Fall 12-1-2019

Managing the Effects of Wireless Sensors on Vehicle Ad Hoc Network (Vanet) Safety

Melvin Hayes
Indiana State University

MANAGING THE EFFECTS OF WIRELESS SENSORS ON VEHICLE AD HOC

NETWORK (VANET) SAFETY

A Dissertation

Presented to

The College of Graduate and Professional Studies

College of Technology

Indiana State University

Terre Haute, Indiana

In Partial Fulfillment

of the Requirements for the Degree

Doctor of Philosophy in Technology Management

---

by

Melvin Hayes

December 2019

Keywords: Technology Management, Intelligent Transportation Systems, Wireless Sensor Networks, IEEE802.11, IEEE1451, 6LoWPAN, Digital Communications Systems, Network Security, VANET, Autonomous Vehicle 5G and Zero Configuration, MultiCast Domain Naming Service (mDNS), XMPP, IoT Harmonization.

VITA

Melvin Hayes

EDUCATION

Doctor of Philosophy in Technology Management – Indiana State University, Terre Haute, IN, August 2010 – present. Dissertation title: "Managing the Effects of Wireless Sensor Networks on Vehicle Ad-Hoc Network Safety.

Master of Science in Electronics and Computer Technology - Indiana State University, Terre Haute, IN, December 2008. Thesis title: "Interference and Security in Wireless Networks."

Bachelor of Arts in Psychology – The University of North Carolina at Charlotte, Charlotte, NC, 2004.

Bachelor of Science in Electrical Engineering Technology - The University of North Carolina at Charlotte, Charlotte, NC, 1994.

Associates in Applied Science in Electronics Engineering Technology – Lenoir Community College, Kinston, NC, 1975.

ACADEMIC EMPLOYMENT

Graduate Teaching Assistant – North Carolina Agricultural and Technical State University, Greensboro, NC, College of Technology, Department of Computer Systems Technology, June 2012 to May 2013. Responsibilities included: assisting my professor with the preparation and presentation of undergraduate courses, supervising laboratory experiments, tutoring, grading, and proctoring examinations.

Instructor – Mechatronics Engineering Technology – Vance Granville Community College, Henderson, NC, January 2019 to present. Responsibilities include: Teaching Electronics and Mechatronics Engineering Technology courses, advising students, conducting assessments and attending staff, department, and college related meetings.

PUBLICATIONS

Hayes, M, Omar, T.; Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), "An IEEE1451.7 Based WSN Design for V2I Localization Services in Smart Cities".; November 2018.

Hayes, M, Omar, T., Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security, "End to End V2I/I2V Secured Communications Platform."; November 2019.

PROFESSIONAL MEMBERSHIP

Member of IEEE – 2008 to present

COMMITTEE MEMBERS

Committee Co-Chair: A. Mehran Shahhosseini, Ph.D.

Professor, Department of Applied Engineering and Technology Management

Indiana State University

Terre Haute, Indiana

Committee Co-Chair: Tamer Omar, PhD

Assistant Professor, Department of Electrical and Computer Engineering

California State Polytechnic University

Pomona, California

Committee Member: Jared Wuerzburger, Ph.D.

Assistant Professor, Department of Electronics and Computer Engineering Technology

Indiana State University

Terre Haute, Indiana

ABSTRACT

This paper proposes to conduct research on the vehicular ad hoc networks (VANET) area of Intelligent Transportation Systems (ITS) with a focus on investigating safety methods that will significantly reduce passenger vehicle collisions which ultimately will help to save lives and reduce property losses. Key areas of this ITS research will include highway infrastructure or wireless sensor networks (WSN) to the cloud (web service) and the cloud (web service) to highway infrastructure or wireless sensor network (WSN). In turn, the cloud (web service) will communicate with passenger vehicles as components of a highway infrastructure (WSN) to vehicle (I2V) systems and a vehicle to highway infrastructure (V2I) systems.

In turn, the cloud (web service) will communicate with passenger vehicles as components of a vehicle to highway infrastructure (V2I) system and a highway infrastructure to vehicle (I2V) system. Active circuit emulation will be used as an analysis tool for this research. The cloud web service in this case, will be a database that will be connected through an IEEE802.11 broadband (Wi-Fi) gateway via a border router or a network capable application processor (NCAP) to hardware and software wireless sensor networks or a simulated wireless network. The highway infrastructure portion of this design will be the IEEE1451 standard-based wireless sensor network called wireless transducer interface modules (WTIM). These WTIMs will be responsible for disseminating information from their multitude of sensors to vehicles and/or to the cloud via NCAP routers.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my sincere gratitude to my advisors and co-chairmen of my dissertation committee; Dr. A. Merhan Shahhosseini and Dr. Tamer Omar for the tireless support of my PhD study and research. Thanks to Drs. Shahhosseini and Omar for their patience, motivation, enthusiasm, and immense knowledge that they shared with me during this research and writing process. These two professors provided me with guidance in all of the aspects of research and writing of this thesis. It has been great to have such a team to advise and mentor me throughout my PhD study. In addition, I would like to thank my third committee member: Dr. Jared Wuersburger for his time and encouragement as well as his feedback to me on this project.

Many sincere thanks also to Dr. Q.A. Zeng for serving as chairperson of my doctoral preliminary committee. Thanks to Dr. Zeng for his early guidance to me in my Digital Communications Systems research and writing and providing me with the opportunity to work with him as a graduate teaching assistant, as well. I would like to thank the other members of my preliminary committee, Dr. Dewayne Brown and Dr. Xiolong Li for their insightful comments and tough questions during the early stage of my doctoral studies.

Dr. Jerry Cockrell was very instrumental in getting focused on my graduate studies as my master's degree adviser and chairperson. I would thank the other member of my master's degree committee, Dr. David Beach and Mr. Kwabena Ekuban, for their advice and support to my graduate work also.

Some of the other undergraduate and graduate support faculty and staff that I would to recognize are: Professor Thomas Owen; Professor W. Scott Terry; Professor Doland Mork; Professor Meg Morgan; Professor Greg Wickliff, Mrs. Ababa Ekuban and Ms. Joanna Hayes.Last, but not least, I would like to recognize and thank my late parents; Mr. Allen Lee Hayes and Mrs. Mary Elizabeth "Channie" Alston Hayes. Thanks to my mother for helping me with my reading and mathematics at an early age and thanks to my father for allowing me to apprentice with him in the carpentry and mechanical trade at an early age.

TABLE OF CONTENTS

COMMITTEE MEMBERS i

ABSTRACT ii

ACKNOWLEDGEMENTS iii

LIST OF TABLES vii

LIST OF FIGURES viii

INTRODUCTION 1

1.1 General Statement of the Problem 5

1.2 The Limitations of this Study 6

1.3 Assumptions of the Study 7

1.4 Definition of Terms 7

TECHNOLOGY MANAGEMENT MODEL 15

2.1 Efficiency Attributes 15

2.2 Communications and Protocols 16

2.3 Coordination of Resources 16

2.4 Learning and Assessment 17

2.5 Alignment and Quality Control 17

REVIEW OF LITERATURE 18

3.1 The Purpose of the Study 18

3.2 Background Information 19

RESEARCH METHODS..30

4.1 Research Methodology..30

4.2 SYSTEM DESIGN..30

4.3 Localization Services..30

4.4 Evaluation of Vehicle Localization Techniques..34

SIMULATION AND RESULTS..36

5.1 Simulation and Results #1: RFID Data Collection/Emulation Techniques...................36

5.2 Simulation and Results #2: Infrared Data Collection/Emulation Techniques................38

5.3 Simulation and Results #3: Data Communications Techniques: NCAP to Cloud Communications..42

CONCLUSION AND SUMMARY..50

REFERENCES..53

APPENDIX A: METHODS RELATED TABLES AND CHARTS...58

APPENDIX B: LEGACY METHODS RELATED INFORMATION......................................63

APPENDIX C: SPECIFICATIONS AND DATA COLLECTION INFORMATION................72

APPENDIX D: REFERENCE RELATED INFORMATION..77

APPENDIX E: CURRENT LAWS, POLICIES AND REGULATIONS INFORMATION.......87

LIST OF TABLES

Table 1: Weekly readings for Longitude and Latitude data collection……….………….30

Table 2: Repeated Measures Model Option……………….……………………….….…45

Table 3: One of the XMPP/mDNS Datasets…………………….……………………..….46

Table 4. The matrix of our data collection design……………………….……………..…47

LIST OF FIGURES

Figure 1. A vehicle to Infrastructure overhead view……………………………….………18

Figure 2. IEEE 1451.5 WSNs…………….……………………………………….………...20

Figure 3. NCAP with the 6LoWPAN protocol stack ………………………….………28

Figure 4. WTIM and NCAP stack including the routing options…………….………. 29

Figure 5. Basic model for the system design ……………………………………..…31

Figure 6. Three Layer Network Hierarchy……....….…………………….....................33

Figure 7. Emulation hardware and accessories……………….…………………..…34

Figure 8. RFID dataset and setup technique………………...…………………..….37

Figure 9. Smart City block layout for Case Study…………………………..…..…38

Figure 10. IR Remote dataset and setup technique…………………………….….…41

Figure 11. XMPP Model for NCAP/WTIM……….……….………….……....…44

CHAPTER 1

INTRODUCTION

This thesis proposed to do research in the vehicle ad hoc networks (VANET) area of Intelligent Transportation Systems (ITS). The prime focus of this work was to develop safety applications that could contribute to reduced collisions, which in turn, could save lives and property losses (Yousefi, 2006). The key areas of this ITS research were cloud to infrastructure, infrastructure to cloud and infrastructure to vehicle (I2V). By using simulation/emulation techniques, this research makes contributions in the infrastructure to cloud as well as contributions to the infrastructure to vehicle area of technology research. The cloud in this case will be through the IEEE802.11 broadband (Wi-Fi) connection to a network database.

Currently, vehicle to vehicle (V2V) research is more mature than infrastructure (sensors) to vehicle (I2V) and infrastructure (sensors) to the cloud research. This conclusion was made mostly due to the number of research reports that are available at present, as well as the funding of research from automobile manufacturers to universities and to private commercial entities, such as Google and Uber.

In the United States, the majority of commercial vehicle safety research in ITS has been conducted by the USDOT's Research and Technology Administration (RITA) group via its Intellidrive research projects ((RITA), 2013). There are also several ongoing independent research projects being conducted by the Google corporation (Google, 2015) and major universities, such as the dedicated short range communications (DSRC) (Li, Yunxin (Jeff), 2011) work at the

University of California at Berkeley's Sustainable Infrastructure Initiative (Berkeley, 2019) the University of Detroit – Mercy's Transportation Center (Mercy, 2019), the University of Virginia's Transportation Center (Virginia., 2019), the Carnegie Mellon University's Transportation Center (Carnegie, 2019), the University of Florida's Transportation Research Center (Florida, 2018), and other similar efforts throughout the USA.

In recent years, heavy investments have been placed on autonomous vehicles. According to a recent Lloyd's of London publication, "Autonomous Vehicles" (Lloyds, 2014), "The idea of transferring control from a human driver to the vehicle itself, however, is a quantum leap which some may struggle to accept" (p. 6). The Lloyd's of London company also mentioned:

> [The] potential for change is great, and yet at the same time this must be balanced against the practicalities of implementation, and the achievement of adequate safety standards to mitigate the new risks that come with new technology. The lengthy considerations that would have to go into reworking laws, systems and infrastructure should not be underestimated, nor should public mistrust of putting lives in the hands of technology (p. 5).

The sentiments of the Lloyd's of London company are taken sincerely in this research as efforts have been put forth to make our contribution into the safety and infrastructure of the growing field of VANET research.

In the European Union (EU) community, there seems to be a larger effort in ITS research than in the USA at this time. This could be in part to the combined resources and efforts of the many countries that make up the EU. The Communication Architecture for Land Mobiles (CALM) (Williams, 2004) group and other EU community researchers have agreed to operate at different standards than the VANET communication standards that are used in the U.S. at the present time.

The US automobile manufacturing companies, which have a vested stake in ITS and Vehicle Ad-hoc network (VANET) research outcomes, have been involved in private as well as public research ventures into this technology. The autonomous vehicle research work that is currently attracting early adopters is a good example of the current global growth in ITS research and development. Some examples of this research are the current Carnegie Melon University's autonomous vehicle research initiatives (Carnegie, 2019) as well as the Google corporation's current autonomous vehicle partnerships (Google, 2015).

In a *Business Insider* magazine article, "Autonomous Cars Could Save The US $1.3 Trillion Dollars A Year" from 2014 (Zhang, 2014), Morgan Stanley estimates that autonomous cars could save the United States $1.3 trillion annually by lowering fuel consumption ($169 billion), reducing crash costs ($488 billion) and boosting productivity ($645 billion). PricewaterhouseCoopers (PWC) company (Pricewaterhouse, 2015), noted that driverless vehicle technology has the potential to "reduce traffic accidents by 90 percent, reduce number of cars by 90 percent, and reduce wasted commute time and energy by 90 percent resulting in savings of $2 trillion per year to the US economy."

The USDOT's early vision for the Vehicle Infrastructure Integration was to have dramatic safety improvements that would help revolutionize vehicle mobility. The aim of this revolution was through wireless communication with and between vehicles. In a recent USDOT's RITA group report ((RITA), 2013), this vision currently remains the same. Having a strong and viable highway infrastructure has been and still is one of the key prerequisites for a healthy and safe vehicle transportation system. A complement to a safe highway infrastructure system would be an infrastructure with safety related sensors to work with state-of-the-art electronic communication systems that will inevitably be installed in land-based vehicles. This would make up the vehicle to infrastructure (V2I) portion of the Intelligent Transportation System (ITS). Ashwin Amanna (Amanna, 2009) of the Virginia Tech's Transportation Institute and Dr. Veeraraghavan of the University of Virginia (Veeraraghavan, 2011) indicated that the vehicle's electronic communications would need to be equipped with DSRC radios that would operate in the 5.9 GHz frequency range. When these in-vehicle DSRC radios communicate with each other, they represent a vehicle-to-vehicle (V2V) communication system. The V2I and V2V systems have been designed to communicate safety message information as well as optional mobility and convenience information when needed.

European Road Transport Telematics Implementation Co-ordination Organization ERTICO (ERTICO, 2014) is the ITS organization that operates on behalf of the European Community. This organization was founded at the initiative of leading members of the European Commission, Ministries of Transport and the European Industry. ERTICO stated that currently safety has been one its key issues for vehicle mobility. Their research shows that more than 40,000 people die on Europe's roads each year, and road accidents cost the European economy around 200 billion Euros each year. While intelligent in-car safety systems have greatly improved the chances of surviving an accident, more attention needs to be focused on smart systems that can actually prevent accidents from ever occurring. ERTICO states that the ITS systems being developed within various projects and initiatives have the potential to save lives and reduce congestion caused by accidents. ITS networks have been designed to detect hazards on the road ahead and inform drivers of them even before they are visible. These systems can also keep vehicles at safe distances from one another and inform drivers of the local conditions by constant communication and information exchange between vehicles and the infrastructure. The ITS systems can also improve the efficiency of passenger and goods transport while easing congestion in the Smart Cities.

The ERTICO organization noted that if current technologies were utilized to their fullest extent through influencing driving and traffic management, the European community's fuel consumption and emissions of pollutants and CO2 could be significantly reduced. This would be advantageous for Smart Cities' initiatives, as well.

1.1 General Statement of the Problem

This research will identify ways and means of reducing traffic accidents. This, in turn, will save lives, reduce transportation costs, and reduce property damage.

The combined average age of all light vehicles on the road in the USA remained steady at 11.4 years, based on a snapshot of vehicles in operation taken Jan. 1 of 2015 ((IHS)., 2014) . In light of the extended lifetime of the vehicles that are being manufactured today, some of the initial VANET technology will have to be upgraded periodically, which is similar to changing out a used internal combustion engine's (ICB) vehicle battery every four years or so. The VANET technology should also generate opportunities for aftermarket off-the-shelf installations, as well.

The authors (Goel, 2015) noted that Connected Vehicle technology leverages recent advances in sensing and communication to transmit information both between vehicles (V2V) and between vehicles and infrastructure (V2I). The authors (Goel, 2015) also wrote about how the addition of electronic and communication technology to the ITS industry is making driving safer, improving mobility, reducing environmental pollutants, and reducing maintenance costs.

Another item of interest that promises to be relevant to this research is that each connected vehicle will act as a node or moving sensor while providing information to other vehicles and the infrastructure. The applications of electronic and communications technology and the possible opportunity to work with vehicles that could be managed as nodes are two of the key reasons that VANET research is an appropriate research topic for technologists at present and in the future.

According to Intelligent Transportation Systems magazine (Goel, 2015), some other key research areas are:

1. Develop/design an inter-operative system for VANET; V2I and I2V.

   This includes software, protocols, hardware, systems, data collection, and metrics.
2. Work on policy for data management, privacy and security in VANET
3. Work to create a contention-based algorithm for V2I and I2V communications
4. Work with ergonomic, social, and user behavior issues of connected vehicle technologies

1.2 The Limitations of this Study

The focus of this preliminary research is limited to the continental United States. While there are many areas and countries that have similar terrain and real estate, this research work does not investigate or claim to represent equipment, designs or systems that could be used for harsh and environmentally unfriendly conditions, such as desert conditions or the sub-freezing conditions of parts of Alaska and Antarctica.

This work was not approved for IRB-based data collection or IRB-based experiments. Therefore, we chose to use emulation, simulation, and packet analysis tools, such as Wireshark (Wireshark, 2015), as our data collection and analysis.

1.3 Assumptions of the Study

The assumptions are that the data collected in this research would be from motes (Brain, 2014) or smart digital sensors that will provide two-way communications to compatible devices and vehicles. This research includes the IEEE802.11 and the IEEE1451.X based standards along with other established network and wireless protocols for its digital communications and data collection. Another assumption is that this study can be conducted and continued as a safe, energy efficient and sustainable vision that can move from design to prototype in a coordinated and minimal disruptive manner as an emerging technology for the IoT community. This proposed design has the intent and vision to be simulated, emulated, verified and validated with respect to all rules and regulations of the associated institutes and organizations that it has been selected to work with, including XEP, HST, FCC, IEEE and ISA.

1.4 Definition of Terms

CAN Bus – Controller Area Network - In February of 1986, Robert Bosch GmbH introduced the serial bus system named Controller Area Network (CAN) at the Society of Automotive Engineers (SAE) congress. Today, almost every new passenger car manufactured in Europe is equipped with at least one CAN network. Also used in other types of vehicles, from trains to ships, as well as in industrial controls, CAN is one of the most dominating bus protocols – maybe even the leading serial bus system worldwide.

Contiki Operating System (OS) – Contiki is an open source operating system for networked, memory-constrained systems with a particular focus on low-power wireless Internet of Things devices. Examples of where Contiki is used include street lighting systems, sound monitoring for Smart Cities, radiation monitoring systems, and alarm systems. Contiki was created by Adam

Dunkels in 2002 and has been further developed by a worldwide team of developers from Texas Instruments, Atmel, Cisco, ENEA, ETH Zurich, Redwire, RWTH Aachen University, Oxford University, SAP, Sensinode, Swedish Institute of Computer Science, ST Microelectronics, Zolertia, and many others. www.contiki-os.org/start.html

Data Aggregation – Data aggregation is any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to get more information about particular groups based on specific variables such as age, profession, or income.

Zolertia - Internet of Things hardware solutions for development of 6lowpan smart applications. Engineers, universities, R+D centers and companies around the world are already using Zolertia boards to design and create their own Internet of Things connected products.

We offer a line of different IoT platforms, such us the RE-mote and the Fire-fly, to prototype and develop connected devices, that can easily convert into a real final product in a short period of time thanks to their core module The Zoul. – From: zolertia.io/

DSRC – DSRC (Dedicated Short Range Communications) is a two-way short to medium-range wireless communications capability that permits very high data transmission which is critical in communications-based active safety applications. In Report and Order FCC-03-324, the Federal Communications Commission (FCC) allocated 75 MHz of spectrum in the 5.9 GHz band for use by Intelligent Transportations Systems (ITS) vehicle safety and mobility applications.

IEEE 802.11p – IEEE 802.11p is an approved amendment to the IEEE 802.11 standard to add wireless access in vehicular environments (WAVE). It defines enhancements to 802.11 (the basis of products marketed as Wi-Fi) required to support Intelligent Transportation Systems (ITS) applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz).

IEEE P1609.0 – A Guide for Wireless Access in Vehicular Environments (WAVE) – This Guide provide details about the WAVE architecture and how the IEEE 1609 standards work together. Also, services necessary for multi-channel Dedicate Short Range Communications (DSRC)/WAVE devices to communicate in a mobile vehicular environment are covered within this Guide publication.

IEEE P1609.6 – Remote Management Services provides inter-operable services to manage WAVE devices. It consists primarily of a remote management service, including identification services for these WAVE devices, utilizing the WAVE management services defined by IEEE Std 1609.3, as well as the use of the identification services with the WAVE short message protocol.

Satellite diversity – Refers to a situation where multiple satellites in the constellation are simultaneously visible to user. The probability system availability is improved by increasing the probability that at least one satellite is in clear Line of Sight.

IPv4 **-** Internet Protocol Version 4 (IPv4) is the fourth revision of the IP and a widely used protocol in data communication over different kinds of networks. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet. It provides the logical connection between network devices through identification for each device. There are many ways to configure IPv4 with all kinds of devices - including manual and automatic configurations - depending on the network type. IPv4 is based on the best-effort model. This model guarantees neither delivery nor avoidance of duplicate delivery; these aspects are handled by the upper layer transport. From: techopedia.com/definition/5367/internet-protocol-version-4-ipv4

IPv6 (FCC, 2018) – IPv6 is the next generation Internet Protocol (IP) address standard that will supplement and eventually replace IPv4, the protocol most Internet services use today. An IP address is basically a postal address for each and every Internet-connected device. Without one, websites would not know where to send the information each time one performs a search or tries to access a website. However, the world officially ran out of the 4.3 billion available IPv4 addresses in February 2011. Experts predict that hundreds of millions of people will still come online in the next few years. IPv6 is the protocol that will allow internet and broadband users to do so by providing enough addresses (2^{128} to be exact) for all users and all of their various devices.

Manual on Uniform Traffic Control Devices (MUTCD) – Overview - The traffic control devices (TCD) are very critical for the safe and efficient transportation of people and goods. By setting minimum standards and providing guidance, the Manual on Uniform Traffic Control Devices (MUTCD) ensures uniformity of traffic control devices across the nation. The use of uniform TCDs (messages, location, size, shapes, and colors) helps reduce crashes and congestion while improving the efficiency of the surface transportation system. Uniformity also helps reduce the cost of TCDs through standardization. The information contained in the MUTCD is the result of either years of practical experience, research, and/or the MUTCD experimentation process. This effort ensures that TCDs are visible, recognizable, understandable, and necessary. The MUTCD is a dynamic document that changes with time to address contemporary safety and operational issues. From: mutcd.fhwa.dot.gov/kno-overview.htm

Matlab – Matlab combines a desktop environment tuned for iterative analysis and design processes with a programming language that expresses matrix and array mathematics directly. It includes the Live Editor for creating scripts that combine code, output, and formatted text in an executable notebook. From: mathworks.com/products/matlab.html

Network-Capable Application Processor (NCAP) (IEEE01) – A device between the transducer modules and the network. The NCAP performs network communications, transducer interface module communications, and data conversion or other processing functions.

Transducer Electronic Data Sheet (TEDS) (IEEE01) – An electronic data sheet describing a transducer Interface module or a Transducer Channel. The structures of Multiple TEDS are described in the standard.

Zigbee – ZigBee is the only open, global wireless standard to provide the foundation for the Internet of Things by enabling simple and smart objects to work together, improving comfort and efficiency in everyday life. The ZigBee Alliance is an open, non-profit association of approximately 400 members driving development of innovative, reliable and easy-to-use ZigBee standards. The Alliance promotes worldwide adoption of ZigBee as the leading wirelessly networked sensing and control standard for use in consumer, commercial and industrial areas.

Wireless Transducer Interface Module (WTIM) – A module that contains the radio

communication module, Transducer Electronic Data Sheet, logic to implement the Transducer interface, the transducer(s) or connection to the transducer(s) and any signal conversion or signal conditioning. From: www.zigbee.org/.

Zero Configuration Networking (Zero ConFig) - is a set of technologies that automatically create a usable computer network based on the Internet Protocol when computers or network peripherals are interconnected. It does not require manual operator intervention or special configuration servers. Invented by Stuart Chershire formerly of Apple Computer.

mDNS – Multicast DNS – in computer networking, multicast DNS networking protocol resolves hosts to IP address within small networks that do not include a local name server. It is a zero-configuration service, using essentially the same programming interfaces, packet formats and operating semantics as the unicast DNS. Although Stuart Chershire designed mDNS as a stand-alone protocol, it can work in concert with standard DNS servers.

Jabber.org is the original IM service based on XMPP and is one of the key nodes on XMPP network. - www.jabber.org

XMPP – XMPP is the Extensible Messaging and Presence Protocol, a set of open technologies for instant messaging, presence, multi-party chat, voice and video calls, collaboration, lightweight middleware, content syndication, and generalized routing of XML data. XMPP was originally developed in the Jabber open-source community to provide an open, decentralized alternative to the closed instant messaging services at that time. XMPP offers several key advantages over such services. From: xmpp.org/about/technology-overview.html

YAXIM – Yaxim (Yet Another XMPP Instant Messenger) is a lean Jabber/XMPP client for Android. It aims at usability, low overhead and security. This protocol also works well on low-end Android devices starting with Android 2.2 – From: yaxim.org.

IoT Broker – (waher.se/Broker.md) – The IoT broker is a message broker that helps insure things connected to the Internet have a secure, open and interoperable environment. The IoT broker helps secure Smart Cities.

" Troubleshoot and Understand mDNS Gateway on Wireless LAN Controller (WLC) " – From: www.cisco.com/c/en/us/support/docs/wireless/wireless-lan-controller-software/210835-Troubleshooting-mDNS.html.

IoT Harmonization – IEEE1451 – 99: Project Details: This standard defines a method for data sharing, interoperability, and security of messages over a network where sensors, actuators and other devices can interoperate, regardless of underlying communication technology. The backend of such a globally scalable, secure and interoperable network would be based on the eXtensible

Messaging and Presence Protocol (XMPP) and rely on infrastructural components, or bridges, with standardized interfaces that provide real-time conversion of other IoT and M2M protocols, such as those based on CoAP (Constrained Application Protocol), HTTP (Hypertext Transfer Protocol), MQTT (Message Queuing Telemetry Transport Protocol), AMQP (Advanced Message Queuing Protocol), etc., and other interoperability interfaces, such as those provided by the IEEE 1451 Smart Transducer Interface, oneM2M, OMA LWM2M (Open Mobile Alliance Lightweight M2M), OIC (Open Internet Connection), UPnP (Universal Plug and Play), IPSO (Internet Protocol for Smart Objects) Alliance, etc. The standard utilizes the advanced capabilities of the XMPP protocol, such as providing globally authenticated identities, authorization, presence, lifecycle management, interoperable communication, IoT discovery and provisioning. Descriptive meta-data about devices and operations will provide sufficient information for infrastructural components, services and end-users to dynamically adapt to a changing environment. Key components and needs of a successful Smart City infrastructure will be identified and addressed. This standard does not develop Application Programming Interfaces (APIs) for existing IoT or legacy protocols. From: standards.ieee.org/project/1451-99.html.

Apple Bonjour App. – From: en.wikipedia.org/wiki/Bonjour_(software) -- Bonjour is Apple's implementation of zero-configuration networking (zeroconf), a group of technologies that includes service discovery, address assignment, and hostname resolution. Bonjour locates devices such as printers, other computers, and the services that those devices offer on a local network using multicast Domain Name System (mDNS) service records. The software comes built-in with Apple's macOS and iOS operating systems. Bonjour can also be installed onto computers running Microsoft Windows. Bonjour components may also be included within other software such as iTunes and Safari. After its introduction in 2002 with Mac OS X

10.2 as Rendezvous, the software was renamed in 2005 to Bonjour following an out-of-court trademark dispute settlement.

Universal Plug and Play (UPnP) is a set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment. UPnP is intended primarily for residential networks without enterprise-class devices. From: en.wikipedia.org/wiki/Universal_Plug_and_Play.

The Simple Service Discovery Protocol (SSDP) is a network protocol based on the Internet protocol suite for advertisement and discovery of network services and presence information. It accomplishes this without assistance of server-based configuration mechanisms, such as Dynamic Host Configuration Protocol (DHCP) or Domain Name System(DNS), and without special static configuration of a network host. SSDP is the basis of the discovery protocol

of Universal Plug and Play (UPnP) and is intended for use in residential or small office environments: From: en.wikipedia.org/wiki/Simple_Service_Discovery_Protocols

CHAPTER 2

TECHNOLOGY MANAGEMENT MODEL

Many managers assume that structure and process are the natural foes of creativity; however, if they are built and used correctly, they can actually enhance creativity by fulfilling five important roles (Tony Davila, 2007).

2.1 Efficiency Attributes

Efficiency was described by Davila, et al as moving great ideas from concept to commercialization, quickly and with a minimum use of resources. We realize that efficiency is the number one attribute that engineers look for in their vision for excellent products and services. During the early days of the industrial revolution, efficiency was the attribute that help roll early automobiles off of the assembly line and that help stretch tele phone wires from New York to Lo Angeles. We know that efficiency helps fuel the completion in the pit crews of Indy and NASCAR racing teams. Each team wants to legally, through minor innovations and adjustments, make their vehicle faster and more agile than their competitors. We see that efficiency and well managed brainpower has propelled Elon Musk and his team to become the leading private earth orbit rocket launcher in the world in the second decade of the 21t century.

2.2 Communications and Protocols

Communications was described by Davila et al as creating the appropriate lines of communication within the company, and with outside constituencies, in order to facilitate timely access to specialized knowledge.

For this research and contributions to technology and innovations, communications holds a two-fold role.

A.) Verbal and written communications are important to working with any teammates. These teammates could be either co-workers or customers. Verbal and written processes has been and will continue to be a paramount part of what makes this kind of innovative research competitive.

B.) In digital communication it is working with various communication protocols to produce an end-to-end communication system that can be used for our data collection purposes which is paramount to maintaining a successful and growing business..

C.) Because of the Moore's Law (Law, 2019) of semiconductor evolution, we realize that out currently used protocols will continue to evolve beyond 5G and 6G digital communication technologies.

Therefore, we made concerted efforts in our research and preparations to provide state works in relation to the communication protocols that we used in this research. Our End-to-End testing and data collection utilized 5G XMPP protocols such SMPP and mDNS for fast, robust and reliable results while doing our data collection and device testing.

2.3 Coordination of Resources

Coordination can also be viewed as one of the key attributes that has made Elon Musk's total enterprises extremely successful. Coordination of resources, technology and talent has made the Amazon company one of the leaders in delivering their product as well as delivering a strong ROI to all of its stock holders. It is no secret that efficiency and coordination has help propel the Walmart company to become the most famous general stores as well as one of the most profitable companies of this century, as well.

2.4 Learning and Assessment

Facilitating optimum coordination between projects and teams; learning (i.e., managing the knowledge that is constantly created in innovation), for this research, we have used this model of efficiency, communication, coordination, learning and alignment as our technology innovation model.

By using SWOT analysis results, we can evaluate the things that we learned in respect to our original goal of efficiency, communication and co-ordination. From our analysis to this point, we evaluated what we have learned thus far.

2.5 Alignment and Quality Control

Aligning the objectives of various constituencies and reinforcing the most favorable individual and two organizations with the same structure will get very different … results based in part on the systems they have in place and the consistency with which they are followed. However, for innovation to happen successfully, there needs to be an explicit quality control process in place to manage all the steps from design, to measurement, and other assessments.

CHAPTER 3

REVIEW OF LITERATURE

This chapter contains a summary of the current literature that illustrates the state-of-the art in IEEE1451 – standards and 6LoWPAN (6LoWPAN, 2015) Wireless Sensor Networks. Some background on how these protocols interface with Intelligent Transportation Systems and Vehicle Ad Hoc networks is included in this chapter as well.

3.1 The Purpose of the Study

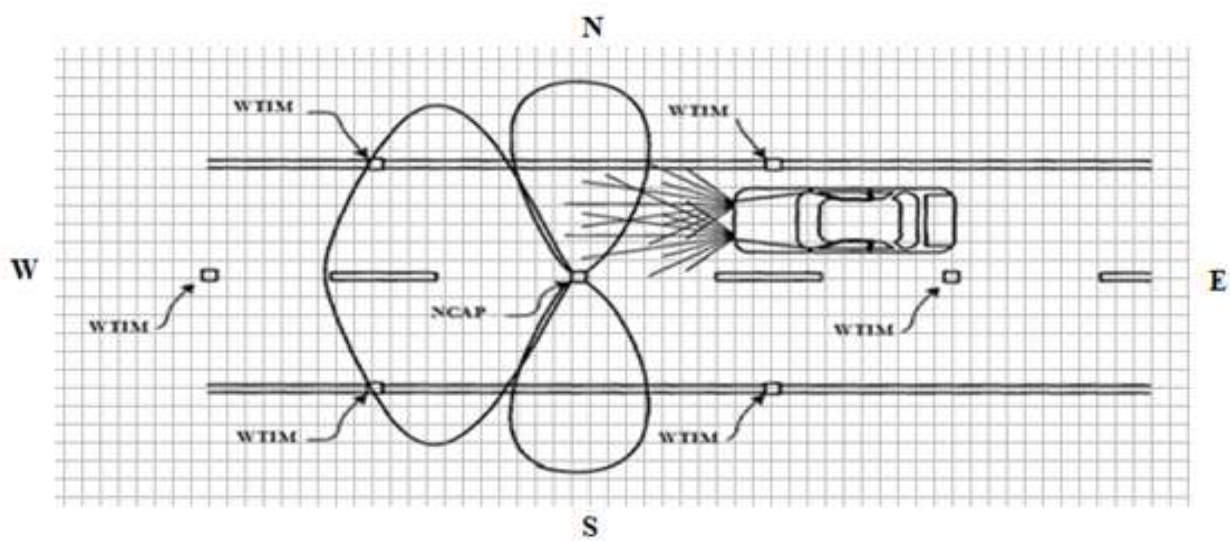


Figure 1: – A vehicle to Infrastructure overhead view (Hayes M. O., 2019).

The above figure illustrates an example of a possible layout for our WSN to Vehicle or Infrastructure to Vehicle design.

One of the primary purposes of this study is to investigate how the area of Intelligent transportation systems and more specifically, the VANET and wireless access for the vehicle environment (WAVE) community have a void and a strong need for more advance technology in order to increase highway safety, save lives and reduce property damage and insurance costs. Also, there is a demand for applications that will advance the integration of wireless network technology in the vehicle to vehicle (V2V) (Ding, 2009), vehicle to cloud, vehicle to infrastructure (V2I), infrastructure to vehicle (I2V), infrastructure to cloud interfaces. This chapter will discuss some of the background research, policies and developments that have culminated into the technology of ITS and VANET research.

3.2 Background Information

The IEEE1451.5 (2007) 'Standard for a Smart Transducer Interface for Sensors and Actuators - Wireless Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats' defines a wireless interface for sensors [20]. It specifies radio-specific protocols for this wireless interface. It defines communication modules that connect the wireless transducer interface module (WTIM) and the network-capable applications processor (NCAP) using the radio-specific protocols. It also defines the Transducer Electronic Data Sheets (TEDS). This standard is beginning to see more use in designs that require metadata tags and wireless sensor applications.

In their research, on Intelligent Transportation Systems the authors (Barrero, 2014) illustrated how the use of the IEEE1451 standard can be applied to safety applications in the wireless access for vehicle environment. The authors (Barrero, 2014). produced two experiments in which the effectiveness of the IEEE1451 was illustrated in a Wireless Sensor Network. Barrero and others performed experiments using an IEEE1451 compliant mobile environmental sensor network. The group also was successful in testing and collecting data using artificial vision-based equipment.

The author's (Barrero, 2014) research also demonstrated well researched applications in relations to how the IEEE1451 protocol could be used. However, this report did not mention the QoS and Bandwidth issues that might occur within a Wireless Sensor Network data collection system. Furthermore, there was no work performed using the IEEE1451.5 to 6LoWPAN protocol designs found in this research.

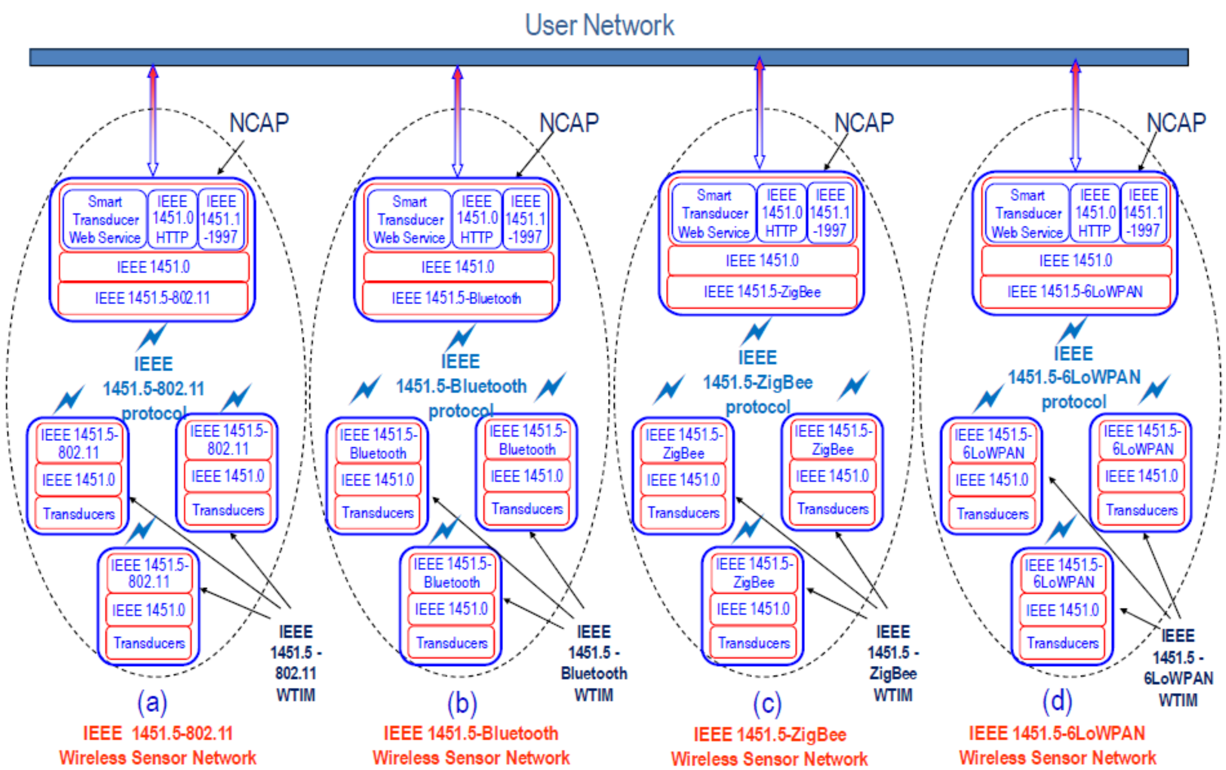


Figure 2: IEEE 1451.5 WSNs

In Figure 2, the IEEE 1451.5-802.11 Standard is illustrated (Song, Y.S., Lee, K.B. et al, 2011). The IEEE 802.11 standard is a Set of standards for Wireless Local Area Network (WLAN) communications in the 2.4 GHz, 3.6 GHz and 5 GHz frequency bands. The IEEE 1451.5-802.11 wireless interface adopts IEEE 802.11 a/b/g wireless protocols. It is compatible with IEEE 802.11e and IEEE 802.11i security constructs. The IEEE 1451.5-802.11 standard stack is shown in Figure 2. The standard uses the IEEE 802.11 Physical (PHY) and Medium Access Control (MAC). The network layer in this stack supports Internet Protocol (IP). The transport layer uses either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). The application layer consists of IEEE 1451.5-802.11 and IEEE 1451.0 transducer services and either the NCAP application or WTIM application. The NCAP can wirelessly communicate with the WTIM using IEEE 1451.0 messages through the IEEE 802.11 protocol. The four diagrams show some of applications of the IEEE1454 standard that have been tested by the National Institute of Standards organization.

After reviewing the dissertation titled 'Self-Organizing Communication in Vehicular Ad Hoc Networks' (Wischhof, 2007), it was noted that the author did a fine job of addressing the state of the art at the time of the work; multi-hops and security were addressed in this report for the years 2006/2007. However, present day digital communications technology has gotten faster and has more processing power. This would make latency an issue to be factored into the self-organizing VANET protocols and dissemination techniques that were demonstrated by this well researched and well written report of the 2006 and 2007 VANET/DSRC/WAVE technology development era.

In the article titled 'Vehicle Density Based Forwarding Protocol for Safety Message Broadcast in VANET' by Jiawei Huang, et al. (Huang, 2014), it was noted that the author utilized the p-persistent CSMA/CA, which is contention based, but it still utilized its bandwidth inefficiently as compared to a greedy algorithm, such as the short path algorithm.

This Vehicle Density Forwarding (VDF) protocol process did not account for round trip or one-way latency in the signal integrity, nor did this protocol account for security in its VANET information exchange. The authors (Huang, 2014) did not investigate a routing protocol that might be compatible with its multi-hop capable vehicle density based forwarding protocol for safety message broadcast in VANET.

According to B. Arief, et al. (Arief, 2006), the last few years have seen the emergence of many new technologies that can potentially have major impacts on Intelligent Transportation Systems (ITS). One of these technologies is a micro-electromechanical device called smartdust. A smartdust device a mote (Brain, 2014) is typically composed of a processing unit, some memory, and a radio chip, which allows it to communicate wirelessly with other motes (Brain, 2014) within range. These motes (Brain, 2014) can also be augmented with additional sensors – such as those for detecting light, temperature and acceleration – hence enhancing their features and making their application areas virtually limitless.

The authors (Arief, 2006) conducted research with wireless sensor networks using what they defined as smartdust sensors or mote (Brain, 2014).. This work was novel at the time because it was directed at the transportation industry and was supported by the sponsorship of several transport-related EU and UK projects. The projects included the ASTRA project in 2005, the ASK-IT project in 2007, the EMMA project in 2007, the Foot-LITE project in 2007, the MESSAGE project in 2007, and the TRACKSS project in 2007. The well-funded research provided the team with an opportunity to carry out experiments and develop demonstrations of smartdust applications in transport systems. This innovative research also gave (Arief, 2006) an opportunity to investigate how smartdust can be used in collaboration with other (more traditional) transport sensors for developing better Co-operative Transport Systems (CTS).

This project shows strong WSN research contributions from a non-IEEE research affiliation, as the team did a fine job in outlining their experience in projects and provided excellent illustrations on the evolving role that the smartdust technology can play in future Intelligent Transportation Systems.

According to J. Li, et al. (Li J. e., 2014), due to the large scale of wireless sensor networks (WSN) and the huge density of WSN nodes, classical performance evaluation techniques face new challenges in view of the complexity and diversity in WSN applications. This paper presents a “state-event transition” formal description for WSN nodes and proposes an event-driven QPN-based modeling technique to simulate the energy behaviors of nodes. Besides, the framework architecture of a dedicated energy evaluation platform has been introduced, which can be used to simulate the energy consumption of WSN nodes and to evaluate the system lifetime of WSN. Case studies prove that this platform can be utilized for the selection of WSN nodes and network protocols, the deployment of network topology, and the prediction of system lifetime as well.

Zaher M. Merhi (Merhi, 2010) indicated that localization systems for wireless sensor networks are complex systems that have many applications in real life. In this dissertation, an efficient localization system tailored for wireless sensor networks is proposed. The system is comprised of four subparts that work together to perform target localizations. The first subpart is a node localization system (TALS) that is capable of generating estimates of the nodes' location based on ranging measurements and anchor nodes. TALS utilizes trigonometric properties and identities to compute the nodes' locations with low computational overhead and high accuracy. Moreover, TALS takes advantage of redundancy to employ data fusion techniques to enhance the quality of the estimate.

The second subpart is a medium access control (MAC) that is capable of handling high data traffic when an event occurs in the sensor field. EB-MAC and EVA-MAC are two medium access controls that are tailored for event-based systems that characterize the target localization application. EB-MAC and EVA-MAC share the same principles but different implementations where the latter is the enhanced version of the former. The basic idea is to shift contention generated from the data phase by introducing a control gap, thus achieving a collision free schedule for data transmission. The third subpart is the acoustic target localization which triangulates potential targets based on acoustic sources. The 7-point trilateration technique estimates the target's location based on time difference of arrival. Finally, the data fusion subpart takes advantage of redundancy to enhance the quality of the estimate. The FuzzyART data fusion technique assigns probabilistic weights according to a decision tree based on spatial correlation and consensus vote.

Extensive simulations in software were performed for each subpart where comparisons with popular techniques were made. Enhancements in accuracy, speed and computational overhead were achieved. Furthermore, a hardware implementation of the acoustic target localization system was performed on MicaZ motes (Brain, 2014) and PIC microcontroller demo boards acting as a co-processor. The system presented robustness to noisy measurements, fault tolerance and high accuracy.

The authors (Li Y. L., 2014) indicated that with the popularity of smartphones and explosion of mobile applications, mobile devices become the prevalent computing platform for convenient communication and rich entertainment. Mobile cloud computing (MCC) is proposed to overcome the limited resources of mobile systems. However, when users access MCC through wireless networks, the cellular network is likely to be overloaded and Wi-Fi connectivity is likely to be intermittent. Therefore, device-to-device (D2D) communication is exploited as an alternative for MCC. An important issue in exploring D2D communication for MCC is how users can detect and utilize the computing resources on other mobile devices. In this paper, we propose two mobile cloud access schemes: optimal and periodic access schemes and study the corresponding performance of mobile cloud computing (i.e., mobile cloud size, node's serviceable time percentage, and task success rate). We find that optimally, node's serviceable time percentage and task success rate approach using more practical periodic access scheme, and node's serviceable time percentage and task success rate are determined by the ratio of contact and inter-contact time between two nodes.

In his 2011 doctoral dissertation (Ibrahim, 2011), Khalid Ibrahim noted that, Vehicular Ad-Hoc Networks (VANETs) are a fast growing technology that many governments and automobile manufacturers are investing in to provide not only safer and more secure roads, but also informational and entertainment-based applications for drivers. The applications developed for VANETs can be classified into multiple categories (safety, informational, entertainment). Most VANET applications, regardless of their category, depend on having certain vehicular data (vehicular speed, *X* position and *Y* position) available. Although these applications appear to use the same vehicular data, the characteristics of this data *(i.e.,* amount, accuracy, and update rate) will vary based on the application category. For example, safety applications need an accurate version of the vehicular data with high frequency but over short distances. Informational applications relax the data frequency constraint as they need the vehicular data to be reasonably accurate with less frequency but over longer distances. If each of these applications shares the vehicular data with *only* its peers using its own mechanism, it was stated that this behavior will not only introduce redundant functionalities (sending, receiving, processing, etc.) for handling the same data, but also wastefully consume the bandwidth by broadcasting the same data multiple times. Despite the differences in the data characteristics needed by each application, it was noted that this data can be still shared. Vehicular networks introduce the potential for many co-existing applications. For example, if the problem of data redundancy is not addressed early, it could hinder the deployment and usefulness of many of other applications. In this light, Ibrahim (Ibrahim, 2011) developed a framework, cluster-based accurate syntactic compression of aggregated data in VANETs (CASCADE) for efficiently aggregating and disseminating commonly-used vehicular data. CASCADE was architected as a layer that provides applications with a customized version of the vehicular data, based on parameters that each application registers with CASCADE. Additionally, the framework performed the common data handling functionalities (sending, receiving, aggregating, etc.) needed by its applications.

João Barros can be credited as one of the people that first publicly used the term "The Internet of Moving Things". Dr. Barros is one of the first entrepreneurs to represent this term in his business operations (Veniam., 2015). According to information viewed on his company, João Barros is co-founder of the company Veniam, which utilizes slower moving vehicles, such as trucks, busses, and taxicabs that may follow a more restrictive or repetitive route in their daily movements. Nonetheless this company appears to be having some success with signal strength, QoS and Bandwidth issues. This allows his company to continue its research to improve its product offerings in the near future.

The U.S. Department of Transportation's Intelligent Transportation Systems' Joint Program Office indicated that their Connected Vehicle Safety Pilot equips vehicles with a range of options (Transportation, 2015). One of these options was the installation and utilization of electronic devices. These devices were to be inserted into vehicles during production. This type of device was to be connected to proprietary data busses and provide highly accurate information using in-vehicle sensors. The integrated system both broadcasted and received BSMs and processed the content of received messages to provide warnings and/or alerts to the driver of the vehicle in which it was installed. These devices were developed for light vehicles, trucks, and transit vehicles.

Higuera and Polo (Higuera, J.E. and Polo, J., 2011) noted that the adoption of the Internet Protocol version 6 (IPv6) networking in IEEE 802.15.4 sensor networks, using IEEE1451 standardization, increases the interoperability of low-power smart-sensor devices over IP networks. They illustrated the design and implementation of the IPv6 (FCC, 2018) sensor network over low-power wireless personal-area networks (6LoWPANs), and how it utilized the IEEE 1451 standard in IEEE 802.15.4 sensor networks. They proposed the design of the 6LoWPAN physical-layer transducer electronic datasheet (PHY-TEDS) using data-type redefinition with the header compression.

The authors (Higuera, J.E. and Polo, J., 2011) were also able to encapsulate IEEE 1451 commands in User Datagram Protocol datagrams to establish communication from the network capable application processor (NCAP) to the wireless transducer interface module (WTIM) in an environmental monitoring application. Figure 3 shows how the authors used the network layer implementation in their research.

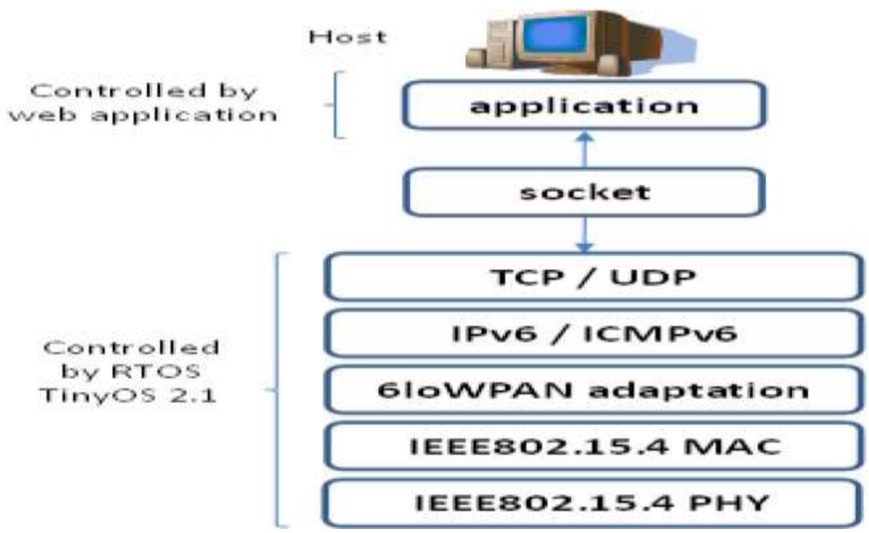


Figure 3: NCAP with the 6LoWPAN protocol stack (Higuera, J.E. and Polo, J., 2011).

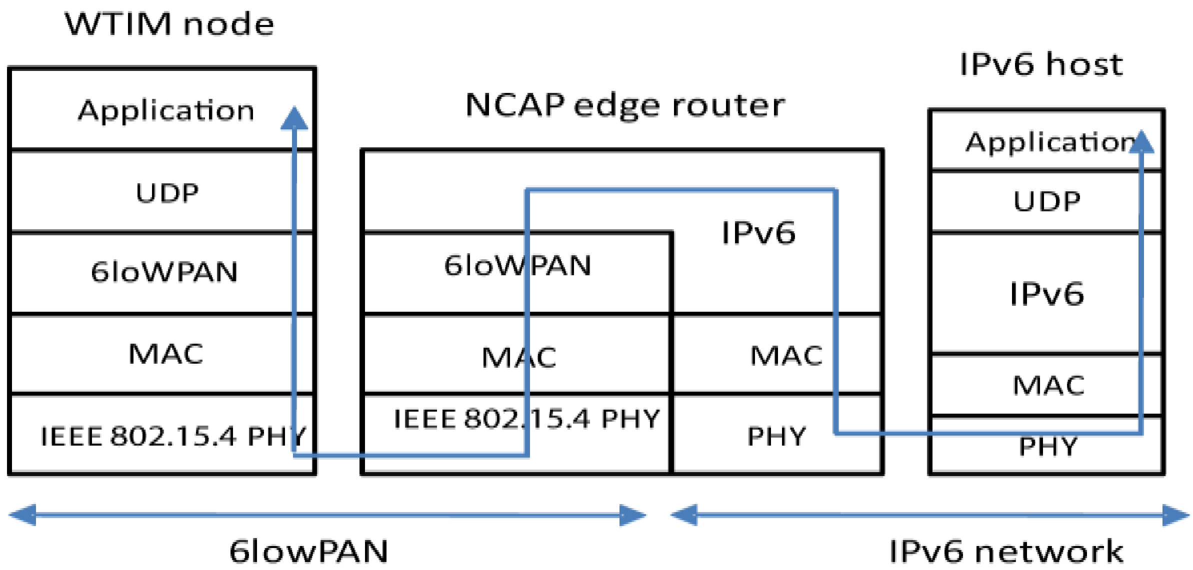


Figure 4: WTIM and NCAP stack including the routing options (Higuera, J.E. and Polo, J., 2011).

The authors (Higuera, J.E. and Polo, J., 2011) noted that the WTIM nodes use the same network layers as the NCAP, except the IPv6/ICMPv6 layer and its adaptation. Figure 4 shows the stack used by the WTIM and the NCAP within the 6LoWPAN (Olsson, 2014) and the stack used by other external nodes within an IPv6 network.

CHAPTER 4

RESEARCH METHODS

4.1 Research Methodology

We successfully verified and validated three separate experiments. The results, summary and conclusion of these experiments show the contributions that our research intended to report and convey.

4.2 SYSTEM DESIGN

4.3 Localization Services

We chose a combination of RFID localization and sensor networks because when combined they should provide tangible data collection options for Smart City projects. RFID tags are robust for data collection and data sharing with smart, semi-autonomous and future fully autonomous vehicles (Eun-Kyu Lee, Young Min Yoo, Chan Gook Park, Minsoo Kim, Daejeon, Korea, Mario Gerla,, 2009). These RFID networks should produce reliable validation methods when they are combined with our D-GPS system techniques. We limited the power output range of our RFID sensor tags to less than 110 yards of coverage per WTIM device in order to manage any interference that our design might cause to any surrounding communication systems.

Table 1: Weekly mean(s) reading for Longitude and Latitude data collection and updates.

Week	Longitude (ave)	Latitude (ave)	Iterations	Desc stats (mean, sd, var)
01	-1.35221	-2.27892	20	(m1, s1, v1)
02	-1.35112	-2.27807	40	(m2, s2, v2)
03	-1.35880	-2.27139	60	(m3, s3, v3)
04	-1.35891	-2.27104	80	(m4, s4, v4)

In the physical experimentation and data collection for this report, we made 20 separate readings of the map-based longitude/latitude combinations. (see Table 1: Week 01) These 20 separate readings were performed each time for four (4) different RFID tag locations. The PsuedoRange of each reading was computed, graphed and plotted against each of the nineteen (19) other readings that were taken from the same RFID PHY sensor tag location. We chose the average of these computations as the computed localization for the specific RFID tag.

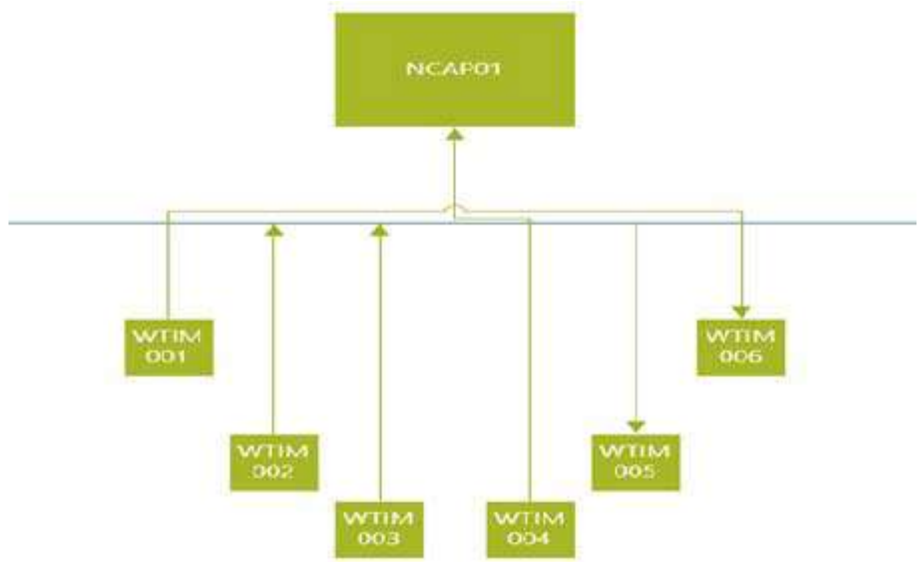


Figure 5: Basic model for the system design

Figure 5 represents one set of six WTIMs that were designed to interface wirelessly with one of the five NCAPs that will communicate with a single NCAP master or edge router to represent a WSN. This network was designed to function with autonomous and semi-autonomous vehicles.

The design used cloud-based data collection with the aim of reducing accidents and increasing road and highway traffic safety. We designed the WTIMs in Figure 5 to operate with RFID localization sensor tags. These tags were designed to operate as data dissemination devices for an ITS infrastructure localization service system or V2I system. The IEEE1451 (IEEE01) and IEEE1451.7 (IEEE02, 2011) standards were instituted within this RFID-based WSN design to facilitate, by emulation, our digital communications system.

This system was designed to operate as a Dedicated Short Range Communication (Li, Yunxin (Jeff), 2011) system that uses the IEEE802.11p (IEEE03, 2010) datalink layer protocol with RFID low power and infrared robust wireless networked sensors. Some key attributes of this novel design are low cost, low power, low latency, and self-configurable sensors or transmitters in a sustainable power system that operates in a robust tree network topology. This design specified solar technology with both active and passive RFID sensors to maximize energy efficiency. Our designed worked with the longitudinal or lengthwise run of the roadway in contrast to a somewhat similar passive RFID study that utilized their passive RFID devices in a transverse or latitudinal design across the roadway (Ali, 2009). We expect some of the early adopters of this technology will be designers and manufacturers of emergency vehicles, law enforcement agencies, manufacturers of semi-autonomous vehicles for ride share service companies, and insurance companies. The authors in (Higuera, J.E. and Polo, J., 2011) used WTIM TEDS to collect data for temperature, humidity, total solar radiation, photo-synthetically active radiation and voltage. The data from their datagram were converted with a Python script into the American Standard Code for Information Interchange for better reading by the end user. Each field of their Protocol packet data unit payload was read and collected in a Web server for display. Similarly, in this project, we used a Python script to transfer our RFID data and our IR remote sensor data into TEDS to be transferred to the webserver via the NCAPs. However, we used different attributes in our RFID and IR remote sensor, Smart Cities data collection project.

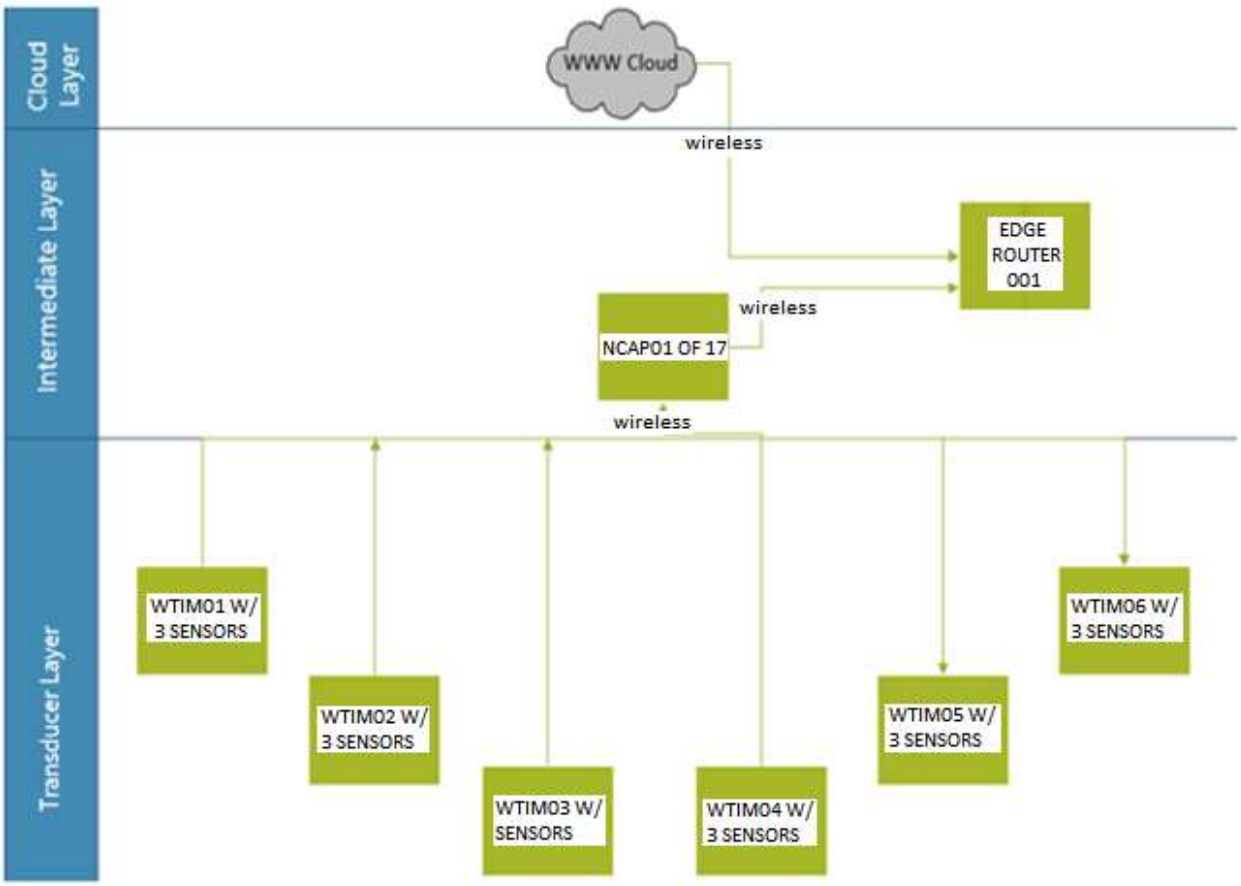


Figure 6: Three Layer Network Hierarchy

Figure 6 illustrates how the IEEE1451.X (IEEE01) protocol was used in our system. RFID tag data communicates with the WTIMs by the IEEE1451.7 (IEEE02, 2011) protocol. Figure 6 illustrates how a trigger mote (Brain, 2014) can be added to this layout for more effective operations.

4.4 Evaluation of Vehicle Localization Techniques

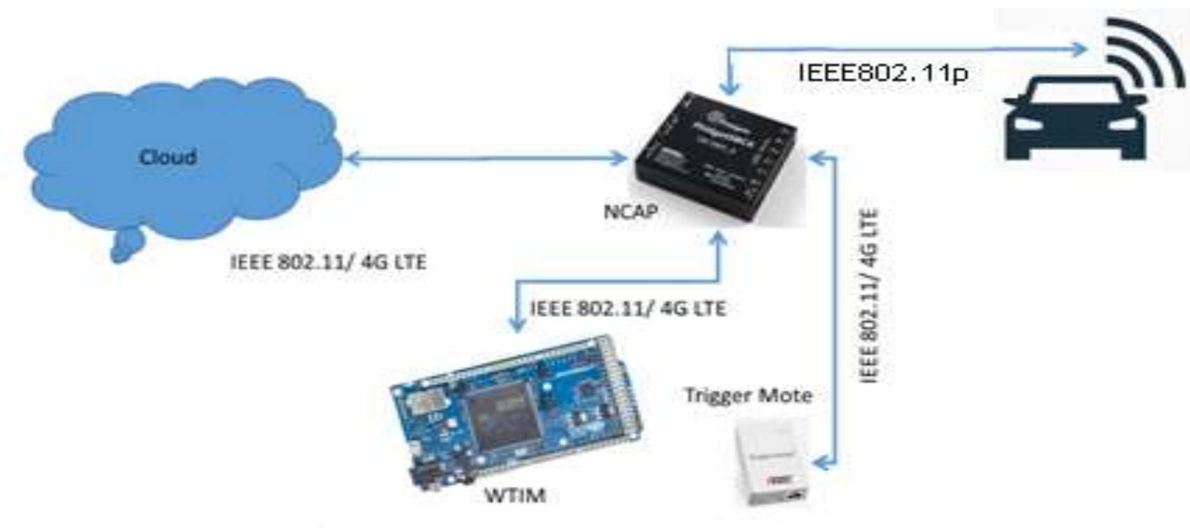


Figure 7: Emulation hardware and accessories (Hayes M. O., 2019)

In this portion of our research, we used computing hardware (Phidgets01, 2013), software (Python coding), RFID read/write hardware and infrared read/write hardware to complete wireless communications with respect to the IEEE1451.7 (IEEE02, 2011) protocol with TEDS. We used 30 RFID tags as data collection devices. We also used 30 infrared read/write units as sensors. We programmed each tag with a unique code to represent a unique location. Each location was prepared to communicate RFID or infrared remote sensor data with any vehicle upon request. The same information had options to be sent to the traffic control center as TEDS for information archives or dissemination to vehicles, as needed and as shown in Figure 7.

We verified that our design could read and write data with the tags, as designed. We verified that our infrared receiver could receive data from its associated infrared remote on request. The RFID Programmed location information is available for less frequent updates, similar to a file such as the PDF or CSV files.

This localization information can be communicated to the network via the Dedicated Short-Range Communications (Li, Yunxin (Jeff), 2011) services channel 174 (SCH 174) through service channel 175 (SCH 175). The infrared location services information (speed, time, date, temp, etc.) can also be communicated to the network via the DSRC services SCH 174 through SCH 176. The trigger motes (Brain, 2014) were set to operate on DSRC control channel 178 (CCH 178).

In addition, our D-GPS technique can be used to address the situation in which the WSN select group may have to automatically re-configure to compensate for an accidentally or intentionally failed node within one of the sections of a specific group. The group must re-organize for specified coverage or simply shut down completely until the maintenance team arrives.

To maintain ongoing accuracy, we developed an update technique for our localization sensors that may become accidentally moved, removed or dislodged from time to time by traffic and highway construction officials. The technique uses a Pseudo-differential GPS that offers various iterations for calculated accuracy over time as is shown in Table 2. The cumulative iterations for a preset time are averaged and checked weekly or monthly for accuracy and for significant deviations. Issues such as new construction and temporary or permanent street closings are prone to affect any WSN, their RSU locations and their proper operations.

CHAPTER 5

SIMULATION AND RESULTS

5.1 Simulation and Results #1: RFID Data Collection/Emulation Techniques

In the experimentation and data collection of our Pseudo – Differential Global Positioning System (P-DGPS) for this report, we made 20 separate readings of the map-based longitude/latitude combinations. (See Table 1: Week 01) These 20 separate readings were performed each time for each of our different RFID tag locations. The PsuedoRange of each reading was computed, graphed and plotted against each of the nineteen (19) other readings that were taken from the same RFID PHY sensor tag location. We chose the average of these computations as the computed localization for the specific RFID tag. The use of GPS for assisted vehicle parking has been well research. But, most of the current research has been with the use of on-board or in-vehicle GPS systems (Alejandro Correa, Guillem Boquet, Antoni Morell and Jose Lopez Vicario, 2017). This design was similar to designs that were mention in the book "Vehicular Networks" (Weigle & Olariu, 2009). However, our design was adjusted to accommodate our specific embedded sensor devices.

Our simulation/emulation demonstrated how data are communicated or transceived between our selected sensors, RFID and IR remotes, and the active smart or autonomous vehicle as it moves through the selected roadway or street domain. Figure 8 shows our RFID sensor (transceiver) dataset. The RFID dataset for the first six (6) WTIMs consisted of an initial WRITE function that performs the setup of the format and data storage into the GPS assigned RFID tags (See Figure 8).

The six WTIM write sequence are initially verified by the yellow stripped READ bar. This process was repeated for each of the 30 localization tags that were used for our experimental design.

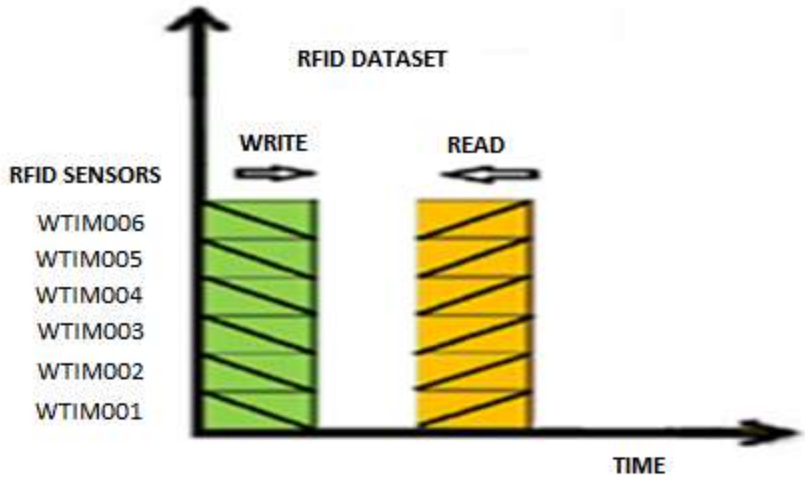


Figure 8: RFID dataset and setup technique (Hayes M. a., 2018).

Our early testing and data collection started with the PhidgetsSBC and its accessories. After early tests with the PhidgetsSBC and the zero-configuration software networking features, we moved to our data collection techniques. The RFID data collection system was our first emulation testing design (see Appendix A).

5.2 Simulation and Results #2: Infrared Data Collection/Emulation Techniques

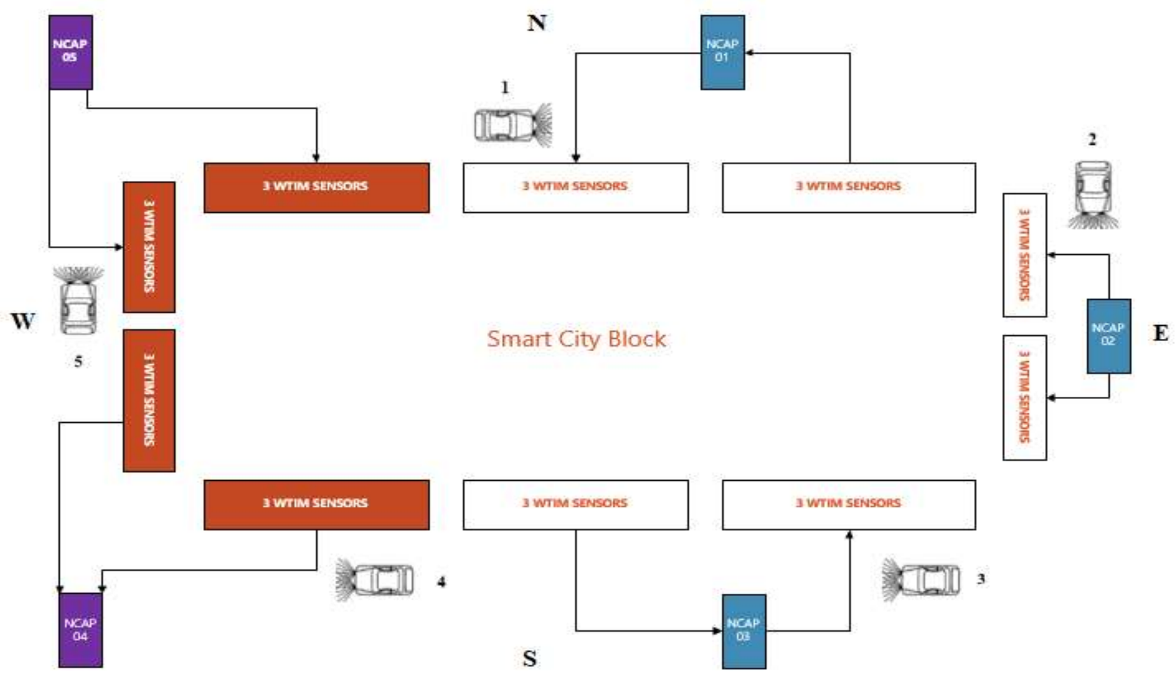


Figure 9: Smart City block layout for Case Study (Hayes M. a., 2018)

Figure 9 shows the layout of a Smart City block with 5 NCAPs and a complement of 30 WTIMs. The North, South, East and West navigation directions are labeled on the diagram. The operations of this diagram are described in our case study that follows. We start with the initiating action in the first quadrant of Figure 9. We will explain the blue, purple, white and red boxes in the first section of our case study design and the numbered vehicle figures will be explained in following paragraphs.

In the small blue box closest to the due “N” indicator, we have NCAP1, which was designed to communicate wirelessly with 6 motes; WTIM1 through WTIM6. There are 3 WTIMs embedded within the first white box that straddles the west and east side of the rectangle to the north “N”. This group represents WTIM1 through WTIM3.

The second white box, to the right of the initial three WTIMs, holds the next group of motes; WTIM4 through WTIM6. This group of three WTIMs also performs wireless communications with NCAP1. As we move to the next section, the small blue box next to the due “E: indicator is NCAP2. In the same manner as just described, inside of the top white box along the east side of the rectangle, WTIM7 through WTIM9 are grouped to communicate wirelessly with NCAP2.

The second white box along the east side of the block holds WTIM10 through WTIM12. This group of WTIMs were designed to communicate wirelessly also with NCAP2. As we make a right turn, heading from South to East, along the bottom border of the rectangular block in Figure 9, we encounter the first white box that holds WTIM13 through WTIM15. Continuing west, the adjacent white box contains WTIM16 through WTIM18. The aforementioned six WTIMs will all communicate wirelessly with NCAP3 that is positioned about halfway between the two previously indicated white boxes.

The next and last white box along the southern border appears as we move from east to west contains WTIM19 through WTIM21. This group will communicate wirelessly with NCAP4. NCAP4 is the purple box located that is located inside of the southwestern corner of our simulated Smart City block. As we move from south to north we encounter the lower red box along the left side of the diagram. This box contains WTIM22 through WTIM24, which were designed to communicate wirelessly with NCAP4 as well. Looking further, heading north, along the west side of the block, we encounter the next red box that holds WTIM25 through WTIM27, which will communicate wirelessly with NCAP5. The adjacent red box that runs from west to east along the top or northern border of the block holds WTIM28 through WTIM30. This final of the ten sensor-based boxes hold the last of the 30 WTIMs for this case study and communicates wirelessly with NCAP5 as well. NCAP5 is located at the northwest corner of the diagram.

In this section, we discuss the numbered vehicle figures that are embedded inside of our Figure 9 diagram. The vehicle figure labeled #1 represents our Veh#1 that has triggered the WSN domain that is supervised by NCAP1 for wireless communication with the cloud.

Our design illustrates how Veh#1 can communicate with WTIM1 through WTIM3 as it progresses through its present WSN domain. Veh#1 will continue its communication with WTIM4 through WTIM6 if it needs additional information as it moves through this NCAP1-supervised domain.

The vehicle figure labeled #2 represents our Veh#2 that has triggered the WSN domain which is supervised by NCAP2 for wireless communication with the cloud. We illustrate how Veh#2 can communicate with WTIM7 through WTIM9 as it moves through the its present WSN domain. Veh#2 will continue its communication with WTIM10 if it needs additional information as it moves through this NCAP2-supervised domain. This continuation in sequencing is performed for each numbered vehicle figure of Figure 9. The vehicle figures #3 through figure #5 are shown to be in position to repeat the sequences of Veh#1 and Veh#2 with respect to their perspective domains until a completed path around the perimeter of the Smart City block has been achieved.

Our simulation/emulation demonstrates how data are communicated or transceived between our selected sensors, RFID and IR remotes and the active smart or autonomous vehicle as it moves through the selected roadway or street domain. Figure 10 shows our IR remote (transceiver) dataset.

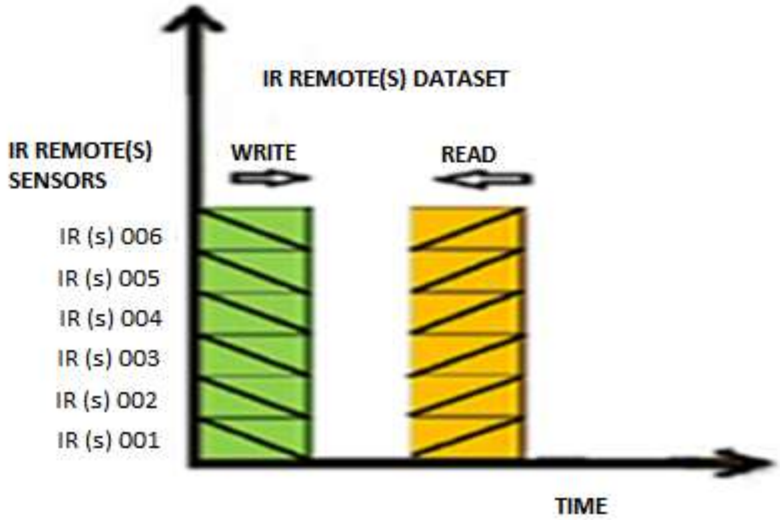


Figure 10: IR Remote dataset and setup technique (Hayes M. a., 2018)

The IR remote sensor dataset for the first six (6) WTIMs consisted of an initial WRITE function that does the setup of the format and data storage into the TEDS of the IR remote sensor's RAM memory as shown in Figure 10. The six WTIM write sequences for the IR remote sensors are initially verified by the yellow stripped READ bar. This process is also repeated for each of the 30 locals that were used for our experimental design. The IR Remote sensors are used to receive the accelerometer information from a vehicle that enters the IR remote sensing range. Once the vehicle's raw accelerometer data, such as acceleration, is received by the WTIM sensors (IR remote's) the vehicle's speed can be computed and written into the TEDS of the WTIM.

$$v = \frac{ds}{dt}$$ (David Halliday, 2000)

Equation 1 is the key equation that we used to compute the oncoming vehicle's speed and location after the infrastructure receives updated accelerometer data form the targeted vehicle. The dynamic variables of v and s (or position) are the key attributes that this design is most interested in investigating.

5.3 Simulation and Results #3: Data Communications Techniques: NCAP to Cloud Communications

In the design of our end-to-end communications, we chose to use a different transceiver device at each end of the system. One of our transceiver devices represented the Infrastructure of the V2I/I2V system. The second transceiver (Samsung smartphone) represented the vehicle or cloud part of the V2I/I2V or I2C/C2I system.

The local end device that we used for our data collection was the Samsung Galaxy Tab A 7-Inch Tablet 4G WI-FI SM-T285 8 GB (March 2016 release date). This device was used to emulate a mote (WTIM) with embedded sensors for data collection and data dissemination to the NCAP module or to a matched NCAP module of an ASIC chipset. This device was loaded with the Yaxim (Yaxim, 2019) smartphone application. The Yaxim, which operates using XMPP Protocol software/middleware, provided end-to-end IoT Harmonization at the Transducer layer of our system model design.

In addition to the above equipment, we also used a Samsung Galaxy S5 smartphone (2014 release date) with both WiFi (IEEE04, 1997) and 4G LTE capabilities. The smartphone and accessories were loaded with the Yaxim software application in order to communicate with the Samsung A6 tablet in end-to-end communications. In our research, the Samsung smartphone represented the Cloud (Traffic Control Center/database) or a licensed/approved Vehicle of our I2Cloud and I2V data collection designs.

Several sets of data were taken from the same three locations. These data sets were taken around the same time of day on different days of the week. The initial time and dates for this set of data were 09:00pm on June 28, 2019 and June 29, 2019. In order not to violate the IRB data collection rules for this research, no data was taken for this research from a moving vehicle.

The three locations that were used for the datasets were the following:

1.) Office/Lab.

2.) Robert's House

3.) Bill's House

The following three messages were sent:

1.) Initial message of "Hello Today"

2.) A second message that reads "Nice Photo"

3.) The second message has a 3.82MB attachment of a colorful "Caribbean Parrot".

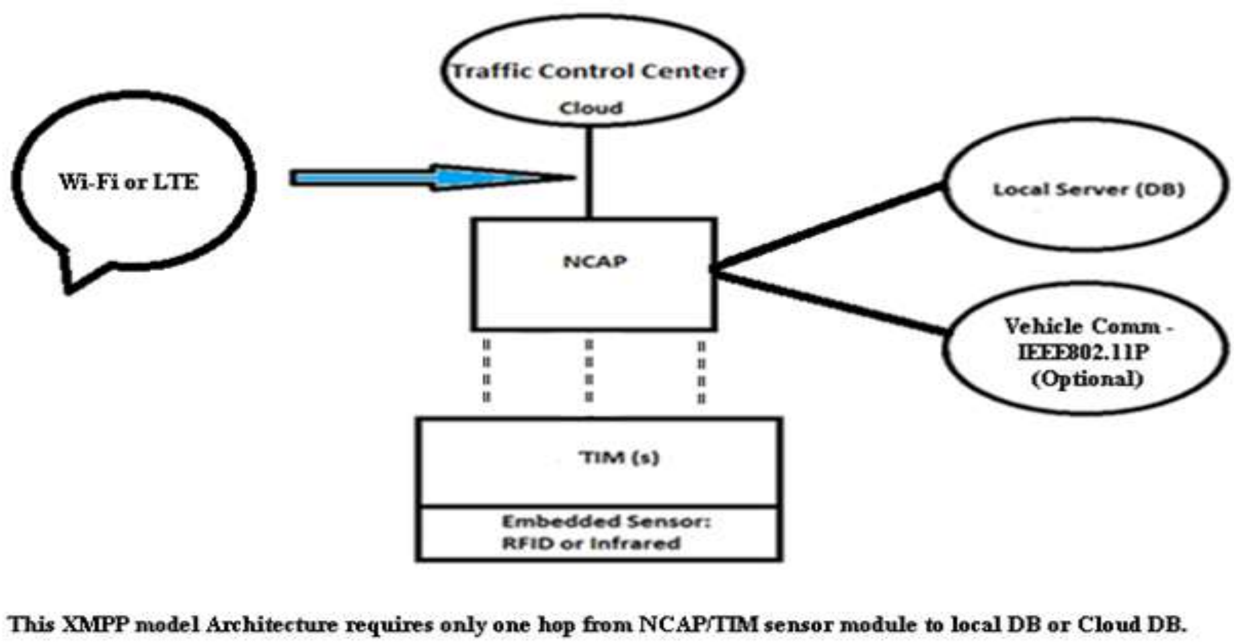


Figure 11: XMPP Model for NCAP/WTIM (Hayes M. O., 2019).

The above figure represents the architecture of our design. As stated earlier, the NCAP of our design operates as an edge router by communication with the cloud and with vehicles in certain circumstances or conditions. Therefore, communication can be made to the cloud to our local data collection database, or to a vehicle in a one-hop schema for fast, robust, and secure communications.

The numbered items below were the steps that we followed in collection of our packet data for analysis and organization.

1. We sent two separate messages to the Pseudo - NCAP via our simulation design.

2. Our sending unit, a Samsung cell phone, represented the Vehicle communications portion of our system design.

3. There were two messages sent and observed via Wireshark (Wireshark, 2015) from three separate locations during each data collection session.

4. Appendix A has the Wireshark (Wireshark, 2015) figure that shows our raw data. Table 3 shows that the text message and photo portions of the second message were treated as separate transmissions.

Table 2: Repeated Measures Model (Optional tests setup)

	Location	Message Type	Protocol	X-mission Time
Dependent Variable	X	X		
Independent Variable			X	X

Our first statistical design option was to follow a repeated measures ANOVA design. However, as we placed our collected data in an Excel spreadsheet for further statistical analysis and organization, we quickly realized this was not the most effective manner in which to represent our collected data for best analysis (see Table 2.). The design was robust but, repeated measures data did not justify a full ANOVA (IBM, 2018) design and analysis. However, the repeated measures data collection did provide us with a true validation of the measured data that we were receiving via this particular design. Therefore, we designed Table 3., which is shown below, to provide a more efficient representation of our analysis and the various details of the valuable data that we collected during each of our data collection sessions.

Table 3: One of the XMPP/mDNS Datasets

Text	Photo	From: Smartphone Sent [TOD]	To: Tablet Rcvd [TOD]	Location of Message sending point	Protocol Used
Hello Today		09:02:10	09:02:12 2 Sec	Home Lab.	mDNS
	Parrot	09:03:17	09:03:18 1 Sec	Robert's House	SSDP
Nice Photo		09:03:18	09:03:19 1 Sec	Tim's House	SSDP
Hello Today		09:06:42	09:06:44 2 Sec	Home Lab.	mDNS
	Parrot	09:07:34	09:07:36 2 Sec	Robert's House	SSDP
Nice Photo		09:07:36	09:07:37 1 Sec	Tim's House	SSDP
Hello Today		09:11:47	09:11:49 2 Sec	Home Lab.	mDNS
	Parrot	09:12:32	09:12:34 2 Sec	Robert's House	SSDP
Nice Photo		09:12:34	09:12:35 1 Sec	Tim's House	SSDP

Table 3 shows End-to-End Data Collection for our XMPP protocol project, which was collected on 06/29/2019.

We were limited to when and how often we could collect a data sample because the data collection method takes a 30-minute plus slot of time for each set of data collections, The above dataset was collected at a specific time of day and on a single day out of the week.

The above diagram shows an example of normal information, devices, protocols and datum that was collected from our End-to-End project and data collection design. As we continued to collect and analyze our data, we constantly checked and examined our data and setup for any deviations in collected data from this table.

Table 4. The matrix of our data collection design

1. mean 2. sd 3. var	Location	Message Type	Protocol	X-mission Time
Dependent Variable	- Ofc/Lab - Bob's house - Bill's house	- Text - Text/Photo		
Independent Variable			- mDNS - SSDP	- mDNS - SSDP

The table above is the matrix of our data collection design. From our initial two-day data collection session, we found little to no variations in our Wireshark (Wireshark, 2015) collected dataset. Those, results represented a validation of the robust quality of our data collection process. When we changed the time-of-day and day-of-week for one of our data collection events, we noticed a change in some of the results in the collected data.

Our regularly defined protocol sequence did not deliver in one of the more than ten total trials that we performed. This one-time variation in our collected data times leads us to believe that more of this kind of research is needed, especially with the various combination of time of day testing and various kinds of test devices and data collection equipment.

Appendix A shows some of our raw data collection files. Our end-to-end application level photo shows the times (3) that the; 1. Text message was sent and received, and 2. The time that the Text/Photo combination was sent and received. A note about the second transmission is that even though the message was sent , or originated, as a text message with an attachment, the Wireshark (Wireshark, 2015) and the screenshot data shows that the second message was broken into a HTTPS-based XML message, while the text message portion of this message may, or may not transmit as an HTTP message. At local ranges, the mDNS options are available for text messaging (see Table 3.)

Our regular data collection yielded similar results with a few exceptions and possibly operator error may have caused some of the infrequent variations in the Wireshark (Wireshark, 2015) data capture results (see Appendix A).

Hardware and Laboratory Equipment

We used the Wireshark (Wireshark, 2015) packet analysis software to capture and analyze the XMPP protocol packets that were created each time we executed a communication transaction between our two communication devices. Our data collection design was used in a manner similar to the one described in the book "*Network Forensics*" (Davidoff, 2012). We used a legacy Dell Optiplex 745 desktop computer to capture our Wireshark (Wireshark, 2015) data as it moved from the smartphone 4G LTE and WiFi platform to the Office/Laboratory-based tablet via the Office/Laboratory broadband router for end-to-end operations.

We used a Compaq Presario CQ57 laptop and associated accessories for our publications and data management. The Samsung Galaxy TAB 6 and its accessories were used as a simulated wireless sensor for our emulated end-to-end testing and data collections.

The PhidgetSBC3 (Phidgets01, 2013) single board computer was used for early testing and evaluations of IoT and cloud database options. We used the PhidgetSBC3 (Phidgets01, 2013) and its accessories for data collection at the Transducer layer of Figure 6 as well. Other items listed in this research are as follows:

Samsung Galaxy S5 smartphone and accessories

Phidget brand - RFID reader and Tags (6) - and accessories

Phidget brand - IR remote reader - and accessories

Remote transceiver(s) (6) and accessories

Dell Desktop and accessories

Canon printer/copier

Samsung Galaxy Tab A 7-Inch Tablet 4G WI-FI SM-T285 8 GB (March 2016). This device was used as a mote (WTIM) with embedded sensors for data collection. This device was loaded with the Yaxim smartphone app. The Yaxim operated as an XMPP Protocol software/middleware to provide end-to-end IoT Harmonization at the Transducer layer of our system model design.

CHAPTER 6

CONCLUSION AND SUMMARY

Within the RFID and Infrared portion of our study, one of our principle challenges was how to visualize a large traffic component of a smart city project that could be reduced to describable parts for modeling and emulation/simulation data and metadata aggregation and dissemination. The RFID dataset consisted of an initial WRITE function that provided the setup of the format and data storage into the GPS-assigned RFID tag. The design also consisted of infrared sensors that could provide fast read/write responses to an autonomous vehicle's request for localization services, such as speed and parking space updates. Immediately after the RFID tags were programmed, the READ process was performed on the device to verify that the correct D-GPS localization data were programmed onto the RFID tag. Our data tables illustrated the 'proof-of-concept' on how a Differential GPS process can effectively manage everchanging WTIM repositioning and system configuration updates; management occurs by using repeated statistics to accurately calculate the nominal position with a minimum number of iterations.

Our RFID dataset diagram shows that after some lapse in time, the data were retrieved as an example of a passing autonomous vehicle accessing localization information. This could represent the dissemination of localization data, such as flash flooding situations within a city's flash flood-prone areas.

Our design used the built-in transceivers of the infrared sensor within the WTIMs to help approaching vehicles to compute and verify their speed and other attributes that the WSN infrastructure system might convey. This design represented an urban V2I metadata collection and dissemination system for Smart Cities.

In some cases, the second three WTIMs within our six WTIMs architecture could be re-programmed and re-positioned to provide expanded WTIM coverage for a separate vehicle. Expanded coverage would enable another vehicle to receive location services while travelling in a separate but parallel traffic lane along-side of our original vehicle shown in Figure 1. This design could be helpful in emergencies when all traffic is being routed in the same direction such as hurricane evacuations in the mid-Atlantic US states region.

Our RFID and infrared sensor techniques provided us with successful ‘proof of concept’ in our emulation design. We achieved success in our ‘proof-of-concept’ experiments. With the Samsung (Samsung01, 2014) smart phone’s 4G/LTE, IEEE802.11 and other features and functions, we were able to satisfactorily achieve our design and results. We achieved strong results from our Phidget (Phidgets01, 2013) emulation hardware as well.

With our End-to-end data collection and hardware emulation system design, we successfully sent and received data over the network using an XML over XMPP application for Android systems. Our mDNS and SSDP data packets were captured and analyzed using a packet analysis tool.

We used the Wireshark (Wireshark, 2015) packet analysis software tool to capture and analyze the XMPP protocol packets that were created each time that we executed a communication transaction between our two communication devices (see "Network Forensics" Davidoff, 2012). However, we found different results than the data described by "Network Forensics" publication. Davidoff identified the plain text that was communicated in his system design from an AOL IM message. Our XMPP used the Chrome bowser with HTTPS IRL. However, by using the Wireshark

(Wireshark, 2015) and local scripting tools, we were not able to unscramble or unencrypt original text messages that were sent and received via the messaging event.

One of the greatest details we gained from this research was that the speed and the bandwidth of the transmitted messages that we worked with were very robust, very fast and rather secure because of encryption techniques. It is worthy to note that an added layer of security can easily be added to our design if we are allowed to use our design over a secure service such as the IEEE802.11P protocol. No intrusive or hacking activities were detected within our data collection. However, we are continuing to evaluate the security and robustness of the XMPP packet traffic that we used for our NCAP to Cloud data collection. It should be noted that our intent to utilize the IEEE802.11p proprietary frequency and bandwidth for Vehicle to Infrastructure communications should add another layer of security and integrity to our overall system design. Also, more work is needed in filtering our packets for greater security, and more research into robust communications that can help manage the impact of the growing requirements of future Vehicle to Infrastructure technology will be needed. We have placed copies and samples of our raw data collection in the Appendices.

REFERENCES

Facts & Statistics – Safety: Federal Highway Administration. (2014, October 15). Retrieved August 21, 2018, from http://safety.fhwa.dot.gov/facts_stats/

Brain, M. *How Motes Work*. (2004, February 28) Retrieved April 14, 2015, from https://sceweb.uhcl.edu/yang/teaching/csci5931WSNfall2007/WSN%20Papers/BrainHowMotesWorks.pdf.

Yousefi, S., M. Siadat MIousavi, and M. Fathy. *Vehicular Ad Hoc Networks (VANETs): Challenges and Perspectives* in *6th International Conference on ITS Telecommunications Proceedings*. 2006. Chengdu, China.

Google. *Google Self-Driving Car Project*. (2015, June 10) Retrieved July 12, 2015, from http://www.google.com/selfdrivingcar/.

University of California Berkeley. *Sustainable Infrastructure Initiative*. (2018, April 8) Retrieved June 5, 2019, from https://citris-uc.org/sustainable-infrastructures/

University of Detroit Mercy. *Transportation Center*. (2017, February 6) Retrieved January 10, 2019, from http://eng-sci.udmercy.edu/research/udmtc.php

University of Virginia. *Center for Transportation Studies* (May 8, 2018) Retrieved May 19, 2019 from http://www.cts.virginia.edu/

Carnegie Mellon University. *Transportation Research*. (2019, January 8) Retrieved March 18, 2019 from http://www.cmu.edu/homepage/computing/2019/winter/transportation-research.html

University of Florida. *Transportation Institute*. (2018, October 7) Retrieved May 13, 2019 from https://www.transportation.institute.ufl.edu/

Lloyds. *Autonomous vehicles; Handing Over Control: Opportunities and Risks for Insurance*. (2014, June 7) Retrieved June 6, 2015 from https://www.lloyds.com/~/media/lloyds/reports/emerging%20risk%20reports/autonomous%20vehicles%20final.pdf

Williams, B. *The Continuous Air-interface and Medium range (CALM)* The Continuous Communications for Vehicles Handbook, 2004.

Zhang, B. *Autonomous Cars Could Save The US $1.3 Trillion Dollars A Year*. Business Insider (2014, April 5) Retrieved June 12, 2015 from http://www.businessinsider.com/morgan-stanley-autonomous-cars-trillion-dollars-2014-9.

PricewaterhouseCoopers *The insurance industry in 2015*. Top Issues, 2015.

USDOT Research and Innovative Technology Administration (RITA) *Achieving the vision: From VII to Intellidrive*. 2013.

Amanna, A., *Overview of IntelliDrive / Vehicle Infrastructure Integration* Vol. 7. 2009, Blacksburg, Virginia: Virginia Technical Institute.

ERTICO – ITS Europe. (2014, November 3) Retrieved November 12, 2017 from http://ertico.com.

Institute on Highway Safety (HIS). *Average Age of Vehicles on the Road Remains Steady at 11.4 years, According to IHS Automotive*. (2014, February 9) Retrieved January 9, 2017 from http://press.ihs.com/press-release/automotive/average-age-vehicles-road-remains-steady-114-years-according-ihs-automotive.

Goel, S. and Y. Yuan, *Emerging research in connected vehicles.* IEEE Intelligent Transportation Systems, 2015.

Jiawei Huang, Yi Huang, & Jianxin Wang. (January 01, 2014). Vehicle Density Based Forwarding Protocol for Safety Message Broadcast in VANET. *The Scientific World Journal.*

IEEE Instrumentation and Measurement Society., Institute of Electrical and Electronics Engineers., American National Standards Institute., IEEE-SA Standards Board., & IEEE Xplore (Online service). (2007). *IEEE standard for a smart transducer interface for sensors and actuators: Common functions, communication protocols, and transducer electronic data sheet (TEDS) formats*. New York, NY: Institute of Electrical and Electronics Engineers.

United States Department of Transportation - Federal Highway Administration. *The Manual on Uniform Traffic Control Devices (MUTCD)*. (2015, July 28) Retrieved August 28, 2017 from http://mutcd.fhwa.dot.gov/kno-overview.htm

Barrero, F., Guevara, J. A., Vargas, E., Toral, S., & Vargas, M. (February 01, 2014). Networked transducers in intelligent transportation systems based on the IEEE 1451 standard. *Computer Standards & Interfaces, 36*, 2, 300-311.

Ibrahim, K., *Data aggregation and dissemination in vehicle ad-hoc networks*, 2011, Old Dominion University.

The Zigbee Alliance. *Zigbee.* (2015, July 8) Retrieved September 17, 2018 from http://www.zigbee.org/.

Olsson, J. *6LoWPAN Demystified*. Texas Instrument Corp. 2014.

Eugene Y. Song, Kang B. Lee, Steven E. Fick, Alkan M. Donmez (2011) *An IEEE1451.5 – 802.11 Standard-based Wireless Sensor Network with Embedded WTIM*, National Institute of Standards and Technology, Gaithersburg, Maryland USA.

Wischhof, L. (2007). *Self-organizing communication in vehicular ad hoc networks*. Aachen: Shaker.

Contiki. (2015 August 28) Retrieved June 8, 2018 from http://www.contiki-os.org/start.html

Arief, B., et al. *Integrating Smartdust Into Intelligent Transportation Systems*.

(2006,September 7) Retrieved May 7, 2018 from http://homepages.cs.ncl.ac.uk/budi.arief/home.formal/Papers/753_Arief.pdf.

Li, J., Zhou, H. Y., Zuo, D. C., Hou, K. M., Xie, H. P., & Zhou, P. (April 29, 2014). Energy Consumption Evaluation for Wireless Sensor Network Nodes Based on Queuing Petri Net. *International Journal of Distributed Sensor Networks, 10*, 4, 262848.

Merhi, Z.M. (2010) An Efficient Decentralized Target Localization System for Wireless Sensor Networks, University of Louisiana at Lafayette.

Li, Y., L. Sun, and W. Wang *Exploring Device-to-Device Communication for Mobile Cloud Computing*, Proceedings of the International Conference on Communications – Sydney, 2014

IPv4 – (2010, June 21) Retrieved October 17, 2018 from https://www.techopedia.com/definition/5367/internet-protocol-version-4-ipv4

IPv6 – (2015, July 12) Retrieved July 12, 2018 from https://www.fcc.gov/consumers/ Guides/internet-protocol-version-6-ipv6-consumers

Office of the Assistant Secretary for Research and Technology - U.S. Department of Transportation. *ITS Research Fact sheets - Connected Vehicle Safety Pilot Program'*. (2015, August 21) Retrieved April 7, 2018 from http://www.its.dot.gov/factsheets/safety_pilot_factsheet.htm#sthash.y54tn1ME.dpuf

Yaxim (Yet Another XMPP Instant Messenger) – (2018, July 18) Retrieved January 8, 2019 from https://yaxim.org.

Zoleria – Z1. (2015, May 12) Retrieved June 9, 2016 from http://zolertia.io/z1.

PhidgetSBC3. (2015, April 12) Retrieved May 11, 2015 from http://www.phidgets.com/products.php?category=21&product_id=1073_0.

S*PSS*. (2011 July 18) Retrieved August 11, 2011) from http://www-01.ibm.com/software/analytics/spss/products/statistics/.

Wireshark. (2015, September 1) Retrieved December 12, 2016 from https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs.

MatLab. (2015, August 16) Retrieved October 12, 2018 from http://www.mathworks.com/products/matlab/.

A 6LoWPAN Network of Embedded Devices. (2015 August 17) Retrieved September 7, 2017 from http://www.ti.com/lsds/ti/wireless_connectivity/6lowpan/overview.page

Veniam. *Delivering the networking fabric for the Internet of Moving Things*. (2011, January 12) Retrieved November 12, 2015 from https://veniam.com/company/

Li, Y., & 7th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, QShine 2010, and Dedicated Short Range CommunicationsWorkshop, DSRC 2010. (December 01, 2012). An Overview of the DSRC/WAVE Technology. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, Lnicst, 74,* 544-558.

Ali, K., Hassanein, H., & 2009 IEEE 34th Conference on Local Computer Networks, LCN 2009. (December 01, 2009). Using passive RFID tags for vehicle-assisted data dissemination in intelligent transportation systems. *Proceedings - Conference on Local Computer Networks, Lcn,* 688-694.

Davidoff, S., & Ham, J. (2012). *Network forensics: tracking hackers through cyberspace*. Upper Saddle River NJ: Prentice Hall.

U.S. Department of Transportation, ‘ITS Research Fact sheets - Connected Vehicle Safety Pilot Program’ (2017, June 7) Retrieved August 8, 2018 from http://www.its.dot.gov/factsheets/safety_pilot_factsheet.htm#sthash.y54tn1ME.dpf

Thackray, A., & Brock, D. C. (2015). *Moore's law: The life of Gordon Moore, Silicon Valley's quiet revolutionary*.

Universitat Politècnica de Catalunya. Departament d'Enginyeria Electrònica, Higuera Portilla, Jorge Eduardo, & Polo Cantero, José. (n.d.). *IEEE 1451 standard in 6LoWPAN sensor networks using a compact physical-layer transducer electronic datasheet*. (Higuera, J.; Polo, J. IEEE 1451 standard in 6LoWPAN sensor networks using a compact physical-layer transducer electronic datasheet. "IEEE transactions on instrumentation and measurement", Agost 2011, vol. 60, núm. 8, p. 2751-2758.)

Correa, Alejandro, Boquet Pujadas, Guillem, Morell Pérez, Antoni, & López Vicario, José. (2017). *Autonomous car parking system through a cooperative vehicular positioning network*. Veeraraghavan, Malathi; "A survey of research literature on Vehicular Networking" University of Virginia, 2011.

Olariu, S. (2009). *Vehicular Networks: From Theory to Practice*. Hoboken: CRC Press.

Ding, R. (2010). *A clustering-based multi-channel vehicle-to-vehicle (V2V) communication system*. Cincinnati, Ohio: University of Cincinnati.

Hayes, M., Omar, T., & 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). (November 01, 2018). An IEEE1451.7 Based WSN Design for V2I Localization Services in Smart Cities. 19-25.

Du, L., Liu, N., & Song, X. (March 01, 2014). Evaluation of IEEE 802. 11p in Vehicular Communication via Simulation. *Journal of Highway and Transportation Research and Development (english Edition)*, *8*, 1, 95-100.

Davila, A., Epstein, M. J., & Shelton, R. D. (2013). *Making innovation work: How to manage it, measure it, and profit from it*.

Halliday, D., Resnick, R., Halliday, D., & Walker, J. (2000). *Fundamentals of physics*.

Hayes, M., Omar, T., Proceedings of the 2019 International Symposium on Technologies for Homeland Security, "End to End VANET/ IoT Communications A 5G Smart Cities Case Study Approach" Woburn, MA., 2019

APPENDIX A: METHODS RELATED TABLES AND CHARTS

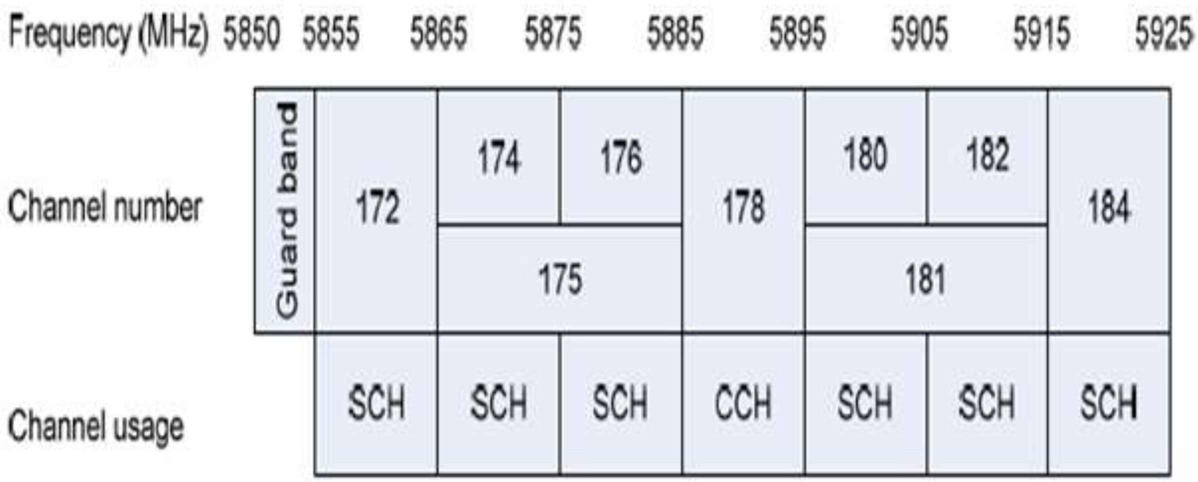


Figure A01 – This figure shows the seven channels of the dedicated short range communications frequencies that and the assigned channels for the DSRC Frequency Allocation in the US.

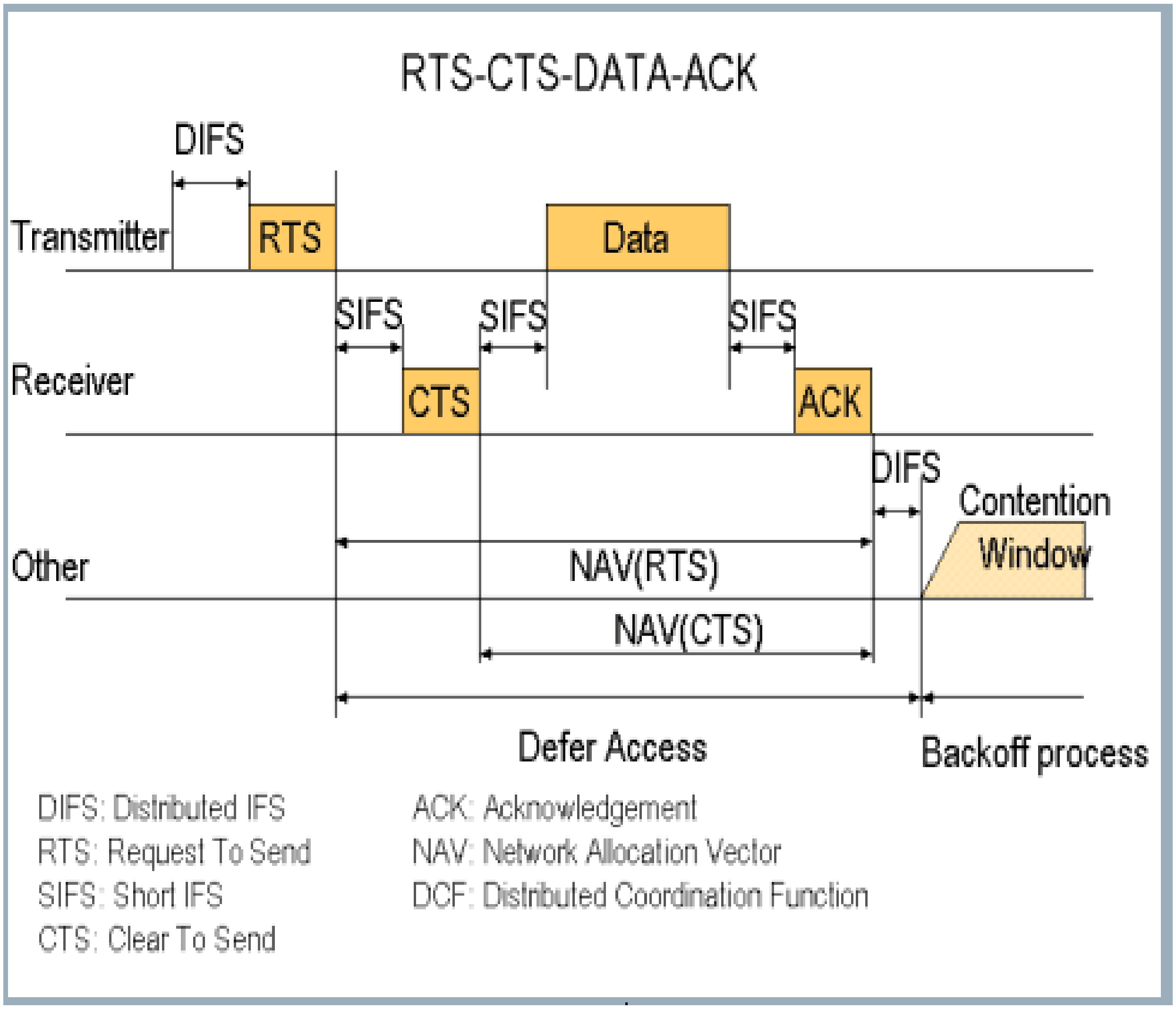


Figure A02: Diagram of CSMA/CA in action. The DIFS operates at the MAC layer of the IEEE 802.11 protocol. This datalink layer contention-based protocol is still a critical part of WiFi and middleware protocols, such as XMPP. The above diagram was retrieved from: https://cs.stanford.edu/people/eroberts/courses/soco/projects/2003-04/wireless-computing/int_interlan.shtml.

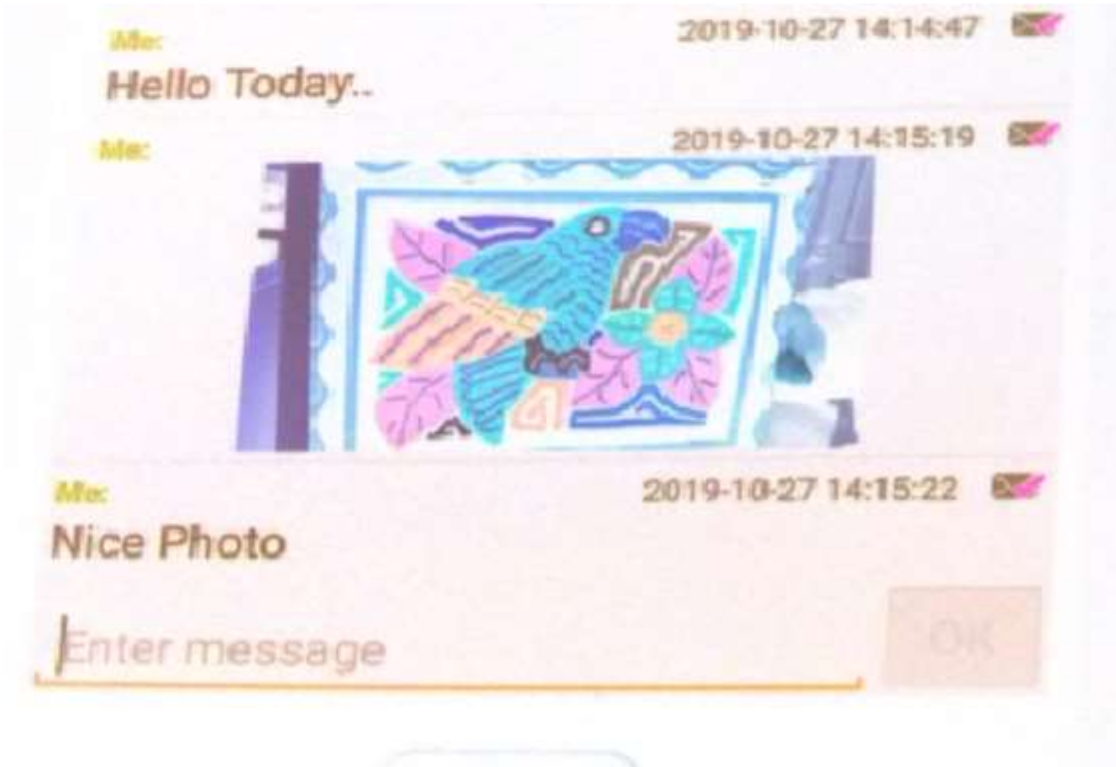


Figure A03: This is a screenshot of the application level data that was transmitted, or sent out, to the receiving unit. The original timestamp could not be documented clearly, therefore we used the reversed video in the next screenshot in order to deliver a higher quality timestamp detail of the real-time date stamp of the graphics.

Figure A04: This reverse video shows a clearer timestamp of our end-to-end graphics transmissions at the applications layer.

No.	Time	Source	Destination	Protocol	Length	Info
400	2019-06-29 09:29:40.731038	fe80::79e6:1394:908…	ff02::1:3	LLMNR	156	Standard query 0xe151 ANY CAVTech003
401	2019-06-29 09:29:40.731295	192.168.0.6	224.0.0.252	LLMNR	116	Standard query 0xe151 ANY CAVTech003
7	2019-06-29 09:01:53.012665	169.254.226.179	224.0.0.251	MDNS	492	Standard query response 0x0000 A, cache flush 169.254.226.179 PTR, cache
8	2019-06-29 09:01:53.013075	192.168.0.6	224.0.0.251	MDNS	992	Standard query response 0x0000 A, cache flush 192.168.0.6 PTR, cache flus
67	2019-06-29 09:05:50.913081	169.254.226.179	224.0.0.251	MDNS	142	Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question
222	2019-06-29 09:18:01.377437	169.254.226.179	224.0.0.251	MDNS	142	Standard query 0x0000 PTR _sleep-proxy._udp.local, "QM" question
37	2019-06-29 09:04:58.524078	169.254.226.179	169.254.255.255	NBNS	160	Name query NB WPAD<00>

Figure A05: The above screenshot is of our Wireshark packet capture data collection sample.

APPENDIX B: LEGACY METHODS RELATED INFORMATION

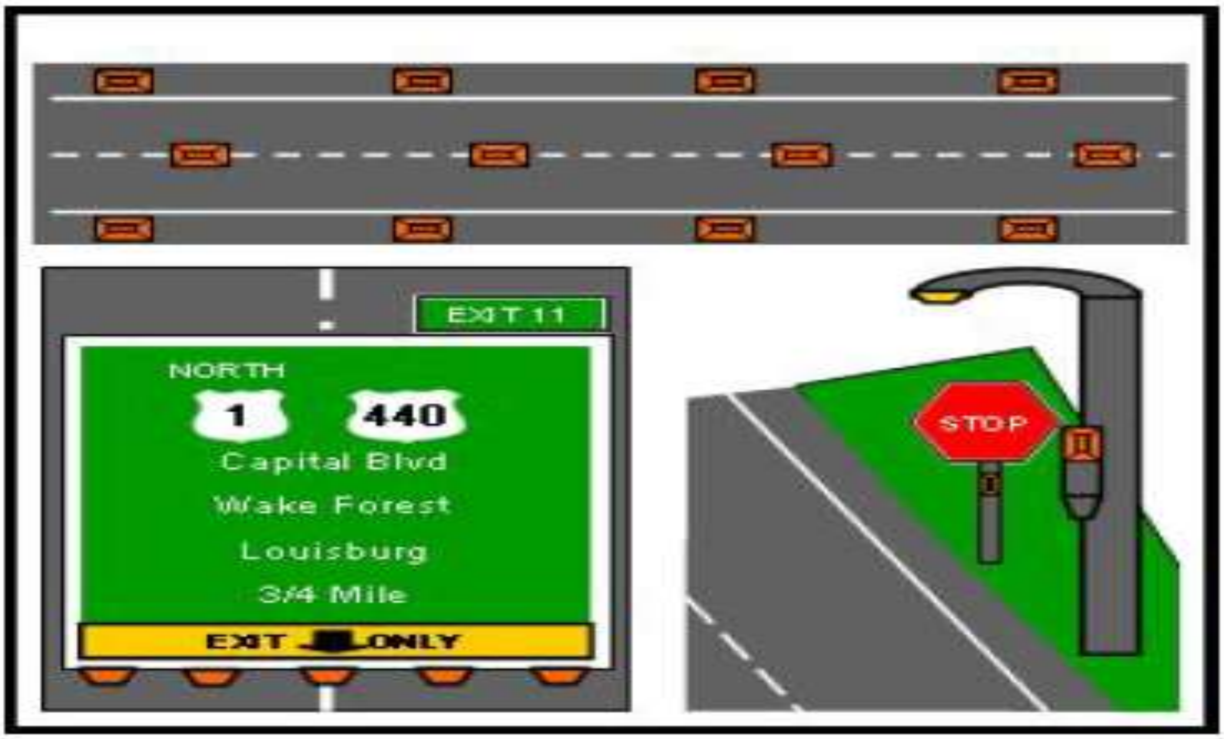


Figure B01: Legacy design graphics. Embedded sensors are clearly indicated.

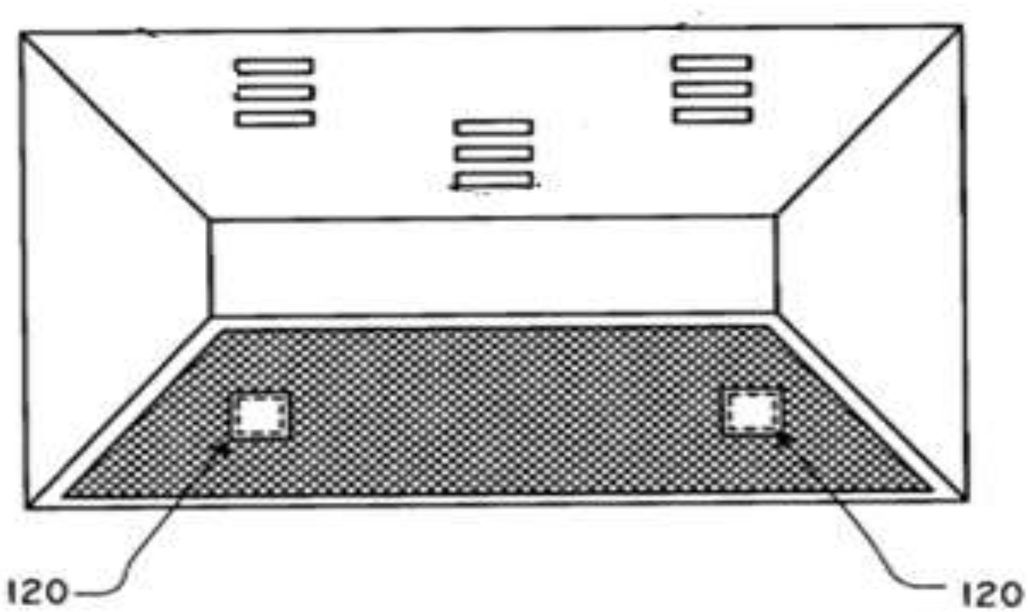


Figure B02: The above diagram shows an embedded sensor or mote. This design was specifically made for in-road wireless sensor applications.

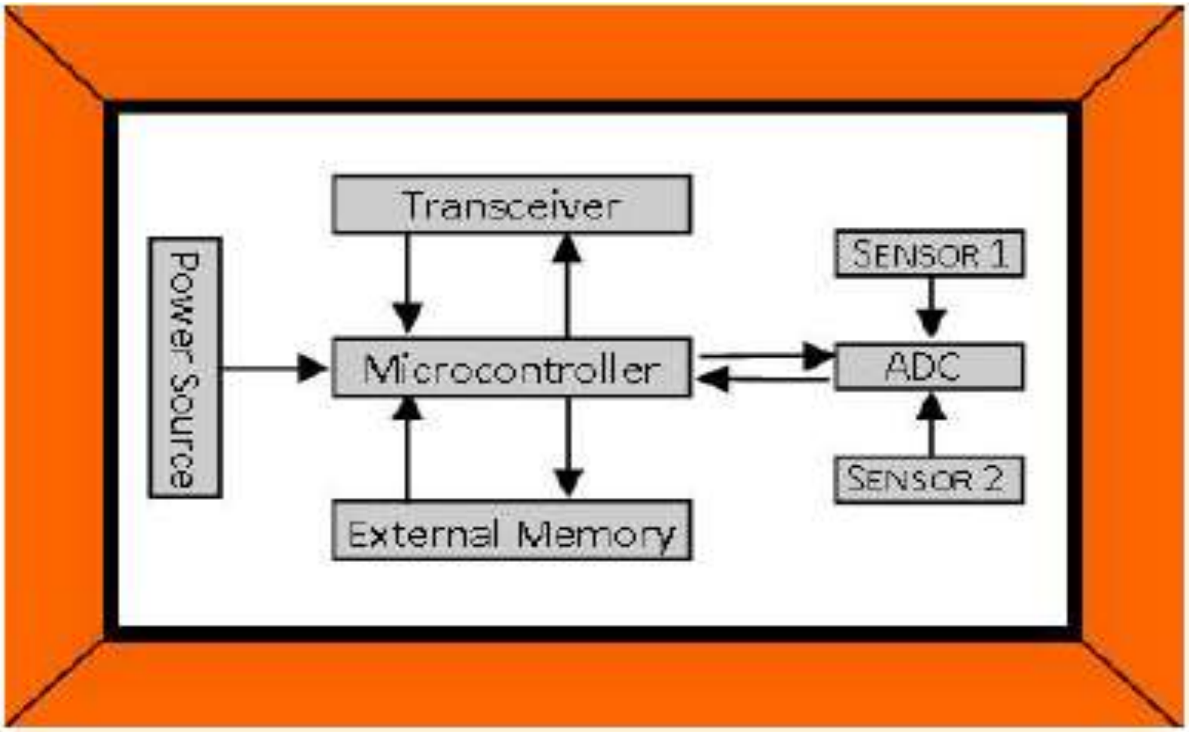
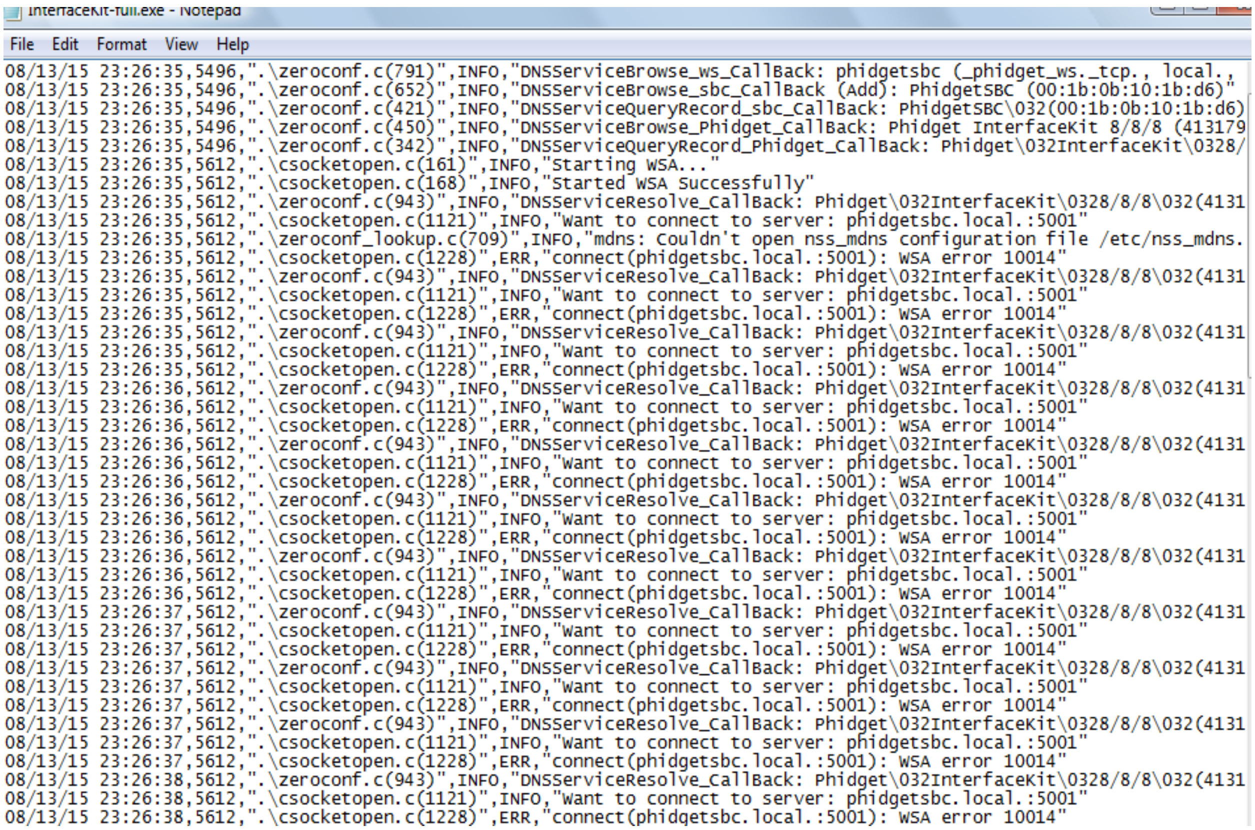


Figure B03: The above diagram represents an internal view of the possible parts of an embedded sensor. http://www.cc.gatech.edu/~keith/classes/ubicomplexity/pdfs/infra/hsw-motes.pdf.

Figure B04: The above single board computer shows the legacy platform that this research used for early designs, testing and data collections.



InterfaceKit-full.exe - Notepad

File Edit Format View Help

```
08/13/15 23:26:35,5496,".\zeroconf.c(791)",INFO,"DNSServiceBrowse_ws_CallBack: phidgetsbc (_phidget_ws._tcp., local.,
08/13/15 23:26:35,5496,".\zeroconf.c(652)",INFO,"DNSServiceBrowse_sbc_CallBack (Add): PhidgetSBC (00:1b:0b:10:1b:d6)"
08/13/15 23:26:35,5496,".\zeroconf.c(421)",INFO,"DNSServiceQueryRecord_sbc_CallBack: PhidgetSBC\032(00:1b:0b:10:1b:d6)
08/13/15 23:26:35,5496,".\zeroconf.c(450)",INFO,"DNSServiceBrowse_Phidget_CallBack: Phidget InterfaceKit 8/8/8 (413179
08/13/15 23:26:35,5496,".\zeroconf.c(342)",INFO,"DNSServiceQueryRecord_Phidget_CallBack: Phidget\032InterfaceKit\0328/
08/13/15 23:26:35,5612,".\csocketopen.c(161)",INFO,"Starting WSA..."
08/13/15 23:26:35,5612,".\csocketopen.c(168)",INFO,"Started WSA Successfully"
08/13/15 23:26:35,5612,".\zeroconf.c(943)",INFO,"DNSServiceResolve_CallBack: Phidget\032InterfaceKit\0328/8/8\032(4131
08/13/15 23:26:35,5612,".\csocketopen.c(1121)",INFO,"Want to connect to server: phidgetsbc.local.:5001"
08/13/15 23:26:35,5612,".\zeroconf_lookup.c(709)",INFO,"mdns: Couldn't open nss_mdns configuration file /etc/nss_mdns.
08/13/15 23:26:35,5612,".\csocketopen.c(1228)",ERR,"connect(phidgetsbc.local.:5001): WSA error 10014"
08/13/15 23:26:35,5612,".\zeroconf.c(943)",INFO,"DNSServiceResolve_CallBack: Phidget\032InterfaceKit\0328/8/8\032(4131
08/13/15 23:26:35,5612,".\csocketopen.c(1121)",INFO,"Want to connect to server: phidgetsbc.local.:5001"
08/13/15 23:26:35,5612,".\csocketopen.c(1228)",ERR,"connect(phidgetsbc.local.:5001): WSA error 10014"
08/13/15 23:26:35,5612,".\zeroconf.c(943)",INFO,"DNSServiceResolve_CallBack: Phidget\032InterfaceKit\0328/8/8\032(4131
08/13/15 23:26:35,5612,".\csocketopen.c(1121)",INFO,"Want to connect to server: phidgetsbc.local.:5001"
08/13/15 23:26:35,5612,".\csocketopen.c(1228)",ERR,"connect(phidgetsbc.local.:5001): WSA error 10014"
08/13/15 23:26:36,5612,".\zeroconf.c(943)",INFO,"DNSServiceResolve_CallBack: Phidget\032InterfaceKit\0328/8/8\032(4131
08/13/15 23:26:36,5612,".\csocketopen.c(1121)",INFO,"Want to connect to server: phidgetsbc.local.:5001"
08/13/15 23:26:36,5612,".\csocketopen.c(1228)",ERR,"connect(phidgetsbc.local.:5001): WSA error 10014"
08/13/15 23:26:36,5612,".\zeroconf.c(943)",INFO,"DNSServiceResolve_CallBack: Phidget\032InterfaceKit\0328/8/8\032(4131
08/13/15 23:26:36,5612,".\csocketopen.c(1121)",INFO,"Want to connect to server: phidgetsbc.local.:5001"
08/13/15 23:26:36,5612,".\csocketopen.c(1228)",ERR,"connect(phidgetsbc.local.:5001): WSA error 10014"
08/13/15 23:26:36,5612,".\zeroconf.c(943)",INFO,"DNSServiceResolve_CallBack: Phidget\032InterfaceKit\0328/8/8\032(4131
08/13/15 23:26:36,5612,".\csocketopen.c(1121)",INFO,"Want to connect to server: phidgetsbc.local.:5001"
08/13/15 23:26:36,5612,".\csocketopen.c(1228)",ERR,"connect(phidgetsbc.local.:5001): WSA error 10014"
08/13/15 23:26:36,5612,".\zeroconf.c(943)",INFO,"DNSServiceResolve_CallBack: Phidget\032InterfaceKit\0328/8/8\032(4131
08/13/15 23:26:36,5612,".\csocketopen.c(1121)",INFO,"Want to connect to server: phidgetsbc.local.:5001"
08/13/15 23:26:36,5612,".\csocketopen.c(1228)",ERR,"connect(phidgetsbc.local.:5001): WSA error 10014"
08/13/15 23:26:37,5612,".\zeroconf.c(943)",INFO,"DNSServiceResolve_CallBack: Phidget\032InterfaceKit\0328/8/8\032(4131
08/13/15 23:26:37,5612,".\csocketopen.c(1121)",INFO,"Want to connect to server: phidgetsbc.local.:5001"
08/13/15 23:26:37,5612,".\csocketopen.c(1228)",ERR,"connect(phidgetsbc.local.:5001): WSA error 10014"
08/13/15 23:26:37,5612,".\zeroconf.c(943)",INFO,"DNSServiceResolve_CallBack: Phidget\032InterfaceKit\0328/8/8\032(4131
08/13/15 23:26:37,5612,".\csocketopen.c(1121)",INFO,"Want to connect to server: phidgetsbc.local.:5001"
08/13/15 23:26:37,5612,".\csocketopen.c(1228)",ERR,"connect(phidgetsbc.local.:5001): WSA error 10014"
08/13/15 23:26:37,5612,".\zeroconf.c(943)",INFO,"DNSServiceResolve_CallBack: Phidget\032InterfaceKit\0328/8/8\032(4131
08/13/15 23:26:37,5612,".\csocketopen.c(1121)",INFO,"Want to connect to server: phidgetsbc.local.:5001"
08/13/15 23:26:37,5612,".\csocketopen.c(1228)",ERR,"connect(phidgetsbc.local.:5001): WSA error 10014"
08/13/15 23:26:38,5612,".\zeroconf.c(943)",INFO,"DNSServiceResolve_CallBack: Phidget\032InterfaceKit\0328/8/8\032(4131
08/13/15 23:26:38,5612,".\csocketopen.c(1121)",INFO,"Want to connect to server: phidgetsbc.local.:5001"
08/13/15 23:26:38,5612,".\csocketopen.c(1228)",ERR,"connect(phidgetsbc.local.:5001): WSA error 10014"
```

Figure B05: The above data was generated from the legacy SBC in Figure B04.

Figure B06: The above circuit board shows the RFID read/write device that we used in our design, emulation and testing.

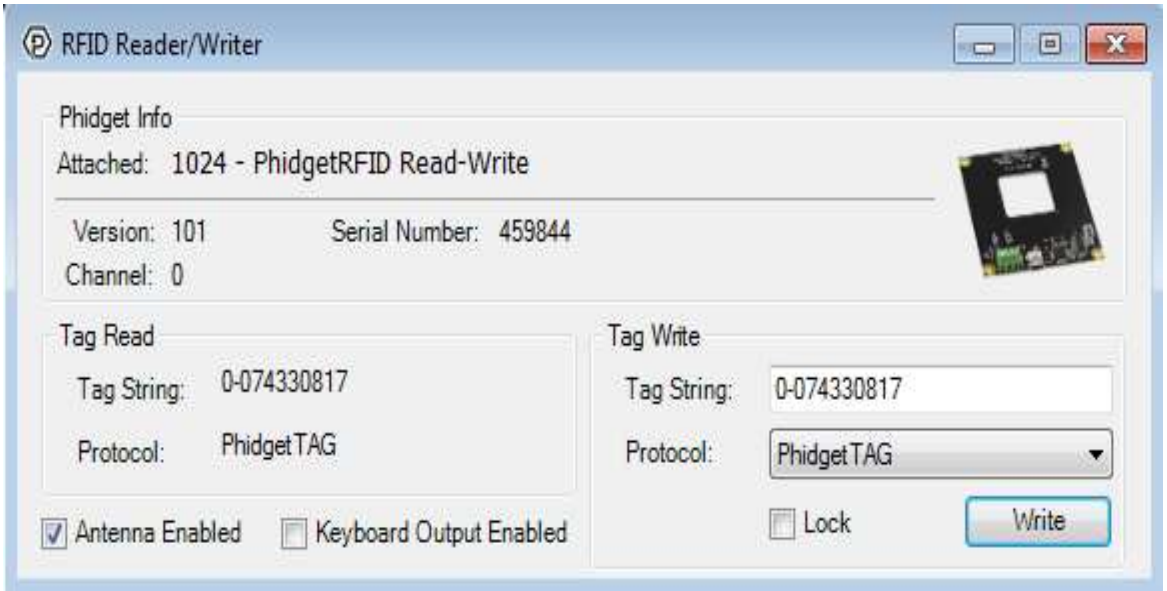


Figure B07: The data shows the fresh reading from an RFID tag. This reading represented our early transducer electronics data sheets (TEDS).

```
INFO [phidget22][2017-08-06T14:36:41]:***** Logging enabled *****
 INFO [_phidget22usb][2017-08-27T03:06:46]:Attaching Phidget:
 \\?\hid#vid_06c2&pid_0034#7&10b7b006&0&0000#{4d1e55b2-f16f-11cf-88cb-  001111000030}
 INFO [_phidget22usb][2017-08-27T03:06:56]:
 Opened USB Device: 0x718
 INFO [phidget22][2017-08-27T03:06:56 usb.c+391
 PhidgetUSBReadThreadFunction()]:
 PhidgetRFID Read-Write(1024) (459844):
 ReadThread starting
 INFO [phidget22][2017-08-27T03:06:56 rfiddevice.c+559
 tagTimerThreadFunction()]:
 tagTimerThread running
 INFO [_phidget22usb][2017-08-27T03:18:28]:
 Closing USB Device: 0x718
 INFO [phidget22][2017-08-27T03:18:28 usb.c+421
 PhidgetUSBReadThreadFunction()]:
 PhidgetRFID Read-Write(1024) (459844):
 ReadThread exiting normally (signaled by Phidget_close)
 INFO [phidget22][2017-08-27T03:18:28 rfiddevice.c+607
 tagTimerThreadFunction()]:
 tagTimerThread exiting normally
```

Figure B08: Raw python code for read/write sequence of an RFID tag. One of our emulation/simulation data collection process.

Figure B09: A snapshot of our initial RFID tag setup and programming for data collection and tests.

APPENDIX C: SPECIFICATIONS AND DATA COLLECTION INFORMATION

Consumer IR

The 1055 can send and receive data encoded in various fashions as pulses of infrared light. The various encoding that the 1055 supports are grouped under the general term *Consumer IR* or *CIR*. CIR is generally used to control consumer products such as TVs, DVD players, etc. with a wireless remote control, but in general can be used for any application that needs to transmit low speed data wirelessly.
CIR is a low speed protocol - commands generally contain no more then 32-bits of data with a bit rate of at the most 4000 bits/second, but usually much less. There is no concession for anti-collision, so only one code can be transmitting at any time. Transmission distance depends on the power of the transmitter, but needs to be line of sight - though generally this can include bouncing off walls/ceilings, etc.
CIR data is transmitted using a modulated bit stream. Data is encoded in the length of the pulses spaces between pulses, of IR light. The pulses of IR light are themselves modulated at a much higher frequency (usually ~38kHz) in order for the receiver to distinguish CIR data from ambient room light

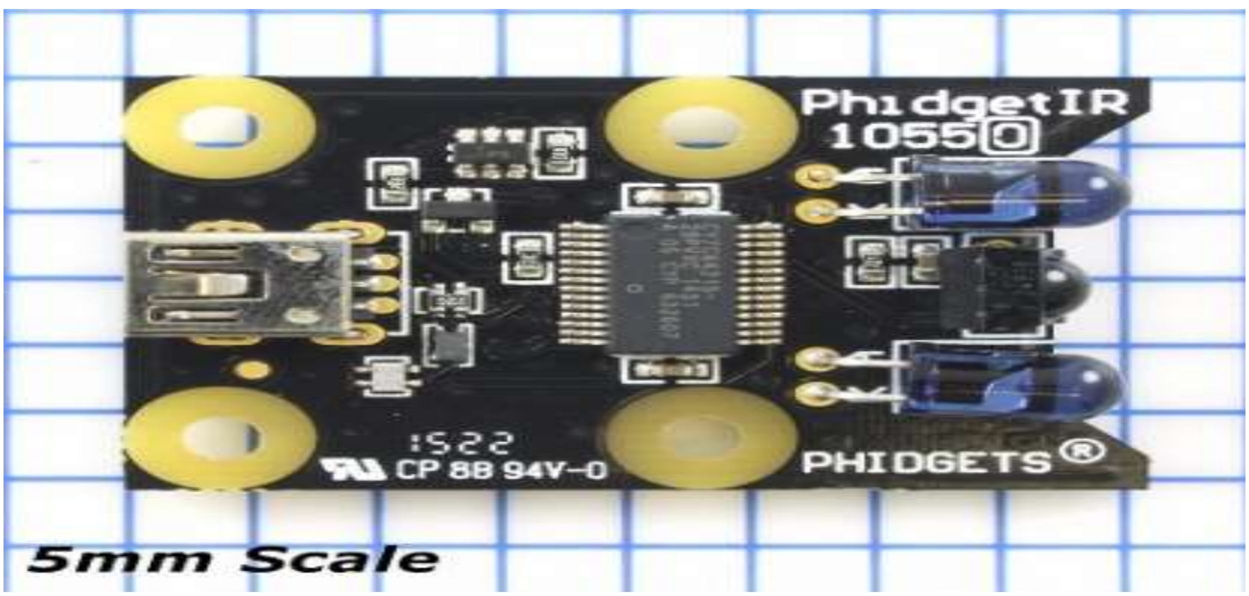


Figure C01: The above information describes and shows a photo of the infrared (IR) reader that we used to collect our infrared remote simulation data.

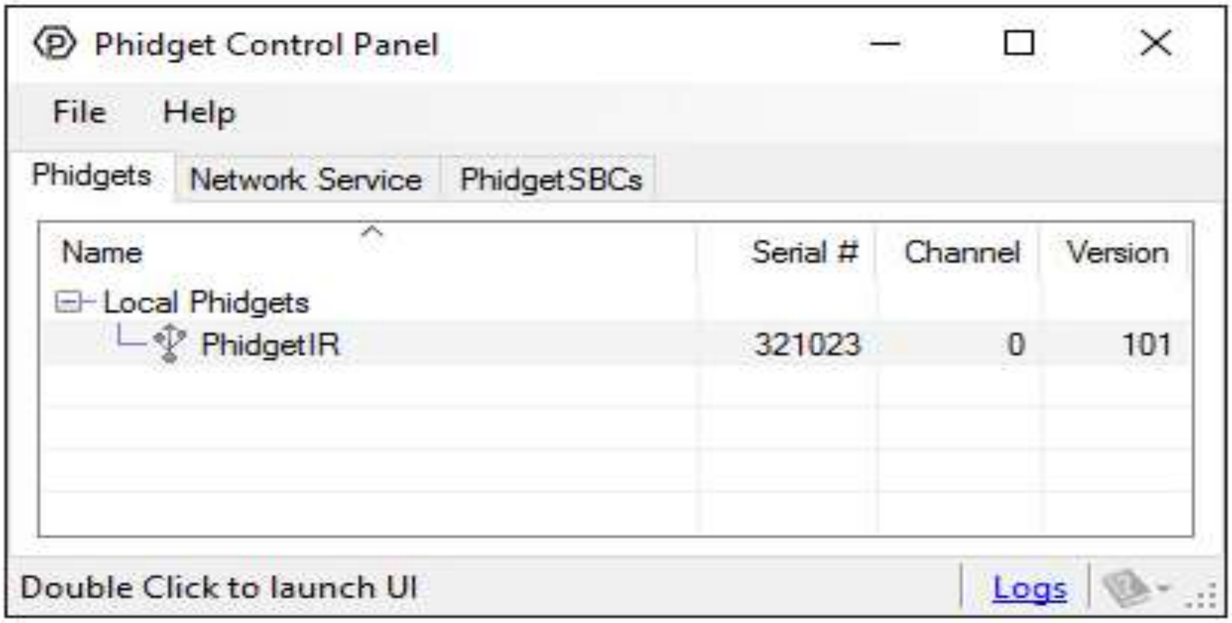


Figure C02: The above diagram shows the control panel entry from the PhidgetsSBC single board computer. This entry shows the registered serial number of the attached Phidgets IR reader.

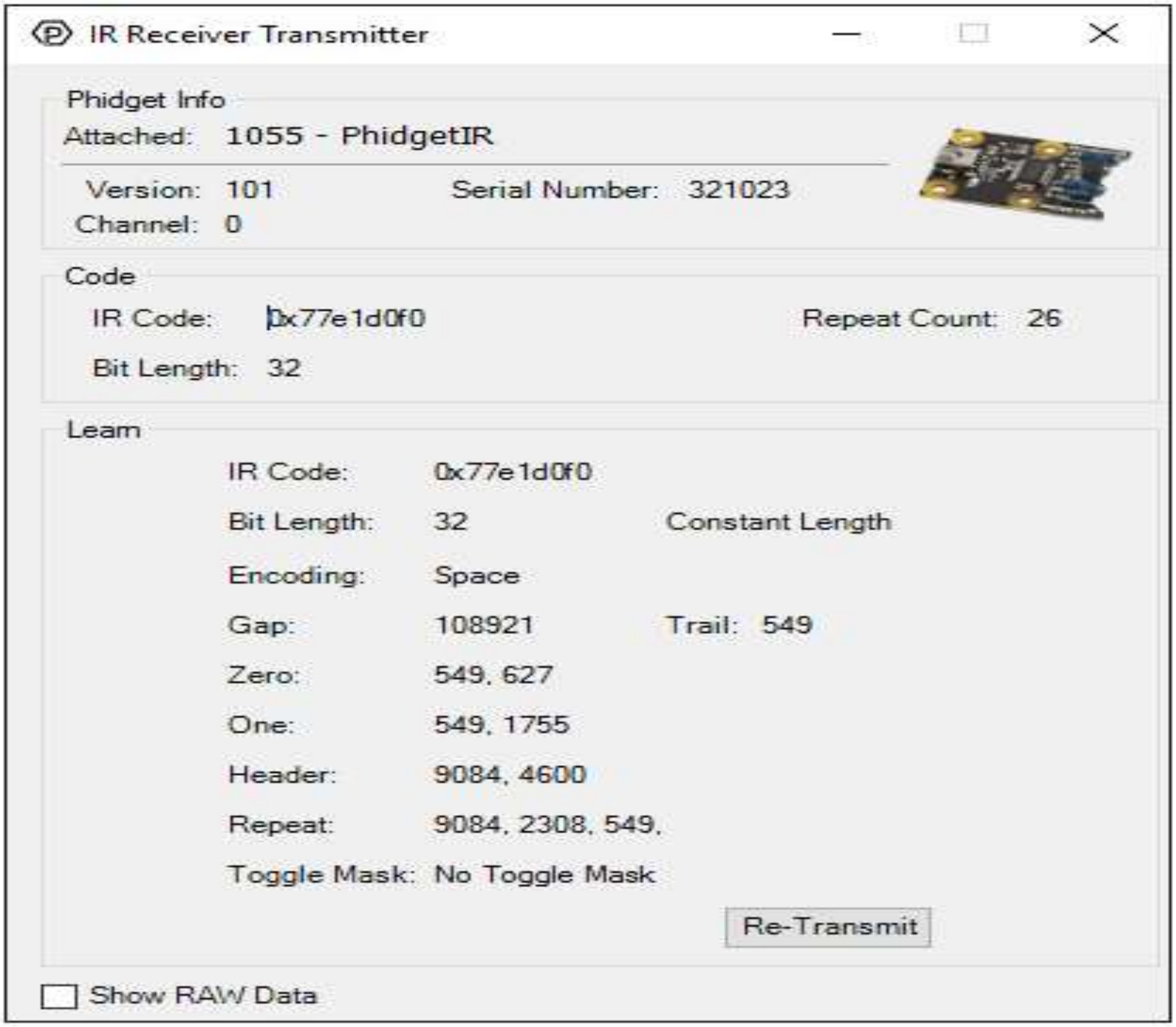


Figure C03: The above diagram shows a fresh reading of the IR reader. The data show represents early transducer electronics data sheet data from our IR reader device.

	Bit Length	Allowable Range
Project ID	14	33 - 0817
Street Name and Number	15	0- 1024
Current Temp and Humidity	5	A – Z (data type Chr5)
Version Number	6	0 - 63
Serial Number	24	0 - 08330817

Figure C04: The above table shows one of the designs that we tested as our custom TEDS datasheet.

Item	Bits	Options Mandatory/Optional	Special Features
1.) Header	XX	**M**/O	
2.) Speed	XX	M/O	Pole Mounted
3.) Time	X	**M**/O	RTC w/WWV
4.) Date	X	**M**/O	RTC w/WWV
5.) Humidity	X	M/O	O.D - Local
6.) Temp	X	M/O	O.D - Local
7.) Wind Speed	XX	M/O	Pole Mounted
8.) Visibility	X	M/O	Pole Mounted [cam]
9.) Rain	X	M/O	Pole Mounted
10.) Snow	X	M/O	Pole/Gnd – O.D.
11.) Ice	X	M/O	Pole/Gnd – O.D.
12.) H2O Level	X	M/O	Pole/Gnd – O.D.
13.) Location	XX	M/O	Pole/Gnd – O.D.
14.)			

Figure C05: Optional TEDS items for datagram considerations – RFID case study

APPENDIX D: REFERENCE RELATED INFORMATION

Safety by the Numbers

- An estimated **39,141** people lost their lives on all modes of our transportation system in 2017. The vast majority—37,133 deaths—were from motor vehicle crashes[A,B]
- *Driver Factors:* Of all serious motor vehicle crashes, **94 percent** involve driver-related factors, such as impaired driving, distraction, and speeding or illegal maneuvers.

  In 2017:

  - Nearly **11,000** fatalities involved drinking and driving.[B]
  - Speeding was a factor in nearly **10,000** highway fatalities.[B]
  - Nearly **3,500** fatal crashes* involved distracted drivers.[B]
- *Commercial Vehicles:* **13 percent** of annual roadway fatalities occur in crashes involving large trucks.[B]
- In 2017, **82 percent** of victims in fatal large truck crashes were road users who were not an occupant of the truck(s) involved.[B]
- *Professional Drivers:* Professional drivers are **ten times** more likely to be killed on the job, and nearly nine times more likely to be injured on the job compared to the average worker.[C]
- *Pedestrians:* **5,977** pedestrians were killed by motor vehicles in 2017, representing 16 percent of all motor vehicle fatalities.[B]
- *Highway-Rail Grade Crossings:* Over the past decade, highway rail grade crossing fatalities averaged **253** per year, representing about one-third of total railroad-related fatalities.[A]

Sources:

A U.S. Department of Transportation, Bureau of Transportation Statistics, special tabulation, September 8, 2018

B NHTSA 2017 Fatal Motor Vehicle Crashes: Overview (DOT HS 812 603)

C Beede, David, Regina Powers, and Cassandra Ingram, *The Employment Impact of Autonomous Vehicles*, U.S. Department of Commerce, Washington, DC: http://www.esa.doc.gov/sites/default/files/Employment%20Impact%20Autonomous%20Vehicles_0.pdf

* *This number is likely underreported.*

Figure D01: Recent statistics on Highway traffic accidents, injuries, and causes.

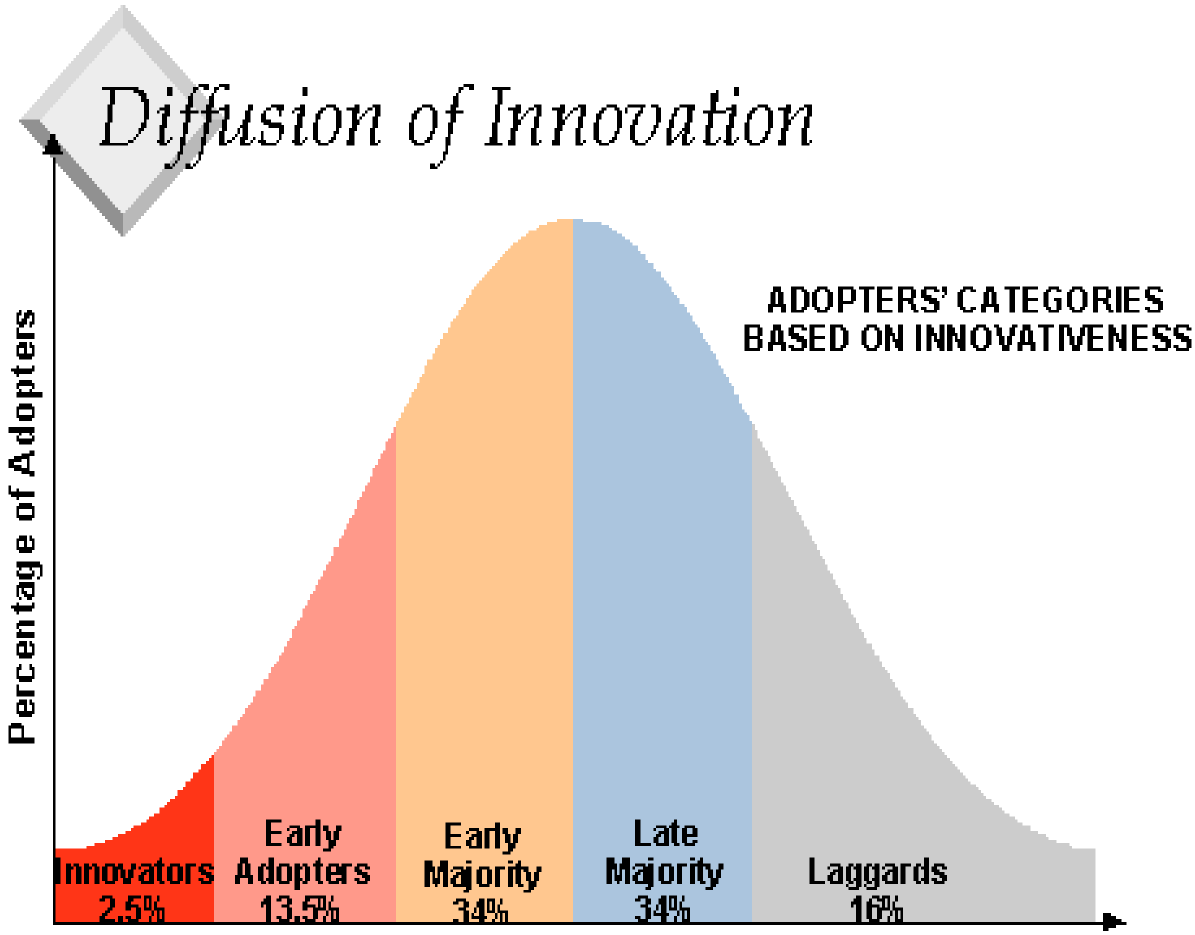


Figure D02: The above graphic shows the trends of various levels of adopters to new technological innovations. From the Everette Roger book, “Diffusion of Innovations”.

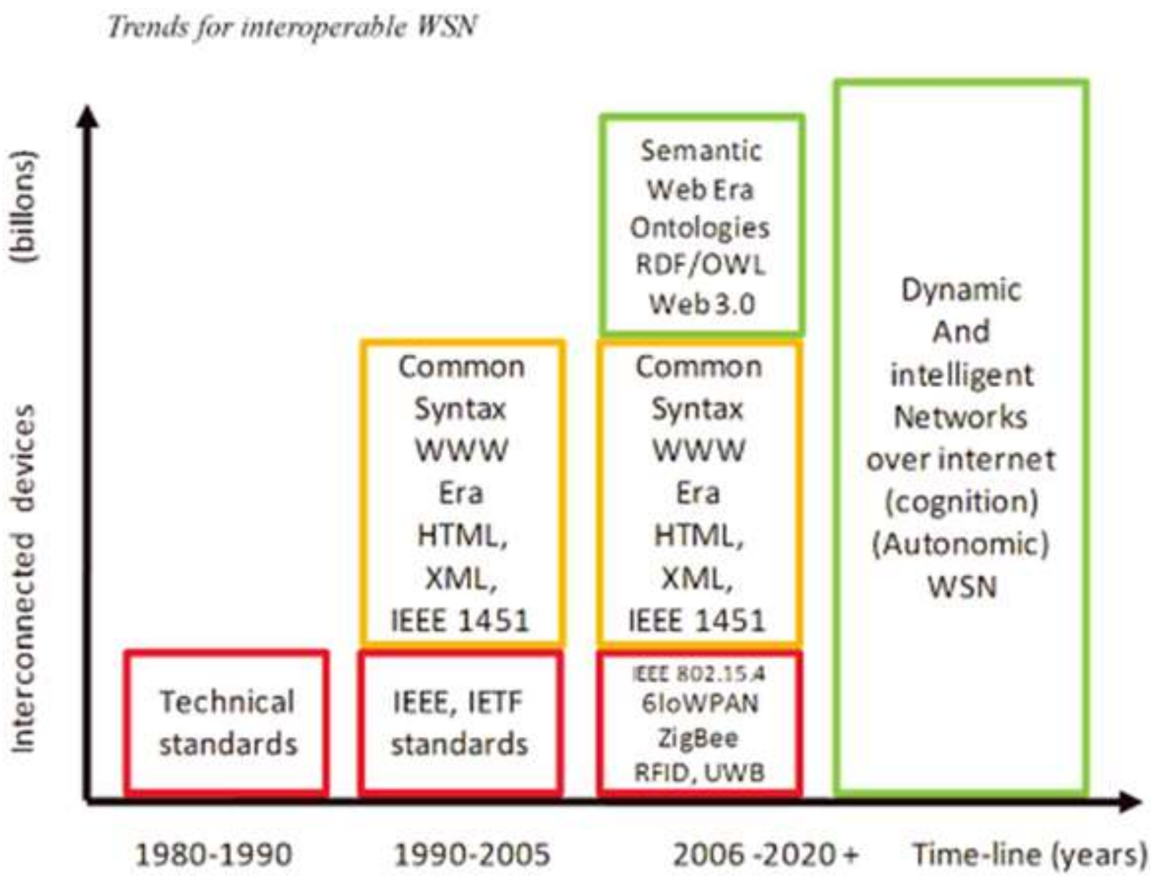


Figure D03: The above diagram shows the billions of interconnected devices plotted against the technology used at the time. Our technology combination of the web, XML and RFID are represented above the years 2006 – 2020. From: Wireless Sensor Networks and Energy Efficiency: Protocols, Noor Zaman.

	Levels of Autonomy	Existing Examples
1 Driver only	The vehicle is entirely under human control but may have some automated systems.	Cruise control, electronic stability control, anti-lock brakes
2 Driver assistance	The steering and/or acceleration are automated but the driver must control the other functions.	Adaptive cruise control: distance to car in front maintained. Parking assistant: steering is automated, driver controls accelerator and brakes.
3 Partial autonomy	The driver does not control steering or acceleration but is expected to be attentive at all times and take back control instantaneously when required.	Adaptive cruise control with lane keeping. Traffic jam assistance.
4 High autonomy	Vehicles are able to operate autonomously for some portions of the journey. Transfer of control back to the human driver happens with some warning.	Prototype vehicles.
5 Full autonomy	The vehicle is capable of driving unaided for the entire journey with no human intervention – potentially without a human in the car.	None

Table 1: Adapted from Autonomous Road Vehicles - POSTnote 443, September 2013, Dr Chandrika Nath, Parliamentary Office of Science and Technology, Parliamentary Copyright 2013

Figure D04: The above chart shows us how far we have come with example of levels of autonomy in connected cars. From: Lloyd's of London 071615

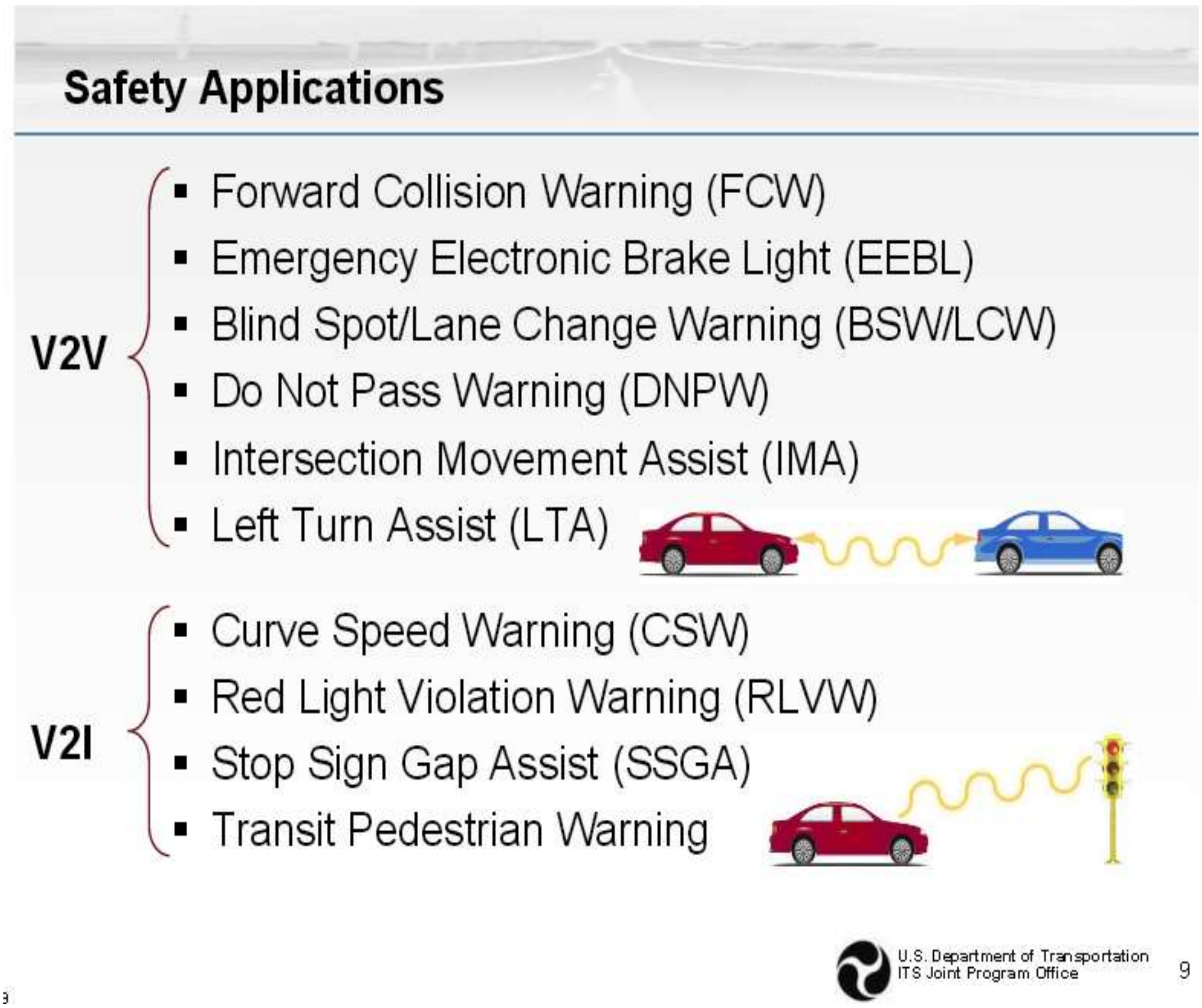


Figure D05: The above chart is an example of the charts and graphs that we studied in order to help us produce competitive designs.

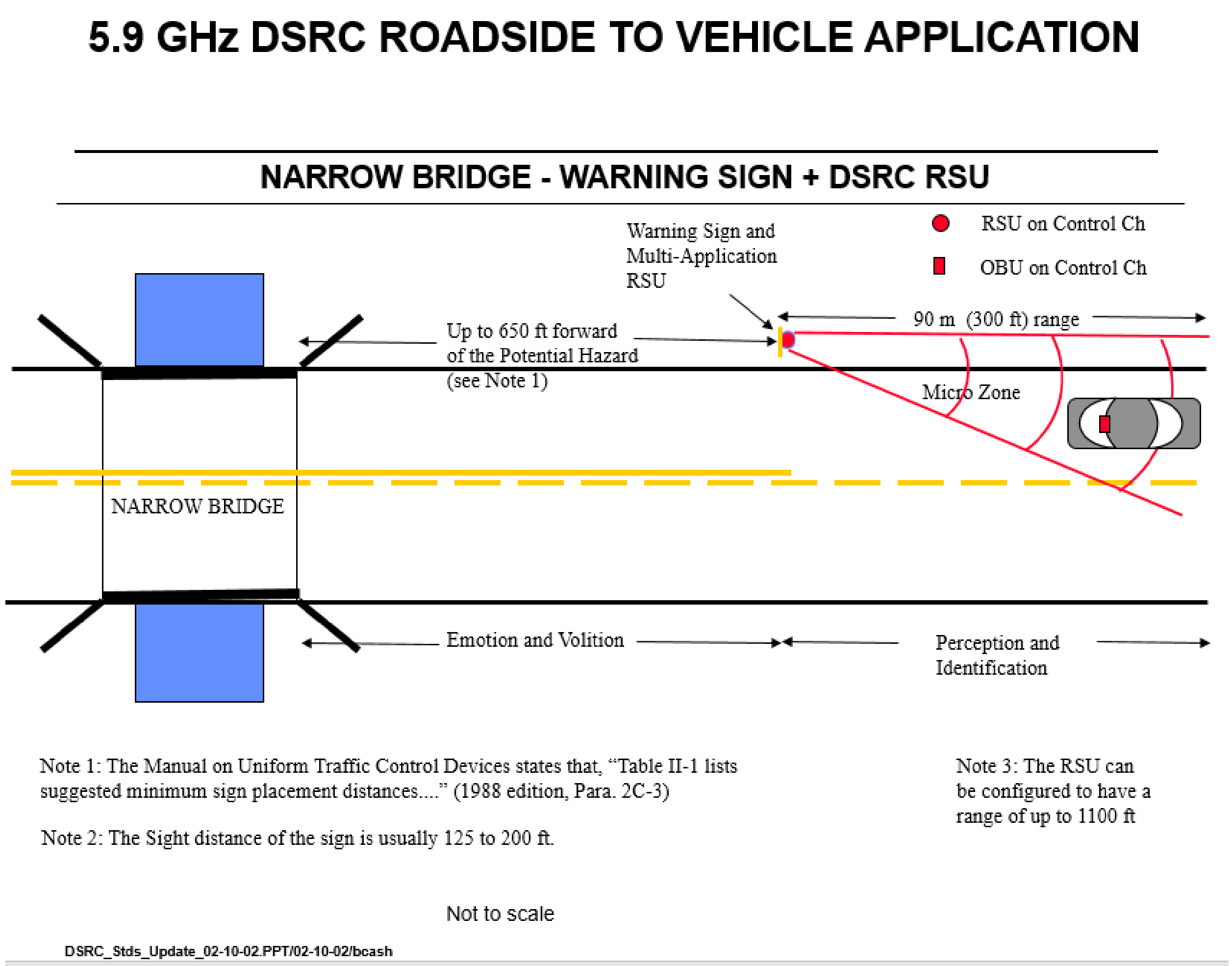


Figure D06: The above chart is an example of the charts and graphs that we studied in order to help us produce competitive designs.

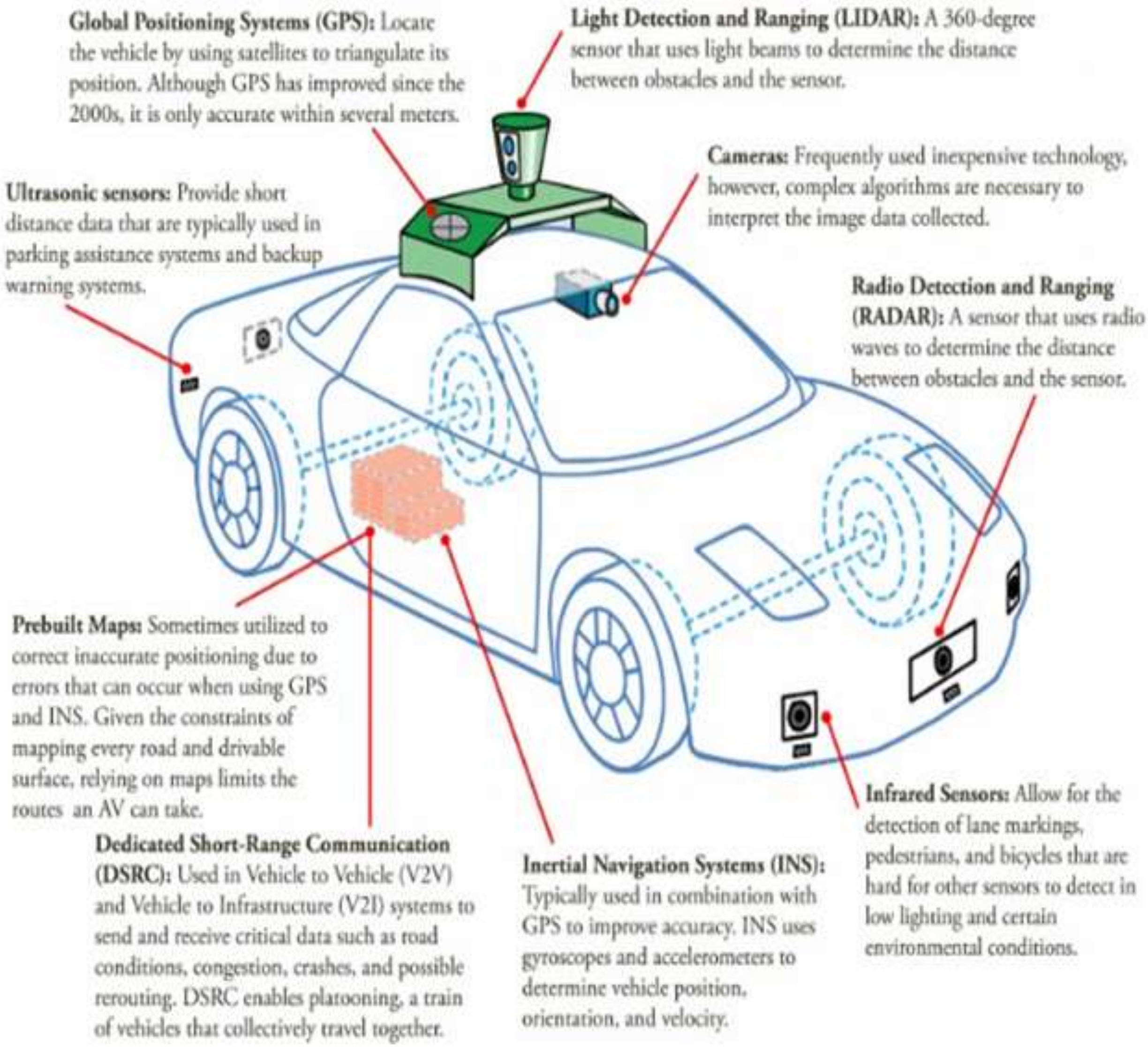


Figure D07: The above chart is an example of the charts and graphs that we studied in order to help us produce competitive designs.

DSRC CAPABILITIES

(in the designated ITS RADIO SERVICE bands)

PARAMETERS	902 - 928 MHz Band	5850 - 5925 MHz Band
SPECTRUM USED	12 MHz (909.75 to 921.75 MHz)	75 MHz
DATA RATE	0.5 Mbps	6 Mbps - 27 Mbps
COVERAGE	Large distances between communication zones	Overlapping communication zones needed and allowed
ALLOCATION STATUS	No protection	Primary Status (high protection)
INTERFERENCE POTENTIAL	Many 900 MHz Phones, Many Rail Car AEI Readers, Many Spread Spectrum Devices, Wind Profile Radars	Sparsely located Military Radars, Very Sparsely located Satellite Uplink
MAXIMUM RANGE	300 ft (at required- 30 dBm sensitivity)	1000 m (~ 3000 ft)
CHANNEL CAPACITY	1 to 2 channels	7 channels
POWER (Downlink)	Nominally less than 40 dBm (10 W)	Nominally less than 33 dBm (2 W)*
POWER (Uplink)	Nominally less than 6 dBm (< 4mW)	Nominally less than 33 dBm (2 W)*

Figure D08: The above chart is an example of the charts and graphs that we studied in order to help us produce competitive designs.

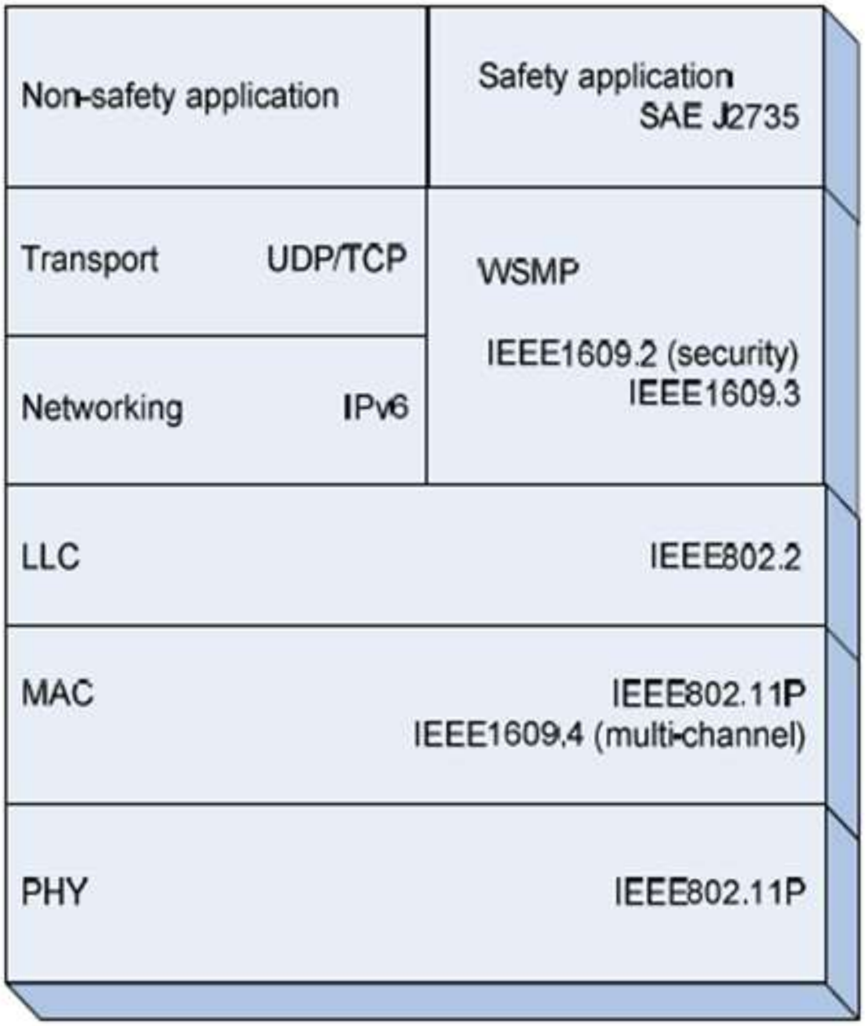


Figure D09: The above chart is an example of the WAVE protocol Stack and its associated standards. We studied this chart in order to help us produce our competitive designs.

IEEE 802.11p

- 802.11p is specified as an amendment to 802.11
- Major differences with 802.11

	802.11b	802.11p
Network acquisition	Association	Fast
Basic Service Set (BSS)	Required	Can operate without first forming a BSS
Latency		Low (for safety applications)
Frequency band	2.4 GHz	5.85-5.925 GHz
Environment	Indoor, low-mobility	Outdoor high-mobility
Number of channels	3 channels	7 channels, each 10MHz
Physical layer	20 MHz per channel	10 MHz per channel

Figure D10: The above chart is an example of the charts and graphs that we studied in order to help us produce competitive designs.

APPENDIX E: CURRENT LAWS, POLICIES AND REGULATIONS INFORMATION

pennsylvania
DEPARTMENT OF TRANSPORTATION

Connected and Automated Vehicle Terminology

A vehicle may be connected to some degree, or have some level of automation, or both. The hardware, software, and applications in each area are different, with different terminology, though connected and automated systems my complement each other. In addition, a vehicle may or may not also be electric or shared (e.g., part of a fleet, car sharing program, or a microtransit service).

Connected Vehicle

A ***connected vehicle (CV)*** enables safe, interoperable networked wireless communications among vehicles, roadside infrastructure, and others. The following are examples of how CVs can interact with other vehicles, infrastructure, etc.

- ***Vehicle-to-Infrastructure (V2I)*** is considered the next generation of intelligent transportation systems (ITS). V2I technologies capture vehicle-generated traffic data, wirelessly providing information such as advisories from the infrastructure to the vehicle that inform the driver of safety, mobility, or environment-related conditions. State and local agencies are likely to install V2I infrastructure alongside or integrated with existing ITS equipment.
- ***Vehicle-to-Vehicle (V2V)*** communications for safety is the wireless exchange of data among vehicles traveling in the same vicinity that offers opportunities for significant safety improvements.
- ***Vehicle-to-Everything (V2X)*** communication is the passing of information from a vehicle to any entity that may affect the vehicle, and vice versa. It is a vehicular communication system that incorporates other more specific types of communication as V2I, V2V, V2P (Vehicle-to-Pedestrian), V2D (Vehicle-to-Device) and V2G (Vehicle-to-Grid).

Figure E01: The above graphics are examples of the policies, laws, and regulations that we studied in order to help us produce competitive designs.

SAE LEVEL	NAME	NARRATIVE DEFINITION
Driver performs part or all of the dynamic driving task		
0	No Automation	The performance by the driver of the entire *dynamic driving task*, even when enhanced by active safety systems.
1	Driver Assistance	The sustained and *operational design domain*-specific execution by a driving automation system of either the lateral or the longitudinal vehicle motion control subtask of the *dynamic driving task* (but not both simultaneously) with the expectation that the driver performs the remainder of the *dynamic driving task*.
2	Partial Driving Automation	The sustained and *operational design domain*-specific execution by a driving automation system of both the lateral and longitudinal vehicle motion control subtasks of the dynamic driving task with the expectation that the driver completes the object and event detection and response subtask and supervises the driving automation system.
Automated Driving System ("System") performs the entire dynamic driving task (while engaged)		
3	Conditional Driving Automation	The sustained and *operational design domain*-specific performance by an *Automated Driving System* of the entire *dynamic driving task* with the expectation that the *dynamic driving task* fallback-ready user is receptive to ADS-issued requests to intervene, as well as to *dynamic driving task* performance-relevant system failures in other vehicle systems, and will respond appropriately.
4	High Driving Automation	The sustained and *operational design domain*-specific performance by an *Automated Driving System* of the entire *dynamic driving task* and *dynamic driving task* fallback without any expectation that a user will respond to a request to intervene.
5	Full Driving Automation	The sustained and unconditional (i.e., not *operational design domain*-specific) performance by an ADS of the entire *dynamic driving task* and *dynamic driving task* fallback without any expectation that a user will respond to a request to intervene.

Figure E02: The above graphics are examples of the policies, laws, and regulations that we studied in order to help us produce competitive designs.

pennsylvania
DEPARTMENT OF TRANSPORTATION

Vehicle automation is enabled by sensors – e.g., radar, lidar, ultrasonic, photonic mixer device (PMD), cameras, night vision devices – and by evolving sensor fusion hardware and software. An equipped vehicle can perceive and monitor near and far fields in every direction, identifying other vehicles, bicycles, pedestrians, traffic control devices, weather, hazardous conditions, etc. The extent to which vehicle systems can process this incoming data, make real time decisions, and actuate control of the vehicle is a key determination of level of automation.

- From Level 1, vehicles are equipped with one or more ***Advanced Driver Assistance System (ADAS)***, e.g., brake assist, adaptive cruise control, lane departure warning, and many others.
    - The wide range of ADAS already contribute to safety, and their continued improvement are essential for vehicles at higher levels of automation. The National Safety Council supports a consumer-oriented site, MyCarDoesWhat.org, that explains dozens of ADAS applications.
- At Level 2, a vehicle has some capability to control steering angle and velocity, but a critical aspect of this level is that a licensed driver must actively monitor the driving environment. This level is currently available to consumers in limited vehicle models from at least two automakers.
- At Level 3 and up, the vehicle system is responsible for monitoring the driving environment, but at Level 3 a licensed driver must remain ready to quickly regain situational awareness and vehicle control. The dynamic driving task capability depends on conditions, and the human is responsible for fallback and safety operation.
    - NHTSA refers to a Level 3-5 vehicle as an ***Automated Driving System (ADS)***, and American Association of Motor Vehicle Administrators (AAMVA) and others may still use the term ***Highly Automated Vehicle (HAV)***.
- A Level 4 vehicle may be referred to as ***driverless***, ***self-driving***, and ***autonomous*** vehicles. These are capable of operating in defined conditions or circumstances, and the system is capable of fallback operation.
- Level 5 adds the capability to perform in any circumstance.

Figure E03: The above graphics are examples of the policies, laws, and regulations that we studied in order to help us produce competitive designs.

Automated Driving Systems 2.0: A Vision for Safety
September 2017
U.S. Department of Transportation (DOT) / National Highway Traffic Safety Administration (NHTSA)
https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

This document replaces the Federal Automated Vehicle Policy released in 2016. This updated policy framework offers a path forward for the safe deployment of automated vehicles by encouraging new entrants and ideas that deliver safer vehicles; making Department regulatory processes more nimble to help match the pace of private sector innovation; and supporting industry innovation and encouraging open communication with the public and with stakeholders.

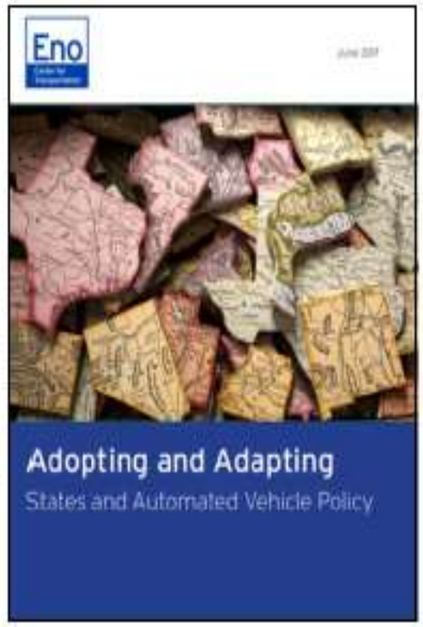
In this document, NHTSA offers a nonregulatory approach to automated vehicle technology safety. Section 1: Voluntary Guidance for Automated Driving Systems supports the automotive industry and other key stakeholders as they consider and design best practices for the testing and safe deployment of Automated Driving Systems (ADSs - SAE Automation Levels 3 through 5 – Conditional, High, and Full Automation Systems). It contains 12 priority safety design elements for consideration, including vehicle cybersecurity, human machine interface, crashworthiness, consumer education and training, and post-crash ADS behavior. Vehicles operating on public roads are subject to both Federal and State jurisdiction, and States are beginning to draft legislation to safely deploy emerging ADSs. To support this, NHTSA offers Section 2: Technical Assistance to States, Best Practices for Legislatures Regarding Automated Driving Systems. The section clarifies and delineates Federal and State roles in the regulation of ADSs. NHTSA remains responsible for regulating the safety design and performance aspects of motor vehicles and motor vehicle equipment; States continue to be responsible for regulating the human driver and vehicle operations. The section also provides Best Practices for Legislatures, which incorporates common safety-related components and significant elements regarding ADSs that States should consider incorporating in legislation. In addition, the section provides Best Practices for State Highway Safety Officials, which offers a framework for States to develop procedures and conditions for ADSs' safe operation on public roadways. It includes considerations in such areas as applications and permissions to test, registration and titling, working with public safety officials, and liability and insurance.

This document serves to support industry, Government officials, safety advocates, and the public.

Figure E04: The above document is an example of the policies, laws, and regulations that we studied in order to help us produce competitive designs.

Adopting and Adapting: States and Automated Vehicle Policy
June 2017
Eno Center for Transportation
http://www.enotrans.org/wp-content/uploads/2017/06/StateAV_FINAL-1.pdf

Provides a collection of policies concerning automated vehicles and outlines how they vary from state to state.



The major topics included about state automated vehicle policies are existing approaches to automated vehicles, state-level regulations, infrastructure investment and funding, and research and workforce training.

States have one of four approaches to automated vehicle policy:

1. They have no regulations or laws specifically for automated vehicles, but may be working to create laws.
2. They have explicitly expressed interest in automated vehicles but have passed no laws. Interest is expressed through executive orders, proclamations, studies, etc.
3. They explicitly allow automated vehicle testing. This is the case in MI, CA, UT, NV, and TN, which all have varying laws to create a framework for automated vehicle testing.
4. They have laws that allow fully automated vehicles to be deployed beyond the testing phase. Only FL and GA allow for the operation of driverless vehicles, while DC allows deployed fully automated vehicles only if a driver is still present.

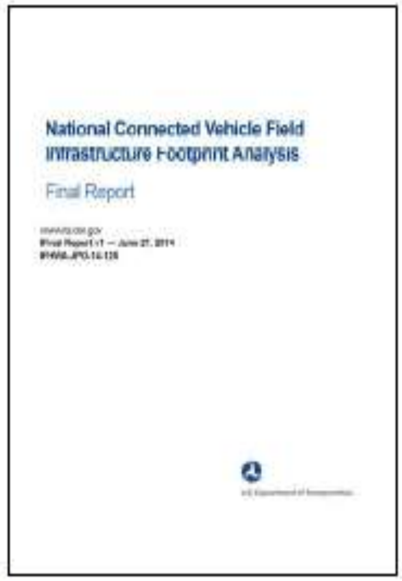
Although legislation varies by state, it will not necessarily attract or deter automated vehicle testing. While some states have steadily housed automated vehicle testing even before legislation was created, others have legislation in place but have attracted no major companies for testing. Some states have stricter regulations then others, potentially requiring certifications and specific reporting requirements.

It is important for states to invest in improving roadways and keeping them in a good state of repair to help facilitate automated vehicles. As this is not always the case, developers are beginning to work towards advancing systems to work with the current state of existing roadways.

Figure E05: The above graphics are examples of the policies, laws, and regulations that we studied in order to help us produce competitive designs.

National Connected Vehicle Field Infrastructure Footprint Analysis
June 2014
USDOT Intelligent Transportation Systems Joint Program Office
https://ntl.bts.gov/lib/52000/52600/52602/FHWA-JPO-14-125_v2.pdf

The American Association of State Highway and Transportation Officials (AASHTO), under the sponsorship of United States Department of Transportation (USDOT) and Transport Canada, undertook a Connected Vehicle Field Infrastructure Footprint Analysis to provide supporting information to agency decision-makers.



This document consists of a vision for a national footprint; a description of the background for and current research on connected vehicle deployments; a set of assumptions underlying the infrastructure footprint analysis; the applications analysis; the deployment concepts, the preliminary national footprint, including the value proposition, deployment objectives, context, scenarios, and experience to date; and a preliminary deployment and operations cost estimation. This document also includes:

- A description of the justification for and value of deployment of connected vehicle infrastructure.
- A compilation of the possible data, communications, and infrastructure needs of the priority applications.
- A set of generic deployment concepts and their needs under different operational conditions.
- A set of scenarios identifying how and where agencies might implement secure, connected vehicle infrastructure, including dedicated short range communications (DSRC); and what funding strategies they might use to support such deployment, and a synthesis of these scenarios into a preliminary national footprint of connected vehicle field infrastructure.
- A set of activities and timelines for deploying connected vehicle field infrastructure across and among State and local agencies.
- Estimates of potential costs for deployment, operations, and maintenance.
- Estimates of workforce and training requirements; and identification of policy and guidance needs.
- Identification of implementation challenges and institutional issues and identification of the timing by which those issues need to be resolved to achieve impactful deployment.

Figure E06: The above document is an example of the policies, laws, and regulations that we studied in order to help us produce competitive designs.

Connected and Automated Vehicles Pilots

In the last few years, connected and automated vehicle research and pilot projects have boomed rapidly. This report documents the most relevant pilot projects deployed. Through this process, the Pennsylvania Department of Transportation (PennDOT) Joint Statewide Connected and Automated Vehicles Strategic Plan will capture knowledge of the most current and successful projects and global best practices. This material will help ensure that Pennsylvania remains among the leaders in development and deployment of the one of the most beneficial transportation technologies.

North America

In North America, there are several major connected and automated vehicle (CAV) developments. At the national level, the US Department of Transportation (USDOT) is expanding its Connected Vehicle Pilot program and has selected sites for its first wave of deployments. Several new automated vehicle trials are in the works on several college campuses, theme parks, airports, downtown areas, etc. States with existing CAV testing centers, such as Michigan, Florida, and Virginia, are expanding and adding to their testing assets.

In September 2015, the USDOT Joint Program Office (JPO) initiated pilot deployments of connected vehicle applications in three locations – Wyoming, New York City, and Tampa. USDOT JPO intends for these pilot deployments to showcase the capabilities of connected vehicle (CV) technologies to improve multi-modal surface transportation system performance and enable enhanced performance-based system management. Each of the three selected deployment sites has completed the Concept Development Phase (Phase 1) of the program and are now in the Design/Build/Test Phase (Phase 2). USDOT expects the deployment sites to be complete and fully operational by May 2018. Once the deployment sites become fully operational, USDOT expects the pilot deployments to become a permanent part of the surface transportation system in these locations, providing a foundation upon which the agencies can expand and enhance their transportation systems management and operations capabilities.

Tampa Connected Vehicle Pilot Deployment

The goal of the Tampa Connected Vehicle Pilot Deployment (CVPD) is to transform the experience of automobile travelers, transit riders, and pedestrian by preventing crashes, enhancing traffic flow, improving transit trip times, and reducing emissions of greenhouse gases in the downtown Tampa area (1). The Tampa Hillsborough Expressway Authority (THEA) and its partner entities will be equipping buses, streetcars, and privately owned vehicles with CV technologies that will allow them to exchange safety and travel condition information with each other and with the infrastructure. The objectives of the Tampa CVPD are to:

- Reduce morning peak-hour delays and rear-end crashes on the Lee Roy Selmon Expressway's Reversible Express Lane (REL) exit to downtown Tampa.
- Reduce vehicle/pedestrian conflicts at a busy mid-block crosswalk near the Hillsborough County Courthouse.
- Support traffic signal optimization on commuting corridors in downtown Tampa.
- Enhance transit signal priority in the Marion Street Transitway.
- Reduce vehicle and pedestrian conflicts with the TECO Streetcar line in downtown Tampa.

Figure E07: The above graphics are examples of the policies, laws, and regulations that we studied in order to help us produce competitive designs. The above info was retrieved from the Pennsylvania Joint Statewide CAV Strategy Plan 2018

SMART Columbus

In December 2016, USDOT awarded the City of Columbus $50 million to serve as the demonstration locations for the Smart City Challenge (*6*). From a transportation perspective, a Smart City is one in which integrates data, applications, and technology to develop, first-of-its-kind smart transportation system to help people and goods move faster, cheaper, and more efficiently The objectives of the Smart City Challenge are as follows:

- Provide first-mile and last-mile service for transit users to connected underserved communities to jobs.
- Facilitate the movement of goods into and within a city.
- Coordinate data collection and analysis across systems and sectors.
- Reduce inefficiency in parking systems and payment.
- Limit the impacts of climate change and reduce carbon emissions.
- Optimize traffic flow on congested freeways and arterial streets.

The City of Columbus, along with their partners, have identified the following projects to be implemented as part of the Smart Columbus Deployment:

- **Integrated Data Exchange** — This project integrates data from multiple sources allowing stakeholders to make better decisions and solve problems to move people more efficiently.
- **Connected Vehicles** — This project installs DSRC devices in vehicles and in the infrastructure, that allows the deployment of safety and mobility applications.
- **Common Payment System** — This project integrates several diverse payment systems that would allow travelers to make only one payment across multiple modes.

- **Multimodal Trip Planning** — This system allows users to plan trips using multiple modes to reach their destination.
- **Smart Mobility Hubs** — This project allows multiple transportation users – cyclists, drivers, transit users – a place to meet to access the transportation network.
- **Smart Street Lighting** — This project adds light-emitting diode (LED) lights and Wi-Fi connectivity in residential areas.
- **Mobility Assistance** — This project focuses on developing technologies and system to help individuals with cognitive disabilities access the transportation system.
- **Enhanced Permit Parking** — This project is deploying technologies that would help reduce the infiltration of unwanted parking in residential areas.
- **Event Parking Management** — This project uses technologies to help users find parking during major events in downtown Columbus.
- **Delivery Zone Availability** — This project is intended to help commercial delivery vehicles to schedule and coordinate deliveries in downtown Columbus.
- **Connected Electric Autonomous Vehicles** — This project involves deploying six electric autonomous vehicles (EAVs) on set routes connecting popular retail and commercial hubs in northeast Columbus.
- **Truck Platooning** — This project permits the electronic coupling of long-haul trucks to allow them to move as a coordinated string on the freeway.
- **Interstate Truck Parking** — This project provides locations, facilities, and amenities for trucks to park in and around the Columbus area.

The City of Columbus is the early stage of system design and expects to begin rolling out these projects mid- to late 2018.

Figure E08: The above graphics shows some of the efforts that specific cities are undertaking in order to maintain a competitive edge as a smart city. Columbus Ohio has certainly show efforts to represent itself as a smart city that is receptive to the new idea of CAVs.

Ann Arbor Safety Pilot Model Deployment

The Safety Pilot Model Deployment (SPMD) was the first large-scale connected vehicle test in the United States. USDOT's purpose for the SPMD was to demonstrate the applicability of V2I and V2V communications to improve safety and to assist in potential rule making associated with the widespread deployment of these devices in the vehicle fleet. As a result, the USDOT, under the leadership of the University of Michigan Transportation Research Institute (UMTRI) acting as the test conductor, equipped nearly 3,000 vehicles and instrumented more than 70 miles of roadway in Ann Arbor, Michigan. The SPMD site encompassed the northeast, and a portion of the southeast corner of Ann Arbor, Michigan. Figure D-4 shows the locations of the SPMD corridors in Ann Arbor (*8*).

USDOT's objective of the SPMD was to support the evaluation of DSRC technology for V2V safety applications in a real-world, concentrated environment. The primary focus of the SPMD was to collect data to support: (1) the functional evaluation of V2V safety applications, (2) the assessment of the operational aspects of messages that support vehicle-to-infrastructure (V2I) safety applications, and (3) comprehension of the operational and implementation characteristics of a prototype security operating concept (*8*).

The deployers equipped the majority of the vehicles with a *vehicle awareness device* (VAD). VADs transmit the basic safety message only and do not perform any safety functions. They act as the "remote vehicles" or the "target vehicles." The SPMD installed VADs on passenger, medium-duty, heavy-duty, and transit vehicles. The VAD installations were a mix of personal and fleet vehicles.

PENNSYLVANIA JOINT STATEWIDE CAV STRATEGIC PLAN |

Figure E09: The above graphics are examples of the policies, laws, and regulations that we studied in order to help us produce competitive designs.

The deployers equipped other vehicles with *aftermarket safety devices* (ASD). The SPMD installed ASDs in passenger vehicles only. ASDs generate warnings with an audible cue to the driver. The SPMD deployed two additional ASD-like devices: the first on motorcycles (ASDM), and the other on one bicycle (ASDB). ASDMs transmit and receive messages, but do not provide warnings to the motorcycle driver. The ASDB received messages only (the opposite of the VAD) and did not provide any safety warnings to support data collection for bicycle crash avoidance research and analysis.

The SPMD also equipped commercial trucks with *retrofit safety device* (RSD) kits. The RSD is a type of aftermarket device but for the commercial fleet. Unlike the ASD used in passenger vehicles, the RSD connects to the truck's data bus, giving additional input for the safety warning threat assessment. The RSD installation also included a tablet to provide a visual cue in addition to the audio to the driver. The deployers installed RSD kits on two local Ann Arbor fleets. An offshoot of the RSD was the Transit Retrofit Platform (TRP). It was specifically designed for transit and installed on UM bus fleet for testing.

Last, there were two integrated device platforms: *integrated light vehicles* (ILV) and *commercial connected vehicle – integrated truck* (CCV-IT). Devices were connected to the vehicle data bus and had a suite of warnings that include visual, haptic, and audio cues. CAMP, as a subcontractor to USDOT, supplied the ILVs while Battelle provided the CCV-ITs.

On the infrastructure side, the SPMD installed DSRC devices known as roadside equipment (RSE) in Northeast Ann Arbor in the SPMD area. Also, the deployment agencies installed signal-phase-and-timing-enabled traffic signal controllers. The deployers developed an interface device to exchange signal time and phasing information between the traffic signal controllers and the RSEs. For TRP, the SPMD deployers also installed pedestrian detection hardware at the intersection in front of the University of Michigan Hospital.

Figure E10: The above graphics are examples of the policies, laws, and regulations that we studied in order to help us produce competitive designs. From: The Pennsylvania Joint Statewide CAV Strategic Plan.

Mcity

Mcity is a test facility built by the University of Michigan, in collaboration with the Michigan Department of Transportation, to provide a realistic, controlled environment for testing automated and connected vehicle technologies. The facility is located on a 32-acre site on the University of Michigan's North Campus. It consists of about 16 acres of roads and traffic infrastructure designed to replicate real-world urban and suburban conditions with approximately five lane-miles of roads with intersections, traffic signs and signals, sidewalks, simulated buildings, street lights, and obstacles, etc. The test facility includes the following attributes:

- 1000′ North/South straight.
- Various road surfaces (concrete, asphalt, brick, dirt).
- Variety of curve radii, ramps.
- Two, three, and four-lane roads.
- Round-about and "tunnels."
- Sculpted dirt and grassy areas.
- Variety of signage and traffic control devices.
- Fixed, variable street lighting.
- Crosswalks, lane delineators, curb cuts, bike lanes, grade crossings.
- Hydrants, sidewalks, etc.

Figure E11: The above information are examples of the policies, laws, and efforts that we studied in order to help us produce competitive designs. From: The Pennsylvania Joint Statewide CAV Strategic Plan.

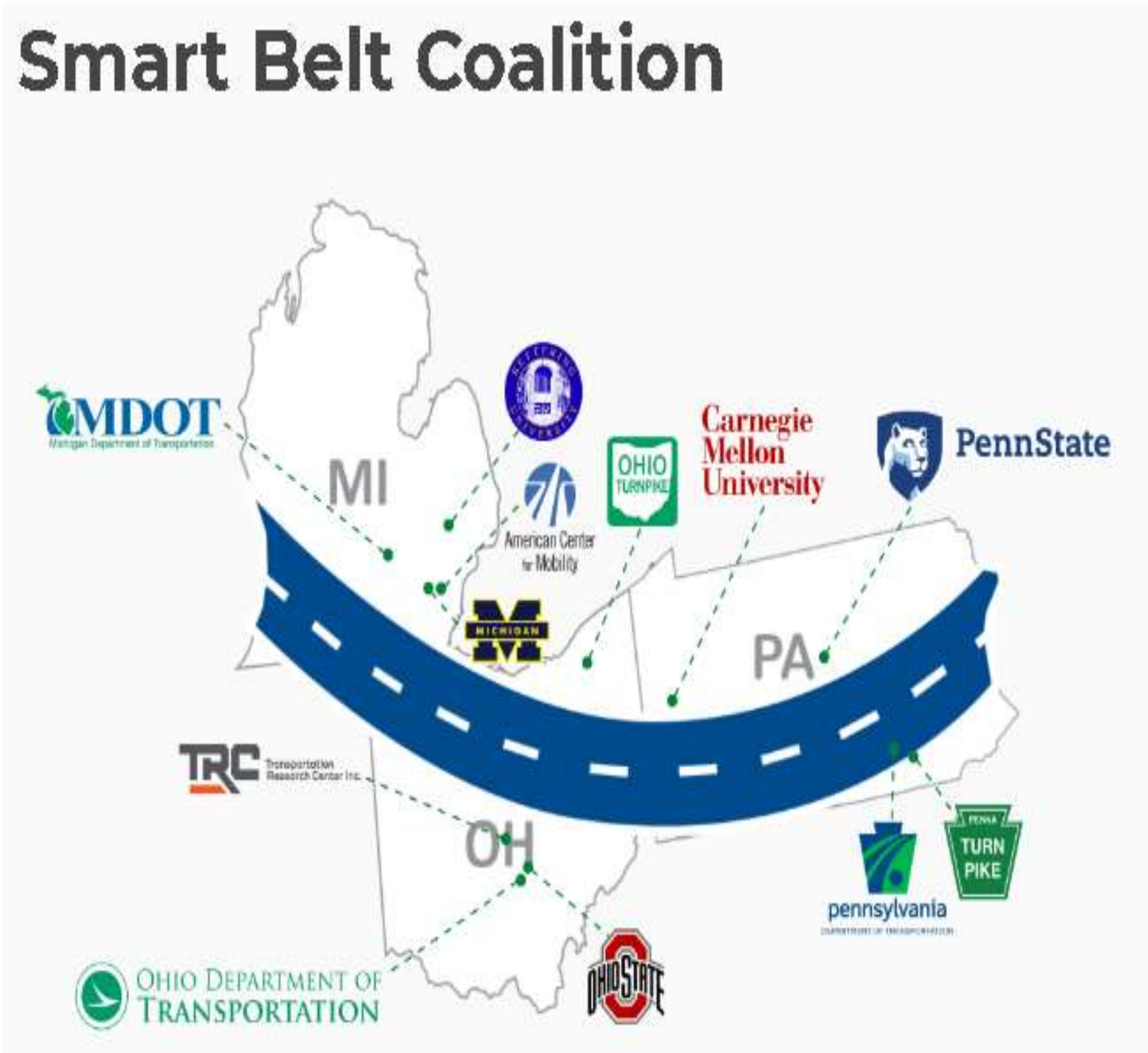


Figure E12: The above graphics are examples of the policies, laws, regulations and efforts that we studied in order to help us produce competitive designs. The Smart Belt Coalition was formed in 2016 and is a strategic partnership comprised of five transportation agencies and seven academic institutions throughout Michigan, Ohio, and Pennsylvania.

Persistent and non – persistent contention-based MAC protocols

By Dr.Malathi Veeraraghavan, 2011.

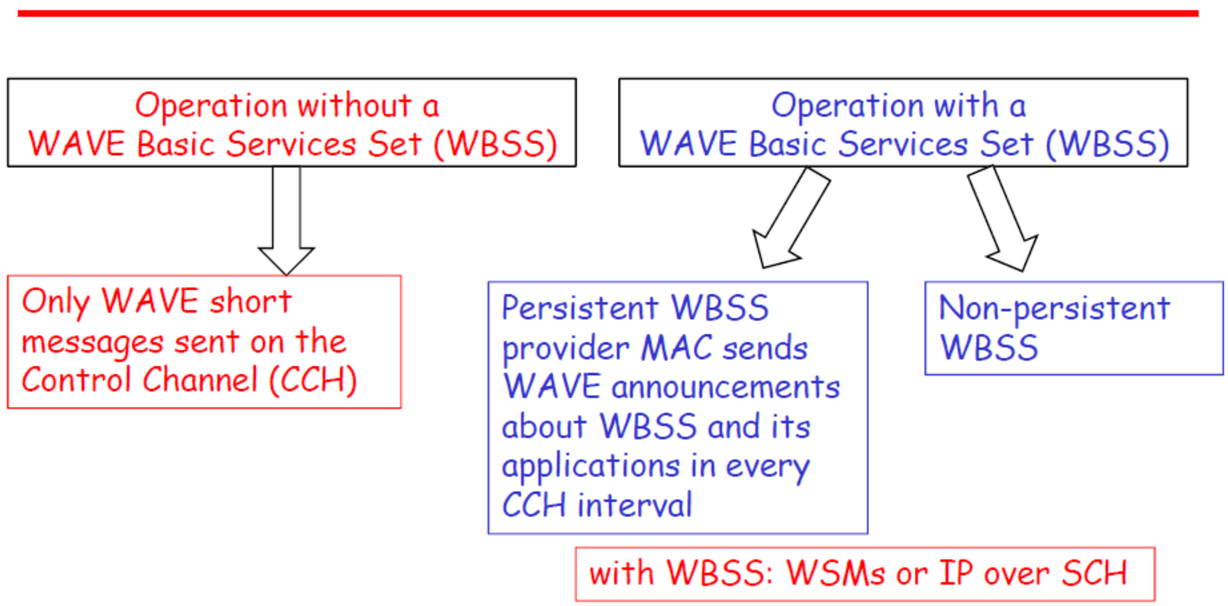


Figure E13: The above graphics are examples of the protocols that we studied in order to help us produce competitive designs. The above information also helped us further focus on our methods related research, testing and data collection.

- Active RFID vs. Passive RFID: What's the Difference?
-
- Long Answer:
- Passive RFID
- Generally speaking, three main parts make up in a passive RFID system – an RFID reader or interrogator, an RFID antenna, and RFID tags. Unlike active RFID tags, passive RFID tags only have two main components – the tag's antenna and the microchip or integrated circuit (IC).
-
- Retrieved from: http://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid on 05172016
- [[##embedded tags]]]

Figure E14: The above graphics are examples of the protocols that we studied in order to help us produce competitive designs. The above information also helped us further focus on our methods related research, testing and data collection.

Figure E15: The above graphics are examples of research from other fields of engineering and technology we studied in order to help us produce competitive designs.

INTERNATIONAL STANDARD

ISO/IEC/ IEEE 21451-7

First edition
2011-12-15

Information technology — Smart transducer interface for sensors and actuators —

Part 7:
Transducer to radio frequency identification (RFID) systems communication protocols and Transducer Electronic Data Sheet (TEDS) formats

Figure E16: The above graphics are examples of the policies, laws, and regulations that we studied in order to help us produce competitive designs.

- **INFO [phidget22][2017-08-06T14:36:41]:***** Logging enabled *******
- **INFO [_phidget22usb][2017-08-27T03:06:46]:Attaching Phidget:**
- **\\?\hid#vid_06c2&pid_0034#7&10b7b006&0&0000#{4d1e55b2-f16f-11cf-88cb-001111000030}**
- **INFO [_phidget22usb][2017-08-27T03:06:56]:**
- **Opened USB Device: 0x718**
- **INFO [phidget22][2017-08-27T03:06:56 usb.c+391**
- **PhidgetUSBReadThreadFunction()]:**
- **PhidgetRFID Read-Write(1024) (459844):**
- **ReadThread starting**
- **INFO [phidget22][2017-08-27T03:06:56 rfiddevice.c+559**
- **tagTimerThreadFunction()]:**
- **tagTimerThread running**
- **INFO [_phidget22usb][2017-08-27T03:18:28]:**
- **Closing USB Device: 0x718**
- **INFO [phidget22][2017-08-27T03:18:28 usb.c+421**
- **PhidgetUSBReadThreadFunction()]:**
- **PhidgetRFID Read-Write(1024) (459844):**
- **ReadThread exiting normally (signaled by Phidget_close)**

Code to read one RFID tag.

- **INFO [phidget22][2017-08-27T03:18:28 rfiddevice.c+607**
- **tagTimerThreadFunction()]:**
- **tagTimerThread exiting normally**

Figure E17: The above graphics are examples of the software and protocols that we used in order to help us produce competitive designs. With respect to the IEEE1451.7 protocol, the above functions were implemented in the python coding for hardware emulation of the RFID V2I system to perform a RFID data tag read sequence.

Figure E19: The above diagram shows some of the legislation and regulation concerning connected and autonomous vehicles in the NC Department of Transportation's Initiative for 2050. June 2019.

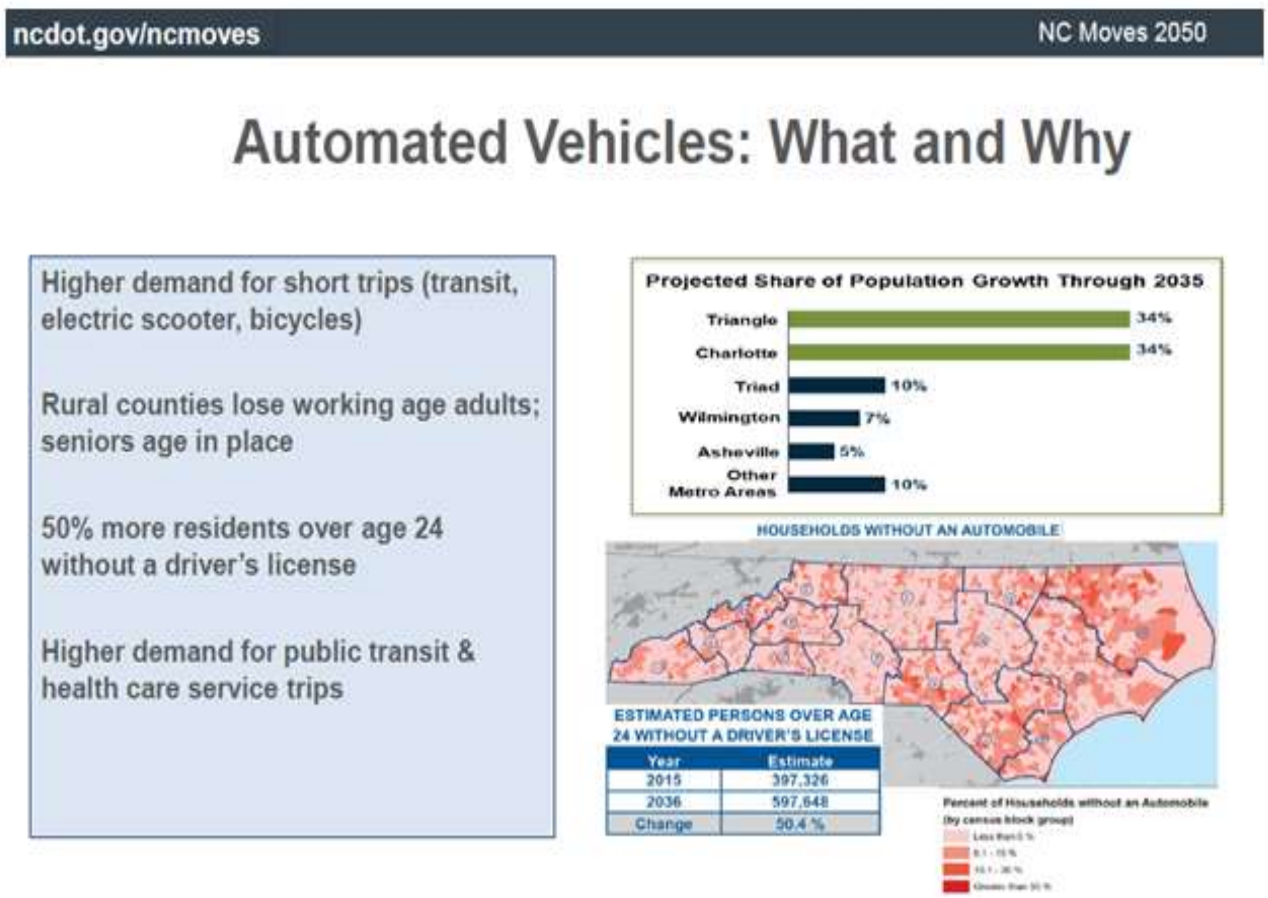


Figure E20: Current information about the NC Department of Transportation's Initiative for 2050. June 2019.

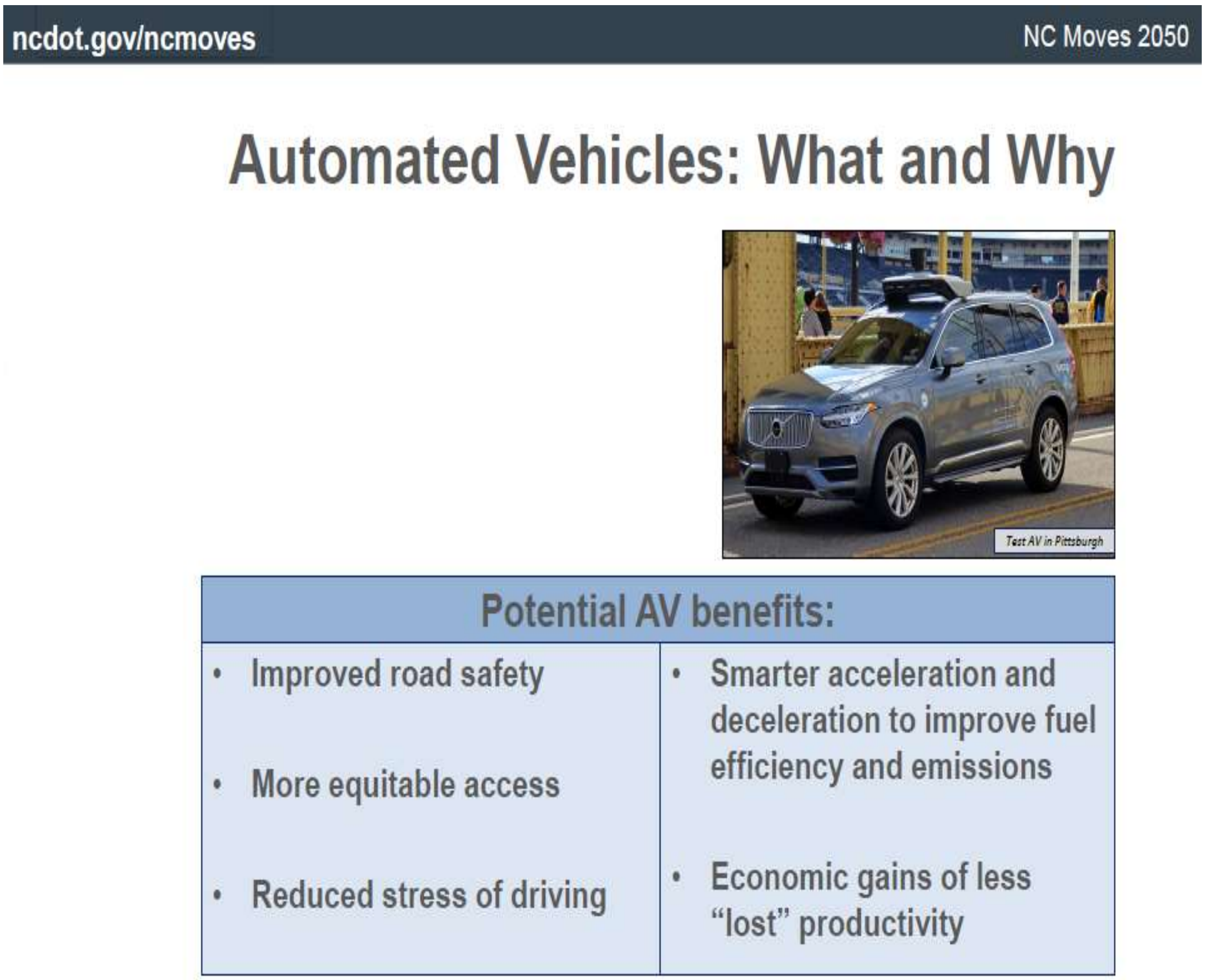


Figure E21: Current information about autonomous vehicles from NC Department of Transportation's Initiative for 2050. June 2019.

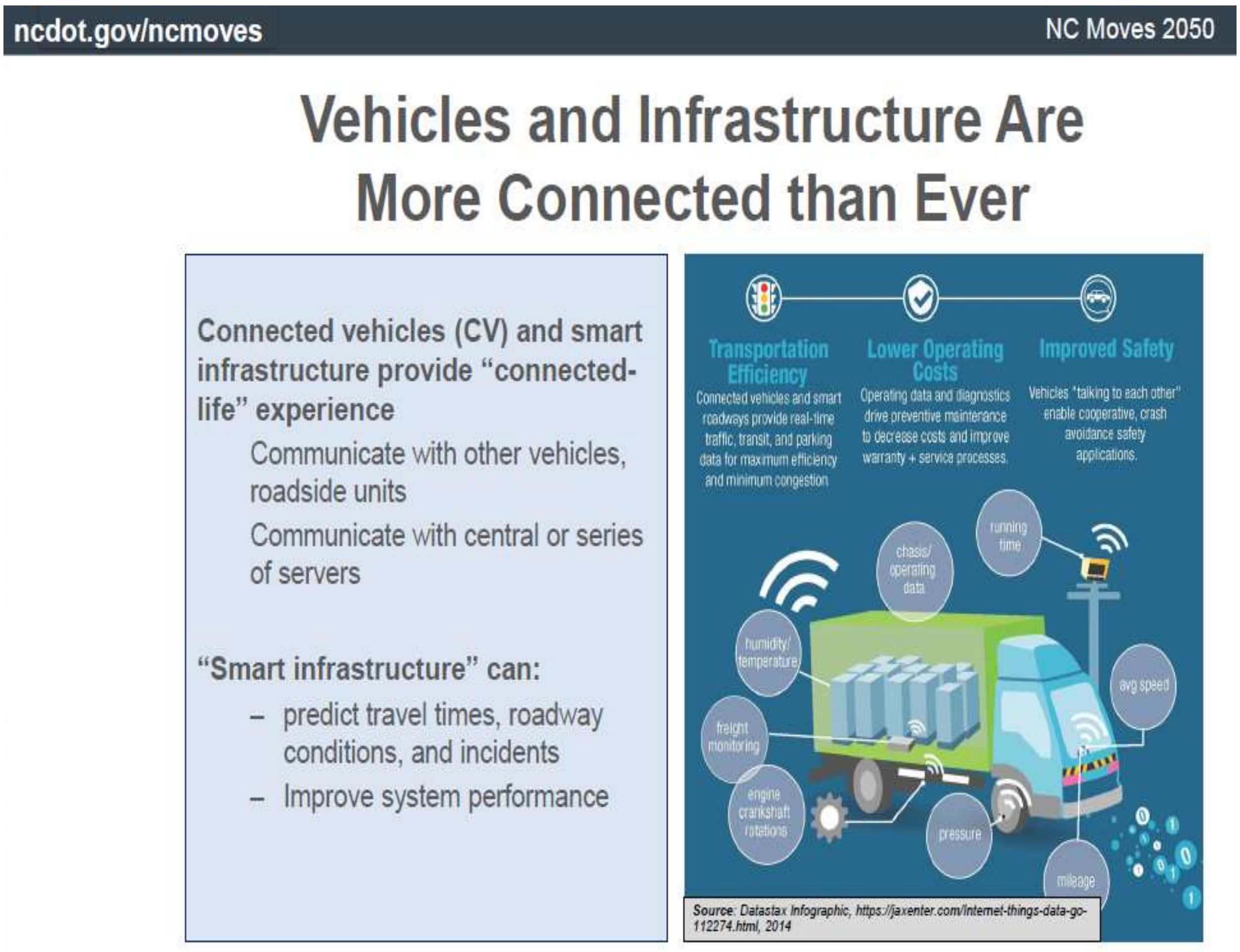


Figure E22: Current information about autonomous vehicles from NC Department of Transportation's Initiative for 2050. June 2019.

Figure E23: Current information about autonomous vehicles from NC Department of Transportation's Initiative for 2050. June 2019.