TED UNIVERSITY

CMPE 491 Senior Project

OWL Border Security Project Specifications Report

Spring 2026

Team members:

Emre Kaan Arslan, 13021093920, Computer Engineering

Mehmet Yiğit Açdoyuran, 10130437010, Computer Engineering

Ege Yavuz, 14872032366, Computer Engineering

Supervisor: Tansel Dökeroğlu

Jury Members:

Mehmet Evren Coşkun

Eren Ulu

Table of Contents

1- Introduction

1.1- Description

The growing intricacy of border security issues, especially in areas impacted by irregular migration and smuggling, has underscored the shortcomings of conventional surveillance systems. Traditional methods mainly depend on identifying the existence of objects or people, frequently missing the ability to analyze behavioral trends or inherent motives. This constraint leads to elevated false alarm rates and a lack of adequate situational awareness for those making decisions. The OWL Border Security Project seeks to tackle these issues by implementing a sophisticated, AI-powered monitoring system that exceeds basic object identification. The system combines video streams and sensor information to conduct real-time analysis of activities in border areas. By concentrating on behavioral patterns, interactions among individuals, and situational cues, OWL aims to ascertain not just what is occurring, but also the reasons behind it. A significant advancement of the OWL system is its capacity to carry out intent analysis. Rather than viewing each detection as a separate occurrence, the system assesses sequences of actions to categorize activities into types such as reconnaissance, preparation, or crossing attempts. This method allows for better risk evaluation and facilitates preventive security strategies. Additionally, the initiative highlights the importance of minimizing false alarms by utilizing multi-sensor verification and smart data integration. By merging various data sources, the system enhances reliability and guarantees that alerts are both significant and understandable. The OWL project enhances next-generation border security technologies by merging artificial intelligence, behavioral analysis, and real-time decision support into a single framework.

1.2- Constraints

1.2.1 Economic Constraints:

The OWL Border Security System needs funding for hardware including cameras, sensors, and processing units, in addition to computing resources for AI model creation. These expenses rise with the growth of the system and ongoing updates. Scalability is a crucial limitation, as implementation over extensive border regions must stay economically viable. Furthermore, costs related to maintenance, energy use, and technical assistance need to be reduced. Minimizing false alarms holds economic significance, as it avoids the wasteful utilization of resources. Thus, effective system design and cost control are crucial for the project's viability.

1.2.2 Time Constraints:

The OWL Border Security Project faces time limitations concerning its development, testing, and deployment stages. As a capstone project, it needs to be finished within a fixed academic schedule, limiting the extent and depth of execution. Creating and training AI models, combining various sensors, and guaranteeing real-time functionality necessitate meticulous time management. Unforeseen technical difficulties, like issues with model optimization or system integration, could lead to delays. Testing the system in realistic conditions is essential for reliability, although it is time-consuming. Thus, emphasizing essential features and adhering to an organized development strategy is crucial for successfully achieving project deadlines.

1.2.3 Safety Constraints:

The OWL Border Security System needs to function within rigid safety standards to guarantee dependable and secure operation. As the system is designed for actual border settings, it must operate correctly under diverse conditions like poor visibility, severe weather, and difficult landscapes. The reliability of the system is essential, as false detections or misclassifications could result in significant repercussions. Consequently, reducing false positives and false negatives is crucial for ensuring operational safety. Moreover, the system should be structured to avoid abuse and guarantee data protection. Data collected from cameras and sensors must be managed securely to prevent unauthorized access. Ultimately, guaranteeing system precision, reliability, and secure data management is essential for upholding safety in the OWL project.

1.2.4 Political Constraints:

The OWL Border Security Project experiences political limitations since border security is tightly linked to national policies, international relations, and migration control. Any system implemented in border regions must adhere to government rules and security measures. Political choices can affect the locations and methods of system usage, along with the degree of backing and financial resources it obtains. Moreover, border monitoring technologies can raise contentious issues in conversations regarding human rights, privacy, and global collaboration. Consequently, the initiative needs to be executed in a manner that complies with legal standards and political anticipations while ensuring robust security assistance.

1.2.5 Manufacturability Constraints:

The OWL Border Security System needs to be developed considering manufacturability limitations to guarantee efficient production and deployment. The hardware elements, including cameras, sensors, and processing units, must be readily available and compatible with current technologies. The system needs to be modular, enabling components to be manufactured, substituted, or enhanced without necessitating a total redesign. This method

streamlines manufacturing and lowers future expenses. Moreover, the design should take into account the simplicity of installation and upkeep in border areas. Utilizing standardized and robust components aids in guaranteeing that the system can be produced, implemented, and serviced efficiently.

1.2.6 Ethical Constraints:

The OWL Border Security System needs to take into account ethical limitations concerning privacy, data usage, and human rights. While the system gathers and examines visual and sensor data, it is crucial to uphold individuals' rights. The system must minimize excessive monitoring and concentrate solely on identifying suspicious behaviors pertinent to border security. Data should be managed carefully, with defined constraints on storage, access, and utilization. Moreover, decisions driven by AI must be transparent and understandable to avoid biased or unjust results. Guaranteeing the ethical application of technology is crucial for upholding public confidence and the responsible implementation of the OWL system.

1.2.7 Social Constraints:

The OWL Border Security System needs to take into account social factors concerning public perception, trust, and societal effects. Surveillance technologies can provoke worries within communities, particularly related to privacy and ongoing scrutiny. It's crucial that the system is viewed as a means of safety instead of unwarranted regulation. Transparent communication regarding the system's objectives and constraints can foster public confidence. Furthermore, the system ought to be structured to reduce adverse social impacts, including discrimination or abuse. Guaranteeing the responsible and clear use of technology is crucial for its societal acceptance.

1.2.8 Maintainability Constraints:

The OWL Border Security System should be created with a focus on maintainability to guarantee lasting reliability and effective performance. Given that the system will function in demanding border conditions, parts might need frequent maintenance and upgrades. The system needs a modular design, enabling individual parts to be serviced or swapped out without impairing the whole system. This minimizes downtime and makes maintenance procedures easier. Moreover, software elements, encompassing AI models, must be readily upgradable to respond to emerging trends and enhance efficiency as time progresses. Well-documented information and uniform design are crucial for promoting effective upkeep and long-term system viability.

1.3- Professional and Ethical Issues

The OWL Border Security Project presents numerous professional and ethical challenges stemming from its implementation of sophisticated surveillance tools and artificial intelligence. Being a system intended for observing and evaluating human behaviors, it should be created with a high level of accountability and expertise. Engineers and developers participating in the project need to guarantee that the system functions precisely, dependably, and in line with legal and ethical guidelines. Mistakes or improper use of the system may result in severe repercussions, such as wrongful allegations or infringements on personal rights. The project should ethically reconcile the requirements of security with regard for privacy and human dignity. Utilizing AI in decision-making necessitates transparency and accountability to prevent biased or unjust results. In summary, upholding professional integrity and following ethical guidelines are crucial for the responsible use of the OWL system and for fostering public confidence.

1.3.1 Security and Responsibility:

The OWL Border Security System necessitates a significant emphasis on security and professional accountability. Given that the system manages sensitive surveillance information and aids in crucial decision-making, it is vital to guarantee data security and system dependability. Developers and operators must ensure the system's integrity and guard against unauthorized access or abuse. To safeguard data and system elements, appropriate security measures like encryption and access control need to be enforced. Moreover, those working on the project must guarantee that the system is utilized solely for its designated purpose and adheres to legal and ethical guidelines. Assuming accountability for system results and upholding stringent security, measures are essential for the secure and dependable functioning of OWL.

1.3.2 Confidentiality and Personal Rights:

The OWL Border Security System must guarantee the safeguarding of privacy and individual rights during the processing of surveillance information. While the system gathers and evaluates information on individuals, it is crucial to manage this data securely and responsibly. Access to personal data must be restricted to authorized individuals and utilized solely for security reasons. To prevent unauthorized exposure or misuse, it is essential to implement measures like data encryption, restricted access, and controlled data storage. Furthermore, the system must honor essential personal rights, such as privacy and dignity. Any observation or assessment must be confined to essential and pertinent actions, steering clear of excessive or unwarranted oversight. Maintaining ethical standards and public trust in the OWL system relies heavily on ensuring confidentiality and safeguarding personal rights.

1.3.3 Environmental Effects:

The OWL Border Security System needs to take into account its environmental effects throughout its implementation and functioning. As the system will be set up in natural border regions, it is crucial to reduce any adverse impacts on the environment. Cameras, sensors, and other equipment must be positioned in a way that does not interfere with wildlife habitats and natural ecosystems. Moreover, energy usage ought to be improved through the utilization of efficient hardware and, whenever feasible, renewable energy sources. Maintenance and installation tasks must be organized thoughtfully to avoid harming the environment. Minimizing physical effects and guaranteeing sustainable functionality are crucial for eco-friendly system implementation.

1.3.4 Professional Responsibility and Accountability:

The OWL Border Security Project demands a strong sense of professional responsibility and accountability from every team member participating. As the system has a direct influence on security operations and human decision-making, developers need to guarantee that it operates correctly, dependably, and ethically. Every design, development, and deployment process must adhere to professional standards and optimal practices. Team members are tasked with confirming system performance, recognizing potential risks, and resolving any problems that might occur. Furthermore, accountability is crucial in instances of system failures or unforeseen results. Well-defined responsibilities necessitate the establishment of clear documentation, transparent decision-making processes, and effective reporting mechanisms. Upholding professional responsibility and accountability is essential for developing a reliable and efficient OWL system.

1.3.5 Legal and Political Effects:

The OWL Border Security System is shaped by legal and political elements because of its use in border monitoring and enforcement. The system must adhere to national laws, regulations, and international treaties pertaining to security, data protection, and human rights. Legal regulations mandate that all data gathering and processing activities adhere to privacy and security guidelines. Any improper use of the system or breach of regulations may result in legal repercussions. Moreover, political elements can influence the implementation location and method of the system. Border security is tightly connected to governmental policies and international relations, which may affect project choices and execution strategies. Hence, guaranteeing adherence to legal standards and acknowledging political repercussions are crucial for the accountable and effective implementation of the OWL system.

1.3.6 Social Effects and Public Confidence:

The OWL Border Security System could have considerable social implications, especially regarding its impact on public trust and perception. Being a surveillance-oriented system, it can lead to worries regarding privacy, observation, and possible abuse. To uphold public trust, it is crucial that the system is utilized openly and solely for security reasons. Transparent communication regarding the system's functionality and the data it gathers can help minimize misunderstandings and foster trust. Moreover, the system must be structured to prevent bias or unjust targeting of individuals or groups.

Guaranteeing equitable and accountable use of AI is crucial for upholding societal approval. In general, public trust relies on the system's reliability, ethics, and alignment with societal values.

1.3.7 Ethical Boundaries and Humanitarian Values:

The OWL Border Security System should function within defined ethical limits while upholding humanitarian principles. While the system aims to improve security, it must not undermine human dignity or essential rights. Utilizing AI for surveillance necessitates thoughtful evaluation to prevent overreach in monitoring or detrimental choices. The system must concentrate on detecting questionable actions instead of unjustly targeting individuals. Moreover, humanitarian principles should be considered, particularly in circumstances concerning vulnerable groups like migrants or refugees. The system must assist security measures while avoiding harm or infringing on fundamental human rights. Upholding ethical boundaries and emphasizing humanitarian principles are crucial for the responsible implementation of the OWL system.

2- Requirements

2.1- Functional Requirements

2.1.1- Behavioral Pattern Analysis:

Beyond simple object detection, the system shall analyze sequences of human movements to identify specific behavioral patterns associated with irregular migration and smuggling, such as reconnaissance, hiding, or preparation for crossing.

2.1.2- Intent Analysis and Classification:

The system shall categorize detected activities into intent-based types ("crossing attempt" vs. "stationary observer"). This analysis must be performed by evaluating movement trajectories and interactions among individuals in real-time.

2.1.3- Multi-Sensor Data Integration:

To minimize false alarms, the system shall merge video streams with available sensor information to verify detections and provide enhanced situational awareness to the decision-makers.

2.1.4- Real-Time Geospatial Alerting:

Upon identifying a high-risk intent, the system must pinpoint the exact GPS coordinates of the activity and display it on the owlbordersec.com interactive map, providing immediate visual cues for preventive security strategies.

2.1.5- Secure Evidence Archiving:

Following the principles of Confidentiality, Integrity, and Availability, the system shall store encrypted logs of detected incidents. These archives must include time-stamped visual data and the behavioral classification result for legal and professional accountability.

2.1.6- Role-Based Dashboard Access:

The system should provide a user-friendly interface accessible only via multi-factor authentication. Access levels must be restricted based on the user's role to ensure data protection and minimize unauthorized surveillance.

2.2- Non-Functional Requirements

2.2.1- Real-Time Processing Latency:

To support "preventive security strategies," the system shall process video feeds and perform behavioral classification within a maximum delay of 2 seconds, ensuring that situational awareness is truly real-time.

2.2.2- Reliability and False Alarm Reduction:

The system shall maintain an uptime of 99.9%. Furthermore, the integration of smart data verification must achieve a false alarm rate low enough to prevent "wasteful utilization of resources".

2.2.3- Scalability and Manufacturability:

The software architecture must be modular to allow for easy hardware upgrades (cameras, sensors) and expansion over extensive border regions without requiring a total system redesign.

2.2.4- Ethical Data Handling (Anonymization):

To comply with ethical and social constraints, the system shall implement automated privacy filters (e.g., blurring faces of non-threatening individuals) during real-time monitoring, unless a high-risk behavior is confirmed.

2.2.5- Robustness in Harsh Environments:

As identified in the safety constraints, the system's algorithms must be optimized to function reliably under diverse conditions, including poor visibility (night/fog) and severe weather.

2.2.6- Maintainability and Documentation:

The system must include a comprehensive technical manual and a modular codebase to facilitate frequent updates of AI models, ensuring long-term viability and ease of service in remote border areas.

2.3- Technical Requirements

2.3.1- Hardware Requirements:

Standard computer hardware that can do AI-based image processing tasks is needed for the system. For effective deep learning model execution, a computer with a multi-core CPU, at least 8 GB of RAM, and optional GPU support is advised. The system might also make use of video input sources like camera streams or recorded security footage.

2.4- Software Requirements

2.4.1- Operating Systems:

The system ought to work with contemporary operating systems like Linux and Windows. For improved performance and interoperability with AI frameworks, Linux-based environments are recommended.

2.4.2- Programming Languages:

Python will be the main language used to construct the system because of its robust support for data processing libraries, computer vision, and artificial intelligence.

2.4.3- Database:

Event logs, detection results, and system outputs will be stored using lightweight data storage options like JSON, CSV, or SQLite. More sophisticated database systems might be incorporated for future scalability.

2.5- Data Requirements

2.5.1- Data Collection:

The system captures video data, both simulated datasets and recorded footage, from surveillance sources. To enhance danger detection and analysis, additional data is incorporated, such as object movement information (speed, direction, duration) and ambient circumstances (day/night situations).

2.5.2- Data Processing:

Preprocessing procedures like frame extraction, filtering, and normalization are applied to the collected data. The outputs of object identification and tracking are further processed to extract behavioral traits, which are subsequently utilized for threat assessment and pattern analysis.

3- References:

1. ACM Code of Ethics and Professional Conduct
2. The Software Engineering Code of Ethics, *IEEE Computer Society*
3. IEEE Code of Ethics
4. Computer and Information Ethics, *Stanford Encyclopedia of Philosphy*