Pacific Northwest
NATIONAL LABORATORY

PNNL-38291

Tactical Analysis for Calculating Contextual Risk at Boundaries

Summary of Laboratory Directed Research & Development Effort

September 2025

Kathryn Otte
Alysha Johnson
Ashley George
Kaelyn Haynie
Hanna Kauffman
Jonathan Mills
Julianna Puccio
Abby Tallman

U.S. DEPARTMENT of ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL-38291

Tactical Analysis for Calculating Contextual Risk at Boundaries

Summary of Laboratory Directed Research & Development Effort

September 2025

Kathryn Otte
Alysha Johnson
Ashley George
Kaelyn Haynie
Hannah Kauffman
Jonathan Mills
Julianna Puccio
Abby Tallman

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Summary

The Tactical Analysis for Calculating Contextual Risk at Boundaries (TACCRAB) tool is an innovative digital twin (DT) platform and automated risk algorithm designed to transform operational decision-making in structured screening environments, with an initial focus on Southern Border Land Ports of Entry (POEs). The invention provides integration points for advanced artificial intelligence, predictive modeling, and real-time data analysis to produce a comprehensive risk management tool that enables proactive, data-informed security strategies.

The core inventive features of TACCRAB center on its unique risk algorithm, which dynamically calculates contextual risk by synthesizing historical data, near real-time streaming data from the checkpoints themselves, and AI-generated predictions. Unlike traditional risk assessment methods, TACCRAB utilizes a DT to provide comprehensive operational insights, allowing stakeholders to visualize, simulate, and optimize checkpoint configurations with unprecedented speed and contextual awareness.

TACCRAB's key innovation lies in its ability to combine multiple complex inputs - including technology detection probabilities, resource availability, screening pathway characteristics, and threat actor behavioral patterns - into a unified risk calculation and update these inputs based on changing operational and environmental conditions. By leveraging a DT that continuously updates and learns from linked data, TACCRAB can suggest adaptive mitigation strategies that minimize risk while maintaining operational efficiency.

Particularly novel is the platform's approach to decision support, which goes beyond static risk assessment. The DT provides dynamic metrics such as wait times, resource allocation effectiveness, and potential emerging threat scenarios, enabling users to view sophisticated, relevant what-if simulations and optimize checkpoint operations in near real-time. The system's architecture allows for generalized application across different screening environments, such as secure facilities, ports of entry, and soft targets, making it a versatile tool for security and operational management.

The invention distinguishes itself through its comprehensive integration of predictive modeling, AI-driven pattern discovery, and user-friendly interface design. By combining these elements, TACCRAB transforms complex risk data into actionable insights, supporting decision-makers at various organizational levels - from booth agents making split-second screening decisions to checkpoint managers optimizing the day's resource allocation to strategic planners managing long-term investments.

Acknowledgments

This research was supported by the National Security Directorate (NSD) Mission Seed, under the Laboratory Directed Research and Development (LDRD) Program at Pacific Northwest National Laboratory (PNNL). PNNL is a multi-program national laboratory operated for the U.S. Department of Energy (DOE) by Battelle Memorial Institute under Contract No. DE-AC05-76RL01830.

The TACCRAB team extends gratitude to Ron Thomas for his continued energetic support of our work, and to Bryan Gerber, whose guidance as our advisor was instrumental in shaping the project's direction and technical approach. The team thanks Ryan Eddy for his leadership and insights as the Department of Homeland Security (DHS) sector lead, providing critical perspective on operational needs and connections to potential sponsors. The team would additionally like to thank Casey Perkins and Aaron Phillips for their advice on various development topics throughout the past two years and for helping us shape our requirements with enough scope to remain open to the next level of impact this cutting-edge research may unlock. Special appreciation is also extended to Rachel Pulliam for her thorough peer review and constructive feedback on this report.

Additionally, the TACCRAB team appreciates the contributions of Margaret Mitchell-Jones and Naeem Jaraysi in the PNNL NSD Communications Office. Their support generating promotional materials, including a flyer and a poster, was critical to marketing this research to potential sponsors.

Disclaimer

Parts of this document were created with the assistance of the PNNL Artificial Intelligence (AI) Incubator (gpt-4o and claude-3-5-haiku-20241022). TACCRAB documentation written solely without the use of AI was fed to the PNNL AI Incubator and then prompts were crafted to generate text for this report. However, all final content was thoroughly reviewed, edited, and approved by K. Otte and A. Johnson to ensure accuracy and relevance.

Acronyms and Abbreviations

AI	Artificial Intelligence
CBP	Customs and Border Protection
DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
DT	Digital Twin
EoC	Element of Concern
FY	Fiscal Year
LDRD	Laboratory Directed Research & Development
ML	Machine Learning
NA-70	Defense Nuclear Security
NSD	National Security Directorate
OFO	Office of Frontline Operations
PMD	Probability of a Missed Detection
PNNL	Pacific Northwest National Laboratory
POE	Port of Entry
S&T	Science & Technology Directorate
SME	Subject Matter Expert
TACCRAB	Tactical Analysis for Calculating Contextual Risk at Boundaries
TRL	Technical Readiness Level
TSA	Transportation Security Administration
UI/UX	User Interface/User Experience

Contents

Figures

Tables

1.0 Project Details

The Tactical Analysis for Calculating Contextual Risk at Boundaries (TACCRAB) tool is an innovative digital twin (DT) platform and automated risk algorithm designed to transform operational decision-making in structured screening environments, with an initial focus on Southern Border land ports of entry (POEs). The invention provides integration points for advanced artificial intelligence (AI), predictive modeling, and real-time data analysis to produce a comprehensive risk management tool that enables proactive, data-informed security strategies.

1.1 Background of Need

TACCRAB was conceived to address critical operational challenges at land POEs along the Southern Border of the United States. The invention arose from the increasing need for enhanced risk assessment methodologies to cope with the complexity and unpredictability of modern border security operations and threat actors. Current screening practices at checkpoints are often reactive, lacking real-time adaptability and up-to-date risk evaluation, leading to inefficiencies in resource allocation and an increased probability of security and smuggling threats evading detection.

This problem was magnified by the fragmented nature of the existing data and decision-making systems (Department of Homeland Security Office of Inspector General, 2021). Security personnel, operating under strict time constraints—such as 20 seconds to assess whether to direct a traveler to secondary screening—often lack access to actionable insights that integrated data from multiple disparate sources can provide to support the officer's intuition and observations (Johnson, 2023). Additionally, traditional risk assessment tools rely heavily on static qualitative or semi-quantitative analyses and are hampered by biases and high levels of uncertainty due to limited predictive capabilities (Cox, 2008; Montibeller & Winterfeldt, 2015).

The origin of TACCRAB stems from the necessity to bridge the gaps of contextual, real-time risk assessment while providing predictive insight into future operational scenarios, enabling the implementation of proactive security measures. The project began as a Laboratory Directed Research and Development (LDRD) effort at Pacific Northwest National Laboratory (PNNL), where the team sought to use DT technology supplemented by advanced predictive modeling and other AI tools to optimize physical security screening processes. The invention was driven by the need to mitigate key vulnerabilities, such as undetected smuggling and intent-to-harm threats, while keeping operational performance metrics, like traveler wait times and throughput, within acceptable thresholds.

1.2 Overview of Solution

TACCRAB's development was informed by subject matter expert (SME) input, real-world observations, and the acknowledgment that existing security systems underutilize valuable institutional knowledge and data. By introducing a unified platform for risk assessment—with an emphasis on scalability, automation, and accuracy—TACCRAB aims to meet the dual goals of enhancing security and improving operational efficiency. In essence, the invention was conceived to deliver a proactive approach to checkpoint operations, addressing not only current deficiencies but also eventually enabling future-focused scenarios to optimize resource allocation and counter evolving and emerging threats.

TACCRAB addresses the challenges of traditional risk assessment and suboptimal checkpoint operations by offering a cutting-edge DT integrated with a dynamic and scalable risk assessment algorithm. This system solves the problem of fragmented data, static analyses, and reactive decision-making by providing a unified, real-time, and predictive risk management solution. By integrating data from historical, (near) real-time, and algorithmic sources, TACCRAB synthesizes complex information into actionable insights that reduce cognitive load for decision-makers at all levels, from booth agents and operational managers to strategic planners.

The risk algorithm at the core of TACCRAB is designed to quantify and contextualize risk continuously and automatically, accommodating constantly changing environmental and operational conditions. This is achieved through continuous updates and predictions based on the interaction of various inputs, including detection technology probabilities, traveler behavior patterns, operational and physical constraints, and checkpoint configurations. Unlike traditional risk tools that depend on static or biased estimates, TACCRAB evaluates risk as a continual, highly granular time series, ensuring that its outputs reflect real-world conditions that may by constantly changing and inaccurate to represent using point estimates (Chatterjee et. al., 2021).

The graph-based nature of the risk algorithm is a critical component of TACCRAB. It effectively models the complex, interconnected nature of checkpoint operations. By representing screening procedures as nodes and edges within a directed graph, TACCRAB captures the nuance of traveler and resource flows, allowing for detailed analysis of vulnerabilities and dependencies within the system (Hagberg et. al., 2008). This approach enables the algorithm to account for variations such as shared resources, temporary unavailability of technologies, or dynamic routing based on prior screening outcomes. Furthermore, the graph framework supports the identification of anomalous pathways that deviate from standard procedures, highlighting potential security risks in real time. The flexibility and granularity of the graph-based methodology enable TACCRAB to provide adaptable, automated risk assessment.

The DT component further addresses the need for a system that goes beyond static assessments. It offers advanced simulation and modeling capabilities, allowing checkpoint operators to view automatically suggested, high-probability, and/or high-value "what-if" scenarios to predict the impact of various actions or resource deployments. For example, users can analyze how changes in lane configurations, staffing levels, or detection technology settings affect both expected risk and operational efficiency. By doing so, the system enables proactive decision-making, allowing security personnel to anticipate and adapt to emerging threats or changing traffic patterns.

TACCRAB's user-centric design ensures that the solution is not only powerful but also accessible. The interface prioritizes key performance metrics, such as risk, throughput, and wait times along with simple visualizations – like dials, gauges, and maps – that are straightforward to interpret (Laubheimer, 2017). Historical checkpoint statistics are displayed to contextualize the metrics users see in real time. Additionally, the system includes hooks for future work to incorporate reinforcement learning feedback loops, where both human input and operational outcomes inform future algorithm adjustments, ensuring continuous learning and refinement and minimizing repeated mistakes.

Overall, TACCRAB transforms checkpoint operations by enabling real-time situational awareness, predictive risk assessment, and proactive resource management, minimizing threats while ensuring operational efficiency. It provides a scalable solution applicable to various

structured screening environments, solving the need for a comprehensive and versatile risk assessment tool that evolves alongside the challenges it addresses.

1.3 Project Management Pivots

Throughout the project's lifespan, the TACCRAB team made several strategic pivots that demonstrated adaptability and a commitment to innovative development. Initially, the project was structured with a two-year plan that separated risk algorithm development in the first year and software development in the second year. However, the team quickly recognized that this linear approach was too rigid for the complexities involved—especially in building a responsive, data-driven dashboard. A more integrated collaboration between the algorithms, web development, and UI/UX design teams was essential. Web developers were brought in early to avoid the common pitfalls of retrofitting backend dirty data science code into client-facing applications (Amrit & Narayanappa, 2025). At the same time, UI/UX designers played a critical role throughout the project lifecycle—translating user needs into meaningful inputs for the algorithm team, while also ensuring that algorithmic outputs were understandable and relevant to end users. This cross-disciplinary feedback loop proved vital to aligning technical development with user value.

Another significant pivot was the team's approach to data and scope. Recognizing the challenges of accessing sensitive border security data, they shifted their focus from obtaining real-life data from the U.S. Southern Border to demonstrating the "art of the possible" using a combination of synthetic data and open-source data provided through CBP with daily port details and wait times. This shift enabled them to demonstrate the tool’s capabilities despite significant access constraints for existing data. The team also broadened the project's potential impact by recognizing that the risk algorithm and DT technology could be relevant beyond Southern Border land POEs (see Table 1). By prioritizing extensibility in the system’s design, the team broadened its applicability across diverse use cases—elevating it from a narrowly focused tool to a flexible, versatile solution.

Table 1. Potential TACCRAB Use Cases

Use Case	Agency	Subagency/Directorate/Office
Airports	DHS	Science & Technology Directorate (S&T); Transportation Security Administration (TSA)
Military Installations	DoD	
Land Ports	DHS	S&T; Customs and Border Protection (CBP) Office of Frontline Operations (OFO)
Seaports	DHS	S&T
Secure Facilities	DOE	Defense Nuclear Security (NA-70)

1.4 Sponsor Engagement

Over the past two years, the TACCRAB team engaged extensively with stakeholders and SMEs to ensure the project remained aligned with sponsor needs and operational priorities. Informational interviews were conducted with PNNL and DHS S&T SMEs, incorporating insights from individuals with experience in border security operations and detection technology data management. Additionally, collaboration with knowledgeable advisors and DHS and Department of Defense (DoD) sector leads within PNNL helped the team understand the complexities of sponsor spaces, including the downstream management of data generated by detection systems. Marketing efforts were also undertaken to introduce TACCRAB's capabilities across DHS components, highlighting its potential to provide proactive, risk-informed decision-making. These interactions guided the development of the web client and risk algorithm, ensuring they addressed real-world challenges such as operational variability, data integration, and usability across multiple levels of decision-making.

Specific activities included presentations to a variety of DHS components (Table 2), knowledge sharing sessions with a DHS modeling team, presentations at the 2025 Military Operations Research Symposium, and three proposals for DHS and DOE. One such proposal—sent to NA-70—to deploy TACCRAB, among other PNNL risk tools, for nuclear facility protection has been approved as of September 2025 and will bring $200,000 to $625,000 in funding to PNNL for fiscal year (FY) 26. While the scope of the approved work has shifted away from piloting TACCRAB at NA-70's test site in Florida, this upcoming project will enable TACCRAB team members to build relationships with established NA-70 commercial partners and become familiar with that sponsor space's needs. This funded proposal has also opened the door for TACCRAB to participate in a joint DoD/NA-70 proposal process beginning October 2026. If approved next spring, this upcoming proposal will enable TACCRAB to transition from LDRD into a sponsor space and pursue a higher technical readiness level (TRL).

Table 2. TACCRAB Presentations to DHS Components

DHS Component	Presentation Date(s)
S&T	May 2024, January 2025, July 2025
National Prioritization Framework Modeling Team	October 2024, November 2024
CBP	November 2024
US Secret Service	May 2025

1.5 Deliverables Status as of September 2025

Table 3 outlines the progress the TACCRAB team has made on various components of the tool suite. Please note that, as an LDRD without access to sponsor systems and data, the deployment, testing, and validation of TACCRAB's components and outputs in a live system have not been possible.

Table 3. Development Status of TACCRAB Components

Component	Current Status	Next Step	Approx. Progress
UI	UI/UX defined, and prototype deployed internally	Continued user feedback	90%[1]
Risk Algorithm	Fully built and documented in NetworkX (Python); tested with mock and open-source data	Test and validate with live feeds	85%
Data Integration	Some CBP technology sources and open-source datasets identified/explored	Identify all relevant sources for sponsor. Build an ingestion pipeline for 1-2 priority feeds	40%[1]
Discrete Event Simulation	Generic model built with notional data for land POEs	Tailor simulation logic to sponsor-specific system; obtain sponsor simulation inputs	30%
AI/ML Model Identification	High-value relevant predictive modeling and data fusion tools identified within PNNL	Identify relevant open source, paid, and/or sponsor models	30%
Digital Twin	Concept design	Model system behavior; define data-to-twin mapping and system architecture	10%
System Integration	Not started	Test end-to-end functionality with live data	0%

[1] Indicates progress for land POEs only. Progress for other use cases likely lower.

2.0 Risk Algorithm

In TACCRAB's risk framework, mission risk and attack risk are distinct but complementary approaches to evaluating potential threats. Mission risk focuses on the probability of a prohibited item successfully entering a protected area through a checkpoint, essentially measuring the likelihood of mission failure for a security agency. Attack risk, conversely, evaluates the potential consequences of an intentional attack at the checkpoint or its protected target, quantifying the potential harm from a realized threat (U.S. Department of Homeland Security, 2010). While mission risk is primarily concerned with the transit of prohibited items, attack risk calculates potential economic and human life impacts. Both risk types are calculated using similar probabilistic components—threat, vulnerability, and consequence—but are applied differently. Mission risk assesses item passage probability *(threat x vulnerability)*, while attack risk estimates the potential destructive outcomes of a deliberate hostile action *(threat x vulnerability x consequence)*.

2.1 Graph-Based Risk Analysis

TACCRAB's graph-based risk analysis represents a sophisticated approach to modeling checkpoint operations as a complex, interconnected network. By structuring checkpoints as a graph, the method transforms each detection resource or screening point into a vertex, allowing for granular analysis of traveler pathways and potential vulnerabilities. Each vertex can generate four unique signals when assessing a traveler: true positive, false positive, true negative, or false negative, enabling a nuanced understanding of detection performance.

Utilizing a graph-based approach provides the necessary flexibility to accurately represent complex checkpoint configurations. Vertices may be shared by travelers from multiple physical lanes or unique to individual lanes, which allows the risk algorithm to account for variations across different checkpoint applications. This approach enables dynamic modeling of potential scenarios, such as temporary detection asset (vertex) unavailability due to maintenance, unexpected operational failures, or changes in the concept of operations (U.S. Department of Homeland Security Office of Inspector General, 2015). The graph structure can address complex questions, for example, how routing to subsequent vertices might depend on alarms or responses from previous vertices, or how different traveler types might interact with the checkpoint's detection resources.

Figure 2.1 depicts an example of pedestrian screening procedures at a notional land POE. It highlights three distinct traveler scenarios within the system:

- John Doe, in the graphic, follows the screening procedures considered typical for pedestrians in this notional system.
- Jane Smith decides to opt out of the biometric identity verification and go through manual identity verification instead.
- Rob Brown attempts to take the typical screening route but triggers alarms for both his person and his belongings. As a result:
    - He is directed to multiple secondary screening procedures.
    - After additional checks, both his person and items are cleared.

- He is eventually allowed to exit the checkpoint.

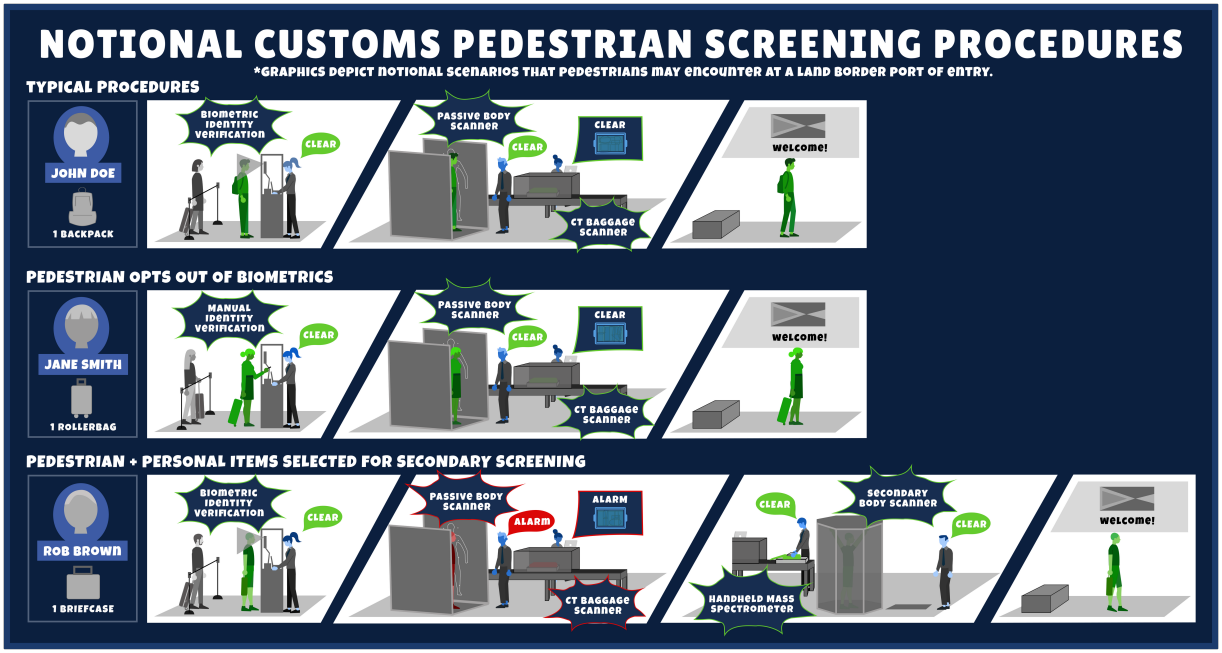

Figure 2.1 Notional pedestrian screening procedures at a land POE

While the experiences of Mr. Doe, Ms. Smith, and Mr. Brown represent three situations that a pedestrian may encounter at a customs land POE, Figure 2.1 actually contains six unique routes that may be taken from the entrance to exit of this pedestrian customs checkpoint (four walks for pedestrian entities, two walks for personal item entities). A walk, in graph theory, is a sequence of vertices and edges that exist to allow travel between defined start and end vertices (Grassl & Levin, 2018). Unlike a path, where vertices may only be visited once, vertices and/or edges in a walk may repeat. Figure 2.2 demonstrates each of the six walks in Figure 2.1, divided by traveler type and shown in graph format, where the boxes with detection resource names represent vertices and the arrows represent edges. The dashed boxes and arrows differentiate secondary screening from primary/typical screening.

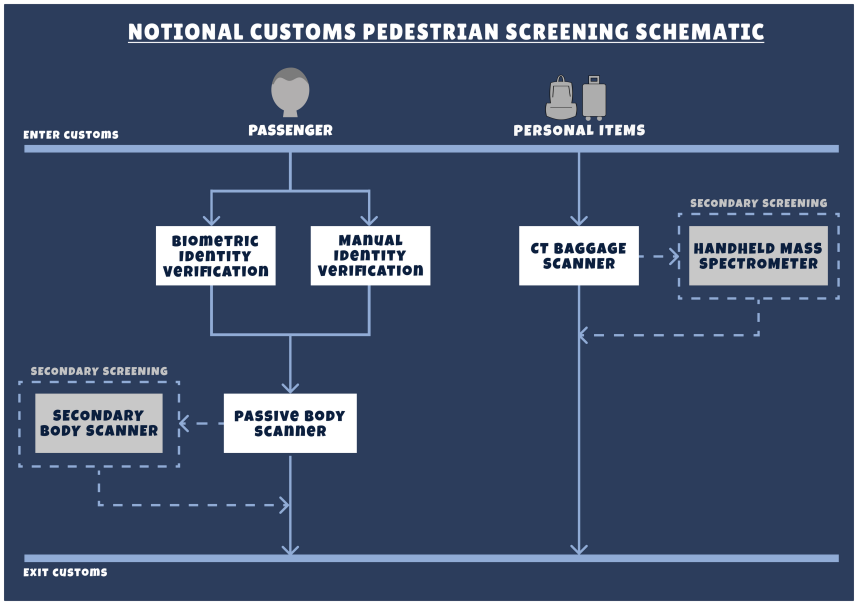

Figure 2.2 Notional land POE pedestrian screening procedures translated into graph format

By representing the checkpoint as a graph, TACCRAB can perform sophisticated risk calculations that go beyond traditional linear models. The approach enables the analysis of variations in checkpoint configurations, understanding interdependencies between different screening technologies, and quantifying risk at multiple levels of granularity. This methodology supports a more comprehensive and adaptable risk assessment, capable of simulating and predicting potential vulnerabilities in the screening process with exceptional detail and flexibility.

2.2 Vulnerability

TACCRAB calculates vulnerability by assessing how well a checkpoint can detect and mitigate threats under specific conditions. The vulnerability component is rooted in four primary inputs:

1. **Availability** determines whether a piece of technology or human resource is operational and functional at the time of screening.

2. **Applicability** evaluates whether the resource in question is capable of detecting a particular type of threat, or element of concern (EoC),

3. **Pathway probabilities** account for a traveler's likelihood of interacting with specific technologies based on screening pathways.

4. **Detection probabilities** represent the chance that a given resource will successfully detect a particular EoC.

These factors are dynamically updated whenever any variable changes, ensuring that the assessment reflects real-time operational conditions.

The vulnerability score effectively represents the overall probability of a missed detection (PMD) across the entire checkpoint system. It adjusts based on the real-time status and performance of the deployed screening technologies and personnel. For example, if a key detection technology is non-functional or unavailable, its absence may significantly impact the

vulnerability score, indicating a higher likelihood that certain EoC could successfully make their way through the security system. This dynamic and data-driven approach ensures that TACCRAB's vulnerability assessment remains highly responsive to changing conditions and provides critical input for broader risk evaluations.

2.3 Consequence

TACCRAB calculates consequence by quantifying the potential economic and human life impacts of a successful attack scenario. The economic consequence component is calculated by multiplying the quantity of assets in a potential harm area by their respective acquisition costs. This equation allows for a precise estimation of direct economic damages that could result from a threat.

The human life consequence portion combines potential deaths and injuries into a single count, deliberately avoiding differentiation by human role or status. This means that in a theoretical attack scenario, a customs agent would contribute the same value to the consequence calculation as a traveler. By grouping human impacts into a unified metric of both potential deaths and potential injuries, TACCRAB simplifies the complex human factors (e.g., crowd behavior, skill level of present law enforcement officers) that would otherwise complicate precise injury and death predictions. The approach provides a standardized and transparent method of assessing the potential human life impact of an attack scenario, enabling decision-makers to efficiently evaluate the severity of a prospective security incident.

2.4 Threat

Conventional approaches to threat quantification frequently lack the capacity to fully capture and assess the intricacies of modern threat environments. Determining threats at the Southern Border involves identifying complex and evolving motivations, tactics, and entities of individual threat actors, who may act independently or as part of larger systems. Threat actors may smuggle various EoCs, such as drugs, firearms, currency, and human trafficking victims, posing challenges for modeling threat activity due to unpredictability of quantities of EoCs over time (United Nations Office on Drugs and Crime, 2025). Seizure rates add complexity to threat quantification, as they may result from increased smuggling attempts, improved detection performance, or a combination of both—obscuring whether a rise in seizures indicates an escalation or reduction in overall threat. Moreover, EoCs often pose indirect threats that manifest harm after crossing the border (e.g., drug smuggling), raising questions about assessing their immediate threat to POEs. Miscommunication or conflation of "threat" (likelihood of occurrence) and "consequence" (severity of outcome) can lead to skewed SME perceptions, as seen in public responses and sentiment to high-consequence, low-likelihood events like plane crashes versus high-likelihood, low-consequence events like phishing emails that are easily detected and/or blocked (Isidore, 2025; Raza, 2024).

These challenges underscore the importance of clear communication and robust AI and machine learning (ML) models for data fusion solutions to characterize and quantify threats effectively. TACCRAB proposes a sophisticated data fusion methodology that leverages advanced AI techniques to overcome traditional threat assessment limitations (Nisa et. al., 2025). By utilizing multiple data fusion levels (low-, mid-, and high-level), the approach can integrate diverse data sources, including historical data, real-time intelligence, third-party threat reporting systems, and varied information streams like law enforcement alerts, social media, infrastructure monitoring, and international security databases (Smolinska et. al., 2019). The

methodology emphasizes extracting and aligning key threat characteristics such as location, impact intensity, source credibility, anticipated time, and threat duration, enabling a more comprehensive and dynamic threat analysis approach.

For threat quantification, TACCRAB relies on EoC weightings. This approach involves identifying and tracking specific threat categories, including direct, indirect, veiled, and conditional threats, while also incorporating additional contextual categories like natural disasters, infrastructure disruptions, and cybercrimes. By applying AI/ML techniques, the methodology can create a time-based weighting function that allows for sophisticated threat correlation, enabling analysis across specific physical paths threats may take and potential threat correlations through advanced graph analysis techniques.

2.5 Risk Algorithm Testing & Validation

To test whether the mathematical equations deployed in this risk algorithm match logical expectations, the researchers built a prototype checkpoint graph generation and risk calculation program using the NetworkX package in Python (Hagberg et. al., 2008). This program allows users to build a notional checkpoint and calculate risk at that checkpoint at a single instant in time. Note the use of the term "notional" - this program uses assumptions and logic across a wide variety of security screening checkpoints rather than explicitly mimicking any specific type or location of a security screening checkpoint.

Six test experiments were conducted, each using a set of vulnerability input range parameters across 1,000 simulations. To ensure consistency, the same set of random seeds was used for both the default and test experiments. The results of each test experiment were then compared to the default experiment using boxplot metrics (Figure 2.3). Only one risk attribute changed between the default experiment and each test experiment. All expected results matched results, indicating that the mathematical equations used by TACCRAB support the logic behind its risk algorithm.

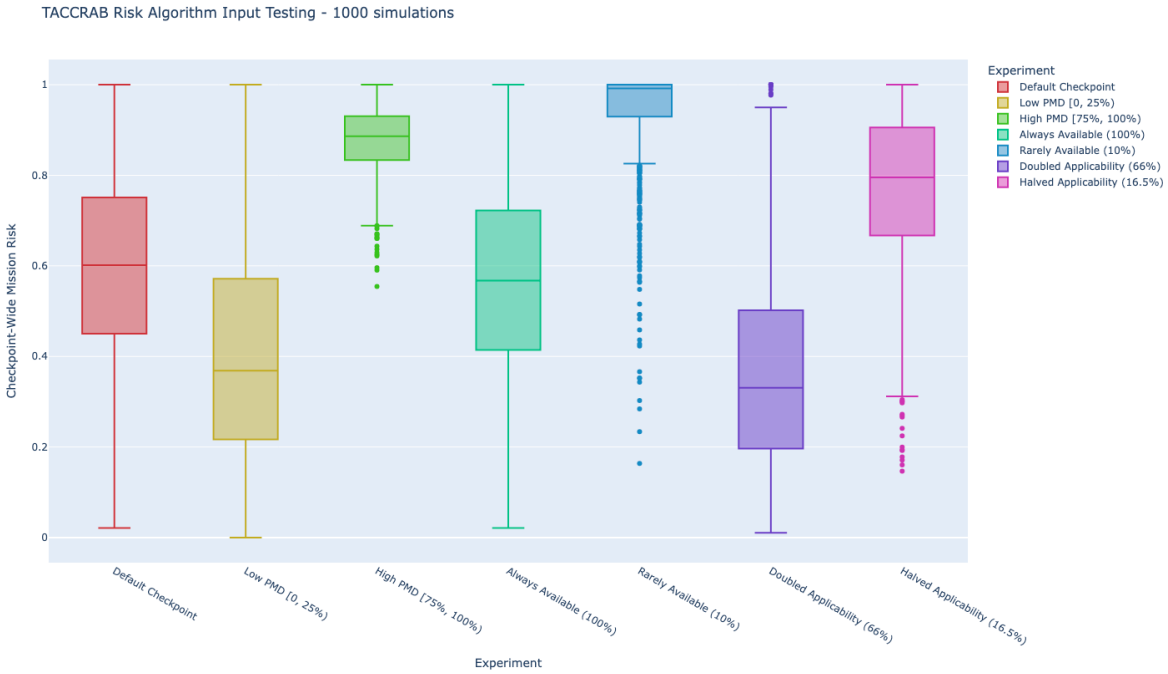

Figure 2.3 Comparative boxplots of checkpoint risk experiment simulation results

3.0 Digital Twin Web Client Prototype

The TACCRAB web client was designed for the project's demonstration use case: Southern Border land POEs. It offers a user-friendly platform that automates the analysis of traffic and threat scenarios, supporting data-driven decision-making and enabling operators to proactively enhance border security. The web client displays several operational metrics and capabilities, including:

- Live throughput counts and wait times for the land POEs
- Simulation of port operations based on user-defined inputs such as:
    - Arrival rates
    - Equipment configurations
    - Staff deployments
- Cost calculations for attack scenarios, with configurable EoCs.

The web client is organized into three main pages: Live View, Simulate, and Profiles. Each page provides a different lens into port operations—from real-time monitoring to configurable simulations and threat prioritization—offering users flexible tools for analysis and decision-making. Most of the metrics shown in the following mock-ups is notional, however, the POE names and wait times were scraped from the public-facing U.S. Customs and Border Protection Border Wait Times website. The underlying POE maps were provided by MapTiler's Leaflet library.

3.1 Live View Pages

This section of the application focuses on real-time metrics—such as risk levels, throughput, and wait time—for a selected POE, along with a map of the crossing and a breakdown of lane types and the resources allocated for each lane.

3.1.1 Metrics Page

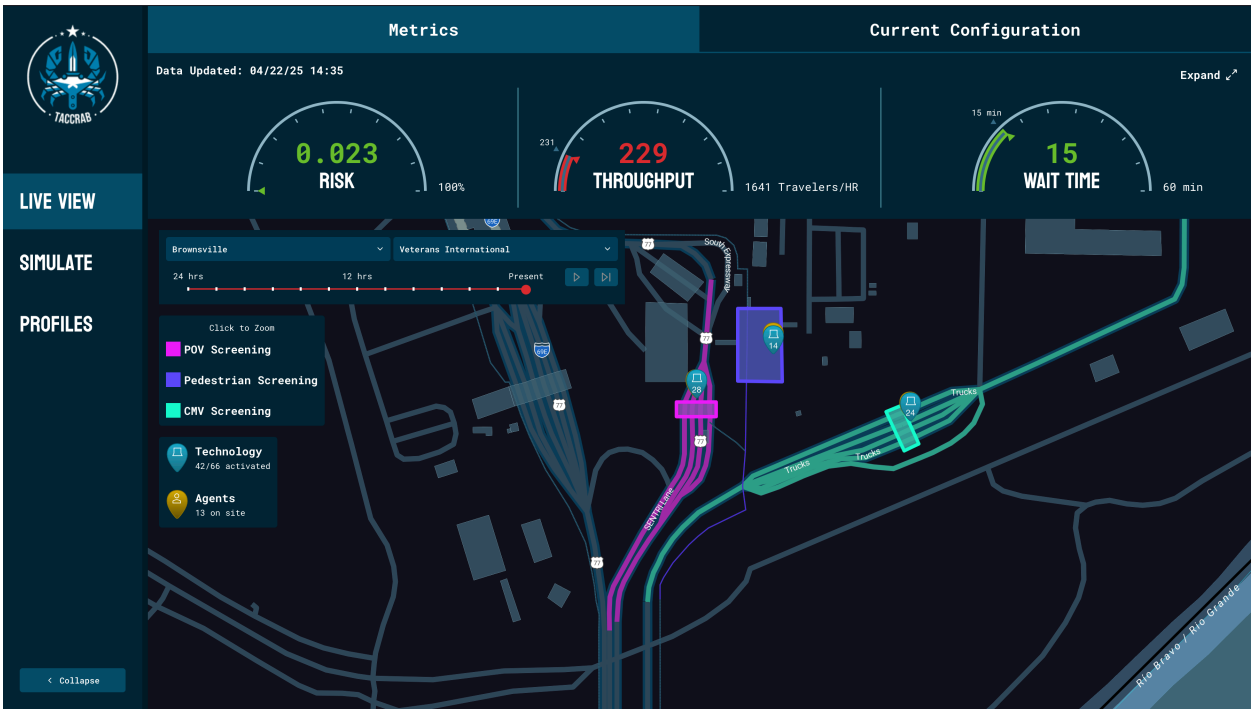

Figure 3.1 Metrics Page Overview

Starting on the live view screen (Figure 3.1), the metrics in the top bar (risk, throughput, and wait time) are all displayed relevant to the current time on the user's device for the present day. Expanding these metrics (Figure 3.2) breaks down each of the numbers by lane type. Additionally, by clicking on a toggle in the expanded metrics view, the risk metric is broken down into individual risk drivers, displayed with each threat weight, probability of missed detection, and corresponding risk value.

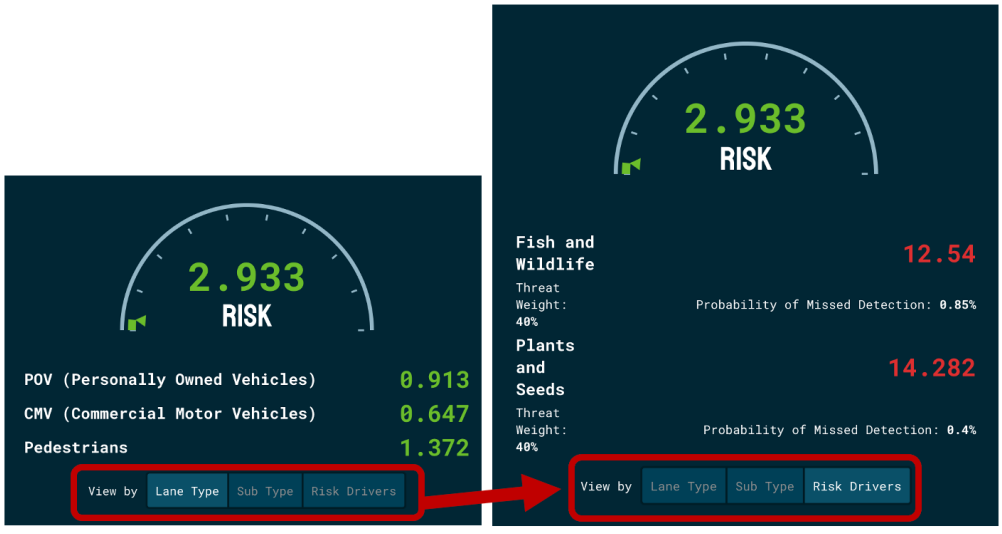

Figure 3.2 Detailed Metrics

The map view defaults to Brownsville's Veterans International Bridge POE, but the port and crossing can be changed using the dropdowns to the lower left of the daily metrics. The time slider (Figure 3.3) can be used to view the historical state of the checkpoint up to 24 hours earlier than the current time; the time value defaults to the current clock time, but once the value is adjusted, the time can be reset to the local time by clicking the fast-forward button (Figure 3.4).

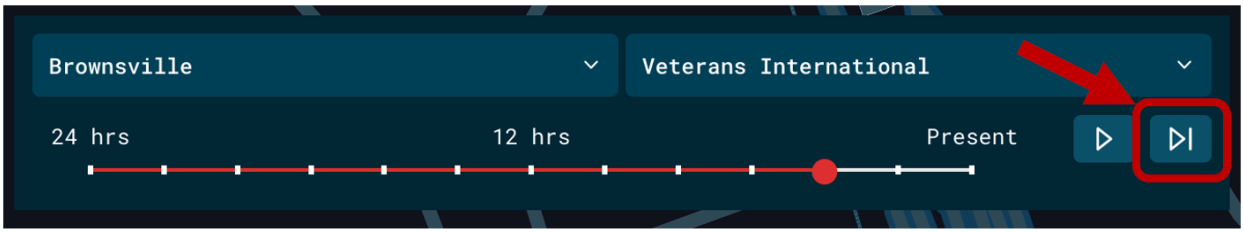

Figure 3.3 Metrics Page Time Sliders

The different traveler types in the map are color-coded according to the legend on the left of the map. Clicking on each traveler type will center the map over the lanes associated with that traveler type. The icons for the technology and agents show the distribution of assets across the currently viewed POE on the map.

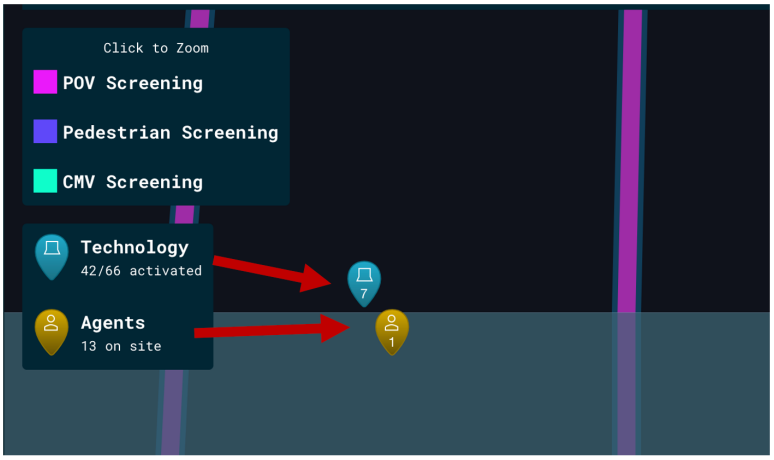

Figure 3.4 Technology and Agent Icons with Color-Coded Traveler Types

3.2 Current Configuration Page

The Current Configuration page (Figure 3.5) displays the data associated with the selected POE. Equipment and agent counts are aggregated in the top left, along with the mission profiles associated with the current POE. The tables provide a quick view of the distribution of lane types and agent presence along each lane. Clicking on these tables will bring up a traveler graph on the right side of the page showing the screening process for different routes that a traveler can take through the POE.

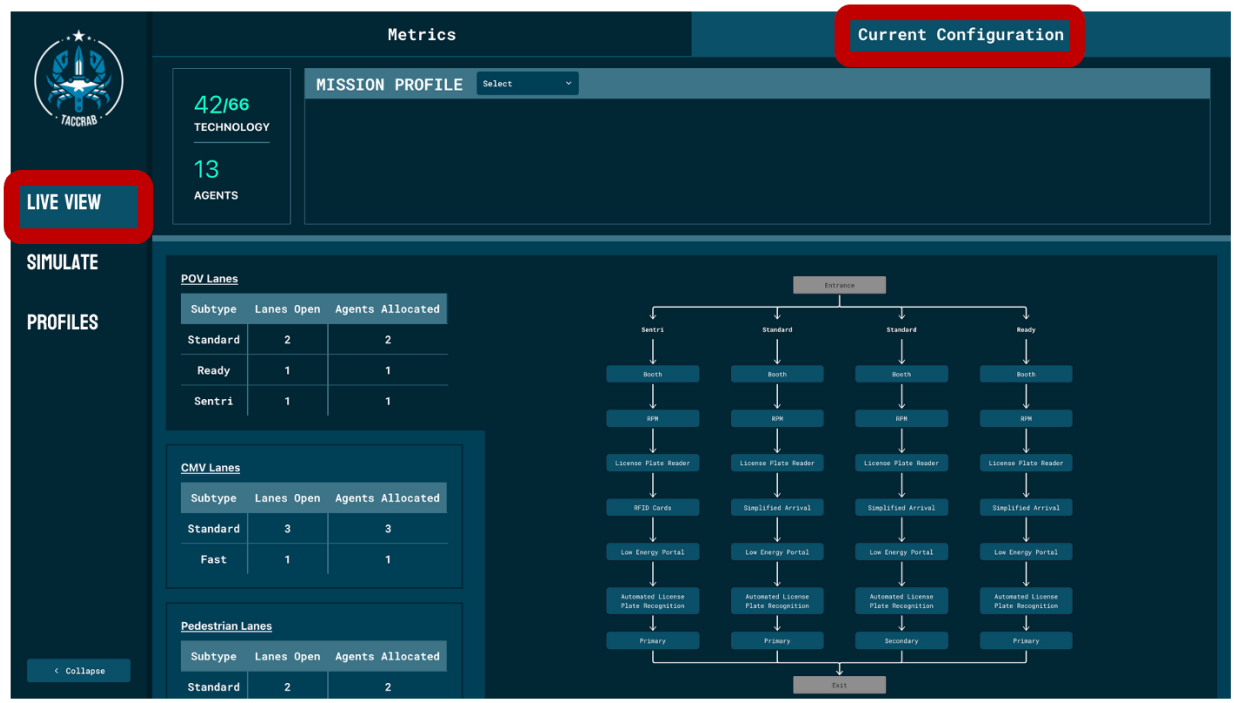

Figure 3.5 Current Configuration Page

3.3 Simulate Pages

The simulation pages provide the user with the ability to configure and run a simulation, set up and calculate the cost of an attack scenario, and view the results produced from both simulations and attack calculations.

3.3.1 Mission Risk Simulator

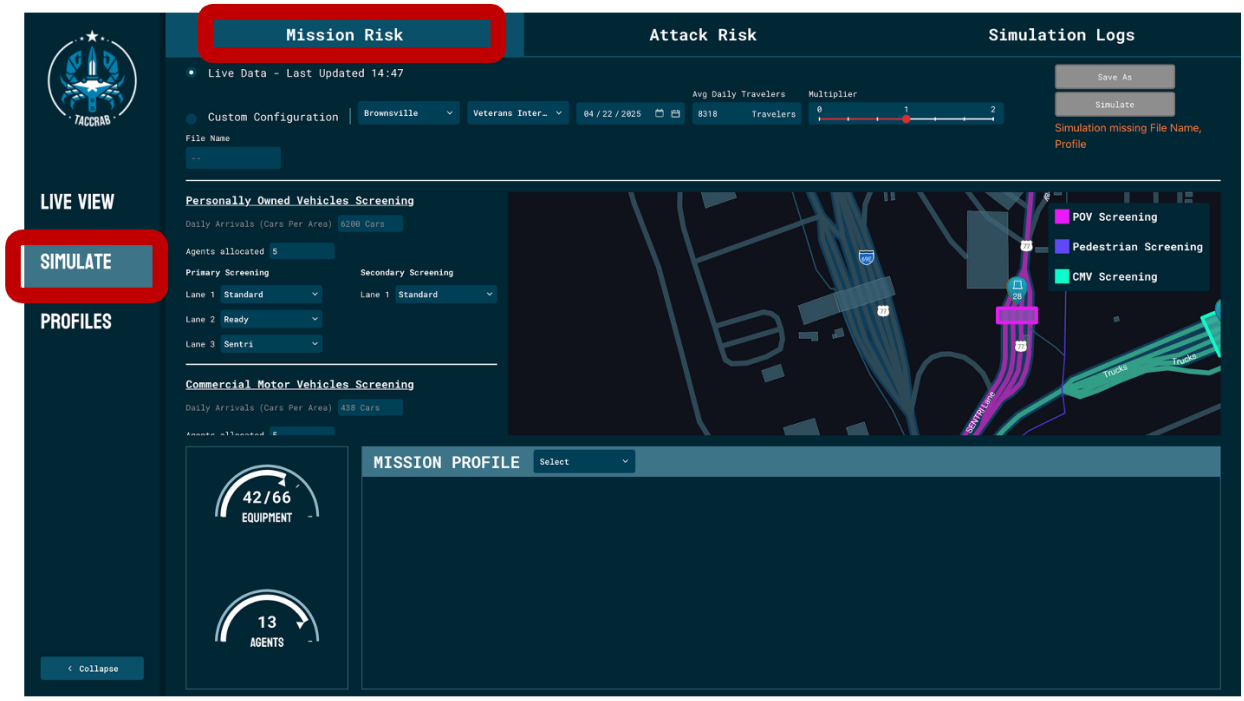

Figure 3.6 Mission Risk Simulator Overview

To run a mission risk simulation from the webpage shown in Figure 3.6, two primary configuration methods are possible: the live data configuration and a custom configuration. The live data configuration will use the current port and day to run a simulation. Otherwise, a different port, date, and traffic rate can be specified as shown below in Figure 3.7.

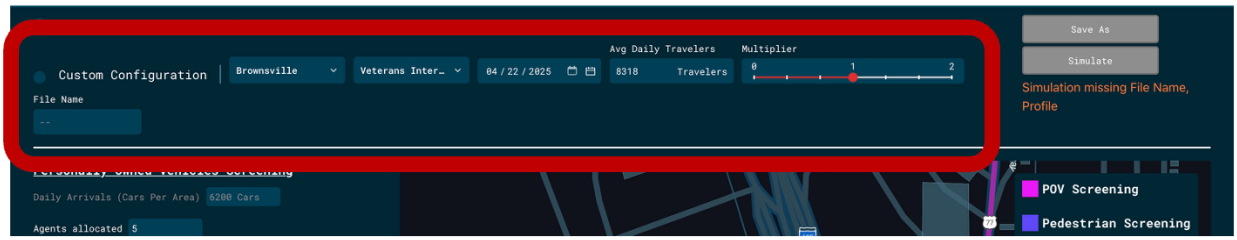

Figure 3.7 Mission Risk Simulation Manual Configuration

In custom simulation configurations, users may also choose to specify the following parameters (not shown above):

1. Determine Lane Quantities: After defining the values for each lane type, assign a specific number of lanes to a lane subtype or turn them off entirely for the simulation.

2. Set Additional Parameters: Provide the volume capacity and agent quantity for lane types, along with a mission profile. The mission profile influences how traffic is handled during the simulation.

3. Ensure Required Lane Subtypes:

    a. Based on the selected POE, the simulation requires a certain number of lane subtypes.

    b. If any required lane subtype is missing, an orange warning message will appear under the respective lane type name.

Once the required lane subtypes are met for the chosen port of entry:

1. The “Save As” button becomes enabled, allowing the user to save the current configuration file for future use (accessible from the Simulation Logs page).

2. The “Simulate” button is also activated, which starts the simulation for the specified port with the configured lane types and subtypes.

If the simulation successfully completes without errors, a notification appears. This notification includes a prompt with a link to the Simulation Logs page, where users can review the results. If the simulation fails, an error message will display. Additional details about the error will be available in the browser console.

3.3.2 Attack Risk Calculator Page

The configuration for an attack risk calculation (Figure 3.8) is very similar to the mission risk simulation; the only addition is the elements of concern that can be added to the map. Both the handgun and the conventional explosive elements have an adjustable radius, and the handgun also has an extendable arc angle. These objects can be dropped onto areas of the map and are automatically adjusted for scale.

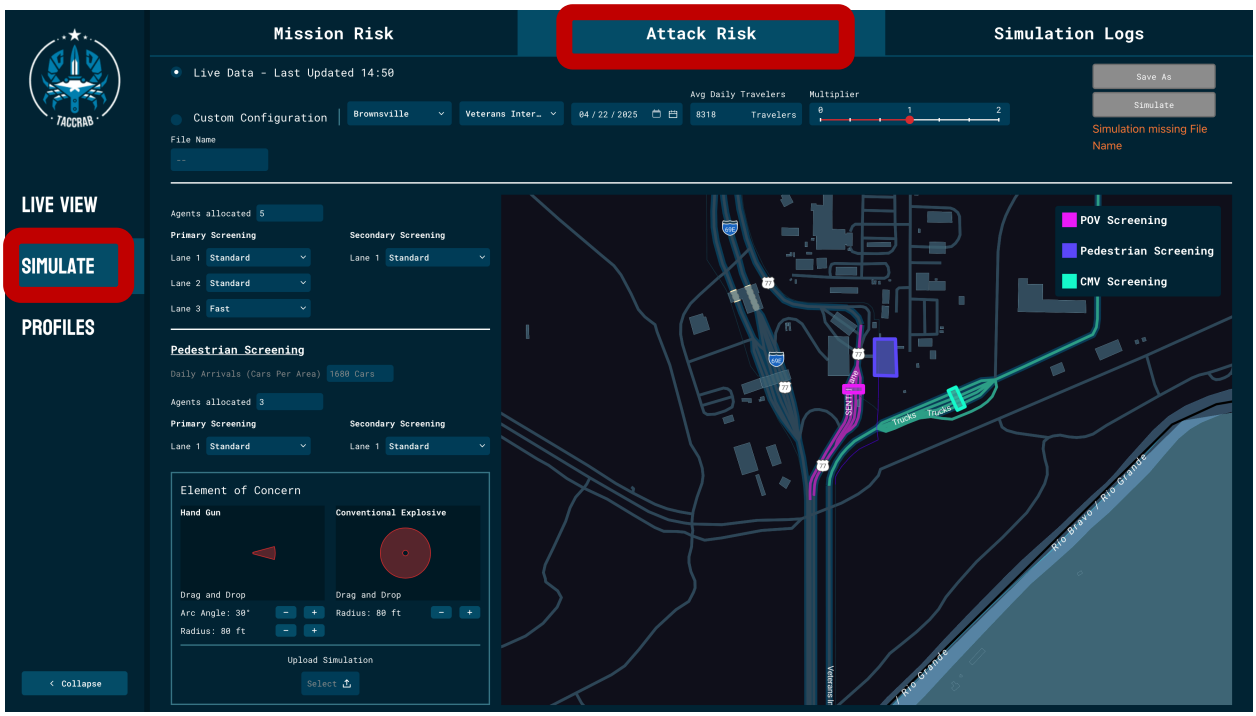

Figure 3.8 Attack Risk Calculator Overview

Provided further development, a user will be able to upload a simulation configuration with elements of concern for a port. Currently, calculating attack risk is not supported, so clicking the “Save As” and “Simulate” buttons will provide a user with a notification that this feature is a work in progress.

3.3.3 Simulation Logs Page

The simulation logs (Figure 3.9) provide a table for viewing prior mission and attack risk simulations. Users can favorite certain results by clicking the star icon to the left of each listing. The search bar in the upper left searches both tables for the given keyword. Currently, there are no viewable results for the yet-to-be-supported attack risk. However, valid risk, wait time, and throughput metrics are available for mission risk and can be accessed by clicking the corresponding row in the mission risk table. Each metric is further broken down by lane type and subtype, except for cost, which is presented as an itemized list. Clicking the “Save As” button redirects the user to the saved record in the simulation log table, and the “Export” button warns the user that the viewable data is not real and undergoing development.

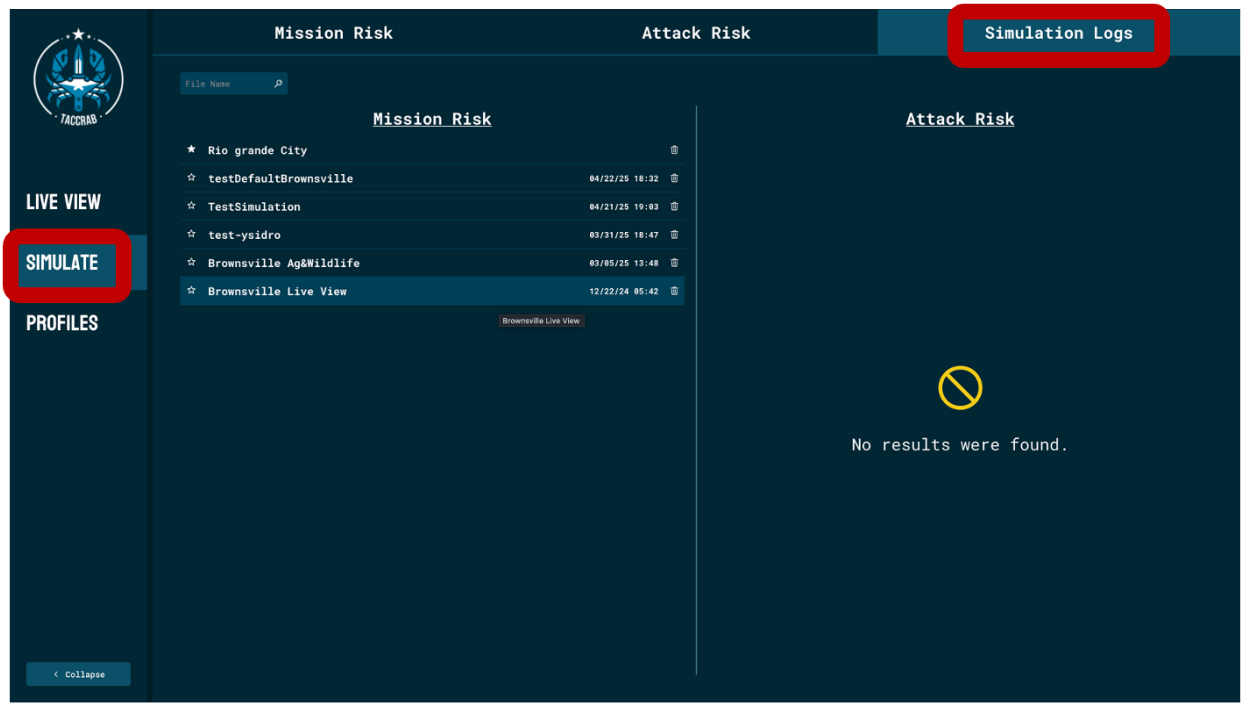

Figure 3.9 Simulation Logs Overview

3.4 Profiles Page

Mission profiles (Figure 3.10) will provide the user with an intuitive way to specify the relative importance of elements of concern for a simulation. Each profile records the date of its most recent edit. Once user registration is implemented, profiles will also be linked to the creator’s name. Profiles are tied to specific ports, so depending on the currently selected port within the application, this page may display no profiles. Each profile has a weighting scale for elements of concern. A minimum of 5% is reserved for elements unspecified by the user yet still relevant to the checkpoint, but the remaining 95% can be distributed to as many elements of concern as the user sees fit.

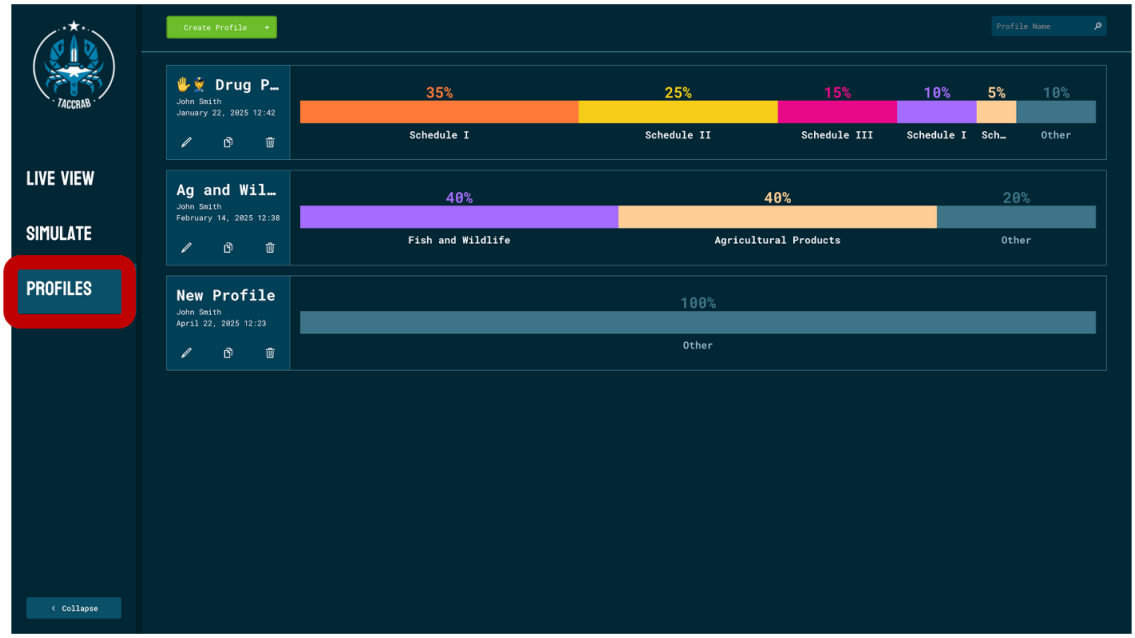

Figure 3.10 Profiles Overview

Each element can either be listed on its own with a threat weight or grouped into a category of elements that receives its own threat weight. As a grouping example, Figure 3.11 shows all drugs classified by the Drug Enforcement Agency as Schedule I grouped together with a category threat weight of 22%.

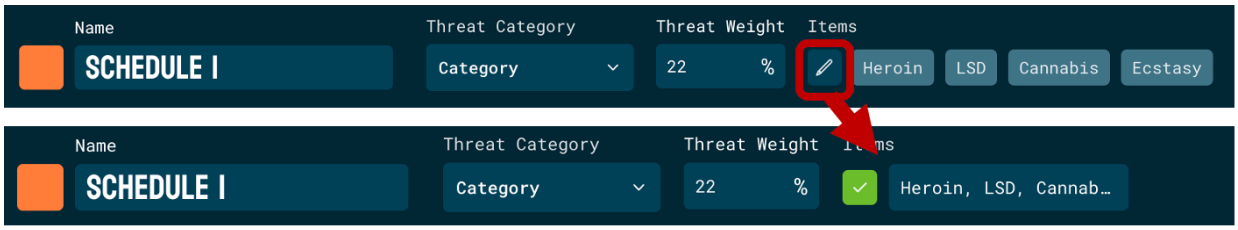

Figure 3.11 EoC Granularity

Entire profiles can be copied, which will duplicate all elements of concern for a new configuration of weightings. These configurations control how a simulation processes elements of concern and affect traffic flow, thus offering a fine-tuned method for controlling simulation details.

4.0 Next Steps for Research & Development

Building on the foundational capabilities and vision for TACCRAB, the next steps in research and development will focus on refining the system's technological components, expanding its applicability, and ensuring it remains adaptable to evolving security challenges. The following initiatives are prioritized to propel TACCRAB from its current state into a fully operational, future-focused solution.

4.1 Incorporate Cybersecurity Threat Intelligence

Physical security of critical facilities does not exist in isolation from the growing landscape of cyber threats. To enhance TACCRAB's ability to address hybrid, multi-domain risks, future development will emphasize the integration of cybersecurity considerations into its risk assessment and decision-making framework.

- Threat Intelligence Integration: Incorporate cyber threat feeds, including indicators of compromise, threat actor behaviors, and vulnerability data, to evaluate risks stemming from advanced persistent threats, ransomware campaigns, and supply chain vulnerabilities that may impact physical systems. Other tools created at PNNL (e.g., MITRE_KG) have been identified to integrate with as another data stream to pull in open-source cyber threat intelligence to our risk algorithm (Donald et. al., 2023).

- Digital Twin Expansion: Simulate potential cyber-physical interplay scenarios; for example, analyzing the cascading effects of cyber disruptions on physical workflow and staffing or detecting coordination between cyber and physical adversaries (Miller et. al., 2024). The upcoming converged security lab is identified as a testing location within PNNL.

- Cyber-Physical Fusion: Bridge the gap between cybersecurity and physical security through AI/ML-driven analysis and visualization tools that identify vulnerabilities across interconnected systems and suggest mitigation actions.

4.2 DoD and NA-70 Sponsor Data, In Sponsor Space

Collaboration with NA-70 and TACCRAB has evolved to include DoD and would be tailored to meet sponsor-specific requirements for structured screening environments. If funded, the upcoming proposal opportunity would support iterative prototyping, test site validation, and secure data integration to align system capabilities with sponsor priorities.

- Requirement Gathering: Conduct stakeholder interviews and environmental analyses to define operational priorities and refine system features.

- Prototype Development: Create sponsor-specific configurations, adapting risk algorithms, digital twin models, and user interfaces as needed to address NA-70's workflows and challenges.

- On-Site Testing: Deploy TACCRAB in operational environments for real-world validation, enabling algorithm refinements based on sponsor feedback.

- Data Security Enhancements: Implement secure data pipelines while potentially integrating cyber threat intelligence to support hybrid risk assessments.

By leveraging funding strategically, TACCRAB will deliver actionable, scalable solutions while ensuring alignment with NA-70's objectives for long-term operational effectiveness.

4.3 Integration with PNNL Resources and Open-Source Data + AI/ML Models

To maximize TACCRAB's predictive capabilities and adaptability, the next development phase would focus on leveraging PNNL collaborations and open-source resources. By integrating these diverse datasets with advanced AI/ML models, TACCRAB will deliver enhanced, context-aware insights for risk assessment and resource optimization across secured environments.

- PNNL Collaboration: Utilize resources from PNNL's Converged Security Lab and MITRE_KG open-source threat intelligence graph database to incorporate cutting-edge research and real-world data on physical and cyber threats. This will enable TACCRAB to identify hybrid risks and adapt to evolving threat landscapes.

- Open-Source Data Integration: Incorporate datasets such as weather patterns, social event scheduling, and geographical data to model external factors influencing operational risks, traffic flows, and situational vulnerabilities.

- Sponsor-Specific AI/ML Models: Integrate historical and real-time sponsor-provided data (e.g., operational statistics, facility layouts) to fine-tune AI/ML algorithms, ensuring outputs align with environment-specific requirements.

- Enhanced Predictions: Develop and train AI/ML models using these diverse datasets to enhance TACCRAB's ability to predict dynamic risks, optimize resource allocation, and model "what-if" scenarios with greater accuracy.

4.4 Reinforcement Learning & Continuous Improvement

Harnessing reinforcement learning-informed feedback loops will be central to refining TACCRAB as it transitions to full operational use.

- Human Operator Collaboration: Implement mechanisms for personnel to provide real-time feedback that informs system updates. For instance, operators can annotate unusual traveler behaviors or suggest adjustments to algorithm-driven risk assessments.

- Operational Outcome Analysis: Continuously track the performance of risk metrics and resource allocation decisions to understand where TACCRAB exceeds or falls short, ensuring targeted algorithm adaptation.

By focusing on these next steps, TACCRAB will evolve into a fully adaptable, dynamic solution capable of mitigating contemporary and future threats, ultimately reshaping the way risk management and operational efficiency are approached within structured environments. These efforts will ensure that TACCRAB remains at the cutting edge of security innovation.

5.0 References

Amrit, C., & Narayanappa, A. K. (2025). An analysis of the challenges in the adoption of MLOps. Journal of Innovation & Knowledge, 10(1), 100637. https://doi.org/10.1016/j.jik.2024.100637

Chatterjee, S., Brigantic, R. T., & Waterworth, A. M. (2021). Applied Risk Analysis for Guiding Homeland Security Policy and decisions. John Wiley & Sons, Incorporated.

Cox, L. A. (2008). What's wrong with risk matrices? *Risk Analysis*, *28*(2), 497–512. https://doi.org/10.1111/j.1539-6924.2008.01030.x.

Donald, S., Meyur, R. and Purohit, S. (2023). Hybrid attack graph generation with graph convolutional deep-q learning. *2023 IEEE International Conference on Big Data (BigData)*, Sorrento, Italy, pp. 3127-3133, doi: 10.1109/BigData59044.2023.10386675.

Grassl, R., & Levin, O. (2018). *More discrete mathematics via graph theory*. Greeley, CO: University of Northern Colorado.

Hagberg, A. A., Schult, D. A., & Swart, P. J. (2008). Exploring network structure, dynamics, and function using NetworkX. In G. Varoquaux, T. Vaught, & J. Millman (Eds.), *Proceedings of the 7th Python in Science Conference (SciPy2008)* (pp. 11–15). SciPy.

Isidore, C. (2025). Fear of flying is pushing ticket sales down in the wake of multiple crashes, airlines say. *CNN Business*. https://www.cnn.com/2025/03/11/business/passengers-air-travel-crashes-fear

Johnson, A. M. and authors not released. (2023). Report title not released. PNNL-35400 Limited Distribution.

Laubheimer, P. (2017). Dashboards: making charts and graphs easier to understand. *Nielson Norman Group*. https://www.nngroup.com/articles/dashboards-preattentive/

MapTiler. (n.d.). Leaflet JS with MapTiler maps. Retrieved 2024, from https://docs.maptiler.com/leaflet/

Miller, J., Kay, B., Mackey, P., and Chatterjee, S. (December 2024). Multi-layer network PageRank for critical infrastructure analysis." *Homeland Security Affairs 20*(4). www.hsaj.org/articles23189.

Montibeller, G., & von Winterfeldt, D. (2015). Cognitive and motivational biases in decision and risk analysis. *Risk Analysis: An International Journal*, *35*(7), 1230–1251. doi: 10.1111/risa.12360

Nisa, U., Shirazi, M., Saip, M.A., and Pozi, M.S.M. (2025). Agentic AI: the age of reasoning—a review. *Journal of Automation and Intelligence*. doi:10.1016/j.jai.2025.08.003

Raza, M. (2024). Phishing Attacks: Protecting Against Them. *Splunk*. https://www.splunk.com/en_us/blog/learn/phishing-scams-attacks.html.

Smolinska, A., Engel, J., Szymanska, E., Buydens, L., & Blanchet, L. (2019). General framing of low-, mid-, and high-level data fusion with examples in the life sciences. Data Handling in Science and Technology, 31, 51–79. https://doi.org/10.1016/b978-0-444-63984-4.00003-x

United Nations Office on Drugs and Crime. (2025). dataUNDOC - Data Portal. https://dataunodc.un.org/dp-trafficking-persons (Accessed on 18 Sept 2025).

U.S. Customs and Border Protection. (2025). Border Wait Times. *Customs and Border Protection*. https://bwt.cbp.gov/api/waittimes

U.S. Department of Homeland Security. (2010). DHS Risk Lexicon. *Homeland Security*.

U.S. Department of Homeland Security Office of Inspector General. (2015). The Transportation Security Administration does not properly manage its airport screening equipment maintenance program (Report No. OIG-15-86). *United States Department of Homeland Security*. https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/2015/OIG_15-86_May15.pdf

U.S. Department of Homeland Security Office of Inspector General. (2021). Summary report: persistent data issues hinder DHS mission, programs, and operations (Report No. OIG-21-37). *United States Department of Homeland Security*. https://www.oig.dhs.gov/sites/default/files/assets/2021-05/OIG-21-37-May21.pdf.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov