PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0021 May 2020

Utilization of Autonomous Vehicles for Security at Airports

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Anne Marie Pellerin
Sean Cusson
Andrew Goldsmith
LAM LHA
Alexandria, VA

Don Zoufal
CrowZnest Consulting
Chicago, IL

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about their perimeter and access control security.

Through the ASSIST (Airport Security Systems Integrated Support Testing) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying security technologies and procedures.

Through the POST (Performance and Operational System Testing) Program, Safe Skies conducts long-term evaluations of airport-owned equipment to track and document a device or system's performance continuously over its life cycle.

Through PARAS (Program for Applied Research in Airport Security), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee, but can be submitted at any time.

A project panel is formed for each funded Problem Statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request of proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies PARAS Program Manager*

PARAS 0021 PROJECT PANEL

Kyle Phillips *Dallas Fort Worth International Airport*
René Rieder *Burns Engineering*
Jeremy Worrall *State of Alaska Department of Transportation*
Cole Lail *National Safe Skies Alliance*
Mike DiPilato *Federal Aviation Administration*
Jim Patterson *Federal Aviation Administration*

AUTHOR ACKNOWLEDGMENTS

LAM LHA would like to thank all of the airport operators that assisted us with this project:

- Dallas/Fort Worth International Airport
- Detroit Metropolitan Airport
- Denver International Airport
- Washington Dulles International Airport
- Edmonton International Airport
- LaGuardia Airport
- Pittsburgh International Airport
- Oakland International Airport
- San Diego International Airport
- San Francisco International Airport
- San Jose International Airport

LAM LHA would also like to thank the following organizations that helped us with this project:

- ACAMP
- Airports Council International (ACI)
- International Aviation Transport Association (IATA)

Finally, LAM LHA greatly appreciates the work of our Project Team members, George Hough, Paige Reiter, Alex Bush, Lauren Peterson, and Ilana Lisann.

CONTENTS

SUMMARY **viii**

PARAS ACRONYMS **ix**

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS **x**

SECTION 1: INTRODUCTION **1**

1.1 Objectives of the Study 1

1.2 Research Methodology 2

1.3 Key Research Findings 2

SECTION 2: DEFINING AUTONOMOUS VEHICLES **4**

2.1 Functional Capabilities 4

2.1.1 Levels of Autonomy 6

2.2 Technical Considerations 7

2.2.1 Navigational Sensors 7

2.2.2 Vehicle-to-Vehicle and Vehicle-to-Infrastructure Communication Systems 8

2.2.3 Mapping Systems 9

2.2.4 Drive Systems 9

2.2.5 System Power and Charging 10

SECTION 3: USE IN AIRPORT ENVIRONMENTS **11**

3.1 Recent Deployments and Demonstrations 11

3.2 Potential Airport Security Applications 13

3.2.1 Deterrence of Criminal Conduct or Security Rule/Procedure Violations 13

3.2.2 Situational Awareness, Potential Threat Identification, and Surveillance 14

3.2.3 Hazardous Task Completion 15

3.2.4 Security-Related Communications 15

3.2.5 Security Threat Response Capabilities 15

3.2.6 Security Threat Analysis Capabilities 15

3.2.7 Security Threat Resolution Capabilities 16

3.2.8 Security Process Automation 16

SECTION 4: CONSIDERATIONS FOR AIRPORT OPERATORS **17**

4.1 Limitations on Existing Technologies 17

4.2 Legal and Regulatory Considerations 18

4.3 Safety Concerns 19

4.4 Development Level of Effort and Costs 19

4.5 Liability and Insurance Issues 20

4.6 Integration with an Airport 20

4.6.1 Integration Touchpoints 21

4.6.2 Onboard vs. Offboard Processing 22

4.7 Cyber and Network Security Challenges 24
4.7.1 Protection Strategy 25
4.8 Maintenance and Total Cost of Ownership/Operation 26
4.9 Environment, Climate, and Terrain 27
SECTION 5: EVALUATION AND COST-BENEFIT ANALYSIS FRAMEWORKS 28
5.1 Evaluation Framework 28
5.2 Cost-Benefit Analysis (CBA) Framework 29
SECTION 6: FUTURE DEVELOPMENTS 33
SECTION 7: CONCLUSION 34
REFERENCES 35
APPENDIX A: AUTONOMOUS VEHICLE TECHNICAL INFORMATION A-1
APPENDIX B: TURING VIDEO NIMBO DEMONSTRATION AT SJC B-1
APPENDIX C: VIRGINIA TECH TURTLE DEMONSTRATION AT SAFE SKIES PTF C-1
APPENDIX D: KNIGHTSCOPE K5 OBSERVATION AT LGA D-1
APPENDIX E: COBALT ROBOTICS OBSERVATION AT BRIGGS & STRATTON E-4
APPENDIX F: TELEROB TELEMAX PRO OBSERVATION AT PIT / ALLEGHENY COUNTY POLICE DEPARTMENT BOMB SQUAD F-1
APPENDIX G: ACAMP AUTONOMOUS SECURITY AV PILOT AT YEG G-1
APPENDIX H: EXAMPLES OF AUTONOMOUS VEHICLES THAT CAN SUPPORT SECURITY APPLICATIONS H-1
APPENDIX I: OVERVIEW OF SECURITY-FOCUSED AUTONOMOUS VEHICLE CAPABILITIES I-1

TABLES & FIGURES

Table 2-1. Capabilities of Industrial AVs 5
Table 2-2. Levels of Autonomy 7
Table 2-3. Navigational Sensor Types 8
Table 4-1. AV System Integration Considerations 22
Table 5-1. Evaluation Framework 29

Figure 3-1. Easy Mile EZ 10 Driverless Shuttle at AUS 11
Figure 3-2. DAIFUKU Autonomous Cart System at DTW 12
Figure 3-3. Vanderlande FLEET Autonomous Checked Baggage Management System at DFW 12
Figure 4-1. NIST Cybersecurity Framework 25
Figure 5-1. Return on the Security Investment (ROSI) Formula 32
Figure A-1. Knightscope Charging Station at LGA A-5
Figure B-1. Turing Video Nimbo B-1
Figure D-1. Knightscope K5 D-1

SUMMARY

An increasing range of commercially available autonomous vehicles (AV) designed for industrial security applications, and recent airport trials of such vehicles, suggest that this technology has the potential to enhance security and safety within the landside, airside, public, and restricted areas of airports in the United States.

The objective of this report is to provide an in-depth assessment of the potential contribution of AVs for airport security. The report seeks to provide airport operators and security managers with technical, operational, safety, security, regulatory, and cost-benefit information to help them determine whether and how such vehicles can address their airport security and safety requirements. It highlights real-world use cases drawn from both non-aviation and airport environments.

The research methodology and basis of findings for this report includes interviews with subject matter experts, a review of literature related to AVs in airport environments, analysis of publicly available information, and direct observation of AVs at Safe Skies' Perimeter Test Facility, LaGuardia Airport (LGA), and Norman Y. Mineta San Jose International Airport (SJC).

The report includes an overview of AV technology, examples of industrial applications, and commercially available AV solutions. The major findings of the report are:

1. Use of AV technology in airports for all applications, including security, is in a nascent stage; as a result, airport operators need to plan carefully before considering deployment.
2. Promising security applications for AVs at airports include:
    a. Improved deterrence of criminal and disruptive behavior
    b. Improved security surveillance, communication, and situational awareness
    c. Reduction in threats to human safety caused by job-related hazards such as Explosive Ordnance Disposal
3. Key considerations for airport operators include IT network and connectivity issues, mapping of airport infrastructure for automated technology, and safety considerations.
4. Observations of AVs at LGA and SJC provided strong evidence that they can add value to airport security operations—provided there is strong integration with existing human security staff and processes.

Finally, the report provides frameworks for assessing specific autonomous vehicle solutions and cost-benefit analysis of AV deployment. Report appendices provide detailed descriptions of the team's observations during demonstrations of AV solutions.

PARAS ACRONYMS

ACRP	Airport Cooperative Research Project
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CEO	Chief Executive Office
CFR	Code of Federal Regulations
COO	Chief Operating Officer
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IP	Internet Protocol
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

ACAMP	Alberta Centre for Advanced MNT Products
ADA	Americans with Disabilities Act
AI	Artificial Intelligence
AOC	Airport Operations Center
ATV	All-Terrain Vehicle
AUS	Austin-Bergstrom International Airport
AV	Autonomous Vehicle
B&S	Briggs & Stratton
COCO	Common Objects in Context
DAL	Dallas Love Field
DFW	Dallas/Fort Worth International Airport
DTW	Detroit Metropolitan Airport
ECU	Electronic Control Unit
GPS	Global Positioning System
GPU	Graphics Processing Unit
LGA	LaGuardia Airport
MAC	Media Access Control
NASA	National Aeronautical Space Administration
NHTSA	National Highway Transportation Safety Administration
NIST	National Institute of Standards and Technology
OSHA	Occupational Safety and Health Administration
PARAS	Program for Applied Research in Airport Security
PIT	Pittsburgh International Airport
RFID	Radio Frequency Identification
SAE	Society of Automotive Engineers
SFO	San Francisco International Airport
SJC	Norman Y. Mineta San Jose International Airport

SSID	Service Set Identifier
TYS	McGhee Tyson Airport
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
WPA2	Wi-Fi Protected Access II
YEG	Edmonton International Airport

SECTION 1: INTRODUCTION

In this section, we discuss the following topics:

- Objectives of the study
- Research methodology
- Key research findings

1.1 Objectives of the Study

Airport operators must mitigate security vulnerabilities with limited resources. Ever-changing regulatory requirements and priorities force airports to shift resources and adapt programs and strategies while maintaining other necessary mitigation measures. Focus areas include preventing security breaches in remote areas of the airfield, preventing vehicles from parking in restricted areas near the terminal, managing access to the Secured Area of the airport, inspecting vendor deliveries, mitigating insider threats, ensuring compliance with safety regulations, and ordinary crime control within airport facilities.

Airport security operators are continually assessing new technologies as potential solutions to these issues. One such technology that has received significant attention within the aviation community recently is autonomous vehicles (AV). Recent reports from Airports Council International (ACI)[1] and the International Air Transport Association (IATA)[2], have highlighted potential uses of such vehicles for various airport operational applications, including airport security.

These reports and a growing number of airport trials suggest that AV technologies[3] have the potential to enhance security and safety within the landside, airside, public, and restricted areas of US airports. Although deployment of this technology in the airport environment is in a nascent stage, the Project Team gathered insights that will assist airport operators who are considering using such systems. A review of the potential impact of these developing technologies on airport security will help shape operational planning and prepare airports for integration of autonomous systems as the technologies mature.

This report provides airport operators and security managers with technical, operational, safety, security, regulatory, and cost-benefit information that will help determine whether and how AVs can address their airport security and safety requirements. It focuses on industrial applications, as opposed to well-publicized potential applications for driverless passenger cars and taxis. As a result, it highlights actual use cases for AVs drawn from both non-aviation and airport environments.

- Section 2 of the report provides a functional definition of AV technology, a discussion of key technical components of AV systems, and examples of AV usage in non-aviation industries.
- Section 3 provides examples of AV use in US and international aviation applications, including security and non-security applications. Security and safety opportunities for AVs within landside, airside, public, and restricted areas of airports are identified.

[1] "Autonomous Vehicles and Systems at Airports Report," ACI, 2019.
[2] "Simplifying the Business," IATA, 2017.
[3] See Section 2 for a discussion of terminology and definitions. In our research, we found many industry participants use "autonomous vehicles," "autonomous robots," and "autonomous mobile robots" interchangeably.

- Section 4 discusses considerations related to technology integration with existing airport systems, IT/network security, communication, data transfer, frequency spectrum, and interference considerations. Safety, insurance, liability, regulatory, climate, and terrain factors are described.
- Section 5 provides a framework for evaluation of AV technology and a guide to developing a cost-benefit analysis of deployment of such technology in an airport environment.

1.2 Research Methodology

The Project Team conducted the following research activities:

- **Literature review:** Subject matter experts documented key features of AV operations. Component parts and sensors of AVs that could positively impact operations within the airport environment were identified. Additionally, rules and regulations, liability, safety, and other operational considerations were reviewed.
- **Demonstrations:** The Project Team conducted two demonstrations of AV operations to better understand how they work and how the technology may integrate into the airport environment. First, the Project Team worked with Norman Y. Mineta San Jose International Airport (SJC) to demonstrate the technology in a terminal operation. Second, the Project Team worked with Safe Skies at their Perimeter Test Facility, located on the grounds of McGhee Tyson Airport, to demonstrate a perimeter AV operation.
- **Observations and Interviews:** To better understand operational concerns related to potential use cases, the Project Team observed autonomous systems deployed at various locations, and interviewed airport operators who have deployed or considered deploying an autonomous system. Additionally, the Project Team interviewed AV companies and robotics laboratories to better understand technical capabilities and future developments.
- **Industry Research**: The team collected and summarized publicly available information on providers of industrial AV solutions, and examples of deployments, with a focus on those that offer security or airport applications.

1.3 Key Research Findings

The following is a summary of the most important findings of the Project Team's research:

1. The use of AVs at airports, for all applications, is in the nascent stage. While most deployments are not security related, there are some systems emerging that are either expressly for, or could be modified for, security purposes.
2. AVs on the market today have the potential to perform a variety of security functions at airports, including replacing or supplementing existing security measures in both indoor and outdoor settings. The potential exists most notably in the areas of:
    a. Deterrence – The ability of AVs to perform random and unpredictable security patrols was observed by the research team in airport and non-airport demonstrations. Briggs & Stratton Corporation, a non-airport user of AVs for security, highlighted this as a key benefit of the technology.
    b. Situational Awareness, Surveillance and Communication – AVs equipped with cameras and recognition software can provide enhanced situational awareness and surveillance

capabilities. For example, the Knightscope K5 tested at LaGuardia Airport was able to patrol a terminal's curbside, as well as collect data on specific security issues for analysis. It also demonstrated the capability to stream live video, support two-way intercom functions, and communicate data and alerts in real-time. The Turing Video Nimbo AV, tested at SJC, demonstrated the ability to navigate high traffic areas while transmitting live video to airport operations and law enforcement, and participate in two-way communications.

   c. Mitigation of Hazardous Tasks – Handling unattended baggage or suspicious packages in the airport environment is a key concern for airport operators. The research team observed that law enforcement officers at Pittsburgh International Airport (PIT) are using AVs for this purpose.

3. AV Security as a Service combines autonomous technology with human monitoring. This provides a potentially attractive model for airports since it may reduce initial implementation costs. This approach is used by Briggs & Stratton Corporation and combines Cobalt Robotics' autonomous robots with Remote Cobalt Specialists as part of their security operations at corporate headquarters.

4. Challenges deploying autonomous systems in an airport include network and connectivity issues, necessary infrastructure for automated technology (i.e., mapping), and safety considerations. Specific findings include:

   a. All successful industrial applications of AVs are predicated on having functional IT support infrastructure. Without the appropriate level of connectivity, AVs cannot perform the requested functions or will shut down altogether. Therefore, it is imperative that the AV can access the network in all areas of the environment where it conducts operations.

   b. Autonomous systems must be interoperable with existing airport systems and account for operational considerations.

   c. With the current technology, an AV's likelihood of operating successfully is directly linked to the level of predictability in how it is expected to move.

   d. Studies have shown current AV solutions perform best in highly controlled environments. Since airport environments can be unpredictable, it is important that AVs demonstrate the ability to safely maneuver through a changing environment with airplanes, tugs, people, and other obstacles. Mapping is closely related to safety considerations.

5. A structured evaluation and cost-benefit analysis framework can assist airport operators in determining if an autonomous system can safely perform security functions in the specified areas of the airport.

   a. A framework based on the National Institute of Standards and Technology (NIST) robotics and AV testing and US Army Developmental Test Command testing standards is provided in Section 5.1. Using this framework will help airports define the objectives and requirements for using an AV security solution.

      In addition, the framework addresses measurement and evaluation methods, data collection, and testing procedures. This information can form the foundation for an airport's business case for AV deployment and help ensure that airport business requirements are achievable.

SECTION 2: DEFINING AUTONOMOUS VEHICLES

In this section, we provide a non-industry-specific review of the common functional and technical capabilities of AVs. Understanding these will help airport operators determine which airport security applications this technology is best suited to support.

2.1 Functional Capabilities

The development of AV technology has accelerated in recent years. Although the popular media has focused primarily on the private and public transportation applications (e.g., self-driving cars, buses, trucks, and taxis), the technology is increasingly being used for industrial and public sector applications, encompassing aviation and airports.

At the highest level, there appear to be several key benefits that the technology can provide:

- **Improving safety and security** by having an AV perform tasks that are high risk or hazardous for humans.
- **Improving productivity** when performing repetitive tasks, since workers may lose attention to detail and have decreased productivity over time.
- **Improving task accuracy and repeatability** for precise activities over long periods of time.
- **Improving data collection, communication and analysis,** since humans have physical limitations relative to their ability to collect, communicate, and process certain types of data.

Examples of relatively mature industrial uses of AVs that provide these benefits include:

MILITARY AND LAW ENFORCEMENT

AVs are being used by the military and law enforcement for applications such as bomb and IED disposal and combat-zone logistics. The common thread linking these applications is the ability of AVs to reduce threats to personnel.

In the US Army’s Expedient Leader-Follower program, supply convoys consist of a driver-operated vehicle followed by driverless vehicles. The primary purpose is to reduce the number of people operating tactical vehicles and limit exposure to a potential attack.

As part of its Next Generation Combat Vehicle program, the US Army wants a family of Robotic Combat Vehicles that integrate into formations to support warfighting operations that involve manned vehicles. Additionally, in 2021, the Army will begin operational user testing of two M113 armored personnel carriers converted to armed robotic platforms.

AGRICULTURE

Farming is a data-intensive industry in which real-time information about weather, soil conditions, and plant health are critically important. Taranis, an Artificial Intelligence (AI)-powered solution supported by the John Deere Startup Collaborator program, uses machine learning in combination with drone and AV technology to enable farmers to gather and analyze plant-level data and make immediate changes to farming operations. The platform is capable of monitoring fields and finding early symptoms of uneven emergence, weeds, nutrient deficiencies, disease or insect infestations, water damage, and equipment issues.

New Holland's T8 Blue Power tractor is an unmanned AV whose sensors can also collect data on soil conditions, offering opportunities to improve maintenance of planted crops. Unlike humans, these AVs can work regardless of light conditions and can provide accurate information even in dense fog, thick dust, and heavy winds.

MINING

Industrial self-driving vehicles have been in use in mining facilities for several years. Mining lends itself to AVs because of the need for worker safety, the material handling requirements, and the 24/7 operational needs. In addition, mining environments are self-contained and controlled: there is no unexpected traffic or additional people to avoid. Rio Tinto's Pilbara iron ore mine uses driverless Komatsu trucks. Using GPS, radar, and laser sensors, the trucks can make their way around the mine site, avoiding obstacles and delivering ore to be processed.

LOGISTICS AND WAREHOUSING

Ryder, a transportation logistics and supply chain company, has implemented AVs for its warehouses and distribution centers to improve its operations and worker safety. The vehicles can maneuver around people and forklifts in crowded and busy warehouse environments, and have sensors that read RFID tags and transmit data to Ryder's operations center.

From these and other examples, it is possible to identify capabilities that industrial AVs provide, regardless of the specific application in which they are being used. Table 2-1 provides a summary of these capabilities. Taken together, they provide a technology-neutral functional definition of AVs.

Table 2-1. Capabilities of Industrial AVs

Capability	Description
Human Safety Enhancement / Hazard Avoidance and Mitigation	AVs may be well suited for applications that are hazardous and dangerous to humans.
Continuous Operation	AVs can be used for applications that need to be performed 24x7, at night, or in challenging weather and terrain conditions.
Data Collection	AVs can be equipped with sensors, cameras, etc. to enable highly accurate and rapid video surveillance, environmental monitoring, acoustic detection, smoke and fire detection, RFID and Bluetooth data capture, etc.
Material Transport and Handling	AVs can be a platform for carrying heavy equipment or transporting items.
Repetitive Task Completion	Similar to industrial robots, AVs can be programmed to perform tedious and repetitive tasks.
Remote Communication and Internetworking	AVs can function as mobile nodes of an IT network, extending its reach and sharing information with other nodes.
Autonomous Mobility	The ability to move over large distances and in complex environments without complete human control is foundational. Section 2.1.1 describes the varying levels of autonomous mobility that affect the applications AVs can be used for.

Another important theme of these examples for airport operators is the vectors of specialization for industrial AVs. These vectors reflect that there is no "one size fits all" technology, given the diversity of user requirements, and the increasingly competitive and differentiated market for AVs. The main vectors of specialization appear to be:

- **Terrain / Environment** – Many AVs are designed with a specific operating environment in mind. Airport operators must ask questions like: Is the vehicle capable of performing only in indoor environments? Can it operate on uneven and unpaved terrain? Can it operate in all weather conditions? Can it maneuver in crowded environments with many moving objects?
- **Customizability / Configurability** – Some AVs are designed to be configurable “platforms” to which users can (for example) add specific sensors for their requirements. This is an intriguing option because airport operators can define what they want the system to do and equip it with specific sensors or capabilities.
- **Functionality** – Although many AVs can perform multiple functions, they often have primary functions or capabilities that dictate their overall design. Examples include:
    - Material handling and transport
    - Data collection, analysis, and transmission
    - Hazard mitigation

For airport operators, this means it is important to prioritize potential uses of AVs within their environment carefully. It may be difficult to find one vehicle that can support multiple, diverse airport security requirements. Considering the capabilities and vectors of specialization discussed above, the primary functional security applications for AVs at airports are:

- **Surveillance and Patrolling:** Includes a broad range of indoor and outdoor data collection, surveillance, and patrolling activities, such as identification and tracking of unauthorized or suspicious persons or vehicles, identification of perimeter breaches, damaged property, or open doors; and identification of potential threats and hazards via collection of visual, thermal, environmental data and acoustic data.
- **All Terrain Material Transport and Handling:** For security applications that require transport of material and equipment (such as surveillance equipment or sensors) in rugged or complex terrain and challenging weather conditions.
- **Explosive Ordnance Disposal (EOD):** AVs designed to help safely identify and dispose of IEDs and other explosives.

Detailed examples of potential security applications can be found in Section 3.2.

2.1.1 Levels of Autonomy

Different AVs move and perform functions at various levels of autonomy. Although driverless vehicles have captured the public’s imagination, the reality is that many AVs require some level of human control or intervention. Understanding the full range of autonomous capabilities and clearly defining levels of autonomy is fundamental to assessing the capabilities, limitations, and vulnerabilities of different systems.

Categorizations of AVs relate generally to how the vehicle will make decisions, and how and when a human will need or want to intervene in an operation. Understanding the technological capabilities and limitations of a given vehicle will help the airport operator understand whether the vehicle can meet their objective.

At least two resources defining autonomy levels are available. In the early 2000s, NIST began assessing unmanned systems with the goal of standardizing autonomy levels. The resulting scale established standard terms and definitions for requirement analysis, specification, and evaluation. A second scale, created specifically for the automobile industry, was published by The Society of Automotive Engineers (SAE) International, and has been widely adopted. These two standardized scales may help decision makers classify and understand differences between how systems operate.

Using the premise of both scales, and applying the 0–5 levels of autonomy developed by SAE International, Table 2-2 identifies general system capabilities to assist the airport operator in understanding limitations and vulnerabilities. Systems found at the higher end of the scale have increased capability to make decisions. Airport operators can use this scale to match operational requirements with the appropriate level of automation, or to determine when it is necessary for a human to assume control of a system.

Table 2-2. Levels of Autonomy

0	1	2	3	4	5
No Automation	**User Assistance**	**Partial Automation**	**Conditional Automation**	**High Automation**	**Full Automation**
Human controls all vehicle movement and security functions.	Human has primary control of vehicle movement and security functions. System provides some assistance in movement and/or function.	System independently performs either vehicle movement or the security function. Human controls function(s) not managed by the system.	System can perform vehicle movement and security functions on its own under certain conditions. Human must take control if issues arise.	System independently performs both vehicle movement and security functions with human monitoring.	All vehicle movement and security functions are performed autonomously in all environments. Option for human control.

The AVs assessed in this report fall into autonomy levels 2–4. From a practical standpoint, this has two important implications for airport operators:

1. AVs should be evaluated in terms of their potential to augment and extend the capabilities of human staff, not completely replace them.
2. The value of AVs is highly dependent on their operating environment.

2.2 Technical Considerations

This section provides a brief description of common technical features and requirements that are associated with many, if not all, AV solutions used for industrial applications. Understanding these technical considerations will help airport operators better understand what is required to use AVs effectively. See Appendix A for a summary of these considerations.

2.2.1 Navigational Sensors

AVs can use multiple types of sensors to collect data for navigational and other purposes. The data collected by these sensors is processed by the vehicle’s computer hardware and machine learning software. Table 2-3 describes the various sensor types.

Table 2-3. Navigational Sensor Types

Navigational Sensor Type	Description
Cameras	Cameras provide AVs the ability to see their environment, including lane markings and signs, and to navigate without human intervention. Cameras provide the data needed to develop a three-dimensional map of the vehicle's surroundings.
Lidar (Light Detection and Ranging)	While cameras provide data on the shape, color, and other visual characteristics of objects, lidar sensors are crucial for maneuverability. Often mounted on the top of the AV, lidar sensors can spin 360 degrees and emit lasers to continuously measure the AV's distance from objects as it moves, based on the time it takes for the reflected light to return to the system.
Radar	Radar assists the AV by collecting and assessing data related to distance, form, and size of objects. Radar operates by sending electromagnetic waves that reflect off objects to the receiver, which assesses patterns and frequency of the returning waves to establish measurements. The series of incoming data from an object enables radar to determine movement direction and speed of the object.
GPS	GPS uses satellites to calculate position and tell the AV where it is located within a space. Currently, GPS systems require additional inertial measurement units, such as tachometers, altimeters, and gyroscopes, to accurately position a vehicle. Most AV systems will rely on GPS systems that are accurate to within a few centimeters.

2.2.2 Vehicle-to-Vehicle and Vehicle-to-Infrastructure Communication Systems

A number of terms are used in connection with AV communication systems. According to the US Department of Transportation, vehicle-to-vehicle communications are often referred to as "V2V." Vehicle-to-infrastructure communications are often referred to as "V2I," which is similar to vehicle-to-environment or "V2E." Vehicle-to-pedestrian communications are often referred to as "V2P." Collectively, these modes of communication are known as Vehicle-to-Everything Communications or "V2X."[4] This document refers primarily to V2V and V2I communication systems.

V2V communications involve AVs sharing data and sending messages to each other via a wireless network. The information being shared can include vehicle speed, location, direction of travel, braking, and loss of stability. Current V2V technology uses dedicated short-range communications (DSRC). DSRC is a networking protocol similar to WiFi that has been set forth by the FCC and has a range of up to 1,000 feet. V2V communications can operate as a mesh network, meaning that every node (AV) can send, receive, and retransmit data to every other network node.

As its name implies, V2I communication systems extend the capabilities of V2V systems to include network nodes that may be part of a building or other fixed structure, a device (e.g., a smartphone) held by a pedestrian, or mounted on a non-autonomous vehicle.

There are potential applications for V2V and V2I communications in an airport environment. For example, V2V could be used to ensure that AVs do not interfere with the activities of traditional airport vehicles, as well as other AVs. V2I-enabled AVs could enhance other airport security features and capabilities, such as perimeter security. An airport perimeter security system could notify an AV of an alarm and direct the vehicle to investigate a potential intrusion.

[4] https://www.transportation.gov/v2x

From an airport operational perspective, the use of V2V and V2I communications raises many of the same considerations associated with other wireless communications systems. In addition to defining communication integration requirements and budgeting for system maintenance, airports need to ensure that the V2V and V2I communications systems meet their privacy, data protection, and cybersecurity requirements.

2.2.3 Mapping Systems

AVs require training before operating in a new environment. Training of a system is often accomplished using environment mapping. Mapping involves generating a software model of the operating environment that illustrates pathways, intersecting human and vehicle traffic routes, and stationary obstacles to avoid. The vehicle can then use data from sensors to ascertain its own position within the map.

In considering a system's mapping capability, the airport operator should determine how remapping is done and how long it will take to complete the process. The AV may have the ability to remap autonomously or with minimal human guidance, allowing non-technical airport staff to complete the task. Conversely, the system could require software coding to learn the new area. This may require a level of technical expertise that the airport may not have on staff. Additionally, the remapping process and complexities of the area may affect how remapping needs to occur and the time needed to complete the process.

Examples of the Mapping Process

As part of the research for this study, the team observed two different examples of AV map acquisition.

The first example involved Virginia Polytechnic Institute and State University's (Virginia Tech) Turtle system. An engineer programmed data into the system and then performed "training drives" in which a person remotely operated the vehicle through its route while the vehicle's sensors recorded the route and learned how to replicate the route in autonomous mode. See Appendix C for more details.

The second example involved Turing Video's Nimbo security surveillance robot, demsontrated at SJC and. In this example, as an engineer steered the vehicle though the desired route, the system set waypoints at set increments on the map developed by the AV's software. During the training, the system mapped the area within its computer and created the path for it to follow. The engineers set multiple paths within the area to direct Nimbo to run different scenarios. See Appendix B for more details.

2.2.4 Drive Systems

AVs can incorporate various drive systems to maneuver. The drive system selected will impact the vehicle's cost, versatility, and load capacity, and is therefore determined by the specific application's requirements. Examples of drive systems include:

- **Tank Drive:** Utilize two interdependent drive train systems with an independent set of wheels for each side of the vehicle for increased maneuverability
- **Ackermann:** Utilize four wheels to increase straight-line stability and reduce steering radius

- **Mecanum:** Utilize special directional wheels that allow maneuvering in all directions without the vehicle itself rotating

Airports should consider their objectives and the area where the vehicle will operate when choosing the appropriate drive system. A system that will operate off-road will require a different drive train and wheels than a system operating indoors on a tile floor.

Drive Systems Used in Airport AVs

The project team observed two different types of drive systems during its research.

The Turing Video Nimbo robot demonstrated at SJC uses a tank drive system. In the demonstration, the system appeared to maneuver easily and efficiently through tight spaces with numerous people present.

The team also observed the Knightscope K5 Autonomous Data Machine at LGA, which uses an Ackermann drive system. In the demonstration, the system appeared to move quickly and avoided people walking on the curb outside LGA’s Terminal B arrivals area. However, the system bounced as it operated on the curb, which affected the camera’s video quality. This system observation is detailed further in Appendix D.

2.2.5 System Power and Charging

The majority of the AVs and industrial robots reviewed by the project team use some type of electric battery to power their operations. They will often have separate batteries for navigation versus computer and sensor operation, because autonomous sensors and computers require precisely controlled electrical voltages and currents to function optimally. The charging requirements for the battery used can vary depending on the type of AV in question. Some vehicles can use docking stations for electric passenger cars while other systems may require a person to plug the vehicle into an outlet or change the battery.

When considering the use of an AV, the system’s power and charging technology needs to be assessed. The airport must balance operational considerations with charging requirements to set operational parameters or assess how many systems they require to achieve a stated goal.

Charging Systems Used In Airport AVs

The project team observed two different charging system methods during its research.

The Turing Video Nimbo can place itself onto a charging pad as necessary. During the demonstration at SJC, which included four hours of mapping and four hours of demonstration time, the system never needed to recharge. It started with a full charge on the first day of the demonstration and had 30 percent of its battery life remaining at the conclusion of day two.

The Knightscope K5, which was demonstrated at LGA, was set up to stop at a charging station along its route as needed. Two charging stations were positioned so that the AV could continue to perform monitoring functions while it was charging. The terminal operator established a charging strategy to maximize patrol time and minimize charging time. As a result, the system would stop at a charging station more frequently but would not need to stay on the charging pad very long.

SECTION 3: USE IN AIRPORT ENVIRONMENTS

This section discusses how airports are using AVs for a variety of non-security related operations. Potential security and safety opportunities within landside, airside, public, and restricted areas of airports are also identified. Appendices B–G provide specific information on AV deployment or pilots at airports. Appendices H and I provide examples of commercially available AV products that can either support or are designed for security applications.

3.1 Recent Deployments and Demonstrations

Airports in the United States and around the world have implemented or are testing AV solutions to gain operational efficiencies and enhance customer service. Discussion of these non-security related initiatives have been grouped into the following categories:

- Autonomous People Movement
- Baggage Handling
- Airside Operational Improvements

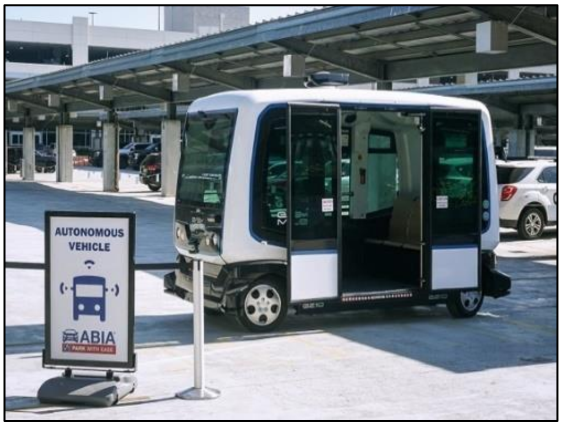
Additional examples can be found in the September 2019 Airports Council International AV Research Paper. They include:

- Autonomous shuttle operations at Christchurch Airport, New Zealand
- Robotics at Kansai International Airport, Japan
- Cleaning robot at Singapore Changi Airport, Singapore
- Valet parking robot at Lyon-Saint-Exupery Airport, France
- Autonomous snowplow at Winnipeg International Airport, Canada

AUTONOMOUS PEOPLE MOVEMENT

Autonomous people-movement systems operate from predefined plans, but can perceive their environment and make decisions and adjustments based on their surroundings. These solutions represent the next step from non-autonomous shuttles and buses currently used to move people around airports.

Figure 3-1. Easy Mile EZ 10 Driverless Shuttle at AUS



An example of how these solutions are being trialed at US airports is the deployment of the Easy Mile EZ 10 driverless shuttle at Austin-Bergstrom International Airport (AUS) in 2019 (see Figure 3-1).

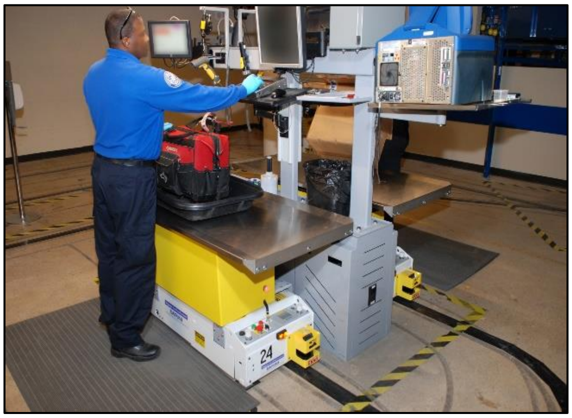
During the trial, the airport used the Americans with Disabilities Act (ADA)-compliant AV to transport passengers with mobility issues between the terminal and the rental car facility. The vehicle operated in a cordoned area away from other traffic and people.

BAGGAGE HANDLING

Detroit Metropolitan Airport (DTW) has deployed a DAIFUKU autonomous cart system to assist the TSA in completing the checked baggage screening process (see Figure 3-2).

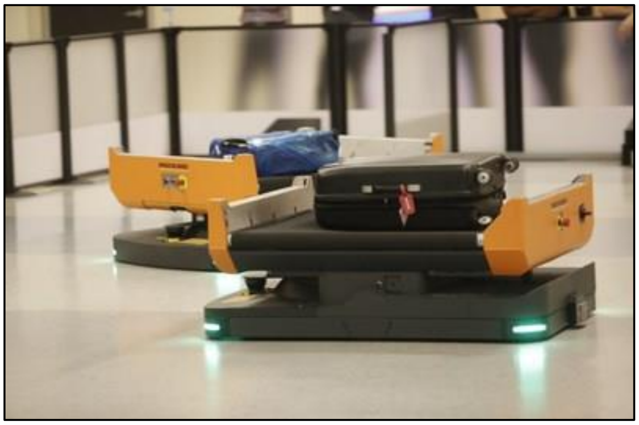
By relieving Transportation Security Officers of the task of moving checked bags, these systems seek to increase the efficiency of TSA's checked baggage screening process. After receiving a flagged bag from a conveyor belt, the cart delivers the bag to an inspection station by following set routes defined by magnetic tape on the ground. When the screening is complete, the cart transfers the bag to another conveyor belt.

Figure 3-2. DAIFUKU Autonomous Cart System at DTW



In another baggage handling application, Dallas Fort-Worth International Airport (DFW) trialed the Vanderlande FLEET autonomous checked baggage management system (pictured in Figure 3-3) in 2019. The system was installed to assist passengers transferring from international flights to domestic flights. After receiving their bags from U.S. Customs processing, passengers brought their luggage to the bag-drop kiosk, entered their travel information, and placed their bag on the kiosk's belt. The belt then placed the bag on an AV, which moved it onto the correct baggage belt. The AV followed a predetermined path between the bag-drop, baggage belt, and charging stations, but it could make decisions and avoid objects as necessary.

Figure 3-3. Vanderlande FLEET Autonomous Checked Baggage Management System at DFW



AIRSIDE OPERATIONAL IMPROVEMENT

Many airports are evaluating AVs to improve their airside operations. San Francisco International Airport (SFO) studied potential efficiency gains of an autonomous aircraft-towing vehicle to improve airfield and gate utilization. SFO chose to analyze aircraft towing because of the controlled nature of the application. Aircraft operate in predictable routes, have V2V capabilities to communicate with autonomous systems, and movement areas have signage and marking. The exercise resulted in two key findings:

1. It was easier and less costly to tow aircraft to remote parking positions
2. Airports could reduce pushback maneuvering time by eliminating engine run-up and tug disconnect time

DUAL PURPOSE

There are cases of AVs serving a dual purpose at airports, such as customer service robots with incidental security functions. AVs in the form of AI robots are staffing airports around the world and performing non-security tasks including check-in, concierge, luggage transportation, translation, and cleaning services. Robots with a dual customer-service/security function are particularly well-developed in East Asian airports:

- Haneda Airport in Japan has an in-house robotics lab that has introduced the Reborg-X. This robot guides visitors through the airport using a touch panel on its front. Its camera and data collection capabilities are also used for security purposes.
- Mt. Fuji Shizuoka Airport in Japan launched Reborg-Z. This robot uses its 360-degree camera and large display for security and passenger guidance in multiple languages. Its AI and sensor capabilities and include facial recognition, emergency detection (e.g., screaming), and fire and smoke detection. It is able to communicate with other Reborg-Z units as well as security staff.
- Incheon airport in South Korea deployed the self-driving customer service robot Troika in 2018. Functionally, it serves a similar purpose to other concierge robots like Spencer at Schiphol Airport in Amsterdam, or porter robot Leo at Geneva Airport in Switzerland. Troika escorts travelers to their boarding gate, speaks multiple languages, and offers information (about weather, estimated time at immigration, security restrictions, etc.) Troika can also take photos of travelers in the airport and send it to them by email or text message. It does not explicitly serve a security function, but its features could lend itself to security as a secondary task.
- Anbot in Shenzhen Airport, China is primarily a security robot with additional customer service features. It patrols autonomously, using its audio and visual sensors to recognize and record illegal activities. It has an “SOS Button” on the touchscreen, allowing passengers to call for help in case of emergency or a security incident. It can also offer information to passengers, monitor air quality or changes in temperature, and alert authorities to possible emergencies like fires.

3.2 Potential Airport Security Applications

This section describes a number of airport security applications where AVs might be used, and identifies specific activities associated with these applications.

3.2.1 Deterrence of Criminal Conduct or Security Rule/Procedure Violations

AVs can support airport security by deterring both the public and individuals working in the airport from criminal conduct or from violating security rules and procedures. One or multiple AVs can provide a presence similar to uniformed security personnel, such as covering preset routes or varying routes and timing to increase unpredictability.

An AV’s ability to move around an airport and collect information through sensors enhances the airport’s security program by introducing an additional form of random and unpredictable surveillance. If an individual cannot predict when, where, or how they are being surveilled, they will have a more difficult time circumventing surveillance.

To maximize deterrence efforts, an airport must show that it is using data collected by the AV in some manner. This can include communicating through the vehicle to individuals in close proximity or taking enforcement action based on data collected from the system’s sensors. This shows the community that the airport is proactively engaged in using the vehicle and continues to collect information.

Varying AV routes and the timing of routes can increase deterrence. Deploying multiple vehicles may also increase deterrence, allowing the airport to cover more ground. This option may work best in a complex layout or larger area to ensure bad actors know that coverage is robust.

Real-World Examples

During the demonstration at SJC, as discussed in Appendix B, the AV system identified people in the baggage area, provided a pre-scripted message, and alerted the operator that a person was identified. The operator could then choose to further communicate with that individual in a live dialogue if needed.

In the case of the AVs used by Briggs & Stratton, as discussed in Appendix E, a human operator in a command center similarly communicated with individuals it encountered. The autonomous vehicle was able to challenge individuals and require a badge swipe on the reading device attached to the vehicle. This allowed for the authentication of the credential and further communication with the operator if necessary.

The research team also observed real world examples of autonomous vehicles being used or trialed to improve deterrence. As discussed in Appendix E, employees working in the warehouses at Briggs & Stratton know that the autonomous vehicle system is present and that the company is paying attention to it because they see action being taken. Briggs & Stratton management believe that this proactive approach has deterrence value.

At LGA, the autonomous system ran on multiple routes, would stop occasionally to charge while continuing to collect data, and could stop anywhere within a route at the command of the operator. These operational variations make it more difficult for a bad actor to predict what the system will do.

3.2.2 Situational Awareness, Potential Threat Identification, and Surveillance

AVs can enhance an airport operator’s situational awareness. Their sensors can detect unauthorized persons or hazardous conditions, and monitor events and activities in specific areas. The system can capture and classify the information in real-time to aid safety and security operations or store the information for later analysis. With these data feeds linked to an operations or communication center, the airport can gather greater insight into the need to deploy assets. Similarly, the airport may use the data for forensic purposes.

These vehicles can augment existing sensor systems or provide coverage in areas without sensors. An airport can deploy a vehicle on a routine patrol or on a unique mission to gather data in a specific area. An airport can also use a vehicle in an emergency response situation to provide real-time data on the situation. The ability to move a platform and dispatch the vehicle quickly can enable deployment at critical times. The autonomous nature of the system allows operational personnel to focus on the content of the data being provided rather than operating the vehicle. However, for both the patrol and response scenarios, the airport operator must consider network connection issues.

Using a multitude of sensors and AI, AVs can collect a variety of data. Video sensors can provide live feeds or images and detect people, license plates, or open doors among other things.

Audio sensors can record noises, recognize sounds like breaking glass or explosions, and provide live or recorded communications. Additionally, sensors can include signal detectors, thermal imagery, Wi-Fi or cellular signal strength detector, smoke and vapor detectors, chemical detectors, and mapping.

3.2.3 Hazardous Task Completion

Autonomous capabilities can enhance robotic devices already in use at airports for hazardous tasks. Currently, airports use robots for bomb removal and other hazardous material response. These robots have already introduced functionalities to assist end users with the repetitive tasks. For example, systems can orient themselves into specific positions, and more advanced systems can manipulate their arms with assist functions. These capabilities reduce pressure on the operator in directing the response, allowing them to focus on the situation as opposed to operating the robot.

An example of this application is the Alleghany County Police Department's Explosive Ordinance Disposal Team (Bomb Squad) use of the Telerob Telemax Pro at PIT. The system's autonomous movement capability enables it to map an area as it is remotely directed by a human operator, and then it can move between set waypoints or return to its initial operating location autonomously. Appendix F contains further information on this solution.

> A real-world example of how the mapping ability of an AV can provide live situational awareness to help emergency responders plan tactical operations comes from PIT and the Alleghany County Bomb Squad. As discussed in Appendix F, the Bomb Squad uses their vehicle's lidar mapping ability to create a current map of the area to enhance their situational awareness and evaluate the scene as they plan their response. This allows the responders to know if anything has been moved or changed and helps to prevent surprises.

3.2.4 Security-Related Communications

Many AVs have two-way communications capabilities. This enables operators to send both scripted messages and messages created in real-time as events unfold. An airport can use the two-way communication function for crowd management as it monitors crowd movement and flow. The AV can act as a localized communication hub providing information and communicating back to a central command or control center.

3.2.5 Security Threat Response Capabilities

A critical airport security requirement or application is the need to respond quickly to a security threat once identified. However, given the current state of technology, we assess that commercially available AV systems may have limits in their ability to perform these types of activities. While they have demonstrated the ability to move to the sight of an alert or alarm, and to track suspicious persons in coordination with other airport surveillance systems, they have not demonstrated the ability, for example, to autonomously follow a suspicious person that is trying to elude them.

3.2.6 Security Threat Analysis Capabilities

The ability to quickly and reliably assess the potential severity of a security threat and determine the appropriate response is a key skill of trained airport security personnel. AI and machine learning tools have advanced significantly in these areas. An AV equipped with the appropriate sensors and software could be used to analyze measurable indicators of threats (e.g., whether a concealed shape in a carry-on bag is likely to be a weapon, or a sound in an airport terminal is likely to be a gunshot). However, current technology is limited in its ability to autonomously use other contextual factors (e.g., a person's behavior, or a person's response to questions) that trained security personnel rely on to determine if something is truly a threat or a false alarm, and then select an appropriate course of action. This suggests that current AV technology may not be well suited for certain airport threat-analysis activities.

3.2.7 Security Threat Resolution Capabilities

Security threat resolution in an airport environment is often the responsibility of trained law enforcement officers. There are many gradations of threat resolution, ranging from a friendly reminder to observe airport regulations to, in the extreme case, physically subduing and apprehending a person who is committing a crime.

In those situations where threat resolution does not involve human interaction, such as disposal of a potential bomb, autonomous vehicle technology can effectively augment trained law enforcement. However, based on our research, autonomous vehicles do not seem well-suited to airport security threat resolution scenarios that require rapid and complex interaction with other human beings.

3.2.8 Security Process Automation

Although not a security application per se, one of the most important ways AVs can help airport security operators is by raising the overall productivity of existing security processes.

These systems excel at repeatable tasks such as collecting images and other data, identifying anomalies, moving items, and requesting ID media checks. Many regulatory requirements encompass mundane tasks that autonomous systems can assist with, supplement, or complete independently. Additionally, these systems can often perform multiple tasks simultaneously. For example, an autonomous system mowing a remote area of the airport perimeter or cleaning a part of the terminal can also collect data and potentially report anomalous behavior or identify unattended baggage.

SECTION 4: CONSIDERATIONS FOR AIRPORT OPERATORS

In this section, we discuss a range of factors airport operators and security managers may wish to consider before deploying an AV system. The factors discussed include:

- Limitations on existing technologies
- Commercial product availability
- Legal and regulatory considerations
- Safety concerns
- Development level of effort and costs
- Liability and insurance issues
- IT Network integration, data transfer, and communications
- Cyber and network security challenges
- Maintenance and total cost of ownership/operation
- Environmental, climate, and terrain

4.1 Limitations on Existing Technologies

OPERATING ENVIRONMENTS

AVs currently available on the market are often limited to specific operational environments. The more complex the operating environment, the less likely a suitable AV will be available. Many systems are also not capable of operating on difficult terrain. This includes not only perimeter areas with uneven ground, unpaved area, and hills, but also indoor areas with slippery floors, changes in flooring, and variations in grade. The choice of chassis, wheelbase, wheels and tires, power source, and sensors all have an impact on a system's ability to operate in different environments.

MAPPING

Most AVs will require advanced coding or training to map new areas or create new routes. An airport without advanced, in-house technical capabilities may still be able to make simple adjustments to route maps and other basic settings, but complicated modifications will likely require intervention by the vendor or leasing company. An airport should consider the level of desired operational control and if they prefer a Security as a Service arrangement.

DATA COLLECTION

In an airport setting, the data collected by a system may lose its value if the volume of data collected exceeds the system's ability to analyze and present that data in a way that airport managers can understand and use. Software and AI may represent a solution for many of these systems, but require additional development to provide value in the airport environment. More complete, airport-relevant datasets must be developed for better use in the airport environment. Whereas most circumstances today require that a human remain involved, more robust AI datasets will help systems make decisions independently.

Additionally, Appendix E discusses the Security as a Service model where the system's overseer analyzes collected data and follows a predetermined decision tree if a situation requires resolution.

DATA TRANSMISSION

Some systems deployed today, including some systems observed for this project, are unable to transmit real-time data. Most often, transmission issues occur because of weak Wi-Fi or cellular signals.

Similarly, poor placement of transmitters and receivers may contribute to transmission problems, as well as the inability to capture appropriate data. The number and location of cameras, sensors, transmitters, and receivers is an important design consideration.

LIMITED FUNCTION

Many robotic systems designed to perform specific tasks tend to have fewer autonomous functions. Robotics experts believe that technology is available to perform more autonomous functions or semi-autonomous functions, but insufficient industry demand limits the availability of more advanced, multifunction systems. Companies that design and manufacture autonomous systems rely on clear direction and purchase commitments from end users regarding system capabilities.

Robotics companies will weigh the value of autonomous movement or function options against overall performance and system cost when deciding a system's level of autonomous capability. When a company chooses to enhance a system with autonomy, the decision is often based on their understanding of customer demands. Telerob, for example, knew that bomb detection teams wanted control over the system, but that they may benefit from certain autonomous capabilities. Telerob adapted their robotic arm by adding an autonomous mapping and movement feature.

4.2 Legal and Regulatory Considerations

Airport operators must consider rules and regulations for AVs to operate in the aircraft movement area, in remote perimeter areas, on public roadways controlled by the airport, and within the terminal in public or restricted areas. Operations in all of these areas will require questions relating to control, communication, and location be addressed. State and local governments' rules and regulations for AVs and FAA movement regulations and guidance provide some direction. As the number of AVs increases, regulatory restrictions will likely grow as well. Development of a program utilizing autonomous technology should anticipate changing regulatory requirements. In the meantime, however, airports will self-impose most protocols.

Pilot demonstrations of autonomous passenger vehicles on public roadways offer insights into relevant information to consider before permitting an AV operation. In these demonstrations, state motor vehicle administrations collect the following information deemed necessary for enforcement:

- The intended level of human control during the operation
- Vehicle specifications
- A list of drivers and controllers
- Training requirements for drivers and controllers for the specific vehicle
- Safety certification of prior-testing
- The manufacturer's safety plan
- Routes that highly autonomous systems will use

Policies allowing AV operations at an airport should also consider pre-operational notifications, communication strategies, training of operators and overseers, and strict requirements regarding where the AV will operate.

FAA regulations and guidance do not prohibit AV operations in the movement area of an airport, but they do require that airport operators ensure the safe movement of ground vehicles and pedestrians in the AOA. According to 14 CFR § 139.329, airport operators must limit movement, implement safety procedures for ground vehicles and pedestrians, have vehicle and tower communication rules, and require initial and recurrent training for vehicle operators. This regulation does not specifically address

AVs, but an airport may want AVs to comply with communications requirements. And, if a vehicle is truly autonomous, rules or exceptions may need to be put in place to satisfy the training requirement.

Airport operators should consider a gradual implementation of autonomous operations in any area of the airport. For example, in the case of an autonomous patrol robot, the airport can require more oversight to ensure the vehicle operates safely as the airport works to refine operational protocol. Once the airport gains confidence in its operation and has established protocol that works for their specific operating environment, the airport can reduce the level of oversight. During the SFO pilot project, the team found that a "progressive relaxation of rules and regulations regarding aircraft movement" was the best approach to finding the appropriate balance for an autonomous tug operation.

4.3 Safety Concerns

The safe operation of an AV is of paramount concern for both the airport and the AV companies. Ensuring the system will avoid people, objects, and aircraft is important to avoid injury and unnecessary damages, and to achieve operational goals.

The concern with these systems around people is how close they will get to a person before stopping and how tightly the robot maneuvers to stay on its planned path or the midpoint of its operating area. Smaller, quieter systems can easily surprise an unsuspecting person, but may include features such as flashing lights to enhance visibility. Larger systems are more noticeable to surrounding people, but have a greater capability to injure a person or cause damage if there is a misstep. Typically, systems use lidar, cameras, or combination of the two to detect objects and safely navigate their environment. A system controller may expand some of the parameters, such as the width of the operating area, but the sensor capability or other physical factors may limit movement changes.

Safety can also depend on the connectivity of the AV's sensors. Maintaining connectivity with sensors like GPS is necessary for navigation. In most cases, the autonomous system will discontinue movement as a default if the GPS signal is lost. However, the failure to move may itself pose a safety hazard in areas of aircraft or other operations. Backup communication capability, particularly linkage to human controllers, is critical to sustaining safe operations.

4.4 Development Level of Effort and Costs

AV movement and function development for a specific airport security purpose will require significant monetary and resource investment. Given that this is an emerging technology, security functions are currently limited. AVs frequently have a camera function and communication ability; other features such as badge and license plate readers are more of a novelty. The cameras that AVs carry for security functions can include the full range of camera technology, including megapixel and thermal imaging. The vehicles may also have lidar sensors for security purposes. Airport operators will have to decide whether to use a generalized system or develop their own system. Generalized systems will require less upfront cost and will deploy faster, but may require the airport to spend time developing and fine-tuning processes and procedures.

Airport operators may choose to create their own autonomous capability like Edmonton International Airport (YEG) did in partnership with a nonprofit, ACAMP (see Appendix G). Working with a nonprofit may cost less than a private corporation, but the system will still require significant resource investment on the airport's part to develop operational procedures.

Few off-road AVs currently exist on the market. With the complex terrains of airport perimeters, an airport may have to work with a third party to develop a system that can handle its terrain and perform the desired functions. Development of autonomous systems to work across diverse terrain can be very expensive.

Many hypothetical use cases for AVs in security operations involve patrolling of a terminal area or a perimeter. These systems will rely on AI to identify anomalies as defined by the end user. Most often, this will involve the use of a camera to send an alert if it sees a specific condition (e.g., a hole in the perimeter fence). AI cameras use detailed datasets that teach the system how to make decisions based on what it sees. Some highly detailed datasets are developed in a laboratory setting, which often creates challenges because the system does not learn discrepancies based on imperfect, real-world conditions, such as shadows, lighting differences, or weather. Many systems use Microsoft's Common Objects in Context (COCO) datasets. COCO develops its datasets of everyday scenes with objects in natural contexts in their lab setting. This type of dataset will lack the diversity needed for long-term autonomy over a variety of situations because of the limited range of pictures and conditions from a non-lab environment. Therefore, significant effort may be needed to develop a catalog of images of specific security situations, such as perimeter fence anomalies.

The current state of the technology is not favorable to customizations without the support of the original manufacturer, unless the vehicle manufacturer has provided its own selection of plug-in solutions. Most systems identified by the Project Team cannot augment their capabilities with plug-and-play sensors. Even with a tailored solution, the addition of sensors adds complications for processing powers and communications, particularly if real-time accessibility is desired. This adds to the cost and size of the operating platform.

4.5 Liability and Insurance Issues

AV experts and the automotive industry argue that AVs drive more safely than human-operated vehicles. However, the absence of reference data from operational use makes those claims difficult to substantiate. Accordingly, while insurance costs for an AV may eventually be lower than that of a human-operated vehicle, it is unclear when that transition will occur. Additionally, questions of liability have shifted to the manufacturer given that a system failure would cause an accident, in most cases.

The lack of comprehensive regulation may further complicate the insurance question. Compliance with federal, state, and local laws or regulations often impacts insurance costs. In the absence of such regulations, insurers will likely require extensive test data to assess the safety of these vehicles before they will insure their use around aircraft. Until the use of AVs becomes more accepted, premiums for ensuring such a vehicle may be substantial.

In most AV leases, the manufacturer or vendor covers liability. This was the case for all the deployments observed during the project.

4.6 Integration with an Airport

This section details the potential touchpoints and processing options the airport must consider when adding an AV to their existing security operations.

4.6.1 Integration Touchpoints

The challenges of integrating an AV into an airport's operation, including but not limited to its IT networks, vary depending on the specific vehicle. Identifying IT and non-IT touchpoints between the vehicle and its environment increases the likelihood of successful integration. Integration touchpoints to consider include:

- **Data:** The AV video and security sensors will interface with the existing video and security sensor management system, and with the personnel analyzing data. This integration will allow the airport to expand situational awareness across a wider area. The airport will also have to decide how to transfer, store, and access this data.
- **Wi-Fi or Cellular:** The AV will need to use a wireless connection or cellular data. The airport will need to consider which option is best based on cybersecurity considerations, signal availability, and cost. Accordingly, an accurate assessment of the cellular or Wi-Fi infrastructure is critical. Auxiliary beacons and antennas may be required. If so, it will be important to consider the number, location, power requirements, etc.
- **Public Communication:** An AV operating in a public or restricted area should have some ability to communicate with people when it comes into contact with them. As some of the demonstrations showed, the ability to conduct two-way communication is possible, but driven in part by signal strength and bandwidth. An airport can pre-program one-way broadcast messages or choose to communicate in real-time. This communication should include safe movement alerts and audio directions based on the mission objective.
- **Drive System:** The drive system of an AV will interact with the roads and walkways of the airport environment. The airport must consider wheel size and type to ensure the wheel and chassis is appropriate for the type of terrain the vehicle will traverse. A vehicle navigating smooth indoor floors will require a different base and wheels than a vehicle operating on rough outdoor terrain. The size of the vehicle also affects the wheelbase and turning radius. The larger the vehicle, the greater the difficulty in maneuvering in close quarters.
- **Navigation:** An AV may function near other operational equipment or manned vehicles. Extra lane markings may prove useful to assist AV navigation. Additionally, the airport should consider whether the pathway is easily recognizable by the vehicle's vision system. The use of such pathways may also serve to reduce traffic in the path of the AV.

  Additional considerations include GPS signal strength for indoor vehicles. If a building is unfriendly to GPS signal reception, then the vehicle that operates inside will need to use an alternative method of navigation.
- **Geofencing:** Most AVs use GPS to navigate. The airport will have areas that are appropriate and safe for AV use and other areas that are not. Appropriate geofencing boundaries provide an AV guidance to operate in specific areas and avoid others.
- **Power Supply:** The AV power supply system will interface with the airport's power distribution systems for charging. The airport should consider where the vehicle will charge, how often it will need to charge, how much power it will consume, and whether the vehicle will require a human attendant to plug it in. A well-placed charging station will enable the vehicle to continue collecting useful data while stagnant. The airport should also consider whether the charging station is safely placed out of pedestrian and vehicle traffic.

- **Employee Interaction:** All employees working in proximity of the AV should receive training regarding the system behaviors and signals to ensure they know how to work safely near the vehicle. For vehicles that need to interact directly with security personnel, long-range RFID tags embedded in employee badges can be used to help the vehicle identify individuals.

From a security standpoint, each of these touchpoints also represents a potential vulnerability. For example, charging stations are an important part of vehicle integration, but disabling a charging station can indirectly disable an AV, rendering it powerless and unable to complete its mission.

Table 4-2 identifies integration considerations when working with AV manufacturers and airport implementers.

Table 4-1. AV System Integration Considerations

AV Security Component	Integration Touchpoints	Airport Environment Considerations
Drive System	Autonomous-Specific Lane Markers/Wheels	Roads/Pathways Uneven Ground Indoor Flooring Stairs People Movers Elevators/Escalators
Power Supply System	Charging Station	Power Distribution System
Camera System	AV Remote Management System	Security Management Personnel Camera and Video Storage System
Sensor System(s)	AV Remote Management System	Security Management Personnel Sensor Data Storage System
Wireless Connectivity System	Auxiliary Antennas/Beacons	Wireless Connectivity Systems
Vehicle-Mounted Visual Status Indicators/Human Interface	Education for humans who will interface with AVs Long-range RFID tags for employees	General Public Airport Employees
GPS	Geofencing	Vehicle Keep-Out Zones

4.6.2 Onboard vs. Offboard Processing

Airports must consider where the AV’s system holds data and where it makes decisions, as these factors will impact the system’s ability to function and its vulnerability to cyberattack. AVs with onboard processing systems make all decisions onboard. Those with offboard processing send the data they collect to an external processing system and receive commands back from that system.

ONBOARD

Onboard processing AVs operate as self-contained units. The onboard system processes image and sensor data required for navigation and security threat assessments.

Wireless communication is used for notifying system managers of security risks as well as providing a “heartbeat signal” at regular intervals to indicate that the AV is functioning normally. Manual override of vehicle controls is still available at any time, initiated by either the vehicle itself or a human operator.

From a functional standpoint, this type of vehicle requires little to no extraneous hardware. However, the system manager cannot use sensor information from multiple vehicles to make high-level decisions. Additionally, recorded video stored onboard the vehicle without any remote backups is at risk for data loss. It also limits functionality for real-time operations. Creating backups for video and sensor data most often requires a physical connection for downloading to an airport system, ideally to occur when the vehicle is recharging its batteries. AVs that process all information onboard are larger in size in order to carry all the extra computing hardware required. Note that an AV system with onboard processing may, or may not be configured to support V2V connectivity, depending on a customer’s requirements.

From a security standpoint, when computation is done onboard the vehicle, wireless communication becomes less of a risk for hacking and jamming. If the AV does not require V2V capability to operate, attempts to disable a single vehicle are not easily spread to the entire fleet of vehicles due to the isolated nature of each vehicle. However, malicious actors may disable a security vehicle and mask the attack by sending false “heartbeat signals” to the system operator.

OFFBOARD

Offboard processing systems use servers for all complex processing. The vehicle transmits camera images and sensor data to the server, and the server interprets the data and replies with commands to the vehicle. However, the AV conducts basic navigation processes onboard because the lag time in wireless communication would prevent the vehicle from navigating in a safe manner.

Offboard processing may incur a delay if the system has a connection error. It also increases the system’s vulnerability to cyberattack, as the data sent wirelessly to and from the server can be intercepted and altered. Therefore, ensuring signal strength is strong and protecting the wireless network using the proper security protocols is especially important with offboard processing.

This type of vehicle also requires more bandwidth and additional server hardware installed on the AV. An offboard processing system generates more communication data and therefore requires more bandwidth to communicate with the vehicle sensors and more server hardware to process that data.

However, the system has the potential to coordinate an autonomous fleet of vehicles simultaneously to make more accurate assessments. Additionally, the server can store all recorded vehicle data as a backup for later reference. The vehicles themselves tend to be smaller because they do not need to carry as much computing power. However, auxiliary Wi-Fi or cellular antennas should cover all areas of operation to ensure thorough security coverage.

As the amount of useful data transmitted wirelessly increases, so do the potential vulnerabilities. Therefore, strong encryption algorithms are important. Encryption scrambles the data so that even if it is intercepted, the data is unreadable by unauthorized personnel. If the data is sent in cleartext and unencrypted, attackers can read it. Encryption helps prevent the unauthorized disclosure of data and the loss of confidentiality. NIST worked with industry and the cryptographic community to develop an Advanced Encryption Standard (AES) which has been published as FIPS 197.

In addition, attacks on the central processing server can potentially cripple multiple security vehicles simultaneously. However, it is much more difficult for attackers to mask a maliciously disabled vehicle from fleet managers.

HYBRID

Hybrid onboard and offboard processing vehicles navigate and make simple risk assessments on their own. For complex situations, the vehicle can initiate communication with its command server for decision-making aid. For example, the vehicle can look at a stretch of road and determine that the road is empty. However, if the road is not empty, then the vehicle can send the image to the main server to identify of classify the object on the road.

4.7 Cyber and Network Security Challenges

Airport operators must understand AV cybersecurity and related digital concerns before permitting a vehicle to operate on airport property or introducing a system into the airport network. AVs rely on a complex system of technologies to operate autonomously, which increases cyber vulnerability. Cybersecurity presents concerns related to the safe operation of the vehicle and network security when data is transferred to an airport system, as attacks may target the onboard processing systems, cloud storage systems, and the airport network.

Among other potential cyberattacks, autonomous systems can be jammed, spoofed, or infected with malware.

While the research team did not identify publicly reported instances of malicious cyberattacks on AVs or industrial robots, the vulnerability of these systems to cyberattack has been the subject of recent research.[5] In addition, a number of cybersecurity experts have demonstrated the ability to hack into the computer systems of automobiles.[6] It seems prudent to assume that as AVs become more widely deployed and connected to IT networks, there will be malicious cyberattacks against them.

As presented in the IEEE Technology and Society Magazine article, “Connected Vehicle Security Vulnerabilities,” common cyberattacks for specific sensors include:

- **GPS jamming and spoofing:** Jamming attacks send a strong radio signal to block all incoming GPS satellite signals from reaching the GPS devices. This would effectively shut down GPS navigation. A spoofing attack typically changes data to trick systems. The goal in a GPS jamming attack is for the AV to relay incorrect geolocation coordinates to the GPS devices by emitting fake GPS signals in range of the vehicle. This could trick the vehicles into avoiding certain areas and make navigation unreliable. The most common GPS is vulnerable to fake GPS satellite signals, and all AVs use GPS in some form or another. A robust vehicle should have the ability to detect when the GPS signal it receives is not correct by comparing the GPS location to its cameras and radar data.
- **Millimeter wave radar:** Radar jamming attacks can blind the radars of AVs. A robust vehicle will cross-check radar data with cameras and GPS signals to recognize a radar jamming attack.
- **Lidar sensor:** A simple transceiver can inject fake objects into a lidar’s field of view. Multiple wavelengths of lidar make it more difficult to project fake objects.

[5] See for example “Connected and Autonomous Vehicles: A Cyber-Risk Framework,” Transportation Research Part A vol. 124 (2019).
[6] See for example, Miller and Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” 2015.

- **Ultrasonic sensor:** Like lidar and radar, fake signals can blind ultrasonic sensors.
- **Camera:** Lasers or extremely bright and focused LED arrays can blind cameras.
- **Telematics service:** AVs may use wireless connectivity to upload video to a storage database, receive commands from the fleet manager, etc. This wireless connection is a potential access route for malicious attacks. Wireless communication needs proper encoding and securing to prevent over-the-air attacks. Ideally, the vehicle will also identify a false signal and alert the fleet manager that hacking attempts were made.

4.7.1 Protection Strategy

An airport using AVs should consider incorporating their operation into its broader cybersecurity strategy. Data transferred to an airport's network from a vehicle that has been subjected to a cyberattack may infect that network.

PARAS 0007 – *Quick Guide for Airport Cybersecurity* and ACRP Report 140 – *Guidebook on Best Practices for Airport Cybersecurity* provide cybersecurity-specific guidance for airport operators. These reports adopt the NIST Cybersecurity Framework that recommends five core principles to implement a comprehensive and systematic approach to cybersecurity. These are listed in Figure 4-1. The NIST standard was also adopted by the U.S. Department of Transportation National Highway Transportation Safety Administration (NHTSA) for AVs.

Figure 4-1. NIST Cybersecurity Framework

Identify your important assets, data, elements of risk, and vulnerabilities

Protect through technical tools, policy, or personnel-related methods.

Detect attempts to attack your network or data rapidly using various tools and techniques.

Respond to those attempts to counter the attack and contain any damage.

Recover to pre-event state and use lessons learned from the incident to improve the process.

One of the primary reasons wireless attacks are successful is because access points are misconfigured. The most important step to securing a wireless network is a strong security protocol, such as Wi-Fi Protected Access II (WPA2). WPA2 provides significant security improvements and uses stronger cryptography than older security protocols, which are susceptible to more attacks as the encryption is not as strong.

Staying current with software security updates is also important for maintaining a secure network. Software is not secure, and patch management is one of the most efficient ways to reduce operating system and application vulnerabilities. When software vendors discover bugs, they release code to resolve, or patch, the problem. Administrators must apply these patches to keep their systems up to date and protected against known vulnerabilities.

Good cybersecurity practices also include changing the service set identifier (SSID) on the wireless network from the default name to give the attackers less information about the network. From a defense-in-depth perspective, changing the name of the SSID is an extra layer of protection against attacks. It can also include using media access control (MAC) filtering. MAC filtering is a form of network access control that provides a small measure of security to a wireless network by allowing the airport to restrict access to its wireless network. The airport can use MAC filtering to block all new devices from connecting to the network or only allow for certain devices. However, many attackers can figure out which MAC addresses are allowed on a system and spoof a MAC address. Therefore, though MAC filtering is an important part of a defense-in-depth cybersecurity strategy, it should not be the only component.

A layered approach to AV cybersecurity reduces the probability of an attack's success and mitigates the ramifications of potential unauthorized access. Relying on multiple different sensors makes a vehicle safer and more robust, as each sensor requires a different jamming technique, and every type of sensor added makes it easier to detect attacks. However, the system needs to be able to differentiate attacks from faulty sensors.

Attacks come in various forms, requiring vigilance to ensure that software is up-to-date with the latest encryption and detection algorithms to deter attackers. AV companies that the Project Team interviewed in the course of its research consistently said encryption is their system's best cyber-defense. These companies lease the vehicles to end users and update systems that are already deployed as required.

NHTSA recommends limiting and controlling access to AV systems. Airport operators that allow outside entities to access the system should consider the NHTSA Cybersecurity Best Practices for Modern Vehicles, available on the NHTSA website.[7]

Finally, to remain proactive, the airport authority should consider penetration testing or vulnerability scans of relevant sensors. Penetration testing attempts to exploit vulnerabilities by simulating or performing an attack to determine the impact of a threat against the system and develop corrective measures if the attack is successful. The test helps an organization determine the extent of damage that an attacker could inflict by exploiting a vulnerability. However, penetration testing has the potential to disrupt actual operations, cause system instability, and lead to unexpected results.

Vulnerability scans offer a passive alternative to penetration testing. These scans can enable an airport to proactively identify cybersecurity weaknesses and issues that an attacker could exploit. Though a vulnerability scan does not interrupt operations like a penetration test, it can help determine which systems are vulnerable to attack. Both penetration testing and vulnerability scans allow airports to remain proactive against cyberattacks.

4.8 Maintenance and Total Cost of Ownership/Operation

The development of an AV program raises a host of questions regarding system maintenance. These questions involve the cost and technical requirements for software upgrades, or maintaining or replacing sensors, movement components, or function capabilities. Regular AV maintenance and inspection will, among other things, include sensor cleaning and calibration, false negative tests, visual inspections, and functional tests.

The complexity of these systems and the interrelationship between logical and mechanical components for proper operation require thoughtful consideration of maintenance requirements. As AV systems become more uniquely developed for airport uses, the maintenance challenges compound. Airports may not have on-staff technicians with the skills to maintain these systems.

To address the more complex issues, most manufacturers offer AVs through Security as a Service business models. These models mimic an equipment lease, where the vehicle manufacturer remains liable for maintenance of the vehicle and insurance of its operation. If the AV breaks down, the manufacturer repairs or replaces it. Any accidents or claims against the operation of the vehicle will fall under the company's insurance coverage. Each company will offer a different package that may require an airport to assume certain responsibilities.

[7] **Cybersecurity Best Practices for Modern Vehicles:** https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf

Simpler maintenance issues involve cleaning the sensors or ensuring the operating area is clean. For example, at LGA the terminal operator would wipe off sensors when dust or dirt began affecting the sensors' ability to read. Often, the terminal operator would notice the issue if the camera image was not clear.

Although the Project Team's research found that most AV companies provide maintenance and inspection services as part of their lease agreements, others sell the vehicle to the end user and offer no additional services. In these cases, the airport must ensure they can take on responsibilities or costs associated with maintaining the system or operation.

4.9 Environment, Climate, and Terrain

An airport operator should consider the operating environment when deciding whether the vehicle can operate in the intended area. The material of the indoor floor or features of the outdoor terrain will dictate whether the system requires a different chassis, wheels, or power drive. Similarly, if the system must go up or down a grade, the vehicle must have the appropriate vision, wheelbase, and balancing to handle the elevation change. Other logistical considerations exist as well. For instance, at DFW the system needed a clean area in which to operate properly. Therefore, the airport had to ensure that the floor was clean during the demonstration.

Implementing mitigation strategies to overcome these environmental challenges requires additional cost and complexity. As discussed above, AV systems currently on the market, by design, work either in an indoor or an outdoor environment, with limited exceptions for dangerous or hazardous operations. Further, these systems are often not designed to work in areas of high traffic or around humans.

The more detailed information that an airport operator can provide upfront to an AV company regarding the operating environment will assist in finding a solution that works.

SECTION 5: EVALUATION AND COST-BENEFIT ANALYSIS FRAMEWORKS

An effective test and evaluation plan will enable the airport operator to learn whether an autonomous system can safely perform a valuable function at their facility, and will provide the technology company with adequate information to meet required expectations.

When considering an AV technology, an airport operator must first establish a clear objective that defines the operating scenario. The objective should include a defined high-level scenario with specific goals that identifies the operational need and environment. The objective will enable the airport operator to set evaluation criteria, and enable the AV companies to assess whether they can meet the objective.

In creating this objective, an airport should think about logistics first and autonomy second. For example, in considering autonomous tug operations, SFO found the operation could reduce logistical challenges common to their AOA. Therefore, they looked at how the tug system will communicate within the existing AOA controller workflow and how predictive analysis can safely improve operations. The same concern applies in security. Benefits will come from efficiency and enhancing situational awareness. Communication plans and deciding what needs to be done and the lines of accountability are critical to ensuring the right people have the appropriate information to make decisions. With the communication plan in place, the airport can define what they want the system to report or what action they would like the system to take. This logistics planning will provide a base level for assessment that the airport can refine as it tests and evaluates systems.

With the objective in mind, the airport can then define the capability requirements to meet the airport's desired effectiveness, efficiency, and safety. Capability requirements should describe the overall objective area, desired system, and anticipated operational and support concepts in sufficient detail for a company to assess whether they can meet the requirements. Further, the requirements should provide insights into how the airport will determine if the AV is acceptable.

An airport may require the company to provide a safety assessment report of the vehicle before the evaluation test begins. Having a comprehensive report may reduce the safety testing that the airport will require and may enable the airport to test a more in-depth scenario. The report should identify potential hazards of the vehicle's operation. Similarly, an airport may require the AV's system to have prequalified sensors for specific uses. The airport will then only need to evaluate whether the sensor works as it is supposed to on the moving vehicle.

The initial evaluation should test the system at a high-level to see if it can meet the basic requirements of the operation. This evaluation can focus on the overall logistics of the operations and whether the vehicle under analysis can meet the standard. If the system meets the initial thresholds, additional subtests can analyze how well the vehicle can meet other specific functional requirements.

Finally, the airport should consider testing the logistics concepts they will need to employ to achieve operational efficiencies. This shall include workflow and communication, accuracy and comprehensiveness of the decisions based on the data provided by the system, and maintenance of the vehicle.

5.1 Evaluation Framework

The evaluation framework in Table 5-1 is based on NIST's robotics and AV testing standards, and the U.S. Army Developmental Test Command test standards. The criteria are designed to provide airport operators a thorough but achievable evaluation framework for AVs.

Table 5-1. Evaluation Framework

Objective	Define a clear objective for the operational need that considers the logistics that will provide an operational benefit. The objective should define the threat environment, success and failure, reliability, performance, operational environment, network expectations, and the desired level of safety.
Requirements	Complete description of the behavior of the system desired. Shall include descriptions of all the ways the airport intends to use the system and how the airport would like to interact with the vehicle. The requirements should include movement capability, software, and functional abilities.
Metrics	Metrics should ask questions that will help the airport determine whether the system can safely provide efficiencies and enhance security. Demonstrate that the operator, software, vehicle platform, control unit, mechanical operating devices, and applications can work effectively together.
Test Scenario and Procedure	Specify scenario and operating environment conditions to include subtests that challenge the criteria. This shall include a description of the task, the terrain, grade, and weather.
Data Collection	Consider component, subsystem, sensors, processing, and network.
Assess	Understand AV characteristics and assess reliability, safety, and performance.
Subtests	Conduct additional tests at a subsystem and component level. Airports should evaluate the key component systems that affect their stated objective.

5.2 Cost-Benefit Analysis (CBA) Framework

The merging of technologies such as AVs with traditional uniformed security and other physical security solutions is becoming the standard for many industries. When combined, multiple security components can deliver greater results and maximize budgetary efficiencies.

Facilities that need protection are demanding a comprehensive set of resources, tools, and service providers that generate situational awareness and analytics to ensure the integrity of their organization's systems, and risk mitigation in their security functions using a lower cost, high-value model. For example, some higher education campuses and hospitals compared the costs of manned live-video monitoring versus video analytics and chose to repurpose the stationed dispatcher for alternative uses. Establishing a virtual hub of threat intelligence, situational awareness, and critical event management is becoming a universal practice in the security sector. Many enterprises are realizing significant cost savings by utilizing hybrid solutions to secure a diverse range of properties and assets.

An emerging aspect of a hybrid security program includes AVs or autonomous robots that can assist uniformed security with patrolling, deterrence, communications, and hazardous situations. The addition of an AV for security may also reduce the overall program cost associated with security staff and allow capital to be deployed to other strategic initiatives.

Measuring the effectiveness of security investments is challenging, especially when it comes to proving the usefulness of deterrence and prevention-based mitigation strategies. Therefore, airports need to run their security purposefully, like a business unit, to extract maximum value from every operation.

When making the business case for purchasing security solutions, it is imperative to accurately capture the costs and benefits and compare them to other security assets. Recognizing and quantifying the value of specific security measures that address one or more risks helps to better prioritize an airport's investment. As with other capital expenditures, airports must ensure that a new security system will deliver its intended benefits in a cost-effective manner, which means examining the product’s expected ROI.

Both qualitative and quantitative methods should be used to achieve the best results when evaluating security investments. A well-documented and supportable CBA can be a powerful tool in justifying the need for particular security measures when competing for limited business resources. Below are steps to producing a CBA that can be used in assessing the value of adding AVs to an airport’s security program.

STEP 1: CAPTURE THE PURPOSE

When establishing the need for a security investment, it is important to address two primary decision aspects: value and priority. Is the proposed initiative worth the time, effort, and money that it requires? Answering this question requires a general understanding of what the security solution will accomplish and why it is important. Although risk mitigation is a key factor in prioritizing security expenditures, financial factors also feature high on airport’s priority list.

The description of the investment’s purpose should include a clear statement of the problem or problems to be solved, as well as the solution. Evaluating the airport’s threats and vulnerabilities, and assessing the respective countermeasures, both current and future, will set the stage for capturing those costs in calculating the ROI.

Gathering information that resides outside of the security department is essential and requires collaboration with other stakeholders in (and possibly outside of) the organization. In an airport environment, it is important for key security stakeholders to outline the threats and vulnerabilities that exist, and where there are gaps in addressing them and/or where they need to be addressed better. Then, the group can determine if AVs are an appropriate addition to the overall mitigation of the identified risks and whether they are cost effective.

STEP 2: INFORMATION GATHERING

The real value of ROI calculations is determined by the relevance, accuracy, and completeness of the cost and benefits data captured for the calculations.

The following formula is used to calculate the Total Cost of Ownership (TCO):

TCO = Cost to purchase + Cost to install + Cost to operate + Cost to maintain

TCO is the total cost over the expected lifespan of the system, and should factor in inflation where applicable.

To prepare an accurate ROI analysis, gather as much of the following information as possible. Acquiring the TCO for all the currently deployed security resources (e.g., uniformed security guards, access control systems, CCTV, perimeter detection capabilities, etc.) is necessary for comparing solutions to determine value. Some examples of ownership costs are salaries, training, administrative overhead, uniforms, vehicle maintenance, key cards, system maintenance, equipment service contracts, and background checks.

Other data points to consider for evaluating a security solution, especially one that is technology based, include long-term reliability, support services, hardware and software quality, materials used in construction, level of customization, and performance and maintenance records.

Best practices for data gathering include:

- Including all stakeholders that will be involved in the system's deployment, ongoing use, and outputs (e.g., the finance department, the IT department, customer relations, etc.) to ensure TCO is calculated correctly for each security measure.
- Interviewing potential providers' existing customers
- Reading vendor product data sheets and use case studies

In addition to the costs, it is important for the stakeholder group to also understand what kind of returns are associated with investing in security mitigation strategies. Most come directly from loss or damage prevention, but they can also come through efficiency gains such as automated systems that may reduce staffing levels.

The following techniques can be used to help airport stakeholders quantify the risks, costs and benefits of security:

- **Compare to status quo** – Use information about the existing security measures at the airport to compare with the proposed alternatives. Conduct industry-specific research to identify other airports' risk identification methods, expenditures and best practices.
- **Executive straw poll** – Seek input about the airport's risks, the cost of current security solutions, the cost of potential security incidents, the benefits of countermeasures already in place, and the benefit the proposed deployments could have on the security posture and financial picture.
- **Calculate costs of downtime** – Measure potential losses for not being able to deliver certain security services (e.g., recovery costs, compliance penalties, estimated future losses from reputational damage).
- **Identify regulatory needs** – Airports have baseline security thresholds they need to meet. Identify all areas that need to be managed for compliance (e.g., perimeter fence) and the total cost for managing them, including non-compliance fines. Analyze the results of regular internal audits that check whether all processes align with the security frameworks mandated by the standard, including the grades on recent regulatory audits, and identify areas for improvement.

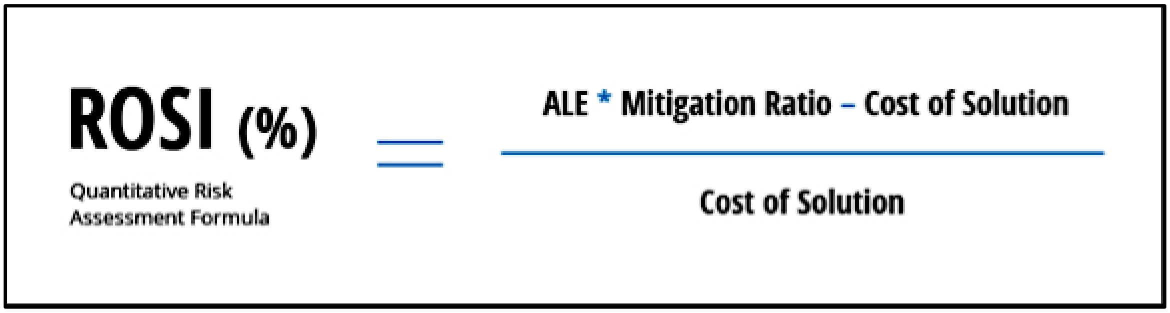
Airport stakeholders must perform the data gathering and ROI calculations for themselves and their own facility's circumstances rather than rely solely on information provided by security solution vendors. It is very important to make sure that risk and savings estimates are grounded in accurate and applicable data.

STEP 3: CALCULATE THE RETURN ON THE SECURITY INVESTMENT (ROSI)

Traditional ROI calculations, as mentioned above, are difficult to perform for security measures since many are aimed at prevention and deterrence.

The SANS Institute developed a method that can be used to determine the ROI for purchasing a security solution called the Return on the Security Investment (ROSI). The formula includes an assessment of the specific risks that a given security investment will address.

Figure 5-1. Return on the Security Investment (ROSI) Formula



$$\text{ROSI (\%)} = \frac{\text{ALE} * \text{Mitigation Ratio} - \text{Cost of Solution}}{\text{Cost of Solution}}$$

Quantitative Risk
Assessment Formula

Source: blog.netwrix.com

The ROSI calculation includes the following components:

1. **Annualized Loss Expectancy (ALE):** The estimated amount of money that will be lost in a single security incident (Single Loss Expectancy) multiplied by the estimated frequency that a threat will strike within a year (Annualized Rate of Occurrence).
2. **Mitigation Ratio:** This is the percentage of security threats that the solution would deter or prevent. For example, if an airport is considering investing in a fleet of AVs that is expected to reduce the risk of unauthorized persons in the secured area by 35%, the mitigation ratio equals 35%.
3. **Cost of Solution:** For the ROSI calculation, this is the annualized TCO. For example, if the TCO is $500,000 for an expected 10-year lifespan, the annualized TCO will be $50,000 ($500,000 ÷ 10).

The higher the ROSI % value, the higher the return on a given security investment.

Even if the data used in the ROSI calculation is slightly inaccurate, using this model in a repeatable and consistent way will enable airports to compare the relative value of different security investments over time.

STEP 4: TEST AND EVALUATION

After implementing a security measure, threat simulations will help test the effectiveness of a security program. Then, comparing the results with previous simulations, airports will be able to establish and track metrics. Collecting the security metrics will further assist airports in allocating the budget wisely by providing actionable data about how the current security strategy and investments are working, determining which areas need improvements, and feeding into the next CBA process for proposed new security investments.

SECTION 6: FUTURE DEVELOPMENTS

Subject matter experts agree that AVs capable of reacting to unexpected changes in the environment without human involvement are unlikely to be commercially available for at least three to five years. Instead, this research indicates that in the next one to five years, there will be incremental capability improvements, primarily in sensors, movement control, and AI/machine learning.

Experts expect lidar technology to become more affordable and accurate over the next few years. The accuracy of GPS technologies is also improving; it is predicted that GPS trackers will soon locate within centimeters of an asset. Increased accuracy provided by GPS technology helps ensure that an AV stays in its lane and away from other vehicles or objects. Improved GPS technology also provides users monitoring a system more precise information regarding where the vehicle is and where it is going.

Cameras are another type of sensor used in AVs that experts expect to see improvements in over the next several years. One area of improvement will be in the development of high-resolution 3D cameras to obtain 3D data for improved object recognition. Another area of improvement will be through the development of advanced “eagle-eye” cameras that have both high central and peripheral image resolution capabilities to reduce the number of cameras required.[8]

AV movement capabilities will also continue to improve, in particular the ability of vehicles to operate in challenging and unpredictable outdoor terrain.

The last major near-term capability improvement for AVs will be in AI/machine learning. For example, it is expected that AVs will have fewer false alarms related to detection of potential threats, suspicious items, and persons.

[8] ““3D Cameras in Autonomous Vehicles,” Future Markets Magazine (https://future-markets-magazine.com/en/markets-technology-en/3d-cameras-in-autonomous-vehicles/)

SECTION 7: CONCLUSION

AV technology, while not yet capable of complete autonomy from human involvement, has progressed sufficiently to be of value to airport security operators, under certain conditions, and subject to airport safety, budget, technical, IT, and other practical considerations.

There have now been enough US airport trials of AVs for security applications to provide a base of empirical data and lessons learned for other potential airport users. In short, there are now "airport tested," commercially available solutions designed for industrial security applications relevant to US airports.

There are certain airport security-related applications that current AV solutions are better suited for than others. These include deterrence of criminal and disruptive behavior through random and planned vehicle patrolling of airport environments; security surveillance, communication, and situational awareness; and using AVs to reduce risks to human safety from hazardous activities such as EOD.

However, most examples of US airport applications of AVs have less than one year of operational performance to rely upon, and that in all the examples examined or observed, deployments required a significant upfront investment in planning, as well as modifications to the airports' existing infrastructure. Trial deployments uncovered unforeseen issues that, while manageable, required extensive involvement by airport staff to resolve. In short, AVs are far from being a plug-and-play solution. It is important, therefore, for airport operators to use a documented framework to assess the AV solution being considered, and to perform an analysis that fully reflects the direct and indirect costs of deployment.

REFERENCES

American Association of Motor Vehicle Administrators. 2018. “Jurisdictional Guidelines for Safe Testing and Deploying of Highly Automated Vehicles.”

AUVSI. 2018. “Automated Vehicles Symposium.” San Francisco, CA.

Beale, Alexander F. 2018. “Who’s Coffers Spill When Autonomous Cars Kill? A New Tort Theory for The Computer Code Road." *Widener Law Journal 27, no. 2*, 215-48.

Beer, Jenay M., Arthur D. Fisk, and Wendy A. Rogers. 2018. “Toward a Framework for Levels of Robot Autonomy in Human-Robot Interaction.” *Journal of Human-Robot Interaction 3*, 74-99. doi:https://doi.org/10.5898/JHRI.3.2.Beer.

Berger, Michael Carroll and Stephen. 2015. “ACRP Report 127: A Guidebook for Mitigating Disruptive Wi-Fi Interference at Airports.” Airport Cooperative Research Program.

Geistfeld, Mark A. 2017. “A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulations.” *California Law Review 105, no. 6*, 1611-1694.

Gopalkrishnan, et al. 2013. “Cyber Security for Airports.” *International Journal for Traffic and Transport Engineering*, 365-376. https://dx.doi.org/10.7708/ijtte.2013.3(4).02.

Hobert, Laurens, et al. 2015. “Enhancements of V2X Communications in Support of Cooperative Autonomous Driving.” *IEEE Communications Magazine 15* (12).

Hui-Min Huang, ALFUS Working Group. n.d. “Autonomy Levels for Unmanned Systems.” National Institute of Standards.

James M. Anderson, Kalra Nidhi, Stanley D. Karlyn, Paul Sorensen, Constantine Samaras, Oluwatobi A. Oluwatola. 2016. *Autonomous Vehicle Technology: A Guide for Policymakers*. Rand Corporation: Rand Corporation.

LG. 2017. “LG Airport Robots Take Over Korea's Largest Airport.” July 21. Accessed August 12, 2018. http://www.lgnewsroom.com/2017/07/lg-airport-robots-take-over-koreas-largest-airport/.

Petit, Jonathan, and Steven E. Shladover. 2014. “Potential Cyberattaches on Automated Vehicles.” *IEEE Transactions on Intelligent Transportation Systems 16* (2): 546-56. doi:10.1109/TITS.2014.2342271.

Phenix, Matthew. 2014. “Hands off with Heathrow’s autonomous pod cars.” November 13. Accessed August 12, 2018. http://www.bbc.com/autos/story/20140910-hands-off-with-heathrows-pods.

Saidi, Kamal. n.d. “Overview of the Challenges and Opportunities for Testing and Use of Robotic Technologies at Nuclear Facilities.” *U.S. NRC’s 28th Annual Regulatory Information Conference Session T9 - Development of Robotic Technologies at Nuclear Facilities.*

Shaw, Kristen Vanderhey. 2017. “Detroit Metro Pioneers Ergonomic Improvements in Checked Baggage Screening.” *Airport Improvement.*

Society of Automotive Engineers International . 2018. *SAE.* December 11. Accessed December 14, 2018. https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-driving-vehicles.

Takefuki, Y. 2018. “Connected Vehicle Security Vulnerabilities [Commentary].” *IEEE Technology and Society Magazine 37* (1): 15-18. doi:10.1109/MTS.2018.2795093.

Transportation Security Administration. n.d. “Security Directive 1542-04-08 Series.”

U.S. Army Developmental Test Command. 2009. “Testing of Unmanned Ground Vehicle (UGV) Systems.”

Vanderhey Shaw, Kristin. 2017. “Detroit Metro Pioneers Ergonomic Improvements In Checked Baggage Screening.” Airport Improvement https://airportimprovement.com/article/detroit-metro-pioneers-ergonomic-improvements-checked-baggage-screening.

Voelzke, Gert Rudolph and Uwe. 2017. “Three Sensor Types Drive Autonomous Vehicles.” *Sensors Online.* https://www.sensormag.com/components/three-sensor-types-drive-autonomous-vehicles.

Wired Brand Lab. n.d. *Wired.* Accessed June 4, 2019. https://www.wired.com/brandlab/2016/03/a-brief-history-of-autonomous-vehicle-technology/.

APPENDIX A: AUTONOMOUS VEHICLE TECHNICAL INFORMATION

OVERVIEW

This appendix details AV technical information for the following areas:

1. Core Navigational Systems
2. Mapping
3. Maneuverability
4. Charging Considerations
5. Maintenance and Inspections

AV NAVIGATIONAL SYSTEMS

- Cameras perform a function similar to human information gathering and rely on advanced computers to analyze the data they collect.
- Lidar uses lasers to create an image of a vehicle's surroundings.
- Radar assists vehicles by collecting and assessing data related to distance, form, and size of objects.
- GPS tells the AV where it is located within a space.
- Ultrasonic sensors measure the distance of objects to a vehicle.
- Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication involves vehicles wirelessly sharing location, speed, and direction data.

Autonomous systems rely on three core sensors to collect data and create AI for assessments: cameras, lidar, and radar. Other systems supplement the core sensors by providing further data and insight to inform the vehicle. Detailed datasets teach systems what they have seen and inform them how to process the data into actions.

CAMERAS

Cameras provide AVs the ability to see a complete view of their surroundings, including lane markings and signs, to navigate without human interdiction. A computer develops a 3D map of the vehicle's surroundings based on the camera's input.

Visual spectrum cameras work well in lit areas, while infrared cameras work well for darker settings. Visual spectrum cameras require an alternative source of light, such as a streetlamp or headlamp, when ambient light is insufficient.

Cameras collect a large number of images, which require significant processing power to analyze. Even with the added processing power expense, cameras cost less than lidar.

An airport should consider their specific environment to ensure the system has proper camera technology. Cameras experience challenges with functioning properly in adverse weather conditions when visibility is limited, such as rain, snow, or fog.

LIDAR

Lidar sensors create an image of an AV's surroundings through the process of echolocation. Lidar systems emit laser lights to measure distance based on the time it takes for the lights to return to the system. A computer couples the echolocation data with GPS coordinates and inertial measurements to create a clear and comprehensive image of the surrounding area. Lidar works well in both long and short ranges and can provide millimeter resolution maps of its environment.

Similar to cameras, lidar requires increased processing power to analyze the highly detailed data it has collected.

Some lidar systems have the ability to convert collected data into images that humans can interpret. For example, a system may measure the density of an area and inform the airport where pedestrian congestion is currently located. Depending on the individual needs of an airport, the ability to visualize lidar data on demand may present useful security information.

Lidar will operate on a specific frequency and wavelength, and these frequencies should be communicated by the AV manufacturers to the airport to avoid laser-based system interference.

The disadvantages of lidar include cost and the potential for inaccurate data in the event of an element or system failure. Weather, dust, and other airborne conditions that scatter lidar’s small wavelengths can also cause lidar to return inaccurate data. Some lidar units have self-cleaning capabilities. If the lidar cannot clean itself, then extra effort will be required on the part of the airport operator to ensure that dust and dirt do not build up on the lidar units. At LGA, the Knightscope K5 AV operated outdoors. The terminal operator would clean its sensors if necessary, and Knightscope would provide maintenance as necessary.

In assessing the strength of the AV’s ability to perform tasks, the airport should inquire about the effect of environmental conditions on the AV’s ability to navigate. Some AVs will only be suitable for operation in controlled indoor environments. However, as noted in the demonstration, even within these environments, structures like glass walls, may adversely affect the ability to operate.

RADAR

Radar assesses distance, form, and size of objects for AVs. Radar operates by sending radio waves that bounce off objects and reflect to their receiver to establish measurements. The receiver assesses patterns and frequency of the returning waves. The series of incoming data from an object enables radar to determine movement direction and speed of the object. Radar systems have varying distance ranges and view angles. Increasing one of these will compromise the ability of the other. Therefore, deploying multiple complementary radars may be necessary to create a complete picture and assess an AV’s surroundings.

Radar is inexpensive and becoming readily available.

Radar is reliable for distance measurements, but not for detailed observation of an object. Lidar provides better detail of objects observed.

Certain weather, such as heavy fog, may affect radar. The manufacturer should communicate these limitations to the airport operator and add sensors to compensate for the airport environment.

Similar to lidar, the airport operator should understand the operational frequencies of radar systems to avoid interference.

GPS

A GPS device uses satellites to determine its position. Standard GPS is accurate within a few meters, especially at high speeds. Currently, GPS systems require additional inertial measurement units, such as tachometers, altimeters, and gyroscopes, to accurately position a vehicle. New GPS technology has increased accuracy capabilities. Most AV systems will rely on GPS systems that are accurate within a few centimeters.

Airports should ensure that all areas where AVs will operate have sufficient GPS reception. Additionally, the airport should understand the AV’s behavior when the GPS signal is lost and what actions, if any, the airport operator must take to revive an AV that has lost the data necessary to localize.

Geofencing is the process by which GPS is used to define the operation boundaries of an AV. The ability to quickly, easily, and dynamically modify geofences is a desirable feature. Both the Turing Nimbo, demonstrated by the Project Team at SJC, and the Knightscope K5, operated at LGA, operated within a 5-meter geofenced area.

ULTRASONIC SENSORS

Ultrasonic sensors emit a soundwave and measure the reflection of that wave off objects to determine distance. Ultrasonic sensors are inexpensive and easy to use. Of the sensors addressed in this report, ultrasonic sensors are the least affected by airborne debris.

Ultrasonic sensors offer excellent secondary obstacle detection but are generally considered insufficient for full autonomous capability.

V2V

V2V systems wirelessly share location, speed, and direction data between vehicles. V2I systems involve the same information sharing that occurs between a vehicle and buildings or other structures. V2V and V2I present privacy and hacking concerns. V2I requires extensive infrastructure investment and maintenance.

V2I-enabled AVs could work in conjunction with other security features that airports already use, such as door-breach detection systems or fence-mounted vibration detection systems around the perimeter. An alarm from one of those systems could potentially alert an AV to investigate the situation faster than a human would respond.

Considerations for airports include asking if the AV is capable of interfacing with security features they already have or if the system can accommodate future systems.

MAPPING

AVs require training before operating in a new environment. Training of a system is often accomplished using a combination of two techniques: environment mapping and training drives. Mapping involves manually generating a software model of the operating environment to function as an internal map for the vehicle. The map illustrates pathways, intersecting human and vehicle traffic routes, and stationary obstacles to avoid. The vehicle uses GPS or other forms of geolocation technology to ascertain its own position within the map.

The Turtle system that Virginia Tech demonstrated at the Safe Skies Perimeter Test Facility in April 2019 uses an environment mapping process. An engineer programmed data into the system based on maps provided by the Safe Skies team. The system then used this data to perform its autonomous functions onsite.

The training drive process involves a human remotely operating the vehicle through its route while the vehicle’s sensors record the route and learn how to replicate the route in autonomous mode. Depending on the type of AV, the number of training hours will vary, but an adequate number of training runs in various light and weather conditions supports robust autonomous function.

The Project Team's first demonstration of Turing's Nimbo at SJC used this combined technique to map its routes. An engineer steered the vehicle though the desired route, and the system set waypoints at set increments on the map developed by the AV's software. During the training, the system mapped the area within its computer and created the path for it to follow. The engineers set multiple paths within the area to direct Nimbo to run different scenarios. Nimbo followed these paths within a preset boundary and hit each of its waypoints. The team mapped three areas and set multiple paths within each area in four hours.

Stationary landmarks and electronic beacons present an alternative geolocation method for AV navigation. The stationary landmarks and beacons can locally triangulate or visually verify a vehicle's position. An AV requires adequate beacon coverage to ensure effective operation. An airport should consider whether the beacons inhibit other airport functions. This option may work best in remote areas of the airport.

Mapping for AVs is slightly different from mapping for vehicles. When mapping for a vehicle, the route is 100 percent pre-planned. The vehicle may stop for obstacles, but it will not deviate from its route. AVs do not map strict routes. They designate operating areas and treat routes as suggestions. The vehicle will then navigate around obstacles, as long as it stays within the boundaries of the operating area. As discussed earlier, AVs use GPS waypoints as a geofence to define operating areas.

In considering a system's mapping capability, the airport operator should think about how remapping is done and how long it will take to complete the process. The AV may have the ability to autonomously remap or will require minimal human guidance, allowing most non-technical airport staff to complete the task. Other systems will require software coding for the system to learn the new area. This may require a level of technical expertise that the airport may not have on staff. Additionally, the remapping process and complexities of the area may affect how remapping needs to occur and the time needed to complete the process.

MANEUVERABILITY

AVs can incorporate various drive systems, which affect vehicle performance, versatility, and load capacity. Tank drive, Ackermann steering, rear-wheel steering, four-wheel Ackermann, Mecanum, and Omni all offer different advantages and disadvantages on AV systems. Tank drive vehicles utilize two interdependent drive train systems with an independent set of wheels for each side of the vehicle for increased maneuverability. Ackermann steering and alternative Ackermann steering utilize four wheels to increase straight-line stability. Four-wheel Ackermann enables the front and rear wheels to steer left and right opposite of each other to reduce the steering radius. Mecanum and Omni drive systems utilize special directional wheels that allow a robot to maneuver in all directions without the vehicle itself rotating.

The Nimbo product demonstrated at SJC uses a Segway-based tank drive system. Knightscope's K5, which was used at LGA's Terminal B arrivals curb, uses an Ackermann drive system.

Airports should consider the area where the vehicle will operate and the objective when choosing if the drive system is appropriate for their scenario. A system that will operate off-road and will require a different drivetrain and wheels than a system operating indoors on a tile floor.

CHARGING CONSIDERATIONS

An airport's AV operation planning process must consider system power. The airport should balance operational considerations with charging requirements to set operational parameters or assess how many systems they require to achieve a stated goal.

AVs typically have dedicated and separate electrical power circuits and controls for the individual systems on the autonomous systems because autonomous sensors and computers require precisely controlled electrical voltages and currents to function optimally. The systems internally regulate and monitor their electric capacity and well-being.

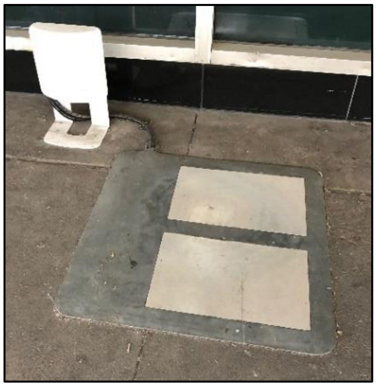
Battery-based electric vehicles require plugging in or docking on a charging station to charge. Both charging processes take time, especially compared to filling up a gas tank. However, many autonomous systems can monitor their own battery charge and automatically return to a charging station to recharge. Other systems may require a person to plug the vehicle into an outlet or change the battery.

Battery life is a significant factor in terms of cost and maintenance. An inverse relationship exists between discharge rate of the battery and the gradual decrease in the battery's capacity.

This ratio changes based on the end user's desired runtime versus downtime. Additionally, the number of systems available to operate will affect planning.

Nimbo, demonstrated at SJC, can place itself onto a charging pad, as necessary. During the demonstration, the system never needed to recharge. The vehicle started with a full charge on the first day of the demonstration and had 30 percent of its battery life remaining at the conclusion of day two. This included four hours of mapping and four hours of demonstration time. Turing recommends that Nimbo run with battery strength between 80 and 30 percent.

Figure A-1. Knightscope Charging Station at LGA



At LGA, the Knightscope's K5 system was set up to stop at a charging station along its route as needed (see Figure A-1). Two charging stations were placed along the route and positioned so that the AV could continue to perform monitoring functions while it was charging. The terminal operator established a charging strategy to maximize patrol time and minimize charging time. As a result, the system would stop at a charging station more frequently, but would not need to stay on the charging pad for as long.

AVs use a variety of voltages for different functions. Using a high voltage circuit in a vehicle will require proper labeling and safety precautions. Employees who perform maintenance on high voltage circuit vehicles should take high voltage training. Such training is usually not required for day-to-day charging operations.

A series of challenges exists regarding charging methods. For small robots, fast charging is normally not necessary, but for a full-size, fully electric vehicle, the goal is to provide as much range as possible in the least amount of time. The traditional chargers that exist for hobby-sized batteries, for small robots, RC planes, or toy cars would be too small to charge these AVs. Meanwhile, the charging infrastructure for electric vehicles provides more power than the small AVs can handle. Therefore, the charging system will likely come with the AV and be designed specifically for the product.

The power necessary for an AV will depend on the vehicle's size and capability. AVs tend to use an electric-based system for a consistent charge distribution. Some vehicles may use a hybrid system. A well-integrated electric battery system will require only one charge for the fully electric system, whereas a gas vehicle may require two separate charging functions: gas refuel and electric charge. Edmonton International Airport's AV uses a Polaris Ace 570 as the base vehicle, which runs on gasoline. The steering, acceleration, and braking were altered to use drive-by wire. The autonomous sensors are powered by a separate onboard battery. Therefore, the airport must fill the vehicle with gasoline and charge the battery running the autonomous systems.

Although not popular, engineers have started to consider fuel cell power systems for AVs that will operate on long missions. Hydrogen fuel cell vehicles rely on hydrogen gas to power an electric motor. Fuel cell vehicles have the advantage of being refueled quickly, like gasoline vehicles, as opposed to the long charge of a traditional battery electric vehicle. They present a strong option for security vehicles but would require a hydrogen fuel storage system in place that can be resupplied.

Infrastructure for hydrogen fuel is expensive and the research team is unaware of any airport at which it currently exists. Once infrastructure is in place, airport operators may consider hydrogen fuel as an option.

MAINTENANCE AND INSPECTION

AVs will require maintenance and inspection. Airport operators that have considered AVs have raised maintenance and inspection as a challenge, as they do not have the in-house resources or expertise. Although the Project Team’s research found that most AV companies provide maintenance and inspection services as part of their lease agreements, others sell the vehicle to the end user and offer no additional services. Therefore, an airport may have to consider whether it can service and maintain the system.

Regular maintenance and inspection will, among other things, include sensor cleaning and calibration, false negative tests, visual inspections, and functional tests.

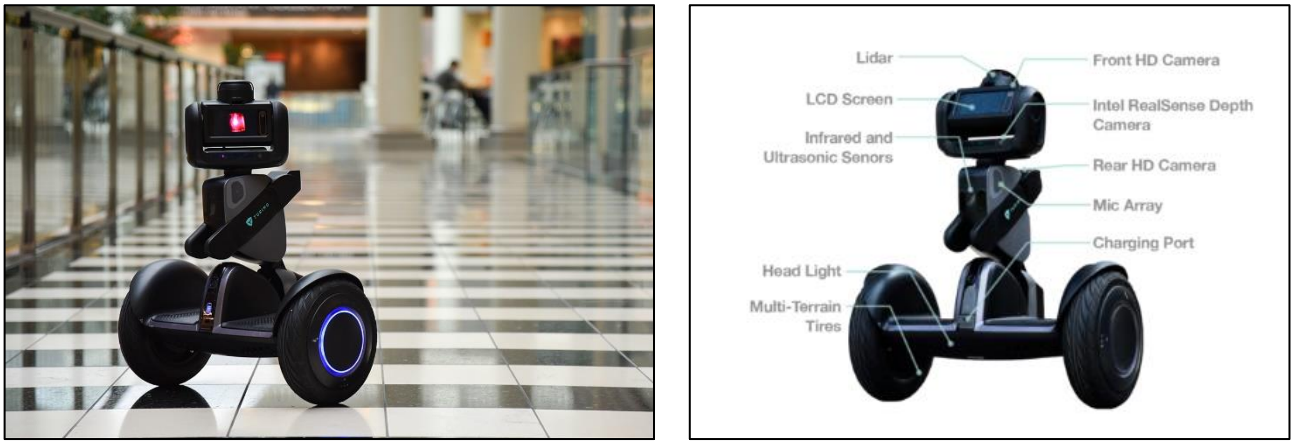
APPENDIX B: TURING VIDEO NIMBO DEMONSTRATION AT SJC

OVERVIEW

Turing Video's Nimbo autonomous robot is a combination of Segway's movement system, Intel's RealSense depth camera, lidar and ultrasonic sensors, as well as proprietary artificial intelligence algorithms. The system was demonstrated at San Jose International Airport (SJC) in San Jose, California in December 2018.

The Nimbo system is capable of autonomous patrol and charging, two-way video and audio communication, customized and automated responses to detected events, unlimited map and route storage, and has over 80 recognition categories. Nimbo can be controlled remotely from an iOS device.

Figure B-1. Turing Video Nimbo



Source: hellonimbo.com

Source: turingvideo.com

SPECIFICATIONS

- Dimension: Height 26 in., Length 23 in., Width 11 in.
- Weight: 42 lbs.
- Speed Limit: 10 mph
- Battery Life: 10 hours. Generally, runs between 80 and 30 percent when deployed.
- Charging Time: 2 hours on dock, 1 hour when directly plugged in.
- Local Storage: 128 GB

DEMONSTRATION OBJECTIVE

Assess whether Nimbo can successfully navigate obstacles and people in the area, effectively communicate with airport stakeholders, and capably follow a person of interest after receiving direction from airport operations.

DEMONSTRATION METHOD

1. Establish a map that patrols areas of concern identified by the airport for Nimbo to follow.
2. Establish communication methods for Nimbo to report its findings to airport operations.
3. Introduce anomalies for Nimbo to identify and report, and for the airport to assess its response.
4. Require Nimbo to autonomously return to its charging station to recharge.

SETTING AND PLAN

SJC’s public area includes two separate terminal baggage claims, ticket counters, and rental car lobbies in a consolidated rental car facility. The demonstration focused on two areas within the public area that have low ceilings and obstructions impeding optimal CCTV coverage.

- **Area One:** The Terminal A baggage claim area consists of two connected areas with two baggage carousels each that are separated by an elevator bank and an escalator in the middle. There is a glass wall between the inside area and an outdoor curb that has some opaque objects lined along the wall in various places at lower heights. The core area allows passengers to proceed to the adjacent parking structure or across a pedway bridge to the terminal ticketing area. Movement around the core allows passage from one baggage claim area to the other. The area is 3,120 square feet.
- **Area Two:** The Blue Dot Lounge is an area adjacent to the Terminal A passenger security screening checkpoint, an exit lane, and a concession stand. The area has a large, circular barrier in the middle with seating sporadically placed around to create a lounge setting, and is enclosed by two pedestrian walkways. The patrol area included approximately 2,000 square feet.

During the day, both areas have pockets of heavy traffic that ebb and flow as flights arrive and depart. The areas have minimal foot traffic overnight, but some individuals use these areas for shelter.

To address day and night operations, the demonstration was set up to assess whether Nimbo had the ability of an AV to navigate the area, avoid people and obstructions, follow a predefined path, record video, transmit that video to airport operations/law enforcement, and communicate with individuals in the area.

In both demonstration areas, Nimbo was programmed with alternative patrol routes. In Area One, the routes followed a circle and a figure-eight pattern. In Area Two, circle and semi-circle routes were used.

SYSTEM MAPPING

To autonomously navigate the SJC public areas, Nimbo was trained through a mapping process that predefines an operational path for the system to run. A Turing engineer remotely controlled the Nimbo around the chosen areas to set pre-planned routes. As the robot proceeded through the terminal, it used its lidar and ultrasonic sensors to create a map of the terminal and a route map with waypoints. The waypoints represent spots in the terminal where the robot makes slight course corrections or changes in direction. Nimbo continuously enhances its map as it patrols an area.

DEMONSTRATION SUMMARY

Nimbo operated over the course of three hours in Area One and one hour in Area Two. Nimbo followed multiple predefined routes within those areas. During the course of this operation, the number of people in the areas varied significantly, from a couple of individuals to over 100 at a time. Nimbo appeared to effectively navigate tight spaces with many people and objects in the area.

In Area One, Nimbo did not appear to impede anyone’s path. In Area Two, near the exit lane, the generally tight area was made smaller when chairs were moved into the walkway. Nimbo appeared to have no problem avoiding the moved obstacles. At one point, a fast-moving pedestrian appeared stuck behind Nimbo moving at its normal pace. It was not clear if the person was hesitant to walk around the system, which he could have, or if he was intrigued by and watching Nimbo.

Traveling within a 3,120 square foot area, Nimbo was able to complete loops within the baggage carousel area without many people around in four minutes at 0.7 meters per second. With numerous people in the area—at times over 100 people—Nimbo was able to complete loops in seven to eight minutes. The Blue Dot Lounge loop had consistent and quick fluctuations in the number of people present. Nimbo completed the loop in this environment in three minutes.

The system was able to navigate through a dynamic crowd without contacting any people. Nimbo's avoidance system created a virtual barrier around the robot, stopping it if an object was discovered in its path. At several points during each operation, Nimbo would stop and adjust its path to move around stationary or moving objects and then continue its route.

Nimbo did contact the low end of a backpack that was thrown into its path. The sensors used for object detection likely were not low enough to sense the backpack's edge.

During the setup period, the Turing team demonstrated Nimbo's capability to stream live video, create and send notices of persons observed in the area, and two-way communicate. Turing operated the system using the airport's public Wi-Fi and reported slow processing speeds. To effectively use these capabilities, Nimbo would need robust Wi-Fi or cellular service.

The Wi-Fi speed was an issue during the demonstration as well, as the system experienced latency in transmission of data to effectively sync alerts with the appropriate video. Turing noted that this issue is easily rectified by stronger Wi-Fi or cellular service.

The Turing team did express concern when Nimbo would move behind an individual. Because of its small profile, they aware of the possibility that an individual would trip over the system without seeing it. Turing had the robot play music while it patrolled to prevent it from sneaking up underfoot. In our observation, people were aware of the robot and did not appear surprised if it approached from behind.

SCENARIO-SPECIFIC FINDINGS

Scenario 1: Operate Nimbo for one hour with people walking in the area as normal

Can Nimbo successfully navigate the area with people walking through? Nimbo appeared to navigate through the baggage claim areas without difficulty. The system avoided people and handled situations where individuals toyed with the system. In the baggage claim area, the number of people present varied from two or three to over 100 when baggage from an arriving flight was being unloaded. The rotations, which took three minutes, were affected by the need to navigate around individuals when the baggage area was full of people, but it was not appreciably different to consider the operation ineffective.

Compare the number of people identified by Nimbo with that of an observer. Nimbo's vision was limited by the front-facing camera on the system. At times, it did not see people sitting on a bench in the corner of its path because the camera was not positioned to face that area. Remedies for the limited vision include: (1) better planning of Nimbo's route to see that area with the camera capability it has onboard; for example, the system could have paused and turned to see the area; (2) placing additional cameras on the AV to see a greater area; (3) putting a different camera on the AV; or (4) extending the range where the camera would alert on individuals.

Compare Nimbo presence in an area to law enforcement presence. In Area One, Nimbo operated for four hours. No law enforcement or security personnel were present, and the situation did not dictate they should have been present. In Area Two, TSA was operating nearby, and airport officials consistently walked past.

Scenario 2: One person walking through the area in a random pattern

Does the robot detect the person? Yes, if the person walks in front of Nimbo's path. If the person saw the robot before entering the area, they could have avoided detection. Again, line of sight of the camera needs to be considered.

How far away does it make the identification? Approximate radius of 5 feet

Scenario 3: One person walking through the area trying to avoid Nimbo detection

Does Nimbo detect the person? Yes, when the person is not expecting Nimbo and Nimbo is near where the person enters at that time.

Does Nimbo or airport operations communicate with the individual? Yes, this system could send pre-recorded messages, or a person could record a message and send. The communication was not live. Live communication was not effectively demonstrated because of signal issues.

Does Nimbo return to its predefined path after interaction? Yes, Nimbo responded well to people entering its path by stopping or moving, and then immediately following its path again once safe to do so.

Scenario 4: One person lying on the ground

Does Nimbo detect the person? Yes

Does Nimbo send an alert to airport operations? Yes, Nimbo sent an alert. The system did not properly sync the alert with the correct video clip. Turing stated this was caused by the public Wi-Fi used to run the demonstration. The robot did not differentiate between a person standing or lying down. Turing stated programming could teach the system to differentiate.

Scenario 5: Five people walking through the area simultaneously

How many people does Nimbo detect? Nimbo would alert once when multiple people walked in its path, but it did not send multiple notifications. Also, when the area became dense, Nimbo did not repeatedly send notifications. It would send a notification when it would turn to face the crowd after looping in the area without people.

Scenario 6: Two people walking into the area working in concert; one person trying to lead the robot away while the other goes around it

How does Nimbo respond? The robot cannot be led away from its path nor can it autonomously follow a suspect. It can only navigate along its set patrol path.

OPERATIONAL QUESTIONS

Can the AV operate without human interaction? Yes. The system will continue to follow a pre-planned path and charge as necessary without human interaction. Changing the route or stopping the operation will require the human to direct the change. If an obstruction is placed in front of Nimbo that it cannot figure out how to avoid within the confines of the operating parameters provided, Nimbo will become inoperable and require human intervention to mitigate the issue and restart the operation.

Is the vehicle able to provide actionable information to the airport? Yes, through live and recorded video. Every time Nimbo alerted on a person and provided a notification, it saved a clip of before and after for monitoring of that individual.

Can the airport respond? Yes, the airport will receive an alert from Nimbo based on the established criteria. The airport will have the option to communicate through Nimbo with the person or send a person to the area.

Can the vehicle maneuver around obstacles in the terminal? Yes, the vehicle appeared to easily handled a busy baggage claim and lounge area. The system stopped when its path was impeded and tried to maneuver around the obstruction. Nimbo did remain very close to the person or object when it tried to avoid the obstruction because the system tried to stay within the midpoint of its planned route.

Can the vehicle effectively communicate? Yes, the system effectively communicated preset messages when it detected a person. Additionally, the controller was able to have a live conversation with a person identified by the robot. The ability to communicate live was affected by the strength of the Wi-Fi network.

How did people react to the system? People in both the baggage claim and lounge areas appeared to react well to Nimbo. Most people allowed the system to operate and did not pay attention to it. A few people were excited by the robot tried to get in its way and talk to it. The interactions were often quick and did not impede the robot’s route.

OBSERVATIONS AND LESSONS LEARNED

- The Nimbo system demonstrated the following capabilities:
    - Self-patrol within a predetermined area and avoid obstacles
    - Real-time human activity and object detection
    - Autonomous voice messaging when people are detected
    - 10-second siren warning
    - 2-way audio communication through Wi-Fi
    - 2-way video communication through Wi-Fi (with some difficulty)
    - Live video streaming and 360-degree video inspection during the setup phase
- The system demonstrated the ability to avoid people in a dynamic environment. Multiple people, including children, approached the Nimbo system and got close to it. In this situation, the Nimbo would stop if necessary, but would typically maneuver around a person and return to its preplanned path quickly.
- The system achieved a high level of autonomy. A controller was able to stop the robot or change routes via a control on their cell phone. The mobile control also allowed for a new path to be mapped.
- Each area was mapped within 30 minutes. During the mapping process, the Turing team initially noted that the glass wall created difficulties for the lidar to sense the size of the area; the engineers were nevertheless able to map the area and no issues were evident during the operation. Once the routes are programmed, they can be changed by operators sending directions to the robot remotely. The robot can store numerous patrol patterns so that different patrol routes can be executed as desired by controllers. Controllers can easily transition between routes.
- The system did not appear to interfere with passengers’ baggage claim or pedestrian flow through either public area.
- People who came in contact with Nimbo appeared to react well to the robot.

- The AV could provide camera coverage in CCTV gaps or more focused coverage if events called for a different viewpoint.
- The AV could potentially provide a presence/deterrence in areas that law enforcement or airport officials do not frequent during low activity time periods, especially at night.

CONSIDERATIONS FOR AIRPORT OPERATORS

- Although achieving a high level of autonomy, the demonstration showed that use of the system requires coordination with airport operations staff and law enforcement.
- The system's sensor and data collection capabilities were limited by the strength of the airport's public Wi-Fi.
- Nimbo was small and had minimal sensor and camera capabilities. The number and placement of the sensors and cameras appeared to limit Nimbo's functionality.
    - When a backpack was thrown in front of the robot on the floor, the robot did not detect the bag due to the lack of floor-facing sensors.
    - Nimbo had difficulties correctly identifying individuals if the individuals were in a crowd.
    - Nimbo was not able to follow a suspect.
- Nimbo's small stature and quiet mechanics have the potential to cause issues, such as a human tripping over the AV. For the demonstration, Nimbo played music to prevent going unnoticed.

APPENDIX C: VIRGINIA TECH TURTLE DEMONSTRATION AT SAFE SKIES PTF

OVERVIEW

The demonstration of Virginia Tech's Turtle AV was held at the Safe Skies Perimeter Test Facility (PTF) in April 2019. The test facility is located adjacent to the AOA and perimeter fence of the McGhee Tyson Airport (TYS) in Knoxville, Tennessee.

The AV, called a Turtle and nicknamed Raphael, operated on differentially driven rear wheels and two unpowered front caster wheels. A brushless DC motor propelled each wheel independently. The motor control received commands from an onboard computer. The Virginia Tech team stated the drive train could operate at high speeds of up to 10 miles per hour on off-road terrain. The vehicle had air-ride suspensions systems paired with a rear spring-loaded chassis suspension for stability.

Operation of the Turtle in the rugged terrain between the Safe Skies PTF fencing and the TYS AOA fence was challenging. The ground included uneven grassy surfaces with significant inclines. While the Turtle was equipped with ruggedized rear tires to assist in operation in this type of terrain, the measures proved inadequate. Additionally, the system had insufficient motor capacity to operate in the terrain. Virginia Tech noted that operational testing of the Turtle before the demonstration occurred only in a level asphalt parking area or on level manicured lawns. Virginia Tech was provided details about the operating environment prior to the demonstration.

While the Turtle could incorporate upgraded navigational and operational capabilities, the system tested had limited navigational capabilities. The navigational system solely used GPS. Virginia Tech explained they designed the system to use computer vision for navigation in connection with the GPS data, but that function would have required an enhanced graphics processing unit (GPU). In the absence of the computer vision, the Turtle was unable to factor visual imagery in its navigation. This meant it could not react to objects in its path and navigate around them. The autonomous navigation could only occur between plotted GPS points without any obstruction between them. If the Turtle encountered an obstruction, the operator would need to take control of the device to stop it and then navigate around the obstruction.

The Turtle's mobility was also limited because it only had forward-looking cameras. The 180-degree camera display limited rearward mobility even in a non-autonomous mode. Virginia Tech acknowledged the limitations of the Turtle's sensor configuration for autonomous navigation. There was also some discussion of equipping the Turtle with lidar to assist in navigation and for conducting sensor operations, but there is no current plan to equip the Turtle with lidar.

The command and control setup included three monitors to control the vehicle's navigation and track its performance. One of the three monitors allowed for viewing the camera sensor system included sensor systems installed on the device. The sensors were enabled to operate in conjunction with AI for object detection.

While the Virginia Tech team was prepared to use their internet hotspot to communicate with the robotic device and to receive sensory inputs, it was determined that utilizing the Safe Skies facility's internet would optimize performance.

DETECTION CAPABILITY

Two camera sensors mounted to the exterior of the Turtle provided the user with first-person visual feedback. A customized neural network algorithm capable of detecting objects-of-interest within the visual field processed stimuli sensed by the onboard cameras. The neural network training allowed the system to identify everyday objects, including people, vehicles, small animals, etc.; however, additional training and fine-tuning may afford the system the capability of detecting predetermined objects of interest with a displayed level of confidence. The visual sensors used in the current demonstration were short-range webcams. Specialized sensors such as long-range or high definition cameras can be retrofitted in conjunction with the existing object detection neural network to enhance visual awareness and threat detection capabilities.

OPERATIONAL SETTING AND PLAN

The areas selected for testing included a level area along a Safe Skies' fence as well as substantially more hilly and uneven terrain in the area between the TYS AOA fence and the PTF fence. Mechanical difficulties prevented testing in the area with uneven terrain. The area along the Safe Skies fence where testing was actually conducted was approximately 500 by 100 feet. It included a gravel road and grassy area. Bordering the testing area was a fence line on one side and a wooded area on the other.

DEMONSTRATION OBJECTIVE

The purpose of the demonstration was to observe: (1) how the system maps and develops its autonomous operating plan; (2) how the system handles the rough terrain and elevation changes; and (3) the data collection process and the value of the data collected.

DEMONSTRATION

During preparation for operations testing, the Turtle navigated with direction from the command center down the gravel roadway adjacent to the PTF fence to test the system's ability to operate on the terrain and plot a GPS path on the map that had been preloaded onto the Turtle's computer. The equipment operated along the roadway easily without incident under human control. However, when the Turtle passed out of line of sight from the command center down an incline in the road and turned to move into an open field, the system began experiencing movement difficulties.

Degradation of the Wi-Fi connection between the Turtle and the command center caused camera image latency of three seconds between the Turtle and controller, which created operational challenges in avoiding obstacles.

To continue setup, the Virginia Tech team steered the Turtle via a direct link with the controller walking with a laptop directly behind the Turtle. The plan was to get the Turtle to operate through the rugged terrain between the Safe Skies fence and the TYS AOA fence, and then to have the Turtle operate autonomously once a GPS plot was conducted.

Despite repeated attempts to operate the Turtle over the rugged terrain, the mechanical challenge proved insurmountable. After five hours, the Virginia Tech team decided the Turtle was capable of only a more limited demonstration of autonomous movement.

After meeting with the Virginia Tech team leader at the conclusion of day one, it was determined that the autonomous movement demonstration would occur in the parking area of the Safe Skies facility. This terrain was similar to that in which the Turtle had previously operated. If that was successful, the plan was to conduct autonomous operation on the level stretch of gravel road and grass adjacent to the Safe Skies fence to demonstrate the Turtle's AI sensor capabilities.

At the beginning of day two, the Virginia Tech team discovered that the controller motor for the left rear wheel was damaged from work on the system the night before. The mechanical failure left the Turtle incapable of moving either autonomously or non-autonomously.

Given the inability of the Turtle to move, it was determined that the only capability that could be demonstrated was the AI capabilities of the Turtle's camera sensors. These sensors were simple consumer-grade web cameras that were attached in an array of two cameras on the front of the vehicle.

The camera data was analyzed by AI software operating at the control center. The team set up a test course along the gravel roadway and measured the distance between objects and the stationary Turtle as they were recognized by the AI engine. That AI engine was programmed to recognize a limited range of objects, including humans, animals, and vehicles. When an object came into the camera's line of sight, the AI would attempt to identify the object. The initial recognition would start at a lower confidence level and then increase as the object continued in the visual field and got closer. The confidence level would begin around 25 to 30 percent and end around 90 percent or higher.

The demonstration was designed to show the sensor-AI combination's ability to discern differing objects. Also examined was the distance from the camera sensors at which those objects could be recognized.

The demonstration showed that the sensors on the Turtle could recognize humans at a range of between 45 and 60 feet. A golf cart was recognizable at a range of 45 feet. A dog was recognized between 3 to 20 feet. The ability of the AI to identify the objects was degraded when the objects were viewed through a fence, but that degradation was only a matter of about 10 percent of the distance, 4 or 5 feet. Significantly, when a human approached holding a sheet in front of his body, the camera did not recognize the object as human.

While most of the AI demonstration was conducted with the Turtle stationary and the objects approaching it, there was a limited demonstration of the Turtle's AI capability while moving. Because of the motor problem, the Turtle was pushed down the road to see if the AI could recognize a human partially obscured in the wood line adjacent to the road. The results were mixed. While the human subject was discernible to a human operator looking at the video screen, it was only when the human subject came to the far edge of the wood line that the AI could recognize a human form.

Some important qualifications should be noted with respect to the AI demonstration. First, there is the issue of the quality of the cameras. The Turtle was equipped with inexpensive consumer-grade web cameras. If the quality of the cameras was improved, the quality of the AI recognition may also improve. However, the Virginia Tech team did note that there needs to be a balance between the sensors inputting data and the processing power of the systems supporting the AI. More simply, if the cameras provide too much data, the AI system will slow because of limited capacity to process the data. In this instance, there is no suggestion that the cameras used were optimized to the capacity of the AI.

The AI worked consistently well to discern the difference between objects. As the AI receives additional training data, the ability to differentiate will be enhanced. It also can be expanded to look for additional items of wildlife that might pose a danger to aircraft. While the system was not equipped with an alarming function, it could be programmed to provide alerts or alarms to operators when the cameras on the Turtle identified an object of interest.

KEY FINDINGS

- The operation of AVs in an outdoor environment presents significant challenges. The vehicle will require ruggedized mechanical systems to support operations and meet the challenges of the variable terrain and environment.
- The interrelationship between mechanical systems and navigational systems in calculating movement is essential to autonomous navigation.

- Ensuring Wi-Fi connectivity was essential to support the system's navigation.
- Outfitting the system with only GPS as a navigation aid did not enable effective movement. The system needed computer vision or lidar to ensure autonomous movement served its intended purpose and was safe.
- As technology continues to improve, it is important to have an AV with modular and upgradable capabilities for navigation and sensor operations.
- AI-based sensors can assist an airport operator in analyzing video footage.

APPENDIX D: KNIGHTSCOPE K5 OBSERVATION AT LGA

OVERVIEW

The Knightscope K5 is an autonomous robot built specifically to perform security functions in conjunction with human security forces. The system uses an Ackermann drive system, lidar, simultaneous location and mapping, several sensors, thermal anomaly detection, and artificial intelligence algorithms. K5 was demonstrated at LGA in Queens, New York, March 2018 – March 2019.

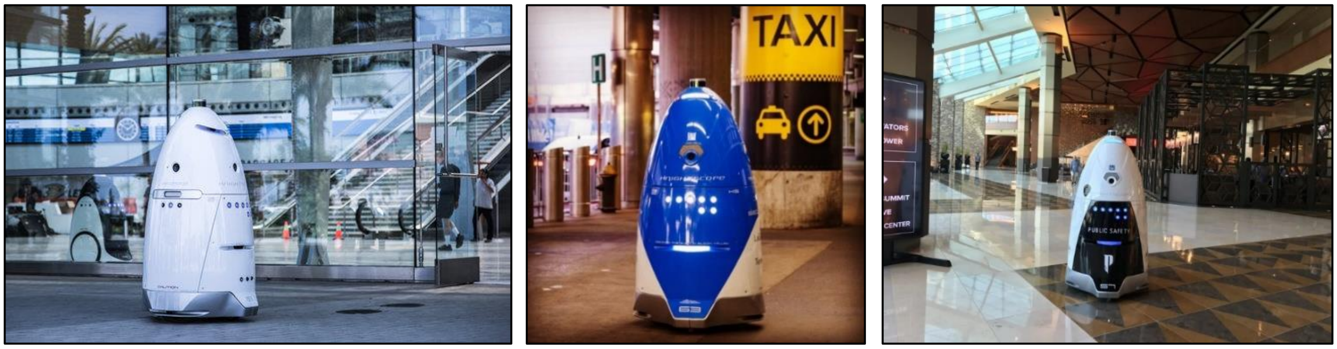
The K5 robot is capable of fully autonomous patrolling and charging itself within a defined area, assessing 1,200 license plates per minute, 360-degree live-streaming eye-level video, two-way audio communication, automatic responses to trigger events, running thermal scans, and checking environmental signals. K5 can be controlled remotely from a web-based dashboard.

K5’s large stature is an intentional design feature meant to provide effective physical deterrence as well as being necessary for the housing of massive data collection hardware using a variety of sensors, cameras, scanners and audio equipment.

LGA’s Terminal B operator deployed Knightscope’s K5 AV and K1 stationary machine at the terminal’s arrival curb. The K5 system was deployed to detect and deter unlicensed taxi-cab operators, and also to provide situational awareness. The initial plan was for the K5 system to patrol the arrival curb and use its license plate recognition technology. However, the curve of the road and bollards on the sidewalk prevented the K5 from reading all license plates and therefore achieving the main objective of the deployment. Knightscope provided the K1 stationary system at no additional cost to supplement the deployment.

The K5 system was deployed through a licensing agreement for the period of one year. The terminal operator paid a fee per month for the AV, supplemental stationary system, software, and cellular data. The license covered maintenance and liability.

Figure D-1. Knightscope K5



Source: Knightscope.com

SPECIFICATIONS

- Dimensions: Height 62.5 in., Length 36 in., Width 33.5 in.
- Weight: 398 lbs
- Max Speed: 3 mph
- Terrain: Indoors and Outdoors

SYSTEM MAPPING

The Knightscope K5 ran on predefined routes determined by the LGA Terminal B operator. The K5 patrolled 1,300 feet of sidewalk using a back and forth pattern along the curb, segmented loops within the area, and intentional pauses along the route. The patrol area was geofenced to enable the K5 to avoid obstacles. The system was also able to navigate the sidewalk handicap ramps to move from one end of the route to the other. Patrol routes and patterns could be easily changed if necessary.

OBSERVATION SUMMARY

The Knightscope K5 demonstration had been in progress for nearly a year when observed by the Project Team.

The K5 patrolled 1,300 feet along the sidewalk that included bumpy cement, ramps, large pillars, and periods of significant congestion. The system handled the dynamic terrain well, and appropriately avoided people and objects. The system did bounce as it operated, which affected the quality of the video, although not to an extent that it negated the ability to use the video for the stated purpose. Over the course of the year, there was only one instance, during a major problem unrelated to the AV, that the area became so crowded that the terminal operator docked the system out of caution.

The system ran on predefined routes defined by the terminal operator. These included a full back and forth of the entire curb, segmented loops within the area, and loops that included pauses in certain locations. The system operated on these loops within a defined geofenced area to enable it to avoid obstacles. The terminal operator was able to easily change routes as necessary.

The terminal operator had access to a web-based dashboard to control the system and see the data collected. The dashboard was user-friendly to change the operating path, view live or saved video, and analyze license plate data collected. The terminal operator was able to tailor the license plate data collection in the dashboard and set alerts when certain vehicles entered the area.

The system did have a signal detection capability that identified cellphones and computers in the area. The terminal operator did not find this information useful as so many technologies were being detected within the airport. The airport did not pursue a use case. This feature would be more useful if law enforcement was looking for a specific person and the system identified when they were present in the airport.

OBSERVATIONS AND LESSONS LEARNED

- The Knightscope K5 demonstrated the following capabilities:
    - Self-patrol within a predetermined area and avoid obstacles
    - Navigation of outdoor areas with inconsistent terrain and through all types of weather
    - Real-time human activity and object detection
    - License plate recognition
    - 360-degree live video streaming and recording
    - Remote monitoring and control
    - 2-way audio and video communication
    - Event-triggered pre-recorded messages
- The K5 system was able to operate in a crowded environment. The system was able to handle a busy arrivals curb that had numerous manmade obstructions for it to navigate.

- The K5 was able to operate outdoors on various types of paved surfaces that included bumps, inclines/declines, drop-offs and other uneven properties. The system was not impacted by weather during its yearlong deployment, however the system operated in a covered area.
- The system was able to navigate to and use handicap ramps that connected different curb areas.
- Patrol routes and patterns could be easily changed, and data collection could also be configured remotely.
- Information derived from the AVs has no value unless the airport analyzes and acts upon that data.
- Communication among airport stakeholders and logistics planning can help facilitate the appropriate flow of information for decision-making and action.
- The K5 has other features that were not tested during the demonstration at LGA.

CONSIDERATIONS FOR AIRPORT OPERATORS

For the presence of K5 to provide successful deterrence over time, additional work by the airport is required. Without follow up action by airport personnel to initiate consequences for the intended population (i.e., unauthorized taxis), there is likely little deterrence value.

The K5 can collect a lot of data, but it has to be transmitted and stored in a way that is useful for airport stakeholders—a process that needs to be developed and configured in advance.

Existing physical configurations in areas for desired patrolling may limit the K5’s capabilities.

APPENDIX E: COBALT ROBOTICS OBSERVATION AT BRIGGS & STRATTON

OVERVIEW

Starting in 2011, Briggs & Stratton Corporation (B&S) began utilizing autonomous security robots provided by Cobalt Robotics as part of security operations at its corporate headquarters campus in Wauwatosa, Wisconsin. The campus includes warehouses, a light manufacturing facility, research/development and office facilities, and a small museum. B&S uses two Cobalt robots to patrol its warehouses and light manufacturing facility. Patrols are conducted at night and on a limited basis during the day. The robots patrol preset paths within the warehouses to enhance security and detect safety, security, and operational issues. The robots have replaced some of the security guard service staff that B&S previously used to perform these tasks.

B&S uses a Security as a Service model to deploy autonomous robots for security. Cobalt maintains a 24/7 operations center linked to the robots. As the robots identify anomalies, predefined by B&S, the information is communicated to the Cobalt operations center. Personnel in that operations center analyze the anomalies based on the B&S criteria and then provide notifications as directed by B&S. Cobalt personnel also remotely assist the directional movements of the robots if they experience navigational difficulties. This business model is used by a number of AV solution providers, and may be of interest to airport operators that want to leverage the technology but want to outsource some of the support functions associated with them.

The project team observed a demonstration of B&S's use of robots for security purposes. A detailed discussion of this demonstration is included below.

OPERATING ENVIRONMENT

At the B&S warehouse facility, robot function was demonstrated in two buildings. The first building housed a combination of warehouse and light manufacturing functions. The second building, which adjoined the administrative office and a company museum, was for warehouse functions. The two settings where the robot functions were demonstrated were similar to areas of an airport such as baggage-handling and make-up areas, hangars, cargo storage areas, and service-related and equipment storage areas.

Within the B&S warehouse/manufacturing facility, there were small delineated paths for pedestrians and vehicular movement. Adjacent to those paths were machinery, carts, and all sorts of tools resembling baggage-handling systems, tugs, and other common objects found in the airport environment. Farther back into the building were assembly-line areas, but because manufacturing operations were ongoing at the time of the demonstration, those areas were not observed. The warehouses had significant pedestrian and vehicle traffic during the day and light traffic at night.

The charging pad was located just inside the door of the facility. This allowed the use of camera features on the robot to cover the door areas even when the robot was charging. During some shift changes, the robot could be positioned directly in front of the exit portal to guard against unauthorized entry (there are occasional problems with reverse entry into the warehouse through the exit). The entrance doors were equipped with access control and a turnstile-type door to address unauthorized entry, but the exit area had no such protection.

Because of the significant movement of personnel and vehicles inside this facility, the robot units were used principally in off-hours to conduct preset patrols. In addition to looking for unauthorized movement, the robots also observe and sense environmental conditions and hazards like spills, or potential OSHA violations like blocked exits.

The second area observed was limited to warehousing functions, though it contained sensitive proprietary equipment in areas caged by chain-link fencing sections. The robot charging station was positioned opposite the main entry doors to provide additional camera coverage while charging. The robot patrolled preset routes in the warehouse area, but it could navigate into the museum area during the demonstrations.

FUNCTIONS

Patrols are conducted at night and on a limited basis during the day using the robots' autonomous functionalities. The daytime usage is limited to times and areas where the foot and vehicle traffic in the facility is lower. The robot patrols preset paths within the warehouses to enhance security and detect safety, security, and operational issues. The robots have replaced some of the security guard service staff that B&S previously used to perform these tasks.

CAPABILITIES AND LIMITATIONS

The robots operating in the B&S facilities are not ruggedized and can only be used indoors on smooth level surfaces or surfaces with slight inclines. Stairs and doorways present impediments. The latter is something that can be solved by installing hardware that allows doors to be opened electronically on demand. Modified ADA-accessible doors that enable people with disabilities to pass through portals offer a potential solution to the door challenge.

B&S uses the autonomous robots for security and operational awareness purposes. The robots perform a range of safety and security functions. As the robots patrol, they can collect a wide range of data and perform several safety and security tasks. The robots inspect doors to ensure they are closed and inspect storage areas to ensure they are secured. The robots are equipped with sound detection sensors to listen for anomalous sounds such as loud noises or breaking glass. The robots also look for movement indicative of human presence.

The system transmits all sensor data to a central facility operated by Cobalt. If the sensor activity indicates an anomaly, then a Cobalt operator checks the data. The operator evaluates the data and then takes appropriate action, including communicating with the B&S operations center. While B&S can set parameters for notifications to simultaneously go to their operations center, most information is transmitted by the Cobalt operator after the data is analyzed.

The robot can be used to communicate with people it encounters and challenge individuals to swipe their badges to verify their identity. This communication does not happen autonomously. A human operator speaks with the person encountering the robot through a video screen, which allows for two-way audio-visual communication. The verification process for swiped media can be linked to the facility's access control system, but that integration is an additional cost. Rather than use such an integration at this time, B&S downloads the access data independently to the robot's control center so that verifications can be made against that dataset. B&S is considering linking the system to their access control system, Honeywell ProWatch, in the future.

While the robot can be directed to follow persons of interest, it does not move quickly enough to keep up with a person determined to evade it. However, if an alarm is triggered, another camera in the facility can track the suspect.

In addition to the traditional security-oriented functions, the robot collects data and provides alarms on a range of safety-related matters and facility conditions. The robots can identify leaks, spills, smoke, and the presence of some dangerous gases, and even potential fire hazards detected as thermal anomalies.

The robot can collect other facility data that may be useful to the operations. For example, as the system operates, it can measure the signal strength of Wi-Fi throughout the facility. Robots can also be equipped with other sensors to take other readings of interest to the facility operator. The robot's visual sensors can check for anomalies of operational importance.

Patrol frequencies and routes can be preset and adjusted. At night, the system patrols the warehouses for situational awareness purposes and asks individuals to swipe their badges. During the day, the system takes smaller loops and sits near the door to check for piggybacking. The robots can be programmed with SOPs to determine levels of alarm and notification.

LESSONS LEARNED

- The robots collect an abundance of data. Cobalt analysts monitor the robots' operation and decide when to alert the client based on preset criteria. Cobalt has protocol from B&S telling them what to do if certain situations occur. For example, if a security event occurs, Cobalt calls the security department. If Cobalt detects a spill or a leak, it will contact the maintenance department.
- B&S uses the Cobalt robots to prevent piggybacking. They position the system at the door during shift changes to look for people entering through the exit. If a person enters through the exit, the robot will communicate with that individual and request a badge check. The system will follow that individual as best it can. At a minimum, B&S has a picture of the person and information regarding the direction they were walking at a specific time.
- The AV system enhances B&S's CCTV coverage. Where data cannot be captured on the robot's CCTV, information can be relayed to the operations center so that an individual can be tracked and located.
- The video and other data collected by Cobalt provides evidence for B&S.
- The system can run a predefined path around the warehouse that checks specific areas while looking for open doors, people, safety concerns, and operational considerations.
- At remote locations, the robot performs a reception service. The robot intakes the truck driver, checks badges, and provides instructions if necessary.
- The vehicle performs numerous safety functions, including looking for pallets in the walkway or unevenly stacked boxes.
- The sensor arrays on the robot can be configured to meet specific operational requirements. The robot is equipped with a standard array of more than 60 sensors—including a 360-degree camera, thermal camera, depth camera, ultrasonic sensors, lidar, and environmental sensors—but additional sensors can be added.
- The robot can perform challenge functions and can be integrated with the access control systems or operated with manual data downloads of active badges. Integration with the access control system for real-time access to data is possible, but it is an additional cost.
- B&S is considering integrating the autonomous robot with their access control system to allow the robot to move through an access-controlled portal. This process will use the same technology

that enables people with disabilities to pass through the same portals. As with the access to real-time badge information, this integration is an additional cost.

- B&S is looking at the robots to add to their active shooter response plan. These devices could be used in the event of an active shooter to move into uncleared areas to provide situational awareness without risk to human life.
- Some examples of success stories from the B&S use of robots include:
    - Identifying unauthorized persons in the facility
    - Pallets and equipment moved into areas that pose safety hazards or potential OSHA violations
    - Leaks in the facility
    - Spills in the facility that pose a hazard
    - The existence of a thermal anomaly in a packing case posing a potential fire hazard
    - Dangerously stacked inventory
    - Toppled inventory

APPENDIX F: TELEROB TELEMAX PRO OBSERVATION AT PIT / ALLEGHENY COUNTY POLICE DEPARTMENT BOMB SQUAD

OVERVIEW

The Allegheny County Police Department Bomb Squad, which services Pittsburgh International Airport (PIT), purchased the Telerob Telemax PRO in November 2018 to assist with bomb detection duties. The Telemax PRO offers autonomous and semi-autonomous capabilities to assist in moving the system within an area and controlling the robot's arm. From an autonomous movement perspective, the system maps its environment upon entry and continuously updates that map as it operates. The user can set waypoints, and the system can return to base on its easiest path based on the map it has created. The robot arm has semi-autonomous functionality to assist the operator in maneuvering the arm. The user operates a joystick based on three available camera views to direct the arm toward the target. The semi-autonomous function tells the joints how to bend and rotate based on the direction of the joystick. Most bomb removal robots require the operator to independently bend and rotate each joint independently.

The airport operator pursued this technology because of the mapping capability and ease of performing tasks with the arm. Prior to procuring the Telemax PRO, the principal robot operated by the Bomb Squad was the Remotec F6B. This robotic device has no autonomous functionality. All movements of the F6B are controlled by the operator, including locomotion and the operation of the robot arm. While an experienced operator can maneuver this robotic device very effectively, the autonomous movement functionality of the Telemax PRO, particularly with respect to the robotic arm, was clearly discernable in the side-by-side operational demonstration that was conducted.

DEMONSTRATION

The Bomb Squad conducted a side-by-side demonstration of the Telemax PRO and the F6B. The demonstration included approaching a suspect vehicle, opening the door handle of the car, and removing an item from the vehicle. The two subject vehicles were sedans with differing door handles. One required an up pull to open, and the other an out pull. The two types of sedan door handles represent the overwhelming majority door handles on modern vehicles in the U.S. In the side-by-side test, both robots were used to open the door on each of the sedans. The door with the upward pull proved to be a more challenging task for both robots, but both were able to overcome the difficulty.

In the side-by-side demonstration, the Telemax PRO semi-autonomous capabilities enabled the operator to complete the task more expeditiously and precisely. The operation of the robot arm on the Telemax PRO appeared smoother than the operation of the arm on the F6B, but both efficiently accomplished the assigned tasks, in part because of the operators' experience with the F6B. Watching the operators as they moved and manipulated the robots, it was clear that the F6B required more experience and skill to work the controls. The Telemax PRO autonomous robot arm allowed a much less skilled operator to achieve comparable results.

The autonomous movement of the robot was not part of the side-by-side demonstration. While the feature could have some usefulness in an overall operation where there is repetitive movement back and forth from the target site, the autonomous movement functionality would not have been useful in the side-by-side testing.

AUTONOMOUS MOVEMENT SYSTEM MAPPING

The Telemax PRO has an autonomous module that enables the robot to move between waypoints and to its home location. The system relies on a two-dimensional laser scanner for localization and mapping. It is also equipped with Xbox Kinect 3D point cloud technology for mapping. This capability provides two attractive functions. First, the system maps an environment as soon as it enters. This provides the team with situational awareness, and the bomb squad can provide this information to other first responders. Second, the system can then autonomously move itself between waypoints and its home base. This allows the end user to quickly pull the robot back and equip it with other capabilities that it may need to resolve the situation.

The mapping and autonomous movement capabilities are limited. The sensors generating data for movement have limited range of 40 meters for the lidar and 15 feet for the 3D point cloud. This means the robot can autonomously move in close areas like a building with small rooms. However, as the limits of the operating space expands beyond the range of the sensors to map, the robot becomes “lost.” As an example, in open bays of the large hangar area where the demonstration occurred, autonomous movement was not possible. When the robot was moved into the confined space of the room in the hangar used as a day room area for the team, the robot was able to provide a 3D map indicating the features of the room, including the furniture.

Unlike other the mapping functions from other robots, multiple trips through an area do not result in an increasingly refined map. On the contrary, the map tends to become more cluttered with double images of some items like furniture. This phenomenon did not seem to affect the ability of the robot to operate within the confined space. It also did not affect the usability of the mapping products.

The Telerob representative who was present at the demonstration noted that the mapping capabilities could be enhanced with additional sensors and processing power. Those enhancements would result in greater cost for the robot. Given the limited use of autonomous navigation, the Telemax PRO’s current sensor package offers a balance between cost and functionality related to purpose.

One other limitation on the mapping capability is the ability to share the maps in real-time from the robotic device’s web interface, which enables the operator to view the map. For maps to be shared, they need to be downloaded from the Telemax system, SD card, or USB, and then shared with other interested entities, such as SWAT and command personnel. The robot can navigate over previously prepared maps, but it must be maneuvered by an operator to a prepositioned start point before it can autonomously navigate using the prepared map.

AUTONOMOUS LEVELING AND STABILIZATION

While the Telemax PRO can move autonomously across the space, the unit has to be stabilized before it can operate its robotic arm. That stabilization cannot be conducted in conjunction with movement, and it is an operator-controlled function, not an autonomous function. Failure to stabilize the unit, particularly before use in uneven terrain or operating the autonomous arm, can result in the robot falling over and being unable to right itself.

The stabilization features do have default presets to assist the operator in manipulating the tracks to stabilize the chassis. The robot is equipped with tracks to assist in movement across uneven terrain, including up and down stairs. These presets help to level the robot, which is also necessary for proper arm movement.

AUTONOMOUS ARM MOVEMENT

The Telemax PRO has preset features in its arm to assist the operator in directing the arm toward a target. As the operator directs the arm toward the target, the presets tell the hinges of the arm how to rotate. Therefore, the operator only must point a joystick at the target as opposed to independently moving each arm joint. This function results in more accurate and smoother movement of the arm. Similarly, these presets prevent the robotic arm from moving in a manner that will damage other parts of the robot. The operator can override these presets if necessary.

At the command of the user, the robotic arm will autonomously return to its starting position by following the route it took toward the target. This assists the user in backtracking the arm out of tight spaces, potentially with an explosive in the arm's grip.

COMMAND AND CONTROL

The robot is controlled from a portable command console. The console is contained in a Pelican™ case and can be rapidly deployed to the field along with the robot. The robot communicates with the console through RF, which can present problems in RF-rich environments. The Telemax PRO does have the ability to adjust to differing frequencies if necessary.

The robot can deploy repeaters to extend the range for communication. These repeaters need to be strategically placed by the robot to ensure continued communications.

LESSONS LEARNED

- The Bomb Squad uses this advanced robot for its mapping capability, to provide situational awareness, and the ease of using its semi-autonomous arm.
- The autonomous movement function would be useful in a long duration operation when the robot would need to move back and forth to a target area.
- Unless a different, more costly sensor package were used, the Telemax PRO could not use autonomous movement outside of closed confined spaces.
- Radio frequency (RF) interference and range limitations should be accounted for on robot operation.
- The Telemax PRO (as well as the F6B) can move across rough and uneven terrain.
- The Telemax PRO requires operator intervention to stabilize, and that stabilization cannot occur as the robot moves.
- The experienced bomb tech was able to quickly operate the F6B, but did not have the same precision as the operator with semi-autonomous assistance. The Telemax PRO robot was able to quickly adjust to the more complex environment.

APPENDIX G: ACAMP AUTONOMOUS SECURITY AV PILOT AT YEG

Edmonton International Airport (YEG) built an outdoor AV with the help of ACAMP. The vehicle is designed to autonomously patrol the airport perimeter to look for human or wildlife intrusions and check the integrity of the fence line. It uses lidar to operate and has sensors that use AI to complete security tasks. The system can communicate its findings back to the operations center to enable appropriate airport response.

The airport reports that deployment and testing of the system has been slow. They are currently working on advanced trials and have upgraded cameras to handle the cold temperatures. Additionally, the airport has expressed cybersecurity concerns. The airport is working to address this cybersecurity system issue before the AV is connected to the airport network. Additionally, the system experiences network connectivity issues when operating in remote areas of the airfield.

The system has responded well to the perimeter terrain and has avoided obstacles. The system operates at a maximum of 9 miles per hour in autonomous mode.

APPENDIX H: EXAMPLES OF AUTONOMOUS VEHICLES THAT CAN SUPPORT SECURITY APPLICATIONS

Company Name Product(s) URL Location	**Primary Functional Security Application**	**Marketed Security Uses?**	**Airport Users**	**Comments**
ACAMP Autonomous Security ATV https://www.acamp.ca Alberta, Canada	Outdoor surveillance and patrolling	Yes	Edmonton Int'l Airport	Customizable to user requirements See Appendix G
National Defense University (China) AnBot www.china.org.cn/china/2016-09/22/content_39347636.htm Shenzhen, China	Indoor surveillance and patrolling	Yes	Shenzhen Int'l Airport	
Autonomous Systems, Inc (ASI) ASI Security https://asirobots.com Logan, Utah USA	Indoor surveillance and patrolling Outdoor surveillance and patrolling	Yes		Customizable to user requirements
Certis Security Group PETER (Patrol and Traffic Enforcement Robot) www.certisgroup.com Singapore	Outdoor surveillance and patrolling	Yes	Changi Int'l Airport	
Clearpath Robotics https://clearpathrobotics.com Kitchener, ON Canada	All Terrain Material Transport and Handling EOD disposal Indoor surveillance and patrolling Outdoor surveillance and patrolling	No		Customizable to user requirements
Cobalt Robotics https://cobaltrobotics.com San Mateo, CA USA	Indoor surveillance and patrolling	Yes		Offers Security as a Service See Appendix E
ECA Group Unmanned Ground Vehicle www.ecagroup.com Saclay, France	All Terrain Material Transport and Handling EOD disposal	Yes		
Fetch Robotics, Inc. https://fetchrobotics.com San Jose, CA USA	Material Transport and Handling EOD disposal Indoor surveillance and patrolling	No		Customizable to user requirements

Company Name Product(s) URL Location	**Primary Functional Security Application**	**Marketed Security Uses?**	**Airport Users**	**Comments**
Honda Autonomous Work Vehicle https://global.honda/innovation/CES/2019/autonomous_work_vehicle.html	All Terrain Material Transport and Handling	No		Customizable to user requirements
Knightscope Autonomous Data Machines K3, K5, K7 www.knightscope.com Mountain View, CA USA	Indoor surveillance and patrolling Outdoor surveillance and patrolling	Yes	LaGuardia Airport	See Appendix D
NXT Robotics www.nxtrobotics.com San Diego, CA USA	Indoor surveillance and patrolling Outdoor surveillance and patrolling	Yes	San Diego Int'l Airport	Customizable to user requirements
OTSAW Digital, Inc. OR-2, OR-3 www.otsaw.com San Francisco, CA USA	Indoor surveillance and patrolling Outdoor surveillance and patrolling	Yes		Offers Security as a Service
QINETIQ North America TITAN Military UGV https://qinetiq-na.com/products/unmanned-systems/titan/ Waltham, MA USA	All Terrain Material Transport and Handling	Yes		Customizable to user requirements
Robot Security Systems SAM3 www.robotsecuritysystems.com Delft, The Netherlands	Indoor surveillance and patrolling	Yes (see comment)		Since the conclusion of project research, security applications are no longer marketed
SMP Robotics Systems Corp. https://smprobotics.com Sausalito, CA USA	Indoor surveillance and patrolling Outdoor surveillance and patrolling	Yes		Offers Security as a Service
Telerob Telemax Pro www.telerob.com Ostfildern, Germany	EOD disposal	Yes	Pittsburgh Int'l Airport	
Turing Video Nimbo https://hellonimbo.com San Mateo, CA USA	Indoor surveillance and patrolling	Yes	San Jose Int'l Airport	See Appendix B

Company Name Product(s) URL Location	**Primary Functional Security Application**	**Marketed Security Uses?**	**Airport Users**	**Comments**
Virginia Tech University “Turtle” Autonomous Vehicle	Outdoor surveillance and patrolling	N/A		Non-commercial system See Appendix C

APPENDIX I: OVERVIEW OF SECURITY-FOCUSED AUTONOMOUS VEHICLE CAPABILITIES

System	Outdoor or Indoor	Function	Own or Lease
ACAMP ATV	Outdoor	Perimeter patrol Intrusion detection Fence line integrity	Own
Cobalt	Indoor	Security as a Service 360-degree camera Thermal and depth camera Ultrasonic sensors Environmental sensors Badge reader 2-way communication Some analytic capabilities	Lease
OSTAW OR3	Outdoor	360-degree camera Data collection Data recording Data analyzed by offsite security team	Lease
Turing NIMBO	Indoor	Image recognition Live and recorded video Two-way communication	Lease
SMP Robotics	Outdoor	360-degree video surveillance Facial recognition Audio warning	Own
Daifuku Airport Technologies	Indoor	Baggage transportation	Unknown
Vanderlande FLEET	Indoor	Baggage transportation	Lease
Segway Solutions Loomo	Both	Camera Has ability to follow	Own
Knightscope K3	Indoor	360-degree camera Video streaming and recording Thermal anomaly detection Signal detection Live audio broadcast Two-way intercom Pre-recorded and custom messages Remote monitoring	Lease
Knightscope K5	Both	360-degree camera Video streaming and recording Thermal anomaly detection Signal detection	Lease

System	Outdoor or Indoor	Function	Own or Lease
		Live audio broadcast Two-way intercom Pre-recorded and custom messages Remote monitoring	
Certis Robot	Indoor	Camera with video analytics and facial recognition Anomaly detection	Unknown