures, interruption technologies, and authentication technologies. Examples of these include: taking keys out of the ignition, locking doors, push button activation (panic button), key fob, and smart keys. Although these simple steps may prevent successful action on the part of a thief, applying practices such as removing keys

---

[4] Hongwei Hsiao, *Sizing Firefighters and Fire Apparatus: Safe by Design*, Center for Disease Control and Prevention, accessed October 14, 2013, http://www.cdc.gov/niosh/topics/anthropometry/pdfs/Sizing%20firefighters%20proposal%20core%20part.pdf.

[5] Frank Scafidi, "Hot Wheels 2012," 2013, National Insurance Crime Bureau, https://www.nicb.org/newsroom/news-releases/hot-wheels-2012; District of Columbia Metropolitan Police Department, "Auto Theft Prevention," accessed October 14, 2013,. http://mpdc.dc.gov/page/auto-theft-prevention.

[6] SERVE model was built by author based on the research findings.

may impact job performance within the public safety community. The devices do not require user specific information. The importance of user-specific information (password/PIN) and characteristics (biometrics) provided by the authorized operator are discussed in Tier II technologies.

B. TIER II—AUTHORIZED USER

This category includes devices in Tier I with the addition of user-specific information or requirements. These devices employ the help of on-board computers (sometimes external computers) to validate user information. Some examples include: user specific smart cards, PINs or biometric, and password. Field Programming Gate Array (FPGA) technology is implemented to ensure authorized changes can occur quickly in the event user privileges are revoked. Tier II—authorized user technology systems may offer safety enhancements related to human error, such as forgetting to set a brake, in addition to security benefits. Additionally, technologies in this category might require a backup or secondary system in case of a primary system failure. The secondary system should provide an opportunity for enhancement without creating a gap in the overall system security. Simply, if the backup system is to easily used or identified, it can exploit the primary system. Encryption of internal and external communications will reduce vulnerability to system components.

C. TIER III—TRACKING AND RECOVERY

This category includes Tier I and Tier II devices. This technology allows on-board systems to communicate with external authorized end users. Information regarding on-board systems, location, vehicle speed, and location are reported to data warehousing. The upper level of Tier III technologies implement protocols and algorithms for identifying patterns of use, on-board system sensors (inventories, vehicle weights, number of personnel on unit), or information gained from V2Connected world via infrastructure, satellite, mobile devices, and other vehicles that indicates wrongful user and/or unauthorized use. Real-time information is enhanced and provides greater need for intelligent systems to deceiver the big data. Big data will require protocols and algorithms to be built by the agency by after exploring internal needs and business

models (e.g., mutual aid, automatic aid, response zone) to ensure the intelligent software performs as expected.

D. TIER IV—HUMAN-MACHINE INTERFACE CONSIDERATIONS

Anthropometric and design theories must be considered to ensure smart practices are identified and disruptive technologies do not impact job performances involved in public safety. The Human-Machine interface is warranted across Tier I, Tier II, and Tier III technologies. Specifically, the implementation of authentication technologies cannot interfere with operator job performance proficiency.[7]

Figure 1. Securing Emergency Response Vehicles with Engineering

[7] Federal Motor Carrier Safety Administration, *Vehicle Immobilization Technologies: Best Practices for Industry and Law Enforcement Final Report*, 2007, accessed November 20, 2013, http://www.fmcsa.dot.gov/facts-research/research-technology/report/vit-best-practices-law-enforcement-nov2007.pdf, 95.

LIST OF REFERENCES

District of Columbia Metropolitan Police Department. "Auto Theft Prevention." Accessed October 14, 2013. http://mpdc.dc.gov/page/auto-theft-prevention.

Federal Motor Carrier Safety Administration, U.S. Department of Transportation. *Vehicle Immobilization Technologies: Best Practices for Industry and Law Enforcement Final Report*. 2007. Federal Motor Carrier Safety Administration. http://www.fmcsa.dot.gov/facts-research/research-technology/report/vit-best-practices-law-enforcement-nov2007.pdf.

Hsiao, Hongwei. *Sizing Firefighters and Fire Apparatus: Safe by Design*. Center for Disease Control and Prevention. Accessed October 14, 2013. http://www.cdc.gov/niosh/topics/anthropometry/pdfs/Sizing%20firefighters%20proposal%20core%20part.pdf.

McKinnon, Colin D., Jack P. Callaghan, and Clark R. Dickerson. "Field Quantification of Physical Exposures of Police Officers in Vehicle Operation." *International Journal of Occupational Safety and Ergonomics-JOSE* 17, no. 1 (2011): 61.

Scafidi, Frank. "Hot Wheels 2012." 2013. National Insurance Crime Bureau. https://www.nicb.org/newsroom/news-releases/hot-wheels-2012.

Science Applications International Corporation. *Hazardous Materials Safety and Security Technology Field Operational Test, Volume I: Evaluation Final Report Executive Summary*, 2004. Federal Motor Carrier Safety Administration. Accessed February 20, 2013. http://www.fmcsa.dot.gov/documents/hazmat/fot/FINAL-Volume-I-Executive-Summary-11-10-04.pdf.

———. *Hazardous Materials Safety and Security Technology Field Operational Test, Volume II: Evaluation Final Report Synthesis*. Washington, DC: U.S. Department of Transportation, 2004.

"Workplace Safety and Health Topics: Anthropometry." Center for Disease Control and Prevention and National Institute for Occupational Safety and Health. Accessed October 14, 2013. http://www.cdc.gov/niosh/topics/anthropometry/.

ACKNOWLEDGMENTS

I would like to thank the Naval Postgraduate School, Center for Homeland Defense and Security for providing an academic institution where homeland security professions gain "**praestantia per cientiam"** together. Thank you to all the professors and special guests who enriched our learning experience.

A thank you goes to my thesis advisors, Nadav Morag and Richard Bergin, for keeping my wheels on the tracks. I have learned a great deal from each of you. A special thanks goes to Catherine Grant for providing thesis final copy expertise.

A sincere thank you also goes to the Seminole County Department of Public Safety Director, Tad Stone, for giving me the opportunity to explore the world of Homeland Security and participate in this program.

To Seminole County Fire Chief Leeanna Mims—NPS graduate, your confidence in me to take on this endeavor and encouragement to do so means a great deal, and I will never forget it. You blazed the path that guided my experience and success.

To Seminole County Assistant Chief Mark Oakes, your mentorship and leadership opened the door to experiences that allowed me to be considered for this program. I greatly appreciate all you have done for me professionally and personally.

To the Seminole County C-Shift Leadership Team and its members, I am proud to be part of your team, and appreciate all of you have done that allowed me to participate in this program and complete it successfully.

To my fellow 1203/1204 participants, although we may never be "royal," we are rich in friendship. The community we built is second to none.

To all of my family and friends who waited patiently for our lives to return to normal, thank you. I always knew you were there when needed.

To my wife, Kandace; son, Jonathan; and daughter, Jocelyn: No words can equal the love, respect, and gratitude I have for each of you. All of your devoted and enthusiastic support gave me the courage to accomplish this "hard fun."

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

The threat of public safety vehicles being used by criminals or terrorists to commit violent acts is real. Public safety vehicle vulnerabilities that result from the lack of security measures make them prone to criminal activity and ideal instruments in executing violent acts. Consequences from such acts create great risk for the public's safety, including significant injury and loss of human life, as well as, exposing agencies to financial liabilities in the form of lost equipment, damage to property and lawsuit settlements.

Many public safety vehicles, such as fire engines, do not contain controlled access mechanisms, such as door locks, keys, or electronic key fob. If vehicle access mechanisms exist, they are not routinely authenticated to a particular individual with authorized access. In the event vehicles are being operated improperly, tracking and recovery devices to inform agency officials are not often implemented. Public safety vehicles are frequently left running and/or unattended (e.g., emergency scenes, in staging parking lots and apparatus bays, and at hospitals during patient transport transfers as part of cultural norms within operating practices). Police cars, fire trucks and ambulances do not draw the same suspicion as unmarked vehicles when parked next to buildings or in emergency locations. Below are some examples of the theft of public safety vehicles:

- April 15, 2012, a man steals ambulance that responded to makeshift bomb call in Tarpon Springs, Florida.[1]
- January 10, 2013, a homeless man steals ambulance out of fire station. The ambulance was not discovered missing for over 39 minutes only then discovered after the crew was dispatched to another call.[2]

[1] Ashley Porter, "Man Armed with Potato Steals Ambulance—Weird," *10 News*, accessed January 30, 2013, http://tarponsprings.wtsp.com/news/weird/115568-man-armed-potato-steals-ambulance.

[2] Jennifer Reeger, "Alert Pa. Officer Recovers Stolen Ambulance," accessed January 30, 2013, http://www.officer.com/news/10851490/alert-pa-officer-recovers-stolen-ambulance.

- July 26, 2012, a man steals ambulance fully stocked worth $140,000.[3] Found 35 minutes later and tapes shows the man was driving with emergency lights on and ran traffic lights.[4]
- November 18, 2004, Healthcare system agrees to pay 12.5 million to the family of man killed by the mentally ill driver of a stolen ambulance.[5]
- February 24, 2012, a man was killed by stolen fire truck driven by naked man who jumped in the truck when it was left running at an emergency scene.[6]
- August 31, 2013, a woman was accused of stealing a police car and crashing into a group of people, killing one and injuring several others.[7]

It is believed by many the theft of public vehicles, as shown in the criminal activity examples above, is a far cry from an act of terrorism. Contrarily, the Committee on Homeland Security and Government Affairs hearing held on September 19, 2012, days after the Benghazi attacks in Libya, addressed the use of trend analysis in the prevention and preparation of terrorist attacks.[8] During the hearing when summarizing events that took place in Benghazi, Senator Collins explained that terrorist acts are predictable. To the surprise of many, Benghazi occurred on September 11, 2012, and it was considered a large-scale terrorist attack on the U.S. consulate in Libya.[9] Although no public safety vehicles were used in executing the attack, the surprise that a terrorist attack could take place with such success against U.S. interest without warning was eerily familiar with that of the attacks on the World Trade Centers on September 11, 2001. The

---

[3] Kenneth Moton, "Stolen Ambulance Joyride Caught on Tape," *ABC7News Chicago Illinois*, accessed October 14, 2013, http://abclocal.go.com/wls/story?section=news/national_world&id=8750037.

[4] Ibid.

[5] "Catastrophic Ambulance Collision Lawsuit Settles for $12.5 Million," *PRNewswired*, accessed January 30, 2013, http://www.prnewswire.com/news-releases/catastrophic-ambulance-collision-lawsuit-settles-for-125-million-75481272.html.

[6] Patrick Donahue, "Stolen Fire Truck Kills Man, Crashes," *The Post and Courrier*, February 25, 2012, accessed October 10, 2013, http://www.postandcourier.com/article/20120225/PC1602/302259977.

[7] Matt Kroschel, Carri Walters, and Laura Christmas, "Update: Woman Charged Following Incident Involving Stolen Police Car in Fayetteville," *WHNT 19 News*, August 31, 2013, accessed October 14, 2013, http://whnt.com/2013/08/31/breaking-stolen-police-car-involved-in-deadly-wreck-in-fayetteville/.

[8] *Homeland Threats and Agency Response, Hearing before Committee on Homeland Security and Government Affairs United States Senate*, 112th Cong. (2012), accessed January 30, 2013, Government Printing Office, http://www.gpo.gov/fdsys/pkg/CHRG-112shrg76070/html/CHRG-112shrg76070.htm.

[9] "How the Benghazi Attacks Unfolded," *Wall Street Journal Online*, accessed October 14, 2013, http://online.wsj.com/news/articles/SB10000872396390444620104578008922056244096.

hearing expanded the concern for predicting acts of violence against the U.S. by identifying three key areas that had merit for special sustained attention by homeland security officials. One of these is the increasing threat from homegrown violent extremism.[10] Utilizing public safety vehicles to cause harm and execute acts of terror is predictable when combined with the increases in homegrown violent extremism and current trends of terrorism in other countries where public safety vehicles are used for such purposes. Additionally, The *National Preparedness Goal* outlines "a secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk" is achieved by taking steps to prevent, avoid, or stop threatened or actual acts of terrorism.[11]

A strategic national risk assessment was conducted and the key findings published in accordance with PPD-8 and in cooperation with federal departments and agencies.[12] Terrorist organizations or affiliates may seek to acquire, build, and use weapons of mass destruction (WMD). Conventional terrorist attacks, including those by "lone actors" employing explosives and armed attacks, present a continued risk to the nation.[13] The use of public safety vehicles by terrorists, including homegrown extremist, is not a new tactic and has been used extensively in Iraq (but not exclusively), as suggested in the following examples:

- April 11, 2005: using a fire truck loaded with explosives, insurgents try to take over a Marine base in Baghdad, Iraq. This is reported to be the second time in less than two weeks this emerging tactic was seen.[14]

---

[10] *Homeland Threats and Agency Response, Hearing before Committee on Homeland Security and Government Affairs United States Senate*, 112th Cong. (2012), accessed January 30, 2013, Government Printing Office, http://www.gpo.gov/fdsys/pkg/CHRG-112shrg76070/html/CHRG-112shrg76070.htm.

[11] Federal Emergency Management Agency, *National Preparedness Goal 2011*, 2011, accessed October 28, 2013, http://www.fema.gov/media-library-data/20130726-1828-25045-9470/national_preparedness_goal_2011.pdf.

[12] Ibid. The complete results of the Strategic National Risk Assessment are classified. For an unclassified summary, see http://www.fema.gov/ppd8.

[13] Ibid., 4.

[14] Ellen Knickmeyer, "New Tactic Seen in Attack on Marine Base," *Washington Post*, April 12, 2005.

- February 24, 2007: a suicide bomber drove a stolen ambulance that was filled with explosives into a police station in Ramadi, killing at least 14 people.[15]
- September 2, 2008: an ambulance with unusual markings was spotted at the Republican National Convention in St. Paul.[16] Activist loaded the ambulance with weapons and 55-gallon drums of feces and urine.[17]
- February 3, 2013: a suicide bomber "driving a police car and wearing a police uniform" killed 36 and wounded 105.[18]

The use of a public safety vehicle, by an unauthorized operator (a criminal or a terrorist), that results in significant damage, serious injury or death, and economic harm from loss of equipment can be prevented by use of existing and emerging technologies. There do not appear to be any standards, across the homeland security environment, with regard to the prevention of the use of public safety vehicles in dangerous or other unauthorized ways. The problem is public safety vehicles are vulnerable to criminal activity and terrorist use because they do not routinely utilize security technology measures involving three core aspects: theft prevention, authentication to specific operators (authorized use), and ability to track and recover public safety vehicle in the wrong hands.

B. BACKGROUND

Public safety vehicles are clearly marked with insignias and considered a sign of authority, assistance, and safety. These vehicles can gain access to restricted areas or reduce suspicion of location or activity at emergency scenes simply because of type of vehicles and markings (e.g., a fire truck parked in the fire lane with red lights activated or police car parked outside of a protected critical infrastructure).

---

[15] Ryan Lucas, "Suicide Bomber Driving Ambulance Strikes Police Station in Ramadi, Second Bombing in a Week in Volatile Anbar Province," *America's Intelligence Wire*, February 2007.

[16] Anthony L. Kimery, "'Cloned' Vehicles Continue to be Security Problem," *HS Today*, December 11, 2008, accessed October 14, 2013, http://www.hstoday.us/blogs/the-kimery-report/blog/cloned-vehicles-continue-to-be-security-problem/c7f442710dc2fc583590b681f319234e.html.

[17] Gary Ludwig, "EMS: Stolen Ambulance," *Firehouse Magazine*, December 3, 2012.

[18] Yasir Ghazi, "Dozens Die in Attack on Police in Iraqi City," *New York Times*, accessed October 22, 2013, http://www.nytimes.com/2013/02/04/world/middleeast/suicide-attack-kills-dozens-in-northern-iraq.html?_r=0.

The American people will surely care on the day a public safety vehicle is used in a successful terrorist attack against our own country. Many of the decision and law makers will be held accountable by the American people for allowing such a vital part of our community, with such a large vulnerability gap, go unchecked for more than 10 years after September 11. The billions of dollars spent through homeland security grant programs have not addressed this vulnerability across any public safety discipline.

A study conducted by the New York City Partnership and Chamber of Commerce estimated the September 11 terrorist attacks at $83 billion dollars in direct and indirect costs in 2001.[19] This does not account for the value of human life. Additionally, the consequences of an American symbol of safety and assistance, such as a police car or fire truck utilized as a weapon of mass destruction in a terrorist attack similar to the Ryder truck bomb used in the Alfred P. Murrah federal building, which killed 168 and injured hundreds more,[20] is exponential. The effects of a coordinated attack, utilizing public safety vehicles to carry, conceal and access restricted areas, on multiple key targets across the U.S. does not take a great deal of imagination. The consequences of such a scenario would be magnified if attacks were successfully executed on significant days of the year for the U.S., such as Black Friday.[21] The failure to "imagine" the potential and magnitude of a coordinated attack in which stolen public safety vehicles are utilized as transporters of weapons of mass destruction on a significant day of the year, in major cities across the nation would only be a repeat of weaknesses pointed out in the *9/11 Commission Report*.[22]

---

[19] Government Accounting Office, *Review of Studies of the Economic Impact of September 11, 2001, Terrorist Attacks of the World Trade Centers*, GAO-02-700R, accessed October 14, 2013, http://www.gao.gov/new.items/d02700r.pdf.

[20] Federal Bureau of Investigations, "Terror Hits Home: The Oklahoma City Bombing," accessed October 14, 2013, http://www.fbi.gov/about-us/history/famous-cases/oklahoma-city-bombing.

[21] Andrew E. Colsky, "Public/Private Partnerships with Hazardous Material Motor Carriers Creating Incentives to Increase Security through Assessed Risk (STAR)" (master's thesis, Naval Postgraduate School, 2008), 1.

[22] National Commission on Terrorist Attacks upon the United States, *Final Report of the National Commission on Terrorist Attacks upon the United States* [*9/11 Commission Report*] (New York: W. W. Norton, 2004), 339.

The focus of this thesis is the prevention of terrorist events and reduction in risk to lives by preventing theft and protecting against misuse of official public safety vehicles; however, the fiscal impacts of stolen equipment is also a matter of concern. For instance, a fire truck including equipment can easily reach one million dollars and an outfitted police cruiser can reach $120,000.[23] Identifying steps that can be taken to reduce risk by enhancing public safety vehicle security can reduce the consequences directly related to loss of life and the fiscal impacts on agencies and communities. Organizational practices, cultural norms and preventative technological controls currently available in the market place and new ones are continually emerging to assist in reducing public safety vehicle security vulnerabilities.

C. SUMMARY

The use of a universal symbol of help by criminals/terrorists in an act of terror has far reaching impacts to national security and public safety at all levels of government. There are clearly many examples of stolen and misused public safety vehicles across the United States and overseas, including successful use of police cars, fire engines, and ambulances in terrorist acts. Additionally, there is a delay from the time the vehicle is stolen to notification of appropriate personnel in many incidents. This provides unauthorized users an opportunity to utilize these vehicles freely. The profile for unauthorized users is diverse as are their motives, including the mentally ill, intoxicated, mischievous, or malicious.

1. Research Questions

- Primary research question
    - How can existing and emerging security technologies mitigate criminal and terrorist misuse of public safety vehicles?

[23] Sam Hall, "What Makes a Police Car Cost $120,000?" January 28, 2013, accessed October 28, 2013, http://news.drive.com.au/drive/motor-news/what-makes-a-police-car-cost-120000-20130128-2dgcd.html.

- Supportive questions
  - Can existing and emerging technologies be measured for effectiveness in reducing vulnerabilities associated with theft prevention, protect against misuse and lack of tracking or recovery means of public safety vehicles?
  - Can the study of design innovation provide scientific insight into successful implementation strategies in the public safety arena to mitigate criminal and terrorist misuse of public safety vehicles?

2. Methodology

This thesis will examine research materials related to vehicle security technologies in an effort to identify effective solutions in reducing public safety vehicle security vulnerabilities. The case study method is utilized in an effort to provide real-world outcomes that prove useful in reducing the threats associated with the use of public safety vehicles in criminal activity or terrorist attacks. A single case study will provide the foundation for answering the research questions. The *Hazardous Material Safety and Security Field Operational Test* conducted by U.S. Department of Transportation's Federal Motor Carrier Safety Administration (FMCSA), which partnered with the U.S. Department of Transportation (DOT's) Intelligent Transportation System Joint Program Office (JPO). The documents will be analyzed for technology strengths, gaps and insight regarding successful implementation strategies.[24] The study was chosen due to the broad array of tested vehicle security technologies in real-world settings and the importance

[24] D. Williams, J. Allen, M. Lepofsky, D. Murray, K. Wahl, D. Vercoe, S. Keppler, and T. Moses, *Hazmat Safety and Security Field Operational Test, Final Report*, 2004, Federal Motor Carrier Safety Administration, accessed February 20, 2013, http://www.fmcsa.dot.gov/documents/hazmat/fot/HMFOT-Final-Report.pdf; Science Applications International Corporation, *Hazardous Materials Safety and Security Technology Field Operational Test, Volume I: Evaluation Final Report Executive Summary*, 2004, Federal Motor Carrier Safety Administration, accessed February 20, 2013, http://www.fmcsa.dot.gov/documents/hazmat/fot/FINAL-Volume-I-Executive-Summary-11-10-04.pdf; Science Applications International Corporation, *Hazardous Materials Safety and Security Technology Field Operational Test Volume II: Evaluation Final Report Synthesis* (Washington, DC: U.S. Department of Transportation, 2004); Federal Motor Carrier Safety Administration, "Expanded Satellite Tracking," March 2006, accessed February 20, 2013, http://www.fmcsa.dot.gov/facts-research/research-technology/report/Mobile-Communications/mobile-communications-tracking-system-requirements.pdf; Federal Motor Carrier Safety Administration, "Untethered Tracking and Control Systems," December 2005, accessed February 20, 2013, http://www.fmcsa.dot.gov/facts-research/research-technology/report/untethered-dec05/untethered-dec05.pdf.

given to end user and machine interaction. Additionally, the study included a Delphi panel of subject matter experts, involved in developing the field operational test, included three state police officials and four firefighters.[25]

Vehicle Immobilization Technologies: Best Practices for Industry and Law Enforcement Final Report,[26] sponsored by FMSCA and Tennessee Department of Safety (TDOS) in partnership with the Oak Ridge National Laboratory (ORNL) and the University of Knoxville (UTK), further expands on the *Hazardous Materials Safety and Security Field Operational Test* findings. It goes on to develop vehicle immobilization technologies (VIT) best practices and concept of operations (COO) for law enforcement associated with hazmat and commercial vehicle security. This study utilized the hazmat field operational test extensively. Additionally, they performed a field operational test in a controlled setting at the Laurens Proving Grounds, a test track in South Carolina. Furthermore, it offers additional insight and clarity regarding best practices involving VITs.[27]

The collection data process from the case study categorizes security technologies by capabilities and effectiveness (best practices). In addition, the research explored discernable characteristics related to successful outcomes or failures related to human error or design. Lastly, the data is analyzed by determining overall average percentages identified in vulnerability reduction that each security technology provides alone, as well as, fused with other security technologies within the study. The findings are expected to provide support for a Tier I—Theft Prevention, Tier II—Authorized Use, Tier III—Tracking and Recovery and relevance for Tier IV—Human-Machine Interface Considerations.

The Michigan Department of Transportation (MDOT) provided the *State Planning and Research Grant* to the Center for Automotive Research (CAR) to explore best practices in connected and automated vehicle (CAV) technologies and intelligent

[25] Science Applications International Corporation, *Hazardous Materials Safety and Security, vol II*, 50.

[26] Federal Motor Carrier Safety Administration, *Vehicle Immobilization Technologies*.

[27] Ibid.

transport system (ITS) across the world.[28] This thesis summarizes the report in an effort to show the emerging trend of interconnectivity of vehicles with their surroundings. Connected technologies can be leveraged to boost the robustness of Tier III security technologies. Additionally, two studies in the area of anthropometrics are explored and summarized. Anthropometrics is the study of a person's (or group's) physical measurements applied to a task(s) form and function.[29] This will assist the reader in understanding the importance of human interaction with security technologies with regard to design and engineering to ensure successful implementation outcomes. The two studies are: *Field Quantification of Physical Exposure of Police Officers in Vehicle Operation*[30] and *Sizing Firefighters and Fire Apparatus: Safe by Design*.[31] The objective of the first study is to enhance anthropometric measurement database information by including findings from evaluations of U.S. firefighters. The second study, *Field Quantification of Physical Exposure of Police Officers in Vehicle Operation*, provides insight into the activities of law enforcement officers within their vehicles.[32]

The findings and proposed benefits offered by these studies and supported by additional fieldwork and research is analyzed to determine gaps and identify smart practices to build upon knowledge gained from design work exploration. Knowledge gained from the anthropometric studies will also be linked to the human interaction finding provided by the Hazardous Materials Field Operational Test case study. The information gained by researching design and anthropometrics will provide the fourth

---

[28] Michigan Department of Transportation and Center for Automotive Research, *International Survey of Best Practices in Connected Vehicle and Automated Vehicle Technology* (Ann Arbor, MI: Michigan Department of Transportation and Center for Automotive Research, 2013), accessed October 14, 2013, http://www.michigan.gov/documents/mdot/09-12-2013_International_Survey_of_Best_Practices_in_ITS_434162_7.pdf.

[29] "Workplace Safety and Health Topics: Anthropometry," Center for Disease Control and Prevention and National Institute for Occupational Safety and Health, accessed October 14, 2013, http://www.cdc.gov/niosh/topics/anthropometry/.

[30] Colin D. McKinnon, Jack P. Callaghan and Clark R. Dickerson, "Field Quantification of Physical Exposures of Police Officers in Vehicle Operation," *International Journal of Occupational Safety and Ergonomics-JOSE* 17, no. 1 (2011), 61.

[31] Hongwei Hsiao, *Sizing Firefighters and Fire Apparatus: Safe by Design*, Center for Disease Control and Prevention, accessed October 14, 2013, http://www.cdc.gov/niosh/topics/anthropometry/pdfs/Sizing%20firefighters%20proposal%20core%20part.pdf.

[32] McKinnon, Callaghan, and Dickerson, "Field Quantification," 61.

and final piece to build a proposed model for reducing public safety vehicle vulnerabilities through successful implementation of vehicle security technologies.

II. LITERATURE REVIEW

Literature on industry standards regarding securing public safety vehicles is limited. More so, there appears to be no minimum level of preventative security measures within disciplines of public safety such as police, fire and medical. Increased vehicle vulnerability is attributed to lack of security measures and cultural norms in operational practices. In order to address the issue with the least impact of disruption, two areas of focus are identified, vehicle security technology and design theory. In addition, the literature can be placed in one of three categories. The first is the limitations within the research. The second is information regarding existing technologies and emerging trends. The last is the application of design theory in the application of security technologies. Specifically, information pertaining to anthropometrics is explored for best practices across multiple disciplines.

There is no shortage of Law Enforcement Sensitive (LES) and For Official Use Only (FOUO), unclassified and open source documents.[33] Many unofficial versions of these reports are easily found on the World Wide Web by utilizing a common search engine and related key terms. Additionally, a synthesized version of these reports can be found in trade journals. Decision makers should examine the information contained in the official reports, ensuring primary source accuracy, prior to implementation of policies or practices related to safe and secure technologies by public safety agencies. One problem that confronts decision makers is the limitations to a comprehensive review. For example, one limitation can be found in the resistance to sharing confidential information

[33] Erek Cyr, *The Road Map to Cloned Vehicles* (Tallahassee, FL: Florida Department of Law Enforcement, 2008), this document is (FOUO); Central Florida Intelligence Exchange, *Nationwide Analysis—Increased Trend of Unoccupied Ambulance Thefts* (Orlando, FL: Central Florida Intelligence Exchange, 2012), this document is (FOUO); Department of Homeland Security and Department of Justice Federal Bureau of Investigation, *Potential Terrorist Use of Public Safety or Service Industry Uniforms, Identification or Vehicles* (Washington, DC: Department of Homeland Security and Department of Justice Federal Bureau of Investigation, 2004), this document is (FOUO); Department of Homeland Security and Department of Justice Federal Bureau of Investigation, *Terrorist Threats to the US Homeland Reporting Guide* (Washington, DC: Federal Bureau of Investigations and Department of Homeland Security, 2004), this document is (FOUO); Indiana Intelligence Fusion Center, *Suspicious Activity Involving Emergency Services and Hospitals* (Indianapolis, IN: Indiana Intelligence Fusion Center, Indiana Department of Homeland Security, 2008), this document is (FOUO); "DHS-FBI Terrorist Tradecraft: Impersonation: Use of Stolen, Cloned, or Repurposed Vehicles," Fire Line, January 18, 2013, Public Intelligence, http://publicintelligence.net/dhs-fbi-cloned-vehicles/, this document is (FOUO).

in the private sector. Industry trade secrets and proprietary information are similar to LES and FOUO concerns that vulnerabilities will be exposed and possibly exploited.

For example, the findings from a case study involving a private sector entity (FedEx) provided valuable information about the possibilities of technology. Fed Ex utilizes technology to reduce rear-end accidents by over 50 percent, and it is looking into global positioning systems.[34] There is litigation between the drivers, impacted by this technology, and Fed Ex executives, resulting in the inability to institute the two million dollar software. In addition to the litigation, the fear of proprietary information being shared with competitors left requests by this author for publishable information unanswered.[35] The ability to utilize Fed Ex as a case study proved futile.

Implementation prevention strategies surrounding public safety vehicle security technologies would provide little to no benefit in threat reduction concerning cloned or repurposed vehicles. Clones or repurposed public safety vehicles offer special challenges to security and as such require a different approach to risk reduction. These vehicles can be purchased for as little as $6,000.[36] The vulnerability created in homeland security by cloned and repurposed vehicles comes from the advantages they provide in terms of blending in and appearing normal. These vehicles could be admitted to areas otherwise off limits, such as next to buildings, secured parking areas, etc. Simply they could be able to bypass security protocols and gain access to strike hardened, high valued targets. Prevention and identification of any cloned vehicle is unrealistic.

A public safety vehicle utilized in an act of terrorism would be inexcusable given the technologies already on the market. Currently, there are no known registration processes for retired "authorized emergency vehicles" at any county, state or federal level. The tracking of emergency vehicles once removed from the internal inventories of the authority having jurisdiction (AHJ) is non-existent outside routine motor vehicle registration. Inventory control associated with homeland security grant inventories (i.e.,

---

[34] "FedEx Freight Adds Technology," *Traffic World* 270, no. 20 (2006): 24–26.

[35] Anonymous Fed Ex employee, personal communication with the author, 2013.

[36] Kimery, "Return of the "Clones."

Urban Area Security Initiative [UASI] and State Homeland Security Grant Programs [SHSGP]) only pertain to those vehicles and equipment purchased from such programs.

The next category of literature will involve identifying existing and emerging technologies. There are currently technologies on the market that specifically claim to aid in theft prevention and misuse of emergencies vehicles (e.g., police, fire or medical).[37] Particular attention will be given to technologies involving biometrics[38] and connectivity.

The research on connectivity within security technologies is an overreaching concept and is addressed in two studies involving interconnectivity. These private/public partnership programs will be analyzed to extrapolate smart practices for use in public safety implementation strategies. One area in connectivity technologies is short-range wireless communications (SRWC) Bluetooth,[39] Radio-Frequency Identification,[40] Near Field Communication,[41] and Dedicated Short Range Communications (DSRC)[42]. SRWC technologies allow users and machines to interconnect for better performance of end user systems. Field programmable gate array (FPGA)[43] (making field programming possible)

---

[37] Tremco Police Products, "Tremco Police Products," Tremco Police Products, accessed September 28, 2013, http://www.tremcopoliceproducts.com/; "Vehicle Immobilization System Touch Activated Brake Lock," Vista Brake Lock, accessed October 18, 2013, http://vistabrakelock.com/.

[38] Eugen Lupu, Petre G. Pop, and Marius N. Roman, "A Survey of Multimodal Biometric Systems," *International Journal of Computer Science and Its Applications*, accessed October 14, 2013, http://www.seekdl.org/nm.php?id=882.

[39] A. Dardanelli, F. Maggi, M. Tanelli, S. Zanero, S. M. Savaresi, R. Kochanek, and T. Holz "A Security Layer for Smartphone-to-Vehicle Communication Over Bluetooth," *Embedded Systems Letters, IEEE* 5, no. 3 (2005).

[40] Bob Violino, "What is RFID?" *RFID Journal* (January 2005), accessed October 18, 2013, http://www.rfidjournal.com/articles/view?1339.

[41] Near Field Communication, "About Near Field Communication," accessed October 18, 2013, http://www.nearfieldcommunication.org/about-nfc.html.

[42] Xinzhou Wu Subramanian, S., Guha, R., White, R.G., Junyi Li Lu, K.W., Bucceri, A. Tao Zhang, "Vehicular Communications using DSRC: Challenges, Enhancements, and Evolution," *IEEE Journal* 31, no. 9 (2005).

[43] Andrew J. Tickle Jiajing Sun, Lu Gan, and Jeremy S. Smith, "Feasibility of an Encryption and Decryption System for Messages and Images using a Field Programmable Gate Array (FPGA) as the Portable Encryption Key Platform," in *Proceedings Optical Design and Engineering III*, 71002N, September 27, 2008, doi:10.1117/12.797732.

and global system for mobile communication (GSM)[44] (which allow for communication with cell towers and utilized in alert notification functions) will be presented. A study by the U.S. Department of Transportation (DOT) addresses security of the hazardous materials trucking industry and technology utilized in a field operation test provide detailed real-life feedback on success and gaps within implementation and end user-machine interface.[45] The study offers detailed results of a variety of security technologies.[46] Another source, the Commercial Vehicle Information Systems and Networks Program, offers insight regarding benefits of public-private partnership and encourages mandates through funding incentives. In addition, the Security through Assessed Risk (STAR) program, a product from thesis work at the Naval Postgraduate School, supports providing incentives to agencies that comply with recommendations.[47] Furthermore, the Commercial Vehicle Information Systems and Networks (CVISN) provides smart practices in service and support of technologies, process and procedures to ensure continued communication takes place between the end users and oversight agencies. Additionally, a world look at connectivity programs regarding infrastructure is analyzed, "Best Practices in Vehicle Connectivity across the World."[48] As the title suggests, the Michigan Department of Transportation, in cooperation with the National Highway Traffic Safety Administration, examined some 400 programs from around the world included in their database.[49]

The third category of literature will explore two types of design, radical and incremental. These terms are synonymous with disruptive and human-centered design,

---

[44] Montaser N. Ramadan, Mohammad A. Al-Khedher and S. Al-Kheder, "Intelligent Anti-Theft and Tracking System for Automobiles," *International Journal of Machine Learning and Computing* 2, no. 1 (2012).

[45] Federal Motor Carrier Safety Administration, "Hazardous Materials Safety and Security Field Operational Test," accessed September 30, 2013, http://www.fmcsa.dot.gov/safety-security/hazmat/fot/safehazmat/results-brochure.htm.

[46] Science Applications International Corporation, *Hazardous Materials Safety and Security, vol II*.

[47] Colsky, "Public/Private Partnerships."

[48] Michigan Department of Transportation and Center for Automotive Research, *International Survey of Best Practices.*

[49] Ibid.

respectively. Understanding how technology impacts end users can be categorized into technology driven change and change driven be meaning.[50] Further examination of these concepts will be addressed in Chapter VI.

As disruptive technologies are introduced into the workforce, end-users build resistance by becoming adaptive to inconveniences, such as people writing their PINs on hands instead of memorizing them.[51] These adaptations may actually be detrimental to security measures. In addition, adaptive behaviors, cultural norms, and expertise will require consideration. "If we did not ask for it, we don't want it"[52] is an attitude that is prevalent in public safety. The consideration of design theory in the implementation of technologies and engineering is an important factor in successful outcomes.[53] This led the researcher into a human-centered design study of anthropometrics.

Anthropometrics is an emerging trend in public safety as it relates to cab design. Previously, measures taken to enhance cab design are driven from various industries that may not offer suitable comparisons of end users' wants and needs as related to public safety personnel and proficient job performance.[54] Several studies have been recently completed or are currently underway were considered as they related to public safety.[55] In addition, the Center for Disease Control and Prevention (CDC) also provides several reports and resources related to occupational health and anthropometrics.[56] The CDC

---

[50] Donald A. Norman and Roberto Verganti, "Incremental and Radical Innovation: Design Research Versus Technology and Meaning Change," March 18, 2012, http://jnd.org/dn.mss/Norman%20%26%20Verganti.%20Design%20Research%20%26%20Innovation-18%20Mar%202012.pdf.

[51] Tim Brown, *Change by Design* (New York: HarperCollins, 2009), 29.

[52] Cynthia Barton Rabe, *The Innovation Killer: How What We Know Limits What We Can Imagine-and What Smart Companies are Doing about It* (New York: Amaco, 2006), 54.

[53] Guy A. Boy, *The Handbook of Human-Machine Interaction: A Human-Centered Design Approach* (United Kingdom: Ashgate Publishing, 2011), 11.

[54] Hsiao, *Sizing Firefighters*.

[55] Johan F. M. Molenbroek, *Anthropometry and Usage Research of Dutch Police Cars* (Netherlands: Delft University of Technology, 2010); Hongwei Hsiao, "Anthropometric Procedures for Protective Equipment Sizing and Design," *Human Factors: The Journal of the Human Factors and Ergonomics Society* 55, no. 1 (2013): 6–35; Hsiao, *Sizing Firefighters*; McKinnon, Callaghan, and Dickerson, "Field Quantification," 61.

[56] "Workplace Safety and Health Topics: Anthropometry," Center for Disease Control and Prevention and National Institute for Occupational Safety and Health, accessed October 14, 2013, http://www.cdc.gov/niosh/topics/anthropometry/.

defines anthropometry as "the science that defines the physical measures of a person's size, form and functional capacities."[57] The research in this area provides additional insight through statistical methods and 3D modeling, which allows for consideration of 95 percent of a given workforce to be accommodated in use of technologies.

The literature review supports the theory that public safety vehicles are vulnerable to theft and misuse by criminals and terrorists alike. Likewise, they do not routinely have adequate tracking and recovery capabilities. Additionally, the concept regarding design theory applied to engineering offers insight in identifying smart practices when executing implementation strategies. Anthropometrics offers some of the latest information on the end-user-machine interface in police and fire disciplines among other industries. In addition, the world is becoming more interconnected every day. Similarly, security systems are becoming more and more intelligent as connectivity continues to enhance real-time information exchange. This creates risks that must be considered when implementing any security strategy. Vehicle security is no different, and cyber-threats related to public safety vehicle security will require active consideration by engineers as well as public safety officials. For example, the electronic control on-board systems can be hacked resulting in loss of critical vehicle controls. Lastly, there are technologies available today that would reduce the risk of vehicle theft and misuse by fortifying vulnerabilities. They offer several levels of protection and authorized user alerts. These are explored in the next chapters.

[57] Ibid.

III. TIER I—THEFT PREVENTION

Theft prevention of public safety vehicles should be given highest priority. Many theft prevention measures have no cost associated with implementation, while others are available on the market for less than $100. Tier I theft prevention measures are categorized into three types: common sense security, authentication devices and interruption devices.

A. COMMON SENSE SECURITY

The National Highway Traffic Safety Administration, an agency with more than 25 years of helping vehicle owners with vehicle theft, list the following common sense measures when parking and exiting a vehicle: remove the keys, secure all windows and lock doors, never leave valuables in the vehicle, and never leave a vehicle running unattended.[58] Common sense practices, effective in preventing vehicle theft, are lacking in the public safety community as a result of cultural norms and industry accepted operational practices. Leaving a police car unlocked and running while chasing a criminal, literally "opens the door" for vulnerability. Public safety trade reports confirm vulnerabilities associated with public safety vehicle thefts often are associated with lack of common sense practices. One article provides six contributing factors associated with 12 ambulance thefts over a one-year period, 2012, in the U.S.:[59]

- Ambulances are left unattended
- Keys are left in the ignition
- The ambulance is left running
- Thieves are under the influence of drugs and alcohol
- Psychiatric patients
- Ambulances are parked outside of hospitals

Although very basic means are recommended, there is no indication of any standards across public safety agencies that include implementing common sense security

[58] National Highway Traffic Safety Administration, *Vehicle Theft Prevention* (Washington, DC: National Highway Traffic Safety Administration, n.d.) 5.

[59] Ludwig, "EMS: Stolen Ambulance."

measures. There is no cost in implementing common sense security measures, and they may prove to have the greatest impact on preventing criminal (mischievous and malicious) activity including opportunistic actors.[60]

B. INTERRUPTION TECHNOLOGIES—ELECTRONIC VEHICLE IMMOBILIZATION DEVICE

Interruption measures, electronic vehicle immobilization devices (eVIDs), provide a means of disabling or enabling at least one vehicle system critical in its effective operation. One example of this would be to have to step on a concealed button to place the car in drive. Another example would be a system that closes an open circuit from the battery supply to the starter when an operator turns on the battery switch, located in an inconspicuous location. There are companies that specifically utilize this technology and claim these measures aid in theft prevention of emergencies vehicles; the technology is currently on the market (e.g., for police, fire or medical).[61] For example, The Tremco Police Package Integrated Anti-Theft System is a popular device used by the law enforcement community. The Tremco company claims the device offers easy installation, low costs and an effective solution to preventing theft of law enforcement vehicles.[62] According to the Tremco's website there are 28 large public safety agencies, 15 federal agencies and hundreds of towns across the U.S and Canada currently utilizing the device.[63]

C. AUTHENTICATION DEVICE

The authentication devices provide users with vehicle access and engage or disengage interruption technologies, such as eVID so only authorized users can operate the vehicle. Some implement short-range wireless technology between the device and

---

[60] Frank Scafidi, "Hot Wheels 2012," 2013, National Insurance Crime Bureau, https://www.nicb.org/newsroom/news-releases/hot-wheels-2012; District of Columbia Metropolitan Police Department, "Auto Theft Prevention," accessed October 14, 2013,. http://mpdc.dc.gov/page/auto-theft-prevention.

[61] Tremco Police Products, "Tremco Police Products;" "Vehicle Immobilization System Touch Activated Brake Lock," Vista Brake Lock, accessed October 18, 2013, http://vistabrakelock.com/.

[62] Ibid.

[63] Ibid.

the vehicle's on-board system; the device is often linked to the ignition module. Authentication technology can be found in the basic key, key fob, transponder keys, laser cut keys, and smart keys (authentication token).[64] The basic key does not need further explanation. The key fob allows remote keyless entry and panic button activation. This wireless device can lock or unlock vehicles and provide remote vehicle disabling in some cases. Transponder keys combine basic key technology with authentication by the addition of a small circuit added to the end of the key for authentication as well as operating the key locking mechanism. When the key is inserted into the ignition, a sensor confirms the key's authenticity and allows the vehicle to start. Laser cut keys are more difficult to replicate than the basic key and in turn provide a higher level of security. The smart key-authentication token utilizes short-range wireless technology to communicate between the device and the vehicle. The vehicle can then be started once the authentication is verified. Smart keys can be found today on many entry-level model automobiles as standard equipment. The vehicle will not unlock or start without the smart key's close proximity to the on-board receiver. The authentication process described in Tier I technology does not take into account if the person in possession of the device is an authorized user.

There are challenges with smart key technology use, such as: battery failure, user authorization not verified, user misplaces the smart key or removes it from a vehicle used by multiple authorized operators. Batteries failure prevents the operator from gaining entry or starting the vehicle. When this occurs, it may require timely steps to be taken for reprogramming.

Another scenario that illustrates the challenges of technology would be if, for convenience, the operator leaves the device in the vehicle for ease of use. In this case, anyone who enters the vehicle would be able to operate it. Yet another scenario might be

64 "The High Cost of Losing Your Keys: Key Technology has Advanced and so has Replacement Cost," Edmunds, accessed October 28, 2013, http://www.edmunds.com/car-care/the-high-cost-of-losing-your-keys.html.

when the person in possession of the smart key leaves the vehicle, making the vehicle inoperative once it is shut down. This scenario could easily play out in public safety where crew changes are part of the job.

Regardless of the limitation, it is clear authentication devices currently on the market continue to evolve based on user needs and are extremely effective, in spite of associated challenges. One report out of Phoenix, Arizona suggests that authentication technology is partially responsible for the decrease of car thefts from 1,089 cars per 100,000 residents in 2002 to 308 cars per 100,000 residents today.[65]

D. TIER I TECHNOLOGY IN THE FMSCA STUDY ON EFFECTIVENESS OF SECURITY TECHNOLOGIES IN HAZMAT TRUCKING

The Federal Motor Carrier Safety Administration (FMCSA) produced findings of a yearlong comprehensive study on technological solutions for hazmat trucking.[66] The panic button (interruption device) and remote vehicle disabling (authentication and interruption device), two of 11 technologies, can be classified within the Tier I technology category.

1. Panic Buttons

A panic button mounted on the dash and key fob carried on the driver allow the driver to disable the vehicle in the event of an emergency.[67] The key fob system is effective from 150 feet away from the vehicle.[68] The key fob could be utilized if the driver who is overtaken by a criminal/terrorist or if he or she witnesses the vehicle being stolen and is in close enough proximity to disable to the operating system.

a. Analysis

The panic button system is simple and effective. The panic button technology provides an average of nine percent reduction in vulnerabilities across all

[65] D. S. Woodfill, "Car Theft Decreases in Metro Phoenix," August 25, 2012, accessed January 30, 2013, http://www.azcentral.com/news/articles/20120810phoenix-car-theft-decrease.html.

[66] Science Applications International Corporation, *Hazardous Materials Safety and Security, vol II*.

[67] Ibid., 6.

[68] Ibid.

hazmat load types with an increase to 21 percent when utilized with key fob. The drivers were accepting of this system, and some even gave excellent reviews of the technology.[69] Positive feedback from the users included the use of the panic button/key fob was not required to operate unless an emergency occurred, so it did not negatively impact their work processes.[70] Additionally, the dash-mounted button was within arm's length of the driver in the seated position, which makes it easy to activate if necessary.

There are some limitations noted in the technology.

- The key fob could be lost or left in the vehicle inadvertently rendering the system useless if the vehicle was stolen when the driver exited.
- The key fob would not work with dead batteries, as noted with key fobs associated with authentication, and no battery indication display was available for the user's convenience.
- The key fob would be difficult to use if the driver is being assaulted.
- False activations should be expected due to inadvertent pressing of the red button.
- A driver authentication and validation process is needed once the button is activated.

2. On Board Computer—Remote Vehicle Disabling

The on-board computer—remote vehicle disabling technology monitors vehicle electronic system and disables the vehicle if there is a security breach. Additionally, the remote vehicle technology would shut down vital components if the signal to the wireless communications module is blocked. The on-board computer—remote disabling technology integrates with the vehicle's factory installed vital electronic components.[71] The disabling methods include shutting down the fuel directly or communicating with the vehicle's data bus wirelessly, which results in loss of throttle control.[72]

---

[69] Ibid.

[70] Ibid., 33.

[71] Science Applications International Corporation, *Hazardous Materials Safety and Security, vol I*, 9.

[72] Ibid., 9.

a. Analysis

On-board computer—remote vehicle disabling technology had an average of 22 percent reduction in vulnerabilities across all hazmat load types. The subject matter expert panel identified the need for security of vehicle electronic systems in the event there is a security breach that would allow unauthorized personnel to tamper with system components.[73]

E. TIER I TECHNOLOGY SUMMARY

There are limitations to general non-user specific technology. First, a vehicle left unlocked and running offers little defense against theft. Second, in the case of hidden button devices and inconspicuous locations of battery switches—if someone knows how it works or where it is located, the devices offer little or no resistance against use of the vehicle. Third, authentication devices do not distinguish from authorized and unauthorized users. Tier I technologies offer effective solutions to reduce public safety vehicle vulnerabilities. The fusion of technologies, such as combining common sense measures, interruption devices and authentication devices clearly offer superior protection over any technology individually. Likewise, although authentication devices offer promising results, fusion of Tier I technologies with advanced technological solutions found in Tier II and Tier III would offer even more superior security measures and greater percentages in vulnerability reduction. Finally, advances in internal vehicle systems require security measures to prevent exploitation and access by criminals or terrorists to security measure programming and on-board vehicle computers. If such a security breach "attack" on the system occurs, an automatic notification must be made to authorized personnel.

[73] Ibid., 9–10.

IV. TIER II—AUTHORIZED USE

Tier II—Authorized use technologies, an enhanced authentication technology; validate user specific information via on-board computers or external software programs. Once the system validates or identifies the user, an approval signal is sent to the interruption technology, eVID, (Tier I), to authorize the use of the critical vehicle component. The validation process requires the user to have a user specific smart card, passcode, PIN number, biometrics (biological identification [ID] through statistics), digital signature or a variety of other technologies in order to operate the vehicle. Authorized use technologies can range from simple authorized user passwords to continuous monitoring of several biometric characteristics and traits. The combination of authentication (Tier I and Tier II) technologies should be considered in high-security operations.[74] This chapter will further discuss passwords and other personal identification criteria, explore the study of biometrics, and identify Tier II technologies evaluated in the FMSCA hazmat trucking study.

A. DRIVER AUTHENTICATION TECHNOLOGIES

In driver authentication technologies (DAT),[75] operators are identified through passport (smartcard), personal identification numbers, and password.[76] One emerging Tier II technology, combining security codes with the vehicle's air brake systems, is hitting the public safety marketplace exhibited at Fire Rescue East 2013 in Daytona Beach, Florida.[77] The device allows only authorized users with the proper code to deactivate the device thus releasing the locking mechanism for critical components, in this case the air brakes. The technology design takes into account human-error. If the driver opens the driver's door and gets out of the driver's seat, the VISTA brake lock system is activated. This ensures apparatus are secured automatically in the event the

[74] Federal Motor Carrier Safety Administration, *Vehicle Immobilization Technologies*, 95.

[75] Ibid., 94.

[76] Lupu, Pop, and Roman, *A Survey of Multimodal Biometric Systems*, 37.

[77] "Vehicle Immobilization System Touch Activated Brake Lock," Vista Brake Lock, accessed October 18, 2013, http://vistabrakelock.com/.

operator forgets to engage the system by setting the brake. Securing the brake system of the vehicle also prevents the vehicle from rolling out of the bay unintentionally—a scenario seen all too often in the fire service.

Password and electronic signatures work in the same way as the PIN identification does. The user applies known information into a computer for validation and verification. Once the password or electronic signature is approved, the system allows "authorized" operation of the vehicle. One limitation to this security measure is the sharing of security information among users. If all users share one code, the specific identification of the current user is unobtainable. This could be problematic when an employee is terminated or has restricted driving privileges. Additionally, if the user writes down the security information in a common place, non-authorized personnel might find it and use it. Lastly, the need to update verification information or routinely change the information as part of the security system's robustness suggests FPGA technologies should be employed for ease of security information changes.

B. BIOMETRICS

A great deal of research is currently available on biometric advancements in vehicle security. Biometric technology is cutting edge and taking the place of PIN numbers, and passwords.[78] For this reason, a deeper understanding of biometrics strengths and the perceived limitations need to be analyzed. Biometric systems have limits, and, as with any other technology, none are perfect for a variety of reasons.[79] For example, take the following scenario: a driver who is authorized to utilize a vehicle through the use of biometric technology is denied access. In this scenario, a secondary system such as a password or PIN number is warranted. Agency representatives should receive an alert notification regarding the biometric login denial to further ensure an attempt to steal the vehicle is not taking place.

[78] P. Sreekala, V. Jose, J. Joseph, and S. Joseph, "The Human Iris Structure and its Application in Security System of Car," in *Engineering Education: Innovative Practices and Future Trends Proceedings*, Kottayam, India, July 2012.

[79] Lupu, Pop, and Roman, *A Survey of Multimodal Biometric Systems*, 39.

1. What is a Human Biometric?

Biometrics works to confirm identity by identify "what I am (what I do)" in the electronic context of "who am I?"[80] Furthermore, biometrics is a digital representation of body characteristics, such as the face, fingerprints, hands, eye, signature, and voice.[81] Features for use in biometrics must be universal—everyone has one, distinct—no two people have the same, permanent—cannot change often, and collectable—can be quantitatively measured. Additional features of biometric technology may require performance, speed, robustness and accuracy of recognition, acceptability (degree the biometric is accepted by the user), and resistance to circumvention.[82] Fingerprint, face, iris, retina, voice, signature, palm print, palm vein, hand vein, ginger vein, knuckle creases can all be used for authentication.[83] However, there are several weaknesses of unimodal or single biometric data acquisition:[84]

- Lack of universal characteristic—approximately four percent fingerprints[85] and seven percent of irises within the population cannot be captured.
- Noisy signals due to user error.
- Unacceptable error rates
- Lack of permanence and variability in time
- Fraud through cloning, voluntary or involuntary.

Biometric face recognition and detection system are the most sophisticated and expensive of biometric authentication technologies.[86] On the other hand, biometric

---

[80] Ibid.

[81] Ibid., 37.

[82] Ibid.

[83] Ibid.; Weiqi Yuan and Yonghua Tang, "The Driver Authentication Device Based on the Characteristics of Palmprint and Palm Vein," in *International Conference on Hand-Based Biometrics*, Hong Kong, November 17–18, 2011.

[84] Lupu, Pop, and Roman, *A Survey of Multimodal Biometric Systems*, 40.

[85] Robert Snelick, Umut Uludag, Alan Mink, Michael Indovina, and Anil Jain, "Large-Scale Evaluation of Multimodal Biometric Authentication using State-of-the-Art Systems," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27, no. 3 (2005): 450–455.

[86] Y. B. T. Sundari, G. Laxminarayana, and G. Vijaya Laxmi, "Anti-Theft Mechanism through Face Recognition Using FPGA," *International Journal of Advancements in Research and Technology* 1, no. 6 (2012): 46–49.

fingerprint anti-theft devices are selling at low cost in the aftermarket automobile industry.[87] Consideration must be given to the fact that fingerprint biometrics utilizes repeated contact of the machine-user interface possibly causing wear, tear and contamination.[88] Biometrics can utilize short-range wireless communication to acquire the necessary biometric data and analyze it against databases and software protocols. Wireless palm print and palm vein acquisition through radio frequency technology is like "taking a picture" of the palm.[89] Biometrics can also offer superior performance through continuous monitoring of authorized user, such as the iris. The iris is ideal for continuous monitoring because there are no two irises alike and the amount of information that can be obtained through iris recognition is much greater than fingerprint recognition.[90]

2. Multimodal Fusion of Biometrics

For these reasons, public safety agencies should consider employing multimodal biometrics to ensure response times and availability of resources are not negatively impacted. Simultaneous acquisition, identification and validation of two or more characteristics of the human body (multimodal), can build a comprehensive and effective biometric identification system, improve overall performance, improve system robustness, and reduce the detection complexity more so than a single biometric.[91] For example, a palm print and a palm vessel print working together are more successful than when used separately.[92] The most popular biometrics fusion today utilizes facial recognition and fingerprint.[93] Multimodal biometrics allow "fusion" to occur at any level within the system (feature extraction sensors, matching parameters, algorithm module). Some biometric features are conducive to fusion as seen in Table 1.[94] The table clearly

[87] Yuan and a Tang, *The Driver Authentication*, 1–5.

[88] Ibid.

[89] Ibid.

[90] Sreekala et al., "The Human Iris Structure," 1–5.

[91] Yuan and a Tang, *The Driver Authentication*, 1.

[92] Ibid.

[93] Sreekala et al., "The Human Iris Structure,"1–2.

[94] Lupu, Pop, and Roman, *A Survey of Multimodal Biometric Systems*, 40.

shows fusion of two to three biometrics favorable to being analyzed at any one time, and there is no requirement for the biometric feature to come from the same body area (it could be fingerprint and face).

Biometric features
Voice, Face, Lips movement
Fingerprint, Face
Fingerprint, Face, Voice
Fingerprint, Face, Hand geometry
Fingerprint, Voice, Hand geometry
Voice, Hand geometry
Facial thermogram, Face
Iris, Face
Palm print, Hand geometry
Ear form, Voice
Voice, Lips movement

Table 1. Biometric Features Suited to Fusion

3. Biometrics at Work

The flow chart (Figure 1) provides a clear representation of the authorized user process utilizing biometrics as the primary identification and a password as the secondary or backup identification technology. Additionally, the flow chart shows how biometric technology collaborates through interconnectivity with the vehicles on-board ECU: fuel control, control of variable valve sensor, electronic valve control, crankshaft sensors and door locks.[95]

[95] Sreekala et al., "The Human Iris Structure,"3.

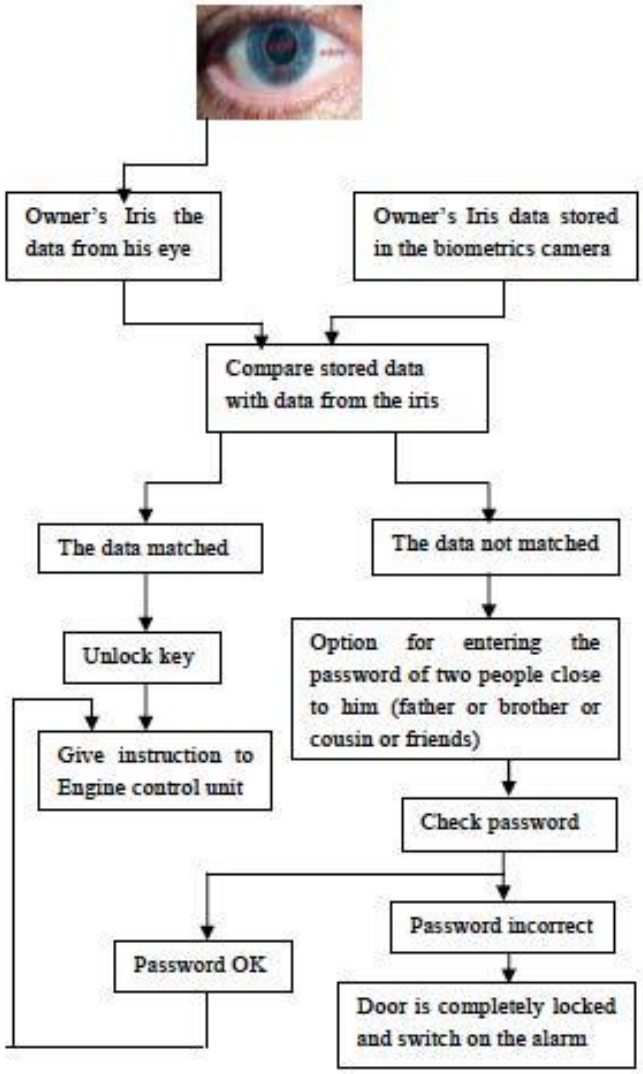


Figure 4.Block diagram of control

Figure 1. Block Diagram of Control

Additional wireless technology, such as global system for mobile communication (GSM) technology, would provide a means for notification of owners or agencies when

the primary and secondary security requirements are not met. Embedded vehicle burglarproof systems are enhanced with the addition of facial recognition and GSM technologies. The five main functions:[96]

1. Human-face recognition: The owners' face information is used as the standards of recognition. It must verify the feature of the human face before the vehicle can be used.
2. Message alarming: When someone tries to steal the vehicle, the message can be send to the owners' mobile phone immediately without any noise.
3. GSM network: The system can call the police or send the message via the GSM network wherever the vehicle was.
4. Two methods of recognition: Besides the human face recognition, the method of password recognition can be also used to the system as a secondary means of identification in the event of primary technology error.
5. GPS (Tier III) technology: The owner can find out the vehicle's location via the GPS technology. This technology will be further discussed in the Tier III—Tracking and Recovery chapter.

It is important to note the collaboration of technologies outlined above: Engine Control Unit ECU interruption device (Tier I), password (Tier II), biometrics (Tier II) and a mention of GPS technology (Tier III) that will be discussed in greater detail in the next chapter, Tier III Tracking and Recovery. For now, the effectiveness of Tier II technologies evaluated in the hazmat security study provides additional promise there are technological solutions for securing public safety vehicles.

C. TIER II TECHNOLOGY IN THE FMSCA STUDY ON EFFECTIVENESS OF SECURITY TECHNOLOGIES IN HAZMAT TRUCKING

1. On-Board Computer with Remote Door Lock

Remote door lock allowed dispatchers to lock/unlock doors remotely.[97] The operator would authenticate the request to open the trailer via the on-board computer.

[96] Yun Yang and JinHao Liu, "The Design of Automotive Burglar-Proof Based on Human Face Recognition," in *Proceedings E-Learning, E-Business, Enterprise Information Systems, and E-Government*, December 2009, 41.

[97] Science Applications International Corporation, *Hazardous Materials Safety and Security, vol II*, 37.

Once approved and the signal is sent to open the trailer from the dispatcher, the operator has 20–60 seconds to open the trailer otherwise the lock would reengage automatically.[98] Wireless communication external to the vehicle is also part of the fusion of technologies in this example.[99] This technology provided an average 18 percent vulnerability reduction across all load types. Securing inventory is directly related to public safety vehicles where cost of lost inventory can exceed $100,000, and security of inventory, such as weapons, is critically important to ensure items do not fall into the wrong hands.

2. Electronic Cargo Seals

Electronic cargo seals allowed documentation, through a web-based program, to track the chain of custody of a given commodity.[100] Through electronic signatures, the E-seal tracked a variety of steps to ensure an authorized operator documented inventory control.[101] However, during testing, the technology required five to six minutes to complete all the steps and became cumbersome to the operator.[102] Further design modification allowed several steps to be combined reducing the time to one to two minutes.[103] Even with design complications to the end user (human-machine interface discussed in later chapter), the technology still offered an 18 percent reduction in vulnerability across all hazmat load types.

3. Global Login

Global login is the use of a wireless system, as well as, on-board verification software that accepts identification with a valid ID number and password only known by the driver and rejects others.[104] The process took on average 33 seconds to authenticate and validate driver credentials and an average of 38 seconds to determine the input

[98] Ibid.

[99] Ibid.

[100] Ibid., 9.

[101] Ibid., 36.

[102] Ibid.

[103] Ibid.

[104] Ibid., 7.

measures were invalid, resulting in notification to the dispatcher.[105] The training was brief and simple and the operators liked the technology even after extensive use.[106] This technology was used as a backup technology for biometric global login in some test.[107] The technology enhanced vehicle vulnerabilities on an average of 20 percent across all load types. This is a significant increase in security and should be given merit in the public safety community.

Requiring a double global login could enhance login technology. Risk to the system includes sharing of login information or inadequate security of login information at the user level. The driver is required to remember ID and password, some of which can be extensive and outside the four-digit bank PIN utilized for ATM cards. Use of characters and symbols strengthens the system's vulnerability in one way, however, may increase the system's vulnerability in another way (i.e., when drivers right down their passwords and ID numbers).

4. Biometric Global Login

Similar to the global login, the driver instead utilizes a user specific smart card (Tier II) and fingerprint (Tier II) scan for access.[108] Another difference worthy of noting is the system verification and validation is on-board the vehicle, and no wireless technology is needed. The technology utilizes a fingerprint protocol for accepting or rejecting the operator. In this case, a single biometric feature (fingerprint) was used.[109] This is proven to be a limitation when compared to multimodal biometric research. Additionally, the ability to provide real-time continuous data to ensure that the authorized user is operating the vehicle throughout the travel is preferable. For instance, a criminal could require an operator to start the vehicle utilizing a fingerprint and smart card only to remove authorized driver once it is completed. Additionally, design and functionality issues were highlighted by the research team in that they hampered evaluation of this

[105] Ibid., 20.

[106] Ibid., 28.

[107] Ibid.

[108] Ibid., 7.

[109] Ibid.

technology during this test.[110] Long wait times for verification often provided operators a reason to utilize the secondary password module.[111] Nevertheless, an average of 20 percent reduction in vehicle vulnerability across all load types was seen when utilizing biometric technology with a global login backup.

5. Electronic Supply Chain Manifest

The electronic supply chain manifest (ESCM) works as follows. After utilizing biometric global login and a smart card to access the system, the driver creates an electronic manifest and identifies the work assignment.[112] The computer automatically keeps a chain of custody by the user logins.[113] This technology is dependent on wireless communication, biometric global login, smart card application, and Internet software.[114] This software simply keeps track of the operator's actions regarding deliveries and system status. Both on-board and external authorized users can access the information in order to determine if predetermined schedules are being met.[115] One limitation of the technology is ESCM with biometrics requires a high level of attention and human interaction.[116] In terms of security, the ESCM technology reduced vulnerabilities across load types by an average of 20 percent.

D. SUMMARY

The use of user specific information clearly enhances vehicle security through reduction in vulnerabilities. Password and PINs provide increased protection; however, have considerable limitations themselves due to potential for lack of code security by the end user. Additionally, many of the technical examples utilized more than one

[110] Ibid., 28–29.

[111] Ibid.

[112] Ibid., 7–8.

[113] Ibid.

[114] Ibid.

[115] Ibid.

[116] Ibid., 32.

technology (e.g. ESCM utilized internal wireless communication, smart card, biometrics and external communication for software data upload).

Overall analysis suggests consideration should be given to primary and secondary security technologies in the event of error or system failure. Lastly, the need for additional technology such as GPS and external remote vehicle shut down will only enhance the overall system and provide a means for tracking and recovery.

THIS PAGE INTENTIONALLY LEFT BLANK

V. TIER III–TRACKING AND RECOVERY

Tier III—Tracking and Recovery technology builds on Tier I—Theft Prevention and Tier II—Authorized Use components. Additionally, Tier III—Tracking and recovery technologies provide enhanced security measures by providing means for tracking vehicle location. This chapter will discuss how wireless communication and GPS provide the backbone for Tier III technology. Second, the hazmat case study Tier III technologies will be explored. Analysis of the reduction in vehicle vulnerability across all technologies when implemented collaboratively will be presented. Finally, emerging infrastructure enhancing vehicle connectivity will be discussed and best practices from a case study will be explored.

A. VEHICLE CONNECTIVITY AND GPS

Wireless communication in combination with GPS technologies for the purpose of remotely monitoring a vehicles location is commonly referred to as "telematics."[117] The use of terrestrial and satellite coverage working together for purposes of global positioning increases the ability to acquire real time data from on-board systems. When in rural areas, the coverage of terrestrial communication may be limited, and the system becomes reliant on satellite communication. Satellites require a clear line of site from ground to space, and there are limitations as well.[118] Infrastructure, natural barriers, and weather can all prove to reduce the ability to acquire satellite communication. Vehicle wireless communications and GPS technologies were limited only a few years ago. Today, it is a national priority. The U.S. Department of Transportation *Strategic Plan for 2012–2016* lists vehicle to infrastructure (V2I) and vehicle to vehicle as one of the top strategies for the future.[119] The report also states, "Conduct vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) research on technologies that enable vehicles to

[117] Scafidi, "Hot Wheels 2012."

[118] Joseph Straw, "Tracking Dangerous Cargo," *Security Management* 51, no. 12 (2007), 66–91.

[119] U.S. Department of Transportation, *Transportation for a New Generation, Strategic Plan, Fiscal Years 2012–2016* (Washington, DC: U.S. Department of Transportation, 2013), 3.

communicate with each other to avoid collision."[120] This infrastructure can be used to communicate other information as well, including tracking and recovery for vehicle security.

There are hundreds of interconnectivity programs all over the world. The demand for intelligent real-time systems is limited only by the current ability for technologies to be 100 percent connected. For example, increased focus on security regarding military assets has moved from command, control, and communications (C^3) programs to command, control communications and intelligence (C^3I) systems.[121] The military, Surface Deployment and Distribution Command (SDDCTEA), is utilizing C^3I capabilities within the Intelligent Road/Rail information Server (IRRIS) to provide worldwide assets tracking and detailed information on the infrastructure.[122] The intelligent systems will analyze information obtained through "data mining" and "data warehousing"[123] via connectivity of the assigned vehicles, goods, or services connected to other machines, including terrestrial satellite, other vehicles, and the infrastructure.

B. BEST PRACTICES IN VEHICLE CONNECTIVITY ACROSS THE WORLD

The Michigan Department of Transportation (MDOT) provided the *State Planning and Research Grant* to the Center for Automotive Research (CAR) to explore best practices in connected and automated vehicle (CAV) technologies and intelligent transport system (ITS) across the world.[124] A summary of the report emphasizes the emerging trend of interconnectivity of vehicles with their surroundings.[125] The importance of connected vehicle technologies can be leveraged to boost the robustness of Tier III security technologies.

---

[120] Ibid., 11

[121] Ron Hughes et al., "The Context for Commercial Vehicle Enforcement Activity 2020: Forecast of Future Directions in Truck Safety and Security," (Washington, DC: Transportation Research Board, 2005).

[122] Ibid., 9.

[123] Ibid.

[124] Michigan Department of Transportation and Center for Automotive Research, *International Survey of Best Practices*.

[125] Ibid., 68–71.

Research was conducted and results were analyzed to identify best practices involved in vehicle connectivity programs across the world. The research started in 2010 with a database of information regarding CAV.[126] Multiple updates have taken place in the period between 2010 and this report.[127] The interest by MDOT comes from recent interest by the National Highway Traffic and Safety Administration (NHTSA) to regulate connected vehicle technology in vehicles (2013) and heavy-duty vehicles (2014).[128] Programs to date included in the database and associated locations: 85 Asian, 159 European, 149 North America and seven in Oceania countries.[129] The report emphasizes funding strategies and other important factors in successful connectivity programs.[130]

1. Funding strategies include:
    - Commit budget allocations requiring matching funds
    - Pursue funding at the national level
    - Tolls to fund program
2. Six other important factors include
    - Forming coalitions
    - Creating industry competiveness
    - Developing programmatic themes and bold goals
    - Generating expertise
    - Regulating technology to build a strong business case
    - Standardize global/regional architecture

All of the other factors listed in MDOT report as best practices for successful programs can be leveraged when implementing a vehicle security program within an agency.

[126] Ibid., 6.

[127] Ibid.

[128] Ibid., 10.

[129] Ibid., 6.

[130] Ibid., 68–71.

C. TIER III TECHNOLOGY IN THE FMSCA STUDY ON EFFECTIVENESS OF SECURITY TECHNOLOGIES IN HAZMAT TRUCKING

1. Wireless Communications and GPS Tracking—Telematics

Use of Global Position Systems (GPS) utilizing wireless satellite technology to determine a vehicle positioning in latitude and longitude outputs.[131] A terrestrial-based system works primarily in the same way as a land-based two-way communications.[132] Each system shows the location of the vehicle through an automated request from the dispatcher.[133] This request can be made as often as needed. The system is relatively transparent to the users and requires little to no interface from the driver. Telematics offer a 15 percent reduction in vehicle security vulnerability across all load types.[134] This technology was also believed by the report authors to be beneficial in recovering stolen assets.[135] A tractor-trailer unit is worth more than $100,000 and the contents even more.[136] Three technologies within the study were 100 percent dependent on both wireless communications and GPS. These are geofencing, tethered and untethered trailer tracking, and the Public Sector Reporting Sector.

a. Public Sector Reporting Center

The Public Sector Reporting Center (PSCR) provided information to local public safety officials through the fusion of several technologies, including satellite communication, geofencing, wireless communications (voice and data), and automatic alert notification regarding off-route information in real-time.[137] Additionally, the information is accessible to authorized users through a web-based application.[138]

---

131 Science Applications International Corporation, *Hazardous Materials Safety and Security, vol II*, 5.

132 Ibid., 5.

133 Ibid.

134 Ibid., 23.

135 Ibid., 45.

136 Ibid.

137 Ibid.

138 Ibid., 95.

Protocols were written specifically to each agencies' end-user needs.[139] The software analyzes big data within a database against the protocols and algorithms written in the software.[140] This results in an intelligent system capable of providing automatic notification of unauthorized use, location, or other criteria.[141]

Analysis of PSRC suggests the fusion of technologies offers an extensive preventative and response capable security system regarding vehicle security. PSRC required the use of geofencing tethered and un-tethered, in tracking vehicles and trailers. This technology offered on average a 23 percent reduction in vulnerabilities across load types.[142] Applications available to end users on mobile devices and unlimited customization that are based on end-user needs proved to be smart practice.[143]

(1) Geofencing. Geofencing notifies carriers if a vehicle leaves a designated route or enters a restricted area. This system is heavily dependent on wireless communications. The route or zone is identified or limited by an electronic fence or geofence.[144] In addition, the carrier can set the automatic vehicle location check based on preferences. The field operational test (FOT) set the parameter at one hour.[145] Alert notifications were sent to designated persons within 30 seconds to one minute of the system determining the vehicle was not within designated zones.[146] However, unauthorized, alternative route alerts might be a false positive because drivers may take different routes, depending on road network and their familiarity with the geographical area.[147]

---

[139] Ibid., 94–100.

[140] Ibid.

[141] Ibid.

[142] Ibid., 23.

[143] Ibid., 94–100.

[144] Colsky, "Public/Private Partnerships," 40.

[145] Science Applications International Corporation, *Hazardous Materials Safety and Security, vol II*, 35.

[146] Ibid., 34–35.

[147] Ibid.

In the event of public safety and security, geofencing technology would allow for timely notification if a vehicle was moving or was out of assigned areas. Theft of public safety vehicles may go unreported for hours or days, especially in rural communities. Utilizing geofencing, staff would be notified of such movements within the prescribed timeframe outlined in the devices algorithm. Geofence events reported during the study were: 165 off route detections and 79 on route detections (notification when on an off-route vehicle returns to approved area), 38 Geofence violations (a driver was alerted the vehicle was in a restricted area), and 38 exited Geofence area.[148]

(2) Analysis. The participants viewed geofencing technology positively because it did not require them to perform additional task to make it function properly.[149] Geofencing technology would require a great deal of planning and background prior to setting limits within the public safety community where vehicles may need to respond to alarms outside primary run areas. The system might be enhanced by the support of other software products interactive with live CAD such as those seen from Deccan International.[150] This company offers several software programs that allow for a standardized algorithm for unit response based on resource availability, previous response data (10 years in many cases), and road network.

b. Tethered and Untethered Trailer Tracking

Tracking of tethered and untethered trailer provides dispatchers with real-time information regarding a trailers whereabouts.[151] This includes if the trailer is untethered from the authorized tractor.[152] Geofencing was utilized along with terrestrial wireless communication for alert notification through established protocols.[153] This included areas of authorized use and identified restricted areas where trailer travel was

[148] Ibid., 34–35.

[149] Ibid.

[150] Deccan International, "Deccan," accessed August 18, 2013, http://www.deccanintl.com/.

[151] Science Applications International Corporation, *Hazardous Materials Safety and Security, vol II*, 10.

[152] Ibid., 10

[153] Ibid., 10–11.

specifically forbidden[154], such as the White House. Trailer tracking offers another example where fusion of technologies, including end user alert notification, enhances the overall robustness in the capabilities. Early notification and authorized user's ability to access real-time data successes suggest they should be included as smart practices.

D. SUMMARY

The case study provides scientific evidence that reduction in vehicle vulnerability is possible through the implementation of security technologies, especially when they are fused together and work as a whole security system, including: vehicle disabling/interruption device (Tier I), require driver ID/password/biometrics (Tier II) and utilize telematics/geofencing/PSRC (Tier III). Panic alert (Tier I), driver ID (Tier II), remote vehicle disabling (Tier II) combined with telematics (Tier III) provide a significant 33 percent average decrease in vulnerabilities across all load types. This is the highest reported reduction in vehicle security vulnerability.

Wireless communication and GPS integration are required for Tier III technologies to perform adequately. Additionally, continuous connectivity to system components is necessary for real-time information sharing between system components and end-user. Although some systems allow "requests" for information feedback, more continuous coverage systems optimize the overall benefits associated with tracking vehicles. The time between data exchanges could reflect a time period where immediate notification is not made if the vehicle is being misused or was stolen. Wireless technology is changing rapidly and can enhance core missions while innovation is bringing new functionality and features.[155] Increasingly powerful data networks and mobile devices are fusing with creative software to better optimize fleets. Technologies are becoming more affordable, easier to use, and quicker to deploy.[156] Three

[154] Ibid., 34.

[155] Frost and Sullivan, *Using Wireless Technology to Manage and Optimize Government Fleets* (Mountain View, CA: Frost & Sullivan, 2011).

[156] Ibid., 3.

components combined: interconnectivity solutions, mobile devices and mobile data networks can provide vehicle locations, driver performance, and compliance tracking and analysis.[157]

Machine-to-machine (M2M, V2I, V2V) refers to digital wireless communication between an endpoint and a back end system that is initiated with or without human intervention.[158] High potential users for M2M solutions are public safety vehicles: police cars, fire engines, and ambulances.[159] Capabilities include:

- Vehicle location—Utilization of GPS and Geofencing to determine a virtual geographical area for alert notification if vehicles travel outside designated zones.
- Vehicle diagnostics—General preventative maintenance oversight for real time vehicle diagnostics to include fuel consumption, tire pressures, RPM's, speeding, and a wide range of other information.
- Driver Performance—hard braking and acceleration, swerving. Not necessarily good for public safety.
- Compliance tracking and analysis—Hours of service.

The potential for enhancing public safety vehicle security through connected technologies is real, and it is a vital link to an overall security strategy. The research information regarding the importance of vehicle connectivity is clearly stated. Both private and public entities recognize the emerging trend of vehicle connectivity.

[157] Ibid., 4–5.

[158] Ibid., 4.

[159] Ibid., 2.

VI. TIER IV—HUMAN-MACHINE INTERFACE CONSIDERATIONS

The human-machine interface plays a vital role in the success of a technology. Security and convenience regarding the human-machine interface need to be considered when implementing technologies that could critically impact job performance. This chapter will discuss several concepts of human machine interface. First, the study of disruptive and incremental design theories will bring light to the situation and offer a better understanding how to alleviate disruption to work processes by new technology. Secondly, two case studies will be presented on the study of anthropometrics. This study provides specific end-user information for use in the design of tools and technologies in the performance of the end-user's job performances. The first study is on law enforcement officers and cab design and the second involves research currently underway on firefighters and cab design.

A. DISRUPTIVE (RADICAL) AND INCREMENTAL DESIGN

Design innovation can be categorized into three spaces: inspiration, ideation and implementation. Inspiration brings to light the problem or underlying motivating factor. Ideation looks to make change through testing of ideas. Finally, implementation provides a framework for bringing innovation to reality. These categories are not linear, and they allow designers to jump from one to another in a nonlinear way.[160] Change by design can be disruptive to end users. Human-centered designers collect data in many ways, including ethnographic (critically important in public safety), job analysis and human culture research. Adversely, design driven by research can be extremely disruptive or radical to work processes.[161] Where machine and human interaction is still needed, it is absolutely necessary both know what they are doing or want to do. [162] Design implementation must consider the human psychological factors when implementing

[160] Brown, *Change by Design*, 16.

[161] Norman and Verganti, "Incremental and Radical Innovation," 29.

[162] Donald A. Norman, *The Design of Future Things: Author of the Design of Everyday Things,* (New York: Basic Books, 2007), 4–5.

design. Support of a product will go down until enlightenment takes place allowing for confidence to increase.[163] Contrary, revolutionary products often do not look for the input from end users. In some cases, this can be very successful and provide technological epiphanies, as seen in Figure 2. The challenge comes when the revolutionary idea is so radical that it misses the mark for the end user. This may not be as negative in the private sector; however, in the public safety sector it can cost lives of citizens as well as the public safety professional.

The following framework (Figure 2) looks at the relationship between two dimensions of change (technology and meaning), defining four types of innovation: technology-push, meaning-driven, technology epiphanies, and market pull. These are further defined and discussed below with public safety examples.[164]

- Technology push innovation comes when the change did not come from the users. Firefighting synthetic foam is a good example where the technology has pushed change.
- Meaning-driven innovation is driven by socio-cultural models with radically new results and meaning. The fire service is the implantation of emergency medical services—paramedicine. In law enforcement the implementation field forces changed the way large crowds could successful be controlled.
- Technology epiphanies bring radical change in the way of emerging technologies or use of existing technologies in a new application. Two examples would be the thermal imaging camera for firefighters and the Taser gun for police officers. Both of these technologies changed the way the end user performed a task in a positive way.
- Market pull innovation develops products to meet user needs. For example, firefighter needs drove the advances in the self-contained breathing apparatus (SCBA) and the bulletproof vest with the law enforcement officer.

[163] Brown, *Change by Design*, 65.

[164] Norman and Verganti, "Incremental and Radical Innovation."

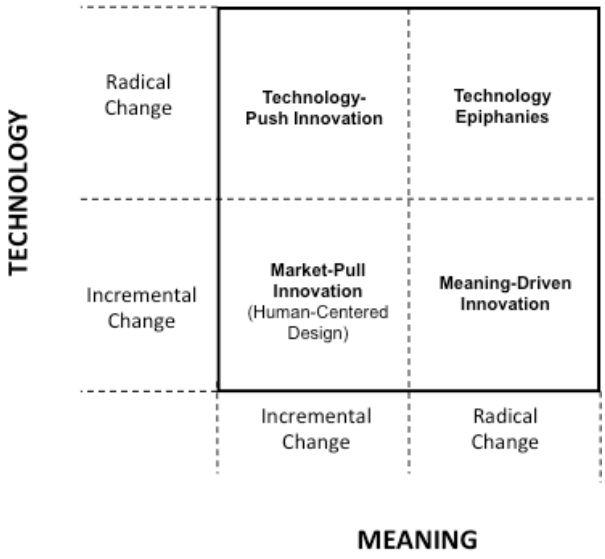


Figure 2. The Two Dimensions and Four Types of Innovation

It is important to understand that there is natural progression from radical to incremental design changes. No matter how radical a product is when it hits the market, it will go through various incremental changes based on end-user satisfaction or it will not be on the market for long and/or not reach expected potential. The thermal imaging camera provides a good example where a radical epiphany was not readily adopted by firefighters. The firefighters often left the very heavy and undependable technology (the camera) on the truck. Over the years, incremental change took place transforming the latest cameras into a lightweight, dependable and lifesaving piece of equipment depended on by firefighters. One area of research that appears to be emerging again in public safety is in the study of anthropometrics.

Tier I and Tier II technologies provided several instances where the technology hampered the end user ability to perform takes proficiently. Consequently, operators often made the security technology useless, frequently choosing secondary systems or bypassing the entire security technology all together. For example, BREW phone technology failed to consider operator features and job performance requirements during the design and implementation phases of the study.[165] Inconveniences experienced in the

[165] Science Applications International Corporation, *Hazardous Materials Safety and Security, vol II,* 27.

real-world environment resulted in the unsuccessful implementation of security system.[166] Feedback and concerns on the mobile device included the need for larger buttons, larger display, and easier navigation menu.[167] Similarly, biometrics technology presented significant challenges for the operators when scanning their fingerprint.[168] The field study mimics research on single biometric technology data being impacted by many variables such as skin thickness and temperature. Additionally, the design and location of the capture/sending unit needs further examination and design. Vehicle operator proficiency must not be negatively impacted by vehicle security technologies.[169]

The next area of will focus on anthropometrics and how design implementation and end-user conveniences coincide with overall proficiency of the end user. Anthropometrics is not a new area of study, the study of body size dates back to 3500 BCE in Sumer.[170]

B. ANTHROPOMETRIC STUDIES

Anthropometrics provides data on end users to be utilized in the design of a product before implementation. There are several recent studies involving anthropometrics as it relates to public safety vehicles. Cab design of public safety vehicles is an important element in the ability for personnel to perform assigned duties and security technologies are located. This includes performing duties under stress and exposure to movements that can be detrimental over time.[171] Additionally, the technology can be disruptive, such as lack of ergonomic considerations or long authentication processing times, simply due to location or lack of convenience for the end user. One report on Dutch police cars provided findings that dramatically showed the

[166] Ibid., 27.

[167] Ibid.

[168] Ibid., 29.

[169] Federal Motor Carrier Safety Administration, *Vehicle Immobilization Technologies*, 95.

[170] *Merriam-Webster Online*, s.v. "Anthropometry," accessed October 22, 2013, http://www.merriam-webster.com/dictionary/anthropometry.

[171] McKinnon, Callaghan, and Dickerson, "Field Quantification," 61.

current cars were not large enough for the current police officers.[172] Several observations provided a real-world look at the problems including: seatbelt, confined weapon, entry and egress space limitations, and steering, pedal and head clearances were inadequate.[173] The need for understanding anthropometrics prior to implementation of technologies involved in security is emphasized in the following studies.

1. Police Officer Performance During Vehicle Operations

This *Field Quantification of Physical Exposure of Police Officers in Vehicle Operation* provides insight of the activities of law enforcement officers within their vehicles.[174] The addition of technologies such as mobile data terminals (MDTs) impacts the operation of police vehicles and the various tasks performed by officers in the execution of their duties. Researchers observed the daily activities of officers performing routine duties.[175] The report can be summarized with the following findings:[176]

- Advances in technologies are changing the workspace within the vehicle
- Injuries associated with prolonged occupational driving, such as lower back, shoulder, hand and wrist problems, are being reported by mobile officers
- Technologies such as MDTs are affecting the operator-machine communication.
- Limited adjustments of vehicle components (e.g., steering wheel and rear protective cage), in addition to items worn as part of the required uniform (e.g., gun, belt, handcuffs, inhibit officer maneuverability within the cab).
- Finding possible solutions by offering adjustable locations and user preferences may reduce injury. Safety and efficiency must maintain priority status.
- Many performance tasks lack procedures or guidelines so there individual interaction with the technologies may vary greatly.

The *Field Quantification of Physical Exposure of Police Officers in Vehicle Operation* study provides real scientific data regarding technology implementations that

[172] Molenbroek, *Anthropometry*, 1–27.

[173] Ibid., 9–15.

[174] McKinnon, Callaghan, and Dickerson, "Field Quantification," 61.

[175] Ibid., 62.

[176] Ibid., 61–67.

could cause harm to the operator from lack of ergonomic consideration or impacts to the proficiency and effectiveness of task performance.[177] For example, use of the MDT by the operator while driving occurs is the most frequently observed task the officer completes while inside the vehicle.[178] This may provide insight regarding priority of tasks. For instance, if the operator of a 50,000 pound fire truck is sharing time between driving and ensuring security technology is capturing necessary data, the results could be catastrophic. Similarly, if human-machine security technology is not conveniently located, the end-user will adapt to their surroundings and find alternatives.

2. Fire Truck Cab Design

The next study provides insight into the measurements of cab design norms, the lack of information of firefighter anthropometrics and the gap created between the two. The objective of the study *Sizing Firefighters and Fire Apparatus: Safe by Design*[179] is to enhance anthropometric measurement database information by including findings from evaluations of U.S. firefighters. The information will be used to improve apparatus design, revise NFPA 1901 *Standard for Automotive Fire Apparatus,* and improve cab, seat, body restraint, egress and bunker gear design.[180] In addition to scientific research finding through anthropometrics, the report clearly identifies enhancement to apparatus manufacturing will be achieved through collaboration among experts and stakeholders within the industry (e.g., National Fallen Firefighters Foundation [NFFF], International Association of Fire Chiefs [IAFC], International Association of Fire Fighters [IAFF], National Fire Protection Association [NFPA], and Fire Apparatus Manufacturers' Association [FAMA]).[181] The report's expected findings will provide support:[182]

- Determine what firefighter measurements are critical in design of identified areas listed above based on expert consensus.

---

[177] Ibid., 64–67.

[178] Ibid.

[179] Hsiao, *Sizing Firefighters.*

[180] Ibid., 22.

[181] Ibid., 30.

[182] Ibid., 22.

- Enhancements in driver controls and visibility as a result of more accommodating cab design will enhance overall safety of vehicle operation.
- Post-crash survivability will be increased as a result of modified seat configurations.
- Body restraints improved to enhance post-crash survivability.
- Improved entry and egress into the cab.
- Bunker gear sizing enhancements to reduce occupational risk from failure to don gear or poor sizing.

Human-machine communication challenges have contributed to injuries in vehicle incidents, including fatalities.[183] Consequences from failing to consider the link between human and machine when implementing new public safety vehicle security technologies may prove as critical. The need for understanding the end user and job performance is clear. The study expects anthropometric data will provide dimensions for 95 percent of the U.S. firefighter population.[184] Firefighter measurements combined with job performances within fire truck cabs will provide results capable of filling gaps in design standardization:[185]

- NFPA 1901 does not provide specification for leg room within the cab.
- Four point and five point seatbelt design requirements.
- Society of Automotive Engineers (SAE) standards are being used for fire truck cab design in the areas of head room, driver-eye position, driver-selected seat positioning due to lack of these standards within NFPA 1901.
- Shin-knee and stomach positioning for steering wheel operation are not currently addressed in NFPA 1901. SAE standards are not representative of 95 percent of the firefighter population.

C. SUMMARY

This study, *Sizing Firefighters and Fire Apparatus: Safe by Design*,[186] is on the forefront of U.S. firefighter research and provides research to support the need for human-machine communication understanding. Furthermore, anthropometrics offer

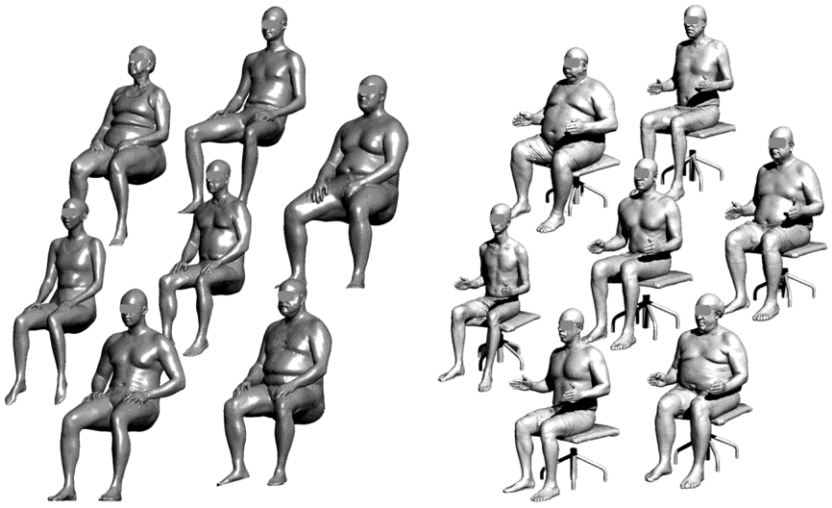
[183] Ibid., 25.

[184] Ibid., 41.

[185] Ibid., 33.

[186] Ibid.

designers real data for end user specifications for enhancing safety. Technologies implemented to enhance security should once again ensure safety and proficiency of the firefighter and remain priority. Incidents and injuries during apparatus use are already on the rise. For example, in 2010 there were 14,200 incidents reported while fire apparatus were responding to alarms or returning to quarters resulting in 775 injuries. In 2011, they were up to 14,850 incidents, resulting in 970 firefighter injuries.[187] A poorly designed cab interface can make firefighter fatigue more severe and negatively impact their health.[188] Fatigue may also contribute to incidents and injuries during apparatus operation. Digital models can be useful in cab design and help avoid further negative impacts. Several models, including 3D, are becoming available for populations such as farm workers, truck drivers, military personnel, and general civilians (see Figure 3).[189]



(a) (b)

Figure 3. Digital Models of (a) Farm Workers and (b) Truck Drivers are Becoming Available, Which Can Be Incorporated into Commercial Digital Human Software to Assess the Safety and Effectiveness of Products and Workspaces.

[187] Michael J. Karter and Joseph L. Molis, "US Firefighter Injuries—2011," National Fire Protection Association, accessed October 22, 2013, http://www.nfpa.org/~/media/Files/Research/NFPA%20reports/Fire%20service%20statistics/osffinjuries.pdf, 12.

[188] Hsiao, "Anthropometric Procedures," 6–35.

[189] Ibid., 32.

VII. FINDINGS/RECOMMENDATIONS/CONCLUSIONS

A. FINDINGS

The threat of public safety vehicles used by criminals or terrorists to commit violent acts is clearly stated and supported with research findings.[190] The use of public safety vehicle security technologies offers some hope in reducing vulnerabilities making them less prone to criminal activities and instruments in executing violent acts. Preventing criminal activity or terrorist acts will directly benefit the public's safety and agency financial liabilities. Those liabilities include significant injury and loss of human life, as well as, financial liabilities in the form of lost equipment, damage to property and lawsuit settlements respectively by reducing the vulnerabilities of public safety vehicles associated with theft, unauthorized use, and lack of tracking and recovery capabilities. Vehicle security technologies have proven to:

- Offer solutions to mitigate criminal and terrorist misuse of public safety vehicles.
- Reduce vulnerabilities, identified in overall average percentage reduction, associated with theft prevention, protect against misuse and lack of tracking or recovery means of public safety vehicles.

The identified technologies and associated vulnerability reductions resulted from real world testing of the security of high-risk vehicles as part of the *Hazardous Materials Safety and Security Field Operational Test*[191] utilized as the case study for this thesis.

The *Hazardous Material Safety and Security Field Operational Test*[192] conducted by U.S. Department of Transportation's Federal Motor Carrier Safety Administration (FMCSA) partnered with the U.S. Department of Transportation (DOT's) Intelligent Transportation System Joint Program Office (JPO) offered real-world knowledge and

---

[190] Moton, "Stolen Ambulance Joyride Caught on Tape;" "Catastrophic Ambulance Collision Lawsuit Settles for $12.5 Million," *PRNewswired*, accessed January 30, 2013, http://www.prnewswire.com/news-releases/catastrophic-ambulance-collision-lawsuit-settles-for-125-million-75481272.html.

Knickmeyer, "New Tactic seen in Attack on Marine Base;" Ghazi, "Dozens Die in Attack on Police in Iraqi City,"

[191] Science Applications International Corporation, *Hazardous Materials Safety and Security, vol II*.

[192] Ibid.

scientific data supporting vehicle security technologies and the ability to categorize them based on capability. A list of technologies, utilized in the hazardous material field operation test, and related cost can be found within the Technology Compendium at http://www.fmcsa.dot.gov/safety-security/hazmat/fot/safehazmat/tech-compendium.htm. These technologies were placed in tiers from low end of 1 (cost of implementation around $250 per vehicle to the high end 6 (cost estimated at $3500 per vehicle).[193]

Dependability of one technology on another is a significant factor on moving the project from theory to practice. The fusion of technologies is being examined and resulting in as many as three technologies working harmoniously. Products fusion is a variety of technologies that provide several solutions in one package.[194] Technologies should be able to collaborate and expand to provide the best possible solutions across the "gaps." These technologies reach far beyond the vehicle itself and will require significant infrastructure and private/public partnerships to be reinforce those that are already in place and explore of new ones. Costs could have a fiscal impact on the sale of commercial vehicles. With this is mind, commercial vehicle manufactures are sure to be against such regulation unless driven by the consumer. Competitive markets are driven by supply and demand.

The current practice for securing, tracking, and automation of alert notifications in the event an emergency vehicle was being misused is not standardized or institutionalized within the public safety discipline. Public safety agencies should work towards standardized alert messages and protocols for response in the case of automatic generation from on-board and wireless systems for geofencing notifications, emergency alert activation, error codes, and pins. Identification of key stakeholders and types of notifications to be put in place. These notification include automatic text, emails, faxes, phone messages etc. This should also include alert levels for seriousness of infraction. Key information on alerts should be consistent and agreeable among response agencies.

---

[193] Ibid.

[194] Hartmut Esslinger, *A Fine Line: How Design Strategies are Shaping the Future of Business* (Hoboken, NJ: John Wiley & Sons, 2009). 113.

The implementation of technologies with public safety vehicles as it relates to this paper resides within the mobile data terminal utilized by many agencies to interact with computer aided dispatch technologies. This infrastructure as well as cellular service providers may be leveraged to implement any national strategy. Additionally, there appears to be much work already in place regarding vehicle-to-vehicle (V2V), vehicle to infrastructure (V2I) and machine-to-machine (M2M utilizes mobile phones). A comparative study of the entire world *International Survey of Best Practices in Connecting and Automated Vehicle Technology, 2013 update* was completed by the Michigan Department of Transportation and Center for Automotive Research (CAR).[195] This technology identifies the infrastructure in place, under testing, and in strategic planning. The research is driving the researcher to believe this technology and the like will be the backbone of all technological vehicle systems connectivity in the future. With increased vehicle connectivity comes the risk of potential cyber-attack. University researchers are already successful in hacking into a car's electronic systems. Cars are predicted to utilize hundreds of millions of software code in the near future. Planning must take place to prevent such incidents in the area of public safety vehicles.[196]

It is important, as implementation occurs, to discuss and explain public safety security technology such benefits and gain insight from end users.[197] If a technology negatively impacts one while enhancing another the overall reaction is expected to be negative and may result in the primary technology being bypassed or use of back up devices when possible. The operator must not be impeded by the implementation of the security technology such as Tier I Theft Prevention and Tier II—Authorized Use that requires human-machine interaction.[198] Override and backup systems could pose a weakness for robust technologies. Redundancy will need to be built into any public safety vehicle security system. Design theory applied to engineering technologies offered insight in identifying smart practices when executing implementation strategies. In

[195] Michigan Department of Transportation and Center for Automotive Research, *International Survey of Best Practices*, 1.

[196] Stuart McClure, "Caution: Malware Ahead," *Vision Zero International* (2013), 35.

[197] Norman, *The Design of Future Things*, 6.

[198] Federal Motor Carrier Safety Administration, *Vehicle Immobilization Technologies*, 95.

addition, anthropometrics is offering some of the latest information on the end-user-machine interface in police and fire disciplines among other industries. *The study of design innovation and anthropometrics provides scientific insight and support of the importance of considering end user needs when implementing successful implementation strategies involving public safety security technologies.*

There is natural progression from radical to incremental change. Successful implementation strategies often provide end users with the opportunity to become part of the design and implementation process. More specifically, when end users find the technology disruptive, they will find a path of least resistance, when available, in overcoming the inconvenience. Alternatives by end users to the primary security measure may prove the weakest link of system and deem the system less effective. Finally, if the end user cannot operate a device, such as a push button, because it is to small for the intended end users, the system is proven so disruptive it may need to be removed until further incremental change occurs where end-user measurements are taken into consideration as seen in the study of anthropometrics.

B. LIMITATIONS

The author experienced two specific limitations found during the research process in addition to those identified in second paragraph of the literature review. The first was limited field studies associated with vehicle security technologies. Fortunately, the case study presented was truly an extensive research product with scientific methods, data, and real-world application. Additionally, the case study is used by many other research articles and experiments as a springboard in outlining vehicle security technologies. The second limitation was the lack of public safety information regarding anthropometrics. Much of this data is found as part of law enforcement investigation practices regarding criminal identification and often side tracked the author's research. Anthropometrics data and studies directly involving public safety personnel are currently underway. Recent studies, along with these future findings, are providing an emerging trend that end user

measurements and human-machine interface considerations are critical in avoiding disruptive technological implementation that impacts job performance that could affect the public's safety.

Further research is needed in the area of vulnerabilities associated with cloned and repurposed vehicles. Extremists have used these vehicles in attempts to inflict harm to lives and property in the U.S.[199] Action is needed to regulate and track repurposed vehicles to ensure they do not become a viable option to frontline vehicles that implemented the vehicle security technologies as part of the recommendation of this thesis. Perhaps best practices in other related areas can offer a solution, such as the security regulation of the sale and possession of ammonium nitrate. Establishing registration procedures, including screening purchasers and sellers against the terrorism screening database, as seen in security of ammonium nitrate may offer viable solutions.

C. CONCLUSION

Public safety vehicle vulnerability reduction is clearly shown through the case study and research to be enhanced with the fusion of technologies both intra-tier and inter-tier. Figure 4 shows reduction in vulnerability average percentages across all load types for all tested technologies.[200] All percentages, except that reported on wireless communications (far left category), are based on the specific technology/technologies listed fused with telematics (wireless communications combined with GPS).[201] Vulnerability reduction percentage increases are seen as technology fusion occurs within and across Tier I, Tier II, and Tier III technologies.

[199] Ludwig, "EMS: Stolen Ambulance."

[200] Science Applications International Corporation, *Hazardous Materials Safety and Security, vol II*, 57.

[201] Ibid., 57.

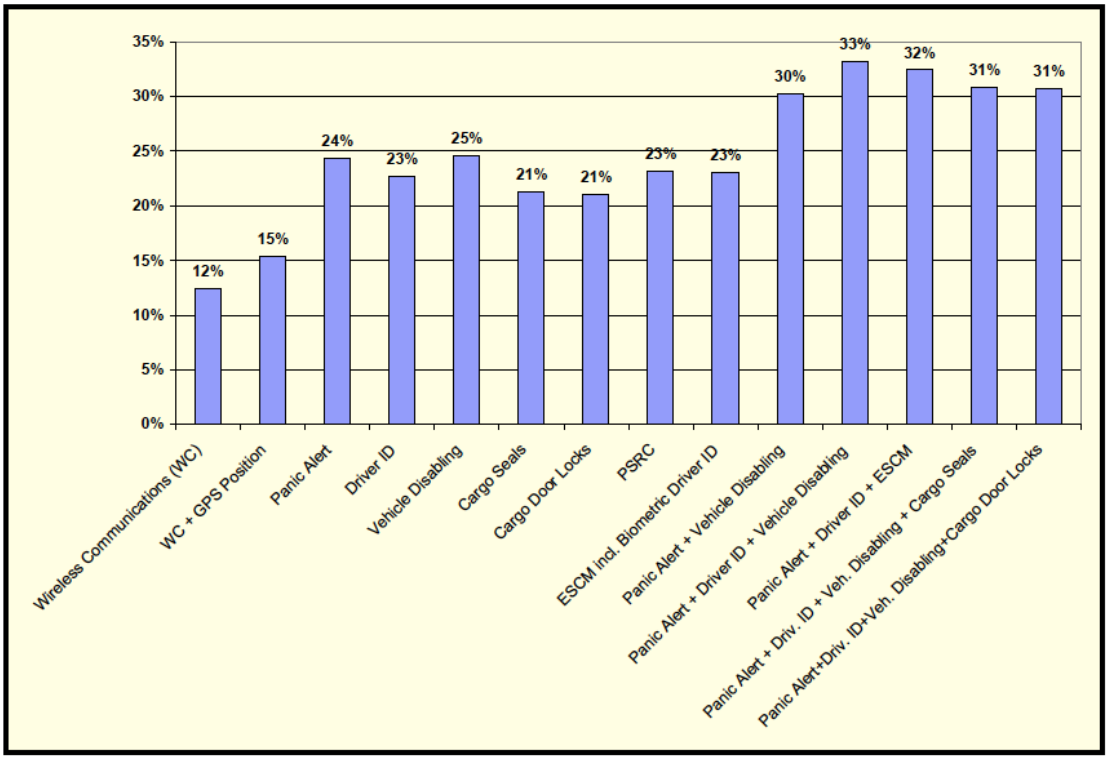


Figure 6-2. Average Percent Reduction in Overall Risk Across Load Types by Technology Combination.

Figure 4. Average Percent Reduction in Overall Risk Across Load Types by Technology Combination

Lastly, anthropometrics offers a scientific approach to design as it applies to the end users as seen in the case study. Studies have shown benefits come to 95 percent of the end users by taking into account the job task, equipment use, and individual variances as it relates to a specific discipline or group of personnel. Although cross section with other industry is useful in understanding the concept of anthropometrics, the diversity from one industry to another may not be an accurate representation to build models upon. The use of 3D modeling is bringing enhancements to anthropometrics and is becoming increasing used in design.

D. EFFECTIVE STEPS IN VULNERABILITY REDUCTION RESULTING IN A MODEL FOR PUBLIC SAFETY USE

Technologies outlined in the case study were used as primary data when developing Tier I–IV categories and sub categories. Knowledge gained from industry

reports supplemented the case study, knowledge such as common sense measures, are not found in the findings of the case study; however, these are described as the simplest and most cost effective way to secure a vehicle by law enforcement agencies and insurance leaders alike.[202] Tier I–IV categories were determined by two criteria: common capabilities based on a specific risk reduction measure and identified end-user impacts resulting from technological interface. First, capabilities based-on best practices were reviewed across all discovered technologies. Three categories quickly emerged: Tier I—Theft Prevention, Tier II—Authorized Use and Tier III—Tracking and Recovery. The tiers can work independently or for maximum vulnerability reduction results, fusion of technologies is desired. In addition to common capabilities within Tier I-III, these categories and subcategories arranged to build a progressive model of implementation for public safety agencies. For instance, a public safety agency should not implement a telematics technology on a vehicle when no theft prevention measures or work practices are in place. Even with Tier III technology implementation, the vehicle remains highly vulnerable without Tier I technology. Additionally, recognizing the current economic times and understanding both local budgetary processes and those associated with state and federal grants, the author developed the model to allow an agency the ability to differ costs of full implementation over time.

Finally, Tier IV—Human Machine Interface provided significant insight in understanding how technologies can disrupt work practices and/or end users and render security technologies useless. The need for end-user examination within the public safety vehicle security process is vital to successful implementation. Continuous end-user consideration during the design phase and feedback after implementation will allow for enhanced performance and overall acceptance of public safety vehicle security technologies.

[202] Scafidi, "Hot Wheels 2012;" "District of Columbia Metropolitan Police Department, "Auto Theft Prevention."

E. SOLUTION

1. Securing Emergency Response Vehicles with Engineering Model a Vehicle Technology Model for Public Safety Use

The securing emergency response vehicles with engineering (SERVE)[203] model was developed by the author and provides a framework for implementing public safety vehicle security enhancements taking the complex interaction between technological fusion, vehicle system integration and end user interface design into account. Although specific interest in developing the model applies to the securing emergency vehicles, the model may prove useful to other industries as well. Figure 5 provides a schematic representation of the complex interaction described above. The three tiers of technology implementation and one tier of human-machine interface considerations are:

a. Tier I—Theft Prevention

These devices interrupt on board mechanical and electronic systems (e.g., parking brake (air or electronic), electronic ignition and power to starter). The devices do not require user specific information. These devices do include common sense measures, interruption technologies, and authentication technologies. Examples of these include: taking keys out of the ignition, locking doors, push button activation (panic button), key fob, and smart keys. Although these simple steps may prevent successful action on the part of a thief, applying practices such as removing keys may impact job performance within the public safety community. The importance of user-specific information (password/PIN) and characteristics (biometrics) provided by the authorized operator are discussed in Tier II technologies.

b. Tier II—Authorized User

This category includes devices in Tier I with the addition of user-specific information or requirements. These devices employ the help of on-board computer (sometimes external computers) to validate user information. Some examples include: user specific smart cards, PINs or biometric and password. FPGA technology is

[203] The SERVE model was built by author based on research findings.

implemented to ensure authorized changes can occur quickly in the event user privileges are revoked. Tier II authorized user technology systems may offer safety enhancements related to human error, such as forgetting to set a brake, in addition to security benefits. Additionally, technologies in this category might require a backup or secondary system in case of a primary system failure. The secondary system should provide an opportunity for enhancement without creating a gap in the overall system security. Simply put, if the backup system is to easily used or identified, it can exploit the primary system. Encryption of internal and external communications will reduce vulnerability to system components.

c. Tier III—Tracking and Recovery

This category includes Tier I and Tier II devices. This technology allows on-board systems to communicate with external authorized end users. Information regarding on-board systems, location, vehicle speed, and location are reported to data warehousing. The upper level of Tier III technologies implement protocols and algorithms for identifying patterns of use, on-board system sensors (inventories, vehicle weights, number of personnel on unit), or information gained from V2Connected world via infrastructure, satellite, mobile devices, and other vehicles that indicates wrongful user and/or unauthorized use. Real-time information is enhanced and provides greater need for intelligent systems to deceiver the big data. Big data will require protocols and algorithms to be built by the agency by after exploring internal needs and business models (e.g., mutual aid, automatic aid, response zone) to ensure the intelligent software performs as expected.

d. Tier IV—Human-Machine Interface Considerations

Anthropometric and design theories must be considered to ensure smart practices are identified and disruptive technologies do not impact job performances involved in public safety. The Human-Machine Interface is warranted across Tier I, Tier

II, and Tier III technologies. Specifically, the implementation of authentication technologies cannot interfere with operator job performance proficiency.[204]

[204] Federal Motor Carrier Safety Administration, *Vehicle Immobilization Technologies*, 95.

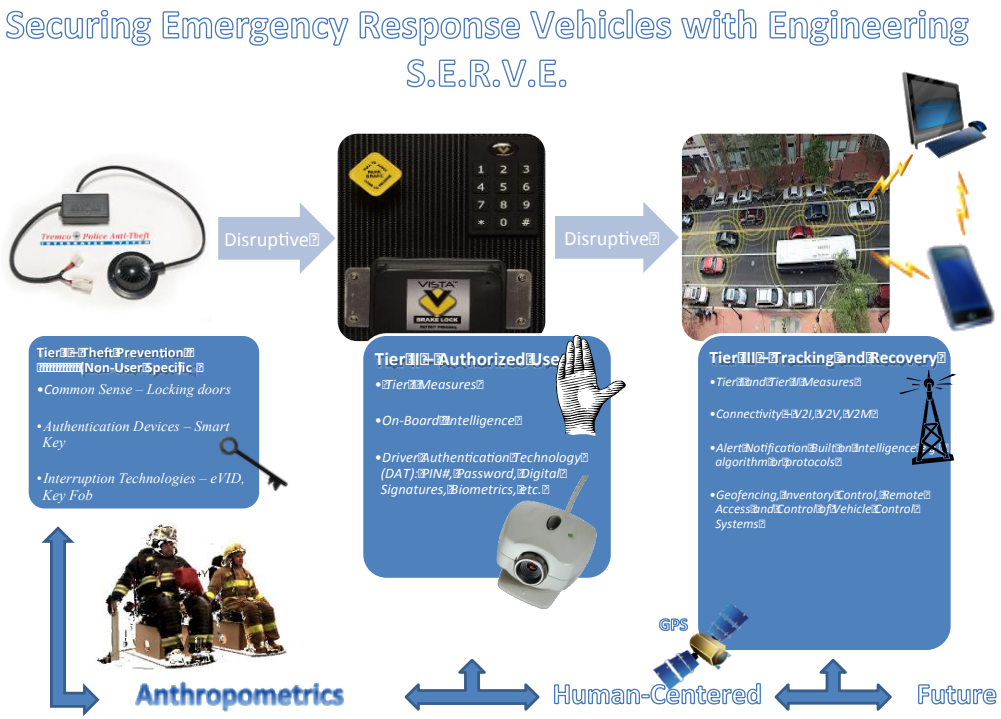


Figure 5. Securing Emergency Response Vehicles with Engineering

This thesis was successful in identifying vehicle security technologies and best practices for implementation strategies to reduce impacts on vehicle operators through the use of design and anthropometrics. The author as part of the analysis of research findings developed the Securing Emergency Response Vehicles through Engineering (SERVE) model. This model can be used to help public safety agency decision makers by offering a basic understanding of technologies tiers and ability to implement based on fiscal budgets. Additionally, the model provides a clear understanding that each tier can offer challenges to operators in the way of disruptive technology implementation but that those challenges can be minimized by including end users early in the decision-making process as well as including scientific data found in anthropometrics for discipline (LEA, medical, fire) specific performance.

LIST OF REFERENCES

Brown, Tim. *Change by Design*. New York: HarperCollins, 2009.

Boy, Guy A. *The Handbook of Human-Machine Interaction: A Human-Centered Design Approach*. United Kingdom: Ashgate, 2011.

Central Florida Intelligence Exchange. *Nationwide Analysis—Increased Trend of Unoccupied Ambulance Thefts*. Orlando, FL: Central Florida Intelligence Exchange, 2012. Document is (FOUO).

Colsky, Andrew E. "Public/Private Partnerships with Hazardous Material Motor Carriers Creating Incentives to Increase Security through Assessed Risk (STAR)." Master's thesis, Naval Postgraduate School, 2008.

Cyr, Erek. *The Road Map to Cloned Vehicles*. Tallahassee, FL: Florida Department of Law Enforcement, 2008. Document is (FOUO).

Dardanelli, A., F. Maggi, M. Tanelli, S. Zanero, S. M. Savaresi, R. Kochanek, and T. Holz. "A Security Layer for Smartphone-to-Vehicle Communication Over Bluetooth." *IEEE Embedded Systems Letters* 5, no. 3 (2005).

Deccan International. "Deccan." Accessed August 18, 2013. http://www.deccanintl.com/.

Department of Homeland Security and Department of Justice Federal Bureau of Investigation. *Potential Terrorist use of Public Safety or Service Industry Uniforms, Identification or Vehicles*. Washington, DC: Department of Homeland Security and Department of Justice Federal Bureau of Investigation, 2004. Document is (FOUO).

———. *Terrorist Threats to the US Homeland Reporting Guide*. Washington, DC: Federal Bureau of Investigations and Department of Homeland Security, 2004. Document is (FOUO).

"DHS-FBI Terrorist Tradecraft: Impersonation: Use of Stolen, Cloned, or Repurposed Vehicles." January 18, 2013. Public Intelligence. http://publicintelligence.net/dhs-fbi-cloned-vehicles/. Document is (FOUO).

District of Columbia Metropolitan Police Department. "Auto Theft Prevention." Accessed October 14, 2013. http://mpdc.dc.gov/page/auto-theft-prevention.

Donahue, Patrick. "Stolen Fire Truck Kills Man, Crashes." *Post and Courier*. February 25, 2012. Accessed October 10, 2013. http://www.postandcourier.com/article/20120225/PC1602/302259977.

"FedEx Freight Adds Technology." *Traffic World* 270, no. 20 (2006): 24–26.

Federal Bureau of Investigations. "Terror Hits Home: The Oklahoma City Bombing." Federal Bureau of Investigations. Accessed October 14, 2013. http://www.fbi.gov/about-us/history/famous-cases/oklahoma-city-bombing.

Federal Emergency Management Agency. *National Preparedness Goal 2011*. 2011. Accessed October 28, 2013. http://www.fema.gov/media-library-data/20130726-1828-25045-9470/national_preparedness_goal_2011.pdf.

Federal Motor Carrier Safety Administration. "Expanded Satellite Tracking." March 2006. Accessed February 20, 2013. http://www.fmcsa.dot.gov/facts-research/research-technology/report/Mobile-Communications/mobile-communications-tracking-system-requirements.pdf

———. "Hazardous Materials Safety and Security Field Operational Test." Accessed September 30, 2013. http://www.fmcsa.dot.gov/safety-security/hazmat/fot/safehazmat/results-brochure.htm.

———. "Untethered Tracking and Control Systems." December 2005. Accessed February 20, 2013. http://www.fmcsa.dot.gov/facts-research/research-technology/report/untethered-dec05/untethered-dec05.pdf.

———. *Vehicle Immobilization Technologies: Best Practices for Industry and Law Enforcement Final Report*. 2007. Accessed November 20, 2013. http://www.fmcsa.dot.gov/facts-research/research-technology/report/vit-best-practices-law-enforcement-nov2007.pdf.

Frost & Sullivan. *Using Wireless Technology to Manage and Optimize Government Fleets*. Mountain View, CA: Frost & Sullivan, 2011.

Ghazi, Yasir. "Dozens Die in Attack on Police in Iraqi City." *New York Times*. Accessed October 22, 2013. http://www.nytimes.com/2013/02/04/world/middleeast/suicide-attack-kills-dozens-in-northern-iraq.html?_r=0.

Hall, Sam. "What Makes a Police Car Cost $120,000?" January 28, 2013. Accessed October 28, 2013. http://news.drive.com.au/drive/motor-news/what-makes-a-police-car-cost-120000-20130128-2dgcd.html.

"The High Cost of Losing Your Keys: Key Technology has Advanced and so has Replacement Cost." Edmunds. Accessed October 28, 2013. http://www.edmunds.com/car-care/the-high-cost-of-losing-your-keys.html.

Homeland Threats and Agency Response, Hearing before Committee on Homeland Security and Government Affairs United States Senate. 112th Cong. (2012). Government Printing Office. Accessed January 30, 2013.

http://www.gpo.gov/fdsys/pkg/CHRG-112shrg76070/html/CHRG-112shrg76070.htm.

Hsiao, Hongwei. "Anthropometric Procedures for Protective Equipment Sizing and Design." *Human Factors: The Journal of the Human Factors and Ergonomics Society* 55, no. 1 (2013): 6–35.

———. *Sizing Firefighters and Fire Apparatus: Safe by Design*. Center for Disease Control and Prevention. Accessed October 14, 2013. http://www.cdc.gov/niosh/topics/anthropometry/pdfs/Sizing%20firefighters%20proposal%20core%20part.pdf.

Hughes, Ron, Steven Keppler, Skip Yeakal, Conal Deedy, Tom Moses, and Charlie Carden. *The Context for Commercial Vehicle Enforcement Activity 2020: Forecast of Future Directions in Truck Safety and Security*. Washington, DC: Transportation Research Board, 2005.

Indiana Intelligence Fusion Center. *Suspicious Activity Involving Emergency Services and Hospitals*. Indianapolis, IN: Indiana Intelligence Fusion Center, Indiana Department of Homeland Security, 2008. Document is (FOUO).

Karter, Michael J. and Joseph L. Molis. "U.S. Firefighter Injuries—2011." National Fire Protection Association. Accessed October 22, 2013. http://www.nfpa.org/~/media/Files/Research/NFPA%20reports/Fire%20service%20statistics/osffinjuries.pdf.

Kimery, Anthony L. "'Cloned' Vehicles Continue to be Security Problem." *HS Today*. December 11, 2008. Accessed October 14, 2013. http://www.hstoday.us/blogs/the-kimery-report/blog/cloned-vehicles-continue-to-be-security-problem/c7f442710dc2fc583590b681f319234e.html.

Knickmeyer, Ellen. "New Tactic Seen in Attack on Marine Base." *Washington Post*. April 12, 2005

Kroschel, Matt, Carri Walters, and Laura Christmas. "Update: Woman Charged Following Incident Involving Stolen Police Car in Fayetteville." *WHNT 19 News*. August 31, 2013. Accessed October 14, 2013. http://whnt.com/2013/08/31/breaking-stolen-police-car-involved-in-deadly-wreck-in-fayetteville/.

Ludwig, Gary. "EMS: Stolen Ambulance." *Firehouse Magazine*. December 3, 2012.

Lucas, Ryan. "Suicide Bomber Driving Ambulance Strikes Police Station in Ramadi, Second Bombing in a Week in Volatile Anbar Province." *America's Intelligence Wire*. February 2007.

Lupu, Eugen, Petre G. Pop, and Marius N. Roman. "A Survey of Multimodal Biometric Systems." *International Journal of Computer Science and Its Applications*. Accessed October 14, 2013. http://www.seekdl.org/nm.php?id=882.

McKinnon, Colin D., Jack P. Callaghan and Clark R. Dickerson. "Field Quantification of Physical Exposures of Police Officers in Vehicle Operation." *International Journal of Occupational Safety and Ergonomics-JOSE* 17, no. 1 (2011): 61.

Merriam-Webster Online. s.v. "Anthropometry." Accessed October 22, 2013. , http://www.merriam-webster.com/dictionary/anthropometry.

Michigan Department of Transportation and Center for Automotive Research. *International Survey of Best Practices in Connected Vehicle and Automated Vehicle Technology*. Ann Arbor, MI: Michigan Department of Transportation and Center for Automotive Research, 2013. Accessed October 14, 2013. http://www.michigan.gov/documents/mdot/09-12-2013_International_Survey_of_Best_Practices_in_ITS_434162_7.pdf.

Molenbroek, Johan F. M. *Anthropometry and Usage Research of Dutch Police Cars*. Netherlands: Delft University of Technology, 2010.

Moton, Kenneth. "Stolen Ambulance Joyride Caught on Tape." *ABC7News Chicago Illinois*. Accessed October 14, 2013. http://abclocal.go.com/wls/story?section=news/national_world&id=8750037.

National Commission on Terrorist Attacks upon the United States. *Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: W. W. Norton, 2004.

National Highway Traffic Safety Administration. *Vehicle Theft Prevention*. Washington, DC: National Highway Traffic Safety Administration, n.d.

Near Field Communication. "About Near Field Communication." Accessed October 18, 2013. http://www.nearfieldcommunication.org/about-nfc.html.

Norman, Donald A. *The Design of Future Things: Author of the Design of Everyday Things*. New York: Basic Books, 2007.

——— and Roberto Verganti. "Incremental and Radical Innovation: Design Research Versus Technology and Meaning Change." March 18, 2012. http://jnd.org/dn.mss/Norman%20%26%20Verganti.%20Design%20Research%20%26%20Innovation-18%20Mar%202012.pdf.

Porter, Ashley. "Man Armed with Potato Steals Ambulance—Weird." *10 News*. Accessed January 30, 2013. http://tarponsprings.wtsp.com/news/weird/115568-man-armed-potato-steals-ambulance.

PRNewswire. "Catastrophic Ambulance Collision Lawsuit Settles for $12.5 Million." Accessed January 30, 2013. http://www.prnewswire.com/news-releases/catastrophic-ambulance-collision-lawsuit-settles-for-125-million-75481272.html.

Rabe, Cynthia Barton. *The Innovation Killer: How What We Know Limits What We Can Imagine-and What Smart Companies Are Doing about It*. New York: Amaco, 2006.

Ramadan, Montaser N., Mohammad A. Al-Khedher and S. Al-Kheder. "Intelligent Anti-Theft and Tracking System for Automobiles." *International Journal of Machine Learning and Computing* 2, no. 1 (2012).

Reeger, Jennifer. "Alert Pa. Officer Recovers Stolen Ambulance." Officer.com. Accessed January 30, 2013. http://www.officer.com/news/10851490/alert-pa-officer-recovers-stolen-ambulance.

Scafidi, Frank. "Hot Wheels 2012." 2013. National Insurance Crime Bureau. https://www.nicb.org/newsroom/news-releases/hot-wheels-2012.

Science Applications International Corporation. *Hazardous Materials Safety and Security Technology Field Operational Test, Volume I: Evaluation Final Report Executive Summary*. 2004. Federal Motor Carrier Safety Administration. Accessed February 20, 2013. http://www.fmcsa.dot.gov/documents/hazmat/fot/FINAL-Volume-I-Executive-Summary-11-10-04.pdf.

———. *Hazardous Materials Safety and Security Technology Field Operational Test Volume II: Evaluation Final Report Synthesis*. Washington, DC: U.S. Department of Transportation, 2004.

Snelick, Robert, Umut Uludag, Alan Mink, Michael Indovina, and Anil Jain. "Large-Scale Evaluation of Multimodal Biometric Authentication using State-of-the-Art Systems." In *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27, no. 3 (2005): 450–455.

Sreekala, P., V. Jose, J. Joseph, and S. Joseph. "The Human Iris Structure and its Application in Security System of Car." In *Engineering Education: Innovative Practices and Future Trends Proceedings*. Kottayam, India, July 2012.

Straw, Joseph. "Tracking Dangerous Cargo." *Security Management* 51, no. 12 (2007): 66–91.

Subramanian, Xinzhou Wu, S., Guha, R., White, R.G., Junyi Li Lu, K.W., Bucceri, A. and Tao Zhang. "Vehicular Communications Using DSRC: Challenges, Enhancements, and Evolution." *IEEE Journal* 31, no. 9 (2005).

Sundari, Y. B. T., G. Laxminarayana, and G. Vijaya Laxmi. "Anti-Theft Mechanism through Face Recognition Using FPGA." *International Journal of Advancements in Research and Technology* 1, no.6, (2012): 46–49.

Tickle, Andrew J. Jiajing Sun, Lu Gan, and Jeremy S. Smith. "Feasibility of an Encryption and Decryption System for Messages and Images using a Field Programmable Gate Array (FPGA) as the Portable Encryption Key Platform." In *Proceedings Optical Design and Engineering III*, 71002N. September 27, 2008. doi:10.1117/12.797732.

Tremco Police Products. "Tremco Police Products." Tremco Police Products. Accessed September 28, 2013. http://www.tremcopoliceproducts.com/.

U.S. Department of Transportation. *Transportation for a New Generation, Strategic Plan, Fiscal Years 2012–2016*. Washington, DC: U.S. Department of Transportation, 2013.

U.S. Government Accounting Office. *Review of Studies of the Economic Impact of September 11, 2001, Terrorist Attacks of the World Trade Centers*. GAO-02-700R. Accessed October 14, 2013. http://www.gao.gov/new.items/d02700r.pdf.

"Vehicle Immobilization System Touch Activated Brake Lock." Vista Brake Lock. Accessed October 18, 2013. http://vistabrakelock.com/.

Violino, Bob. "What is RFID?" *RFID Journal* (January 2005). Accessed October 18, 2013. http://www.rfidjournal.com/articles/view?1339.

Wall Street Journal Online. "How the Benghazi Attacks Unfolded." Accessed October 14, 2013. http://online.wsj.com/news/articles/SB10000872396390444620104578008922056244096.

Williams, D., J. Allen, M. Lepofsky, D. Murray, K. Wahl, D. Vercoe, S. Keppler, and T. Moses. *Hazmat Safety and Security Field Operational Test, Final Report*. 2004. Federal Motor Carrier Safety Administration. Accessed February 20, 2013. http://www.fmcsa.dot.gov/documents/hazmat/fot/HMFOT-Final-Report.pdf

Woodfill, D. S. "Car Theft Decreases in Metro Phoenix." August 25, 2012. Accessed January 30, 2013. http://www.azcentral.com/news/articles/20120810phoenix-car-theft-decrease.html.

"Workplace Safety and Health Topics: Anthropometry." Center for Disease Control and Prevention and National Institute for Occupational Safety and Health. Accessed October 14, 2013. http://www.cdc.gov/niosh/topics/anthropometry/.

Yang, Yun and JinHao Liu. “The Design of Automotive Burglar-Proof Based on Human Face Recognition.” In *Proceedings E-Learning, E-Business, Enterprise Information Systems, and E-Government*. December 2009.

Yuan, Weiqi and Yonghua Tang. “The Driver Authentication Device Based on the Characteristics of Palmprint and Palm Vein.” In *International Conference on Hand-Based Biometrics*. Hong Kong, November 17–18, 2011.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California