Risk-based security: From Theory to Practice

Comparison of Rule vs Risk based security policies using the iCrowd Simulator

Stelios C. A. Thomopoulos

NCSR Demokritos

October 11-12, 2022

eu-LISA Industry Roundtable

Integrated Systems Laboratory

ACKNOWLEDGEMENTS

The research described in this presentation has been supported by the following research contracts focused on Risk-based Security (RBS):

"**FLYSEC**: Optimizing time-to-FLY and enhancing airport SECurity," Programme: Horizon 2020, European Union Grant Agreement No. 653879, Duration: 01/05/2015 - 31/07/2018, http://www.fly-sec.eu.
FLYSEC was the **first EU-funded project** to test RBS in the context of **airport security**

"**TRESSPASS**: Robust Risk Based Screening and Alert System for Travelers and luggage," Grant Agreement No. 787120, Call: H2020-SEC-2016-2017-2, https://www.tresspass.eu/The-project.
TRESSPASS was the first EU-funded project to generalize the testing of RBS to **all three Border Crossing Point (BCP)** modalities: **air, ground, and sea**.

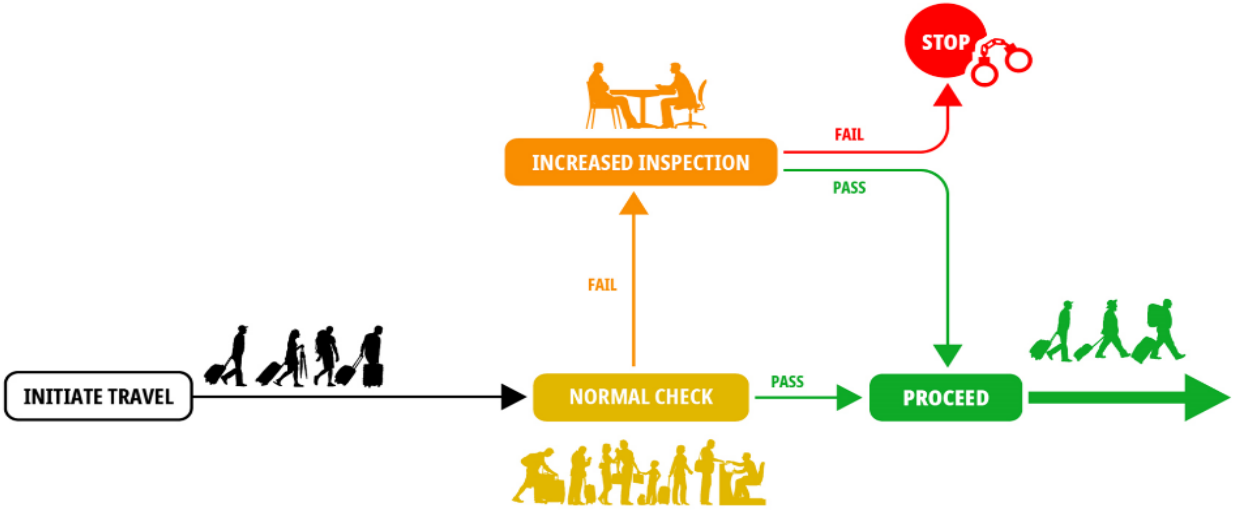
"**D4FLY**: Detecting Document frauD and iDentity on the fly," Horizon 2020 Programme, Contract No. 833704, 2019-2022, funding organization: European Union, https://d4fly.eu. **First EU funded project** to put to **test a biometrics corridor** for on-the-fly biometrics ID testing.

"**SAFETY4RAILS**: Data-based analysis for SAFETY and security protection FOR detection, prevention, mitigation and response in trans-modal metro and RAILway networkS," Horizon 2020 Programme, Call: H2020-SU-INFRA01, Contract No. 883532, 2020-2022, funding organization: European Union, https://safe4rail.eu. **First EU funded project** to create a **risk assessment tools dashboard** for rail & metro infrastructure protection.

The **iCrowd simulator** has been pivotal in all 4 projects for:

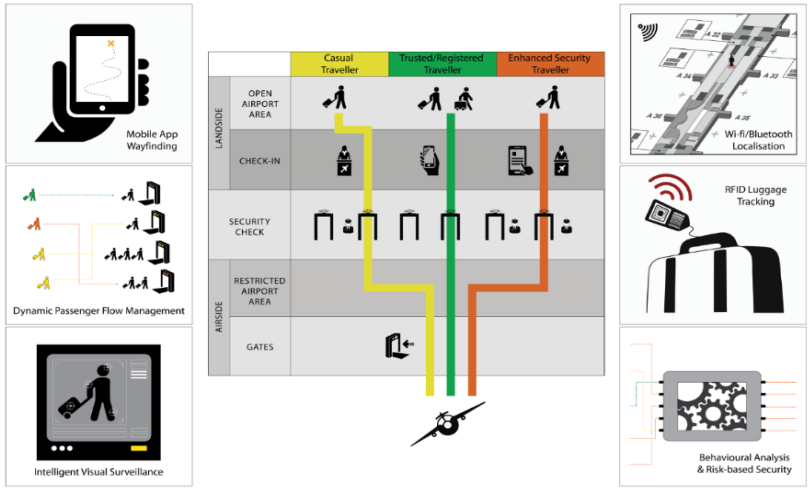
- testing RBS (Risk-based Security) scrutiny implementations,
- comparing RBS with rule-based security doctrines in air, land, and sea BCP's
- Testing new biometric-on-the-fly technologies and logistics concerning the rollout of biometric corridor
- Surveillance technologies (video cameras) for monitoring, tracking, and anomalies detection
- RFID luggage tracking implementation logistics
- Audio broadcast alerting system design and layout effectiveness testing

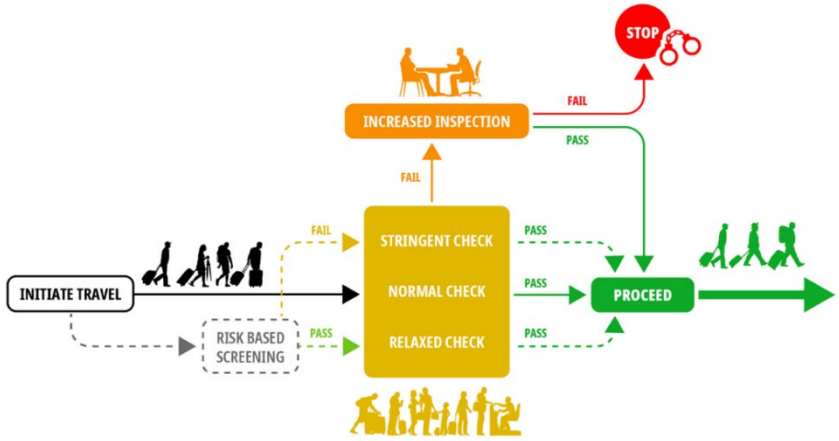
Rule-based current security concept



- ✓ **Less than 5% of travelers represent a threat to the security screening process of a BCP, yet same rule-based security checks, consisting of uniform non-discriminatory screening with random enhanced checks, apply equally to all travelers, leading to low user experience and increased delays.**

Risk-based security concept framework





A. Intelligently combine:

i. information obtained from observable aspects of human identity and possession;

ii. knowledge acquired about hidden aspects of human capability, and

iii. intent

B. Assess risk and **classify travelers into:**

- ***Casual, Trusted,*** *or* ***Enhanced*** (FLYSEC – 3 categories),
- ***Neutral, Bonafide, Malafide,*** *or* ***Unknown*** (TRESSPASS – 4 categories)

C. Apply security screening **procedures commensurate to the assessed risk to**

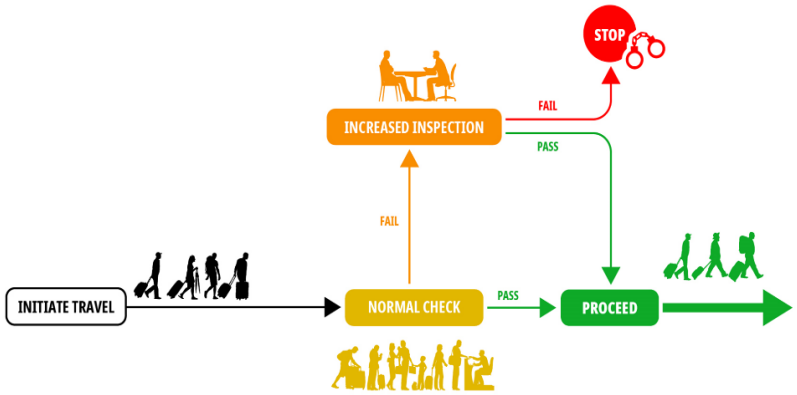
(a) speed up the security screening process;

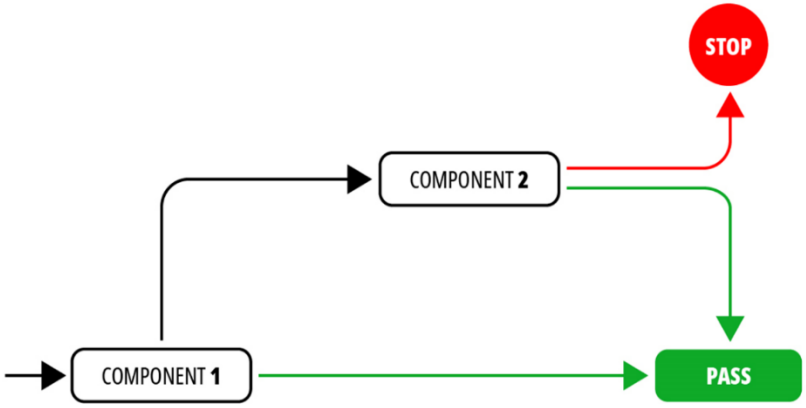
(b) offer a **more pleasant experience** to travelers, and

(c) maintain or improve the level of security at the same time

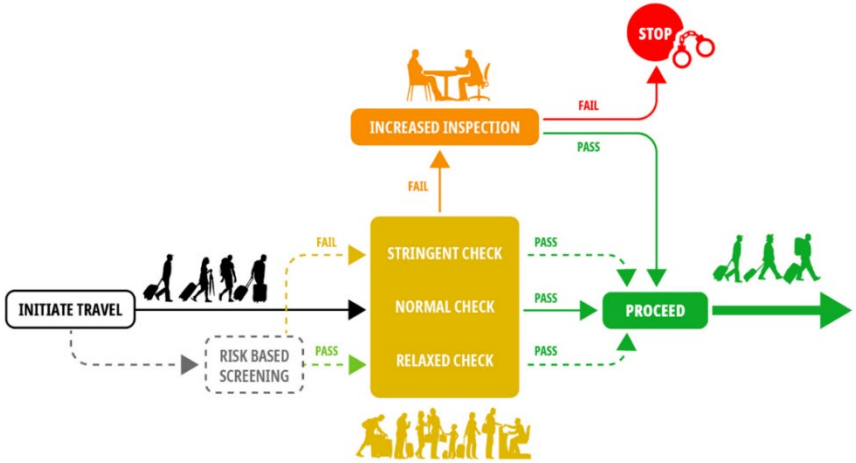
Rule-based & Risk-based BCP security configurations: The need for simulation

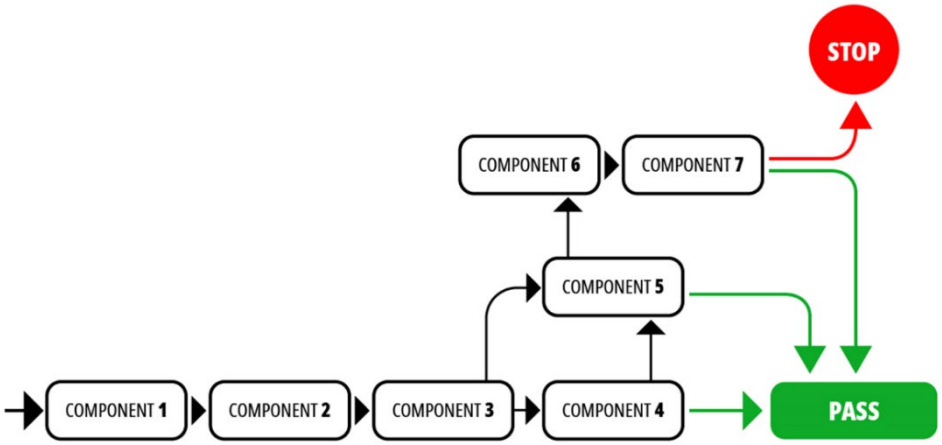
1. Rule-based security checking configuration





2. Risk-based security checking configuration





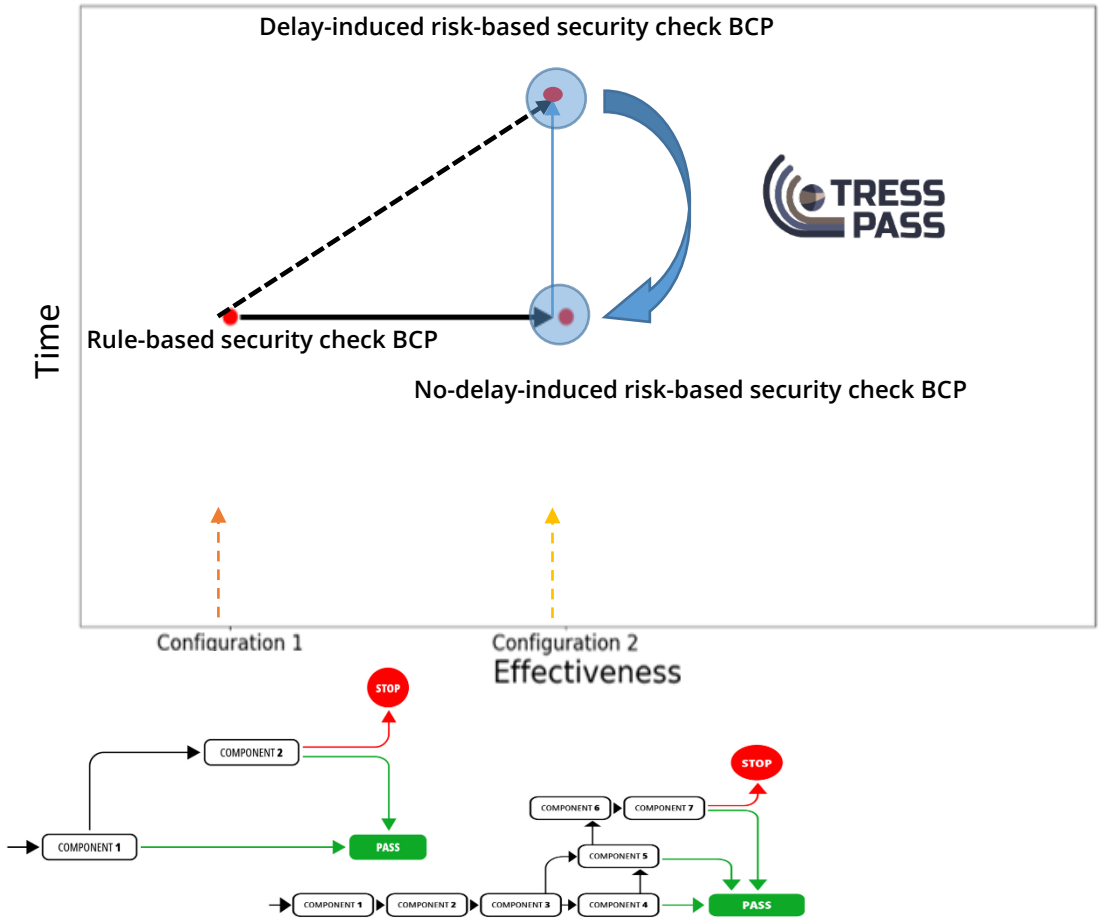
Increase effectiveness vs delay

Monte Carlo Simulation

- A BCP with 100 travelers
- Distribution of traveler types: [Normal, Suspicious]: [0.9,0.1]
- Alarm threshold for each component: 0.5
- Risk calculation: According to a script described in [14]
- **Effectiveness calculation**:

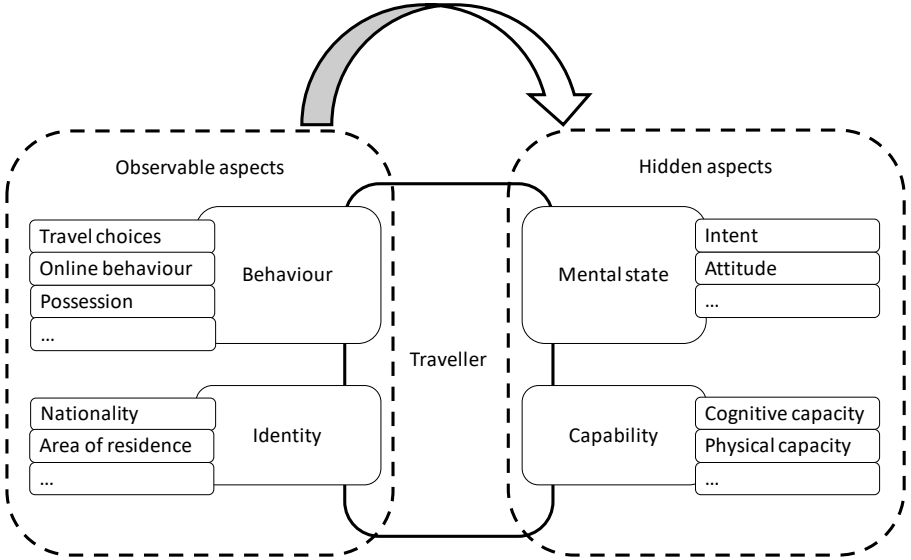
  diff_1 = (mean of total suspicious people – total people stopped)

  effectiveness = 1/absolute (diff_1)
- Ran over 10000 iteration with 100 travelers each time for both the configurations.



- **Can effectiveness increase without increasing delays?**

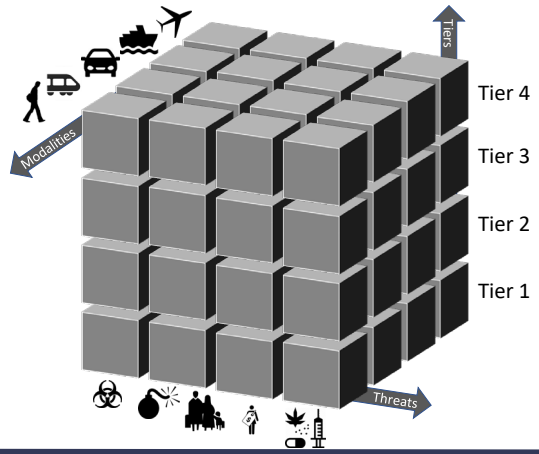
Moving from rule-based to risk-based security: Challenges & Answers



. Observable and Hidden Risk Factors

Multi-modal, multi-tier TRESSPASS Risk-assessment model

1. measures undertaken with third countries or service providers
2. cooperation with neighboring countries
3. border control and counter-smuggling measures
4. control measures within the area of free move



Questions to address via simulation

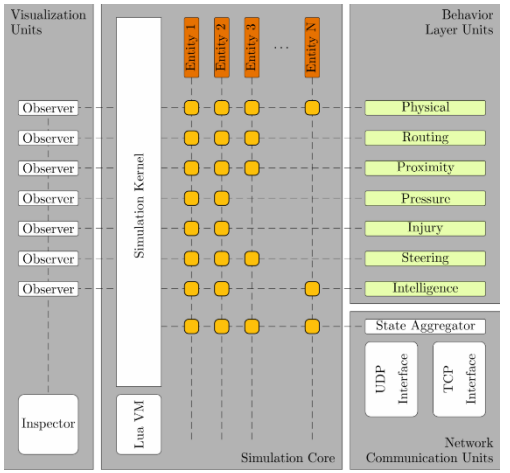
- RBS vs RLBS efficiency
- Travelers satisfaction
- Delays
- Number of personnel needed for the same throughput of travelers
- Number of enrollment kiosks needed
- Number of ABC gates needed
- Surveillance infrastructure
- Detection & biometric technologies

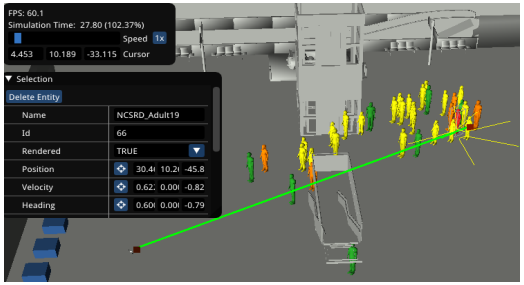
Capabilities required for risk-based security

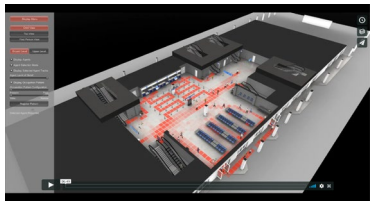
- **Risk Assessment Framework** (FLYSEC & TRESSPASS)
- Control, Command & Information **Fusion System** (OCULUS C2I)
- **Technologies for on-the-fly risk assessment** without inducing delays:
  - Location sensors & cameras for crowd tracking and anomaly detection
  - PNR data (A passenger name record (PNR) is a record in the database of a computer reservation system (CRS) that contains the itinerary for a passenger or a group of passengers travelling together)
  - Web intelligence
  - Across boarder intelligence
  - RFID luggage tracking
  - On-the-fly biometrics with biometrics corridor
  - …
- **Simulation tools** (iCrowd Simulator, Monte Carlo RBBCP Simulator)

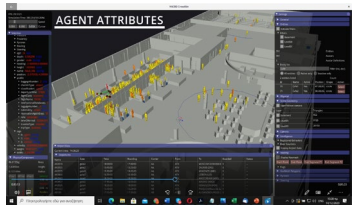
Simulation testing of RBS with iCrowd: A few words about the iCrowd Simulator

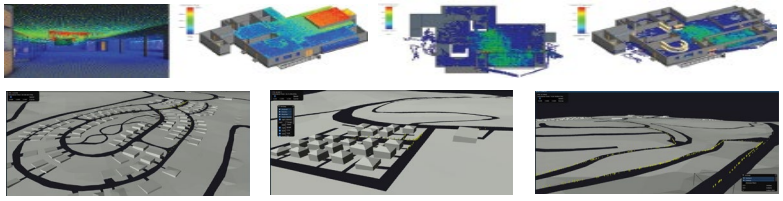
- **Agent-based simulator**
- **User-defined simulation scenarios**
- Sophisticated crowd engine and collision avoidance
- **Multiple and complex behavior models**
- **Distributed simulation**
  - Provides a cross-simulation platform
  - Enables coexistence of multiple engines and behavior models within the same simulation
  - Distributes the simulation load to several machines (neighborhood/buddy/combo simulation)
- **Simulation-as-a-Service (SaaS)**
- **KPI's monitoring and display**
- **Native** and photo-realistic **3D visualization of environment and agents**
- OCULUS C2I Portal Integration
- Integration with third-party simulators
- Anomaly detection for risk-based security performance evaluation
- Cyber-physical simulation







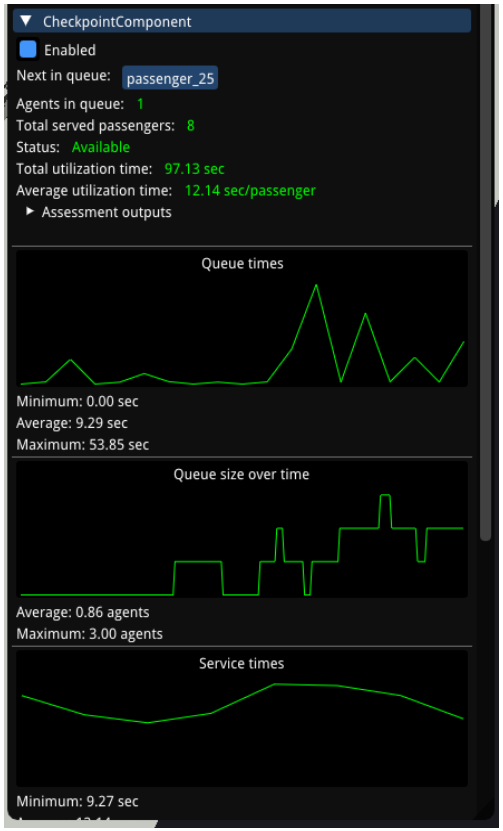


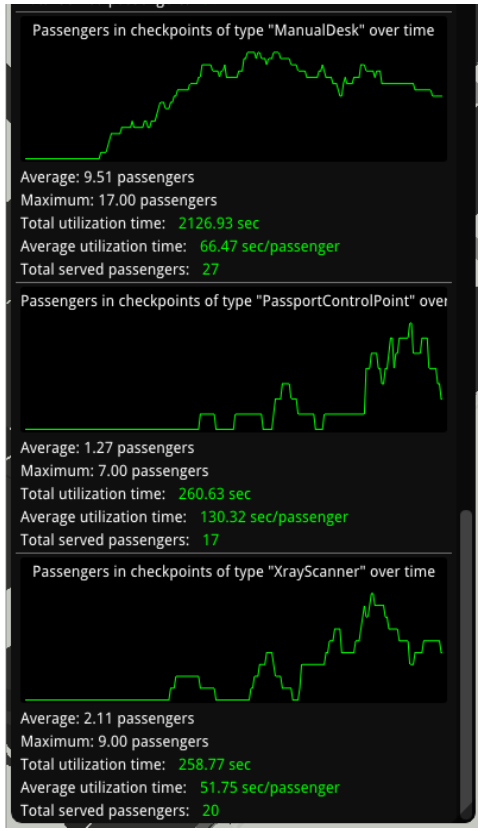


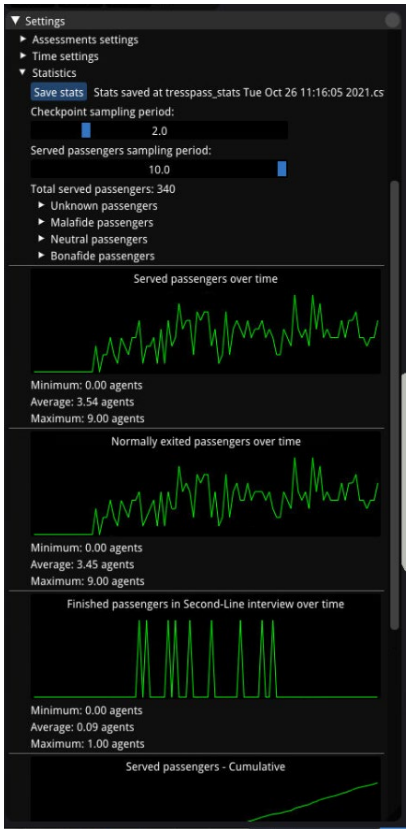
Use case applications of iCrowd in different domains

Graphical monitoring of KPI's

- A **wealth of graphical means** to **monitor KPI's on real time** and provide evaluation output results in the form of cvs files and graphs

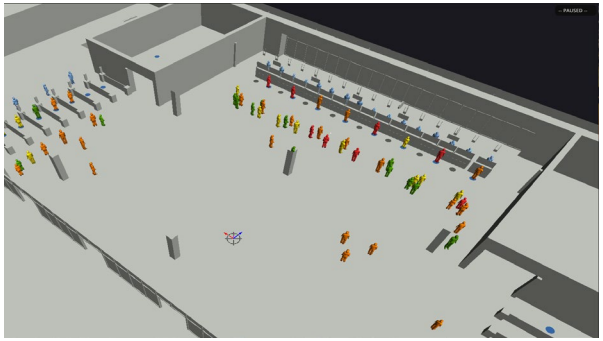
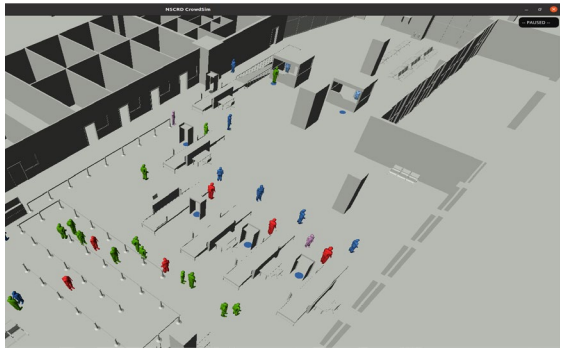
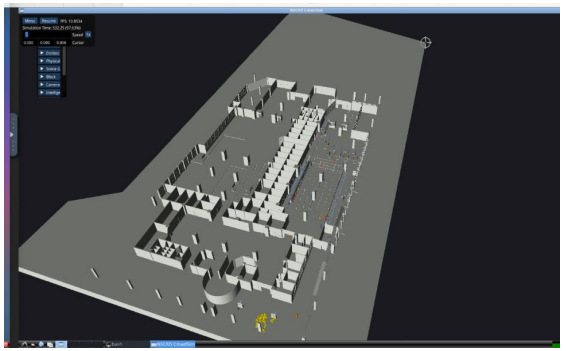






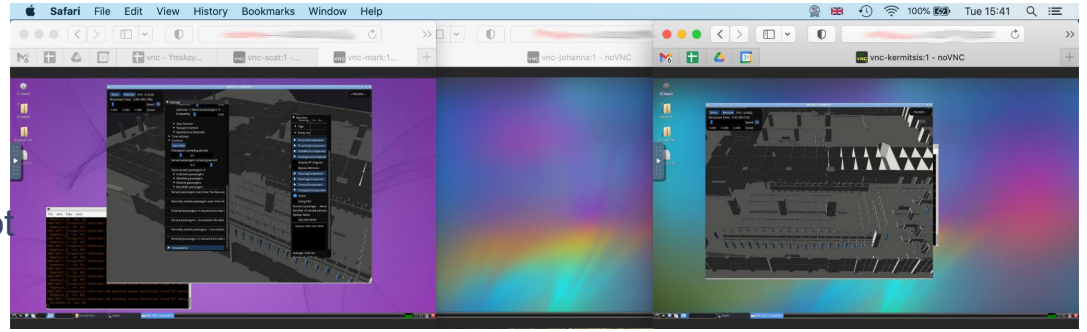
Simulation-as-a-Service (SaaS) capability

- Development of an instructional framework for training end users in understanding and operating RBS

- Development of the iCrowd **Simulation-as-a-Service** (SaaS) capability used to:

(a) train the TRS end user remotely using dockerized VMC's over secure VPN lines; and
(b) perform simulations of different pilot configurations on their own and obtain quantitative RBS performance results



iCrowd & OCULUS C²I: An Embedded Simulation & C²I System

iCrowd Simulator for risk-based strategies, algorithms, infrastructure, & technologies performance assessment

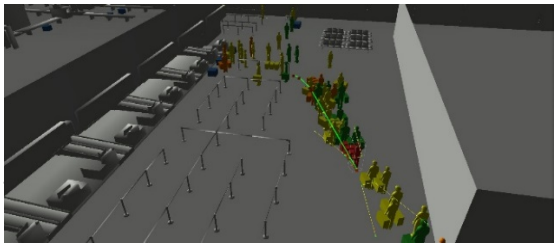
Questions to address via simulation

A. Comparison of Risk-based vs Rule-based security check strategies using iCrowd

- RBS vs RLBS efficiency in terms of travelers' throughput
- Waiting time (Delays) and Queue Length
- Travelers satisfaction
- Number of personnel needed for RBS vs RLBS for the same throughput
- Number of ABC gates needed (cost) to meet a given service level

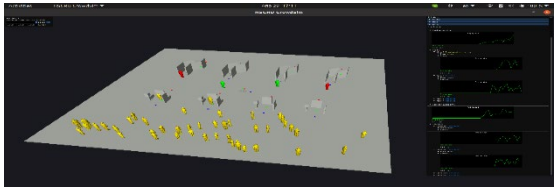
B. Anomaly (suspicious behavior) detection vs investment on camera infrastructure using iCrowd

- Anomaly detection AI algorithms and testing via simulation
- Robustness testing in noise and missing data using simulation
- Estimation of surveillance camera investment cost vs performance in anomaly detection
- Assessment of cost effectiveness of investment on surveillance and/or alerts' infrastructure vs performance

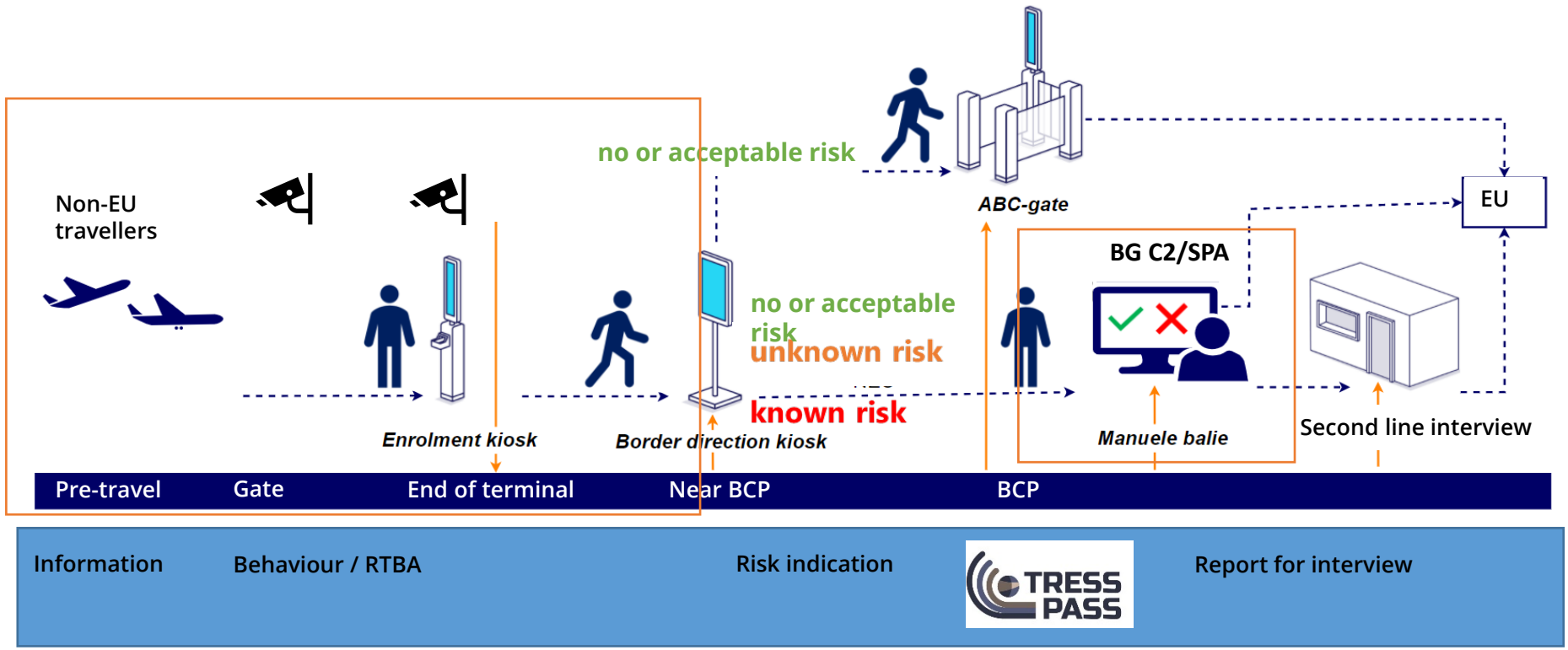


C. Biometrics corridor and biometrics on-the-go technology performance assessment using iCrowd

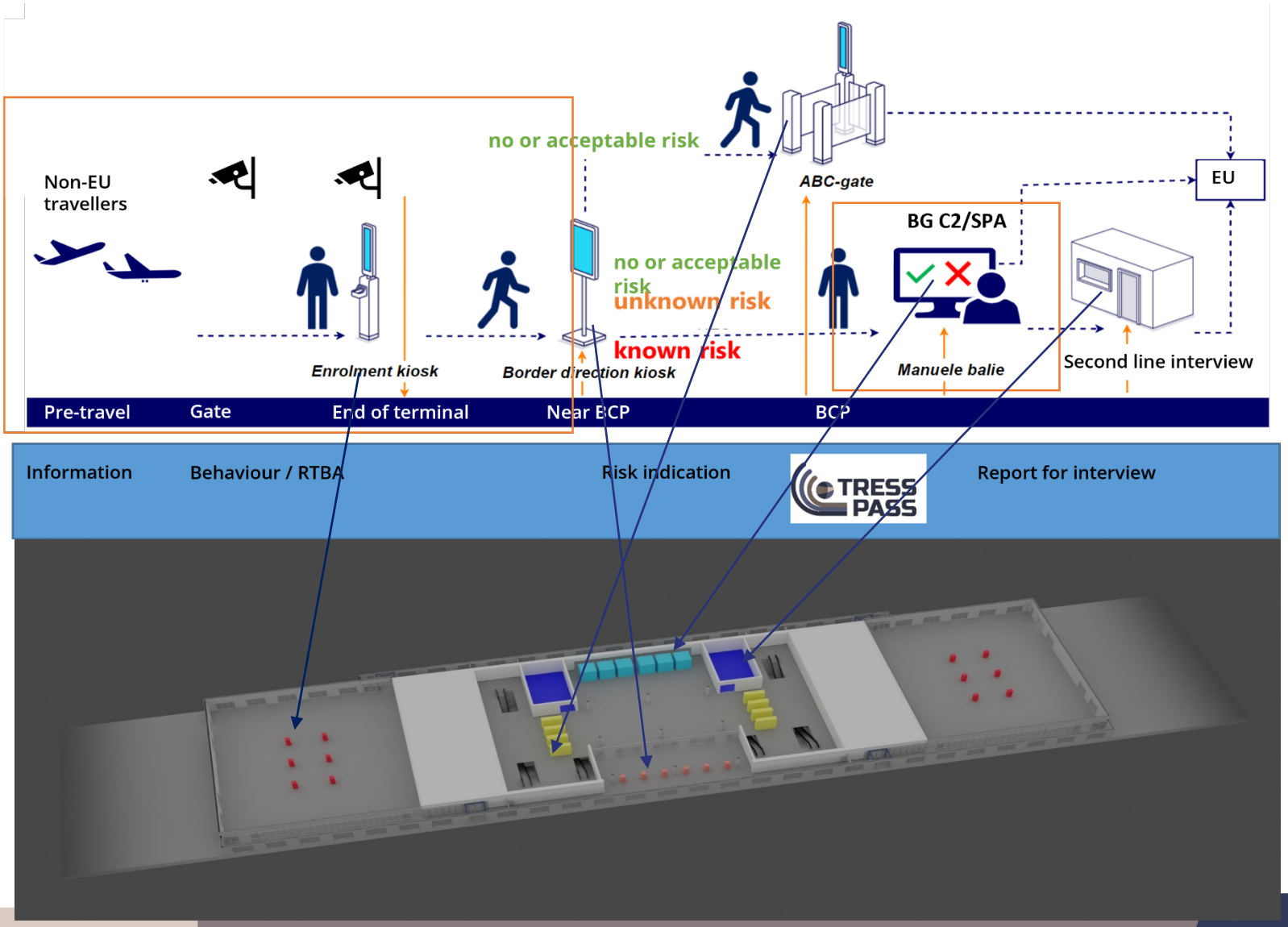
- Biometrics flow simulation and performance assessment
- Biometrics-on-the-fly logistics simulation and performance assessment
- Multi-biometrics corridor performance assessment for BCP on-the-fly traveler ID verification



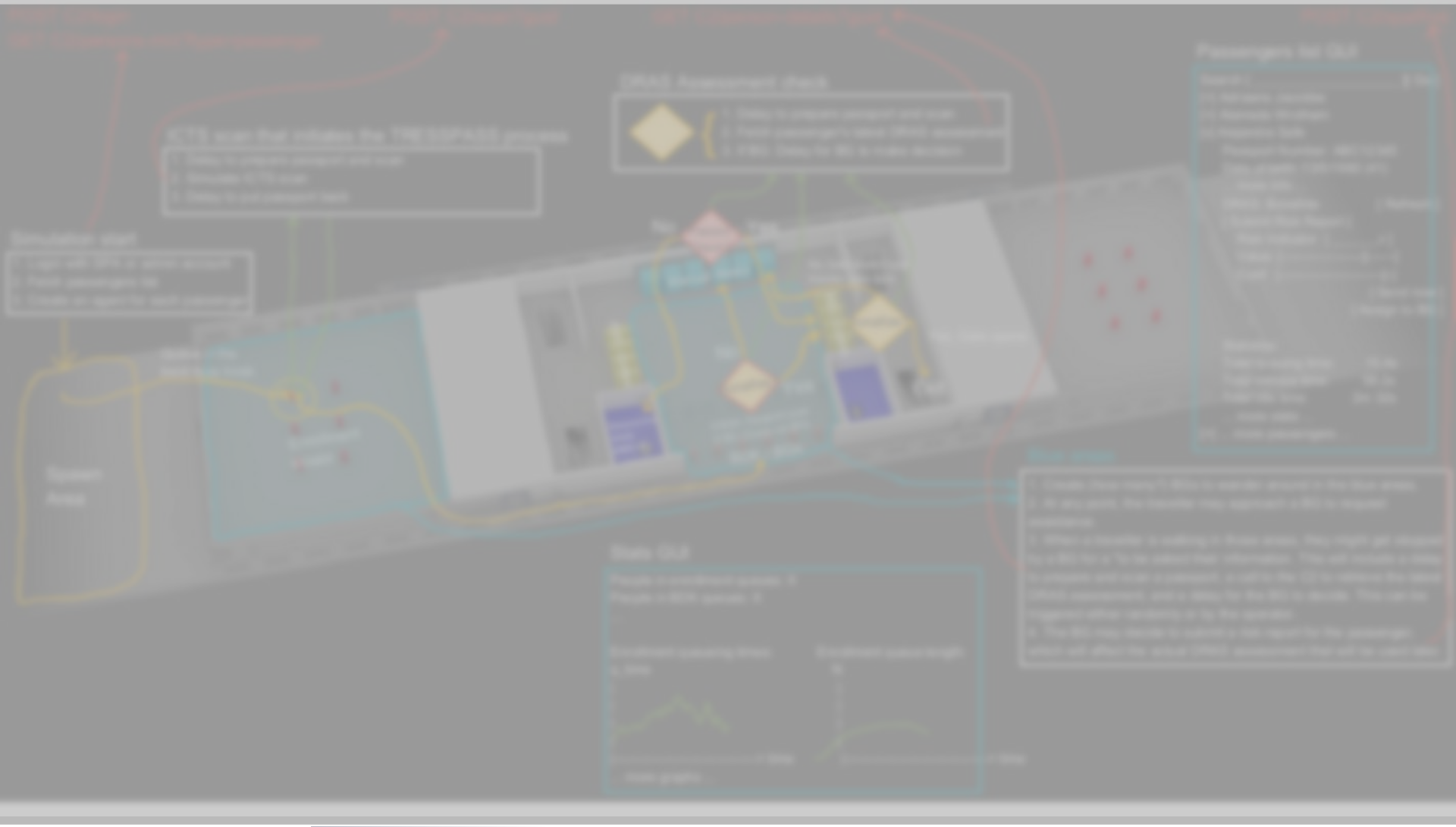
Risk-BS Simulation Scenario @ Airport Arrivals BCP



Airport Arrivals BCP Simulation Model for Risk-BS Logistics Assessment



Risk vs Rule BS simulation testbed configuration parameters setup

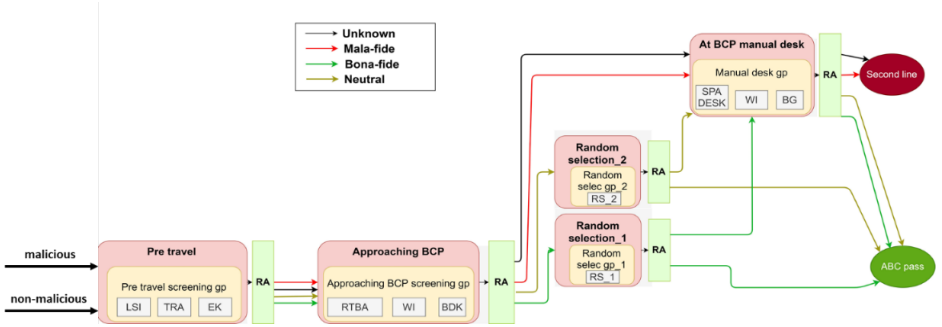


iCrowd parameters setup through native GUI or photo realistic GUI

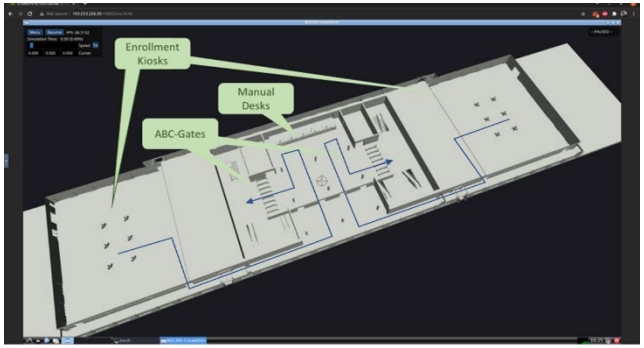
Simulation Parameters Definition

- Provided **detailed quantitative evaluation** of the performance of an RBS system using a wide spectrum of KPI's ranging from risk, service times, operational flows, labor estimates, cost analysis, …

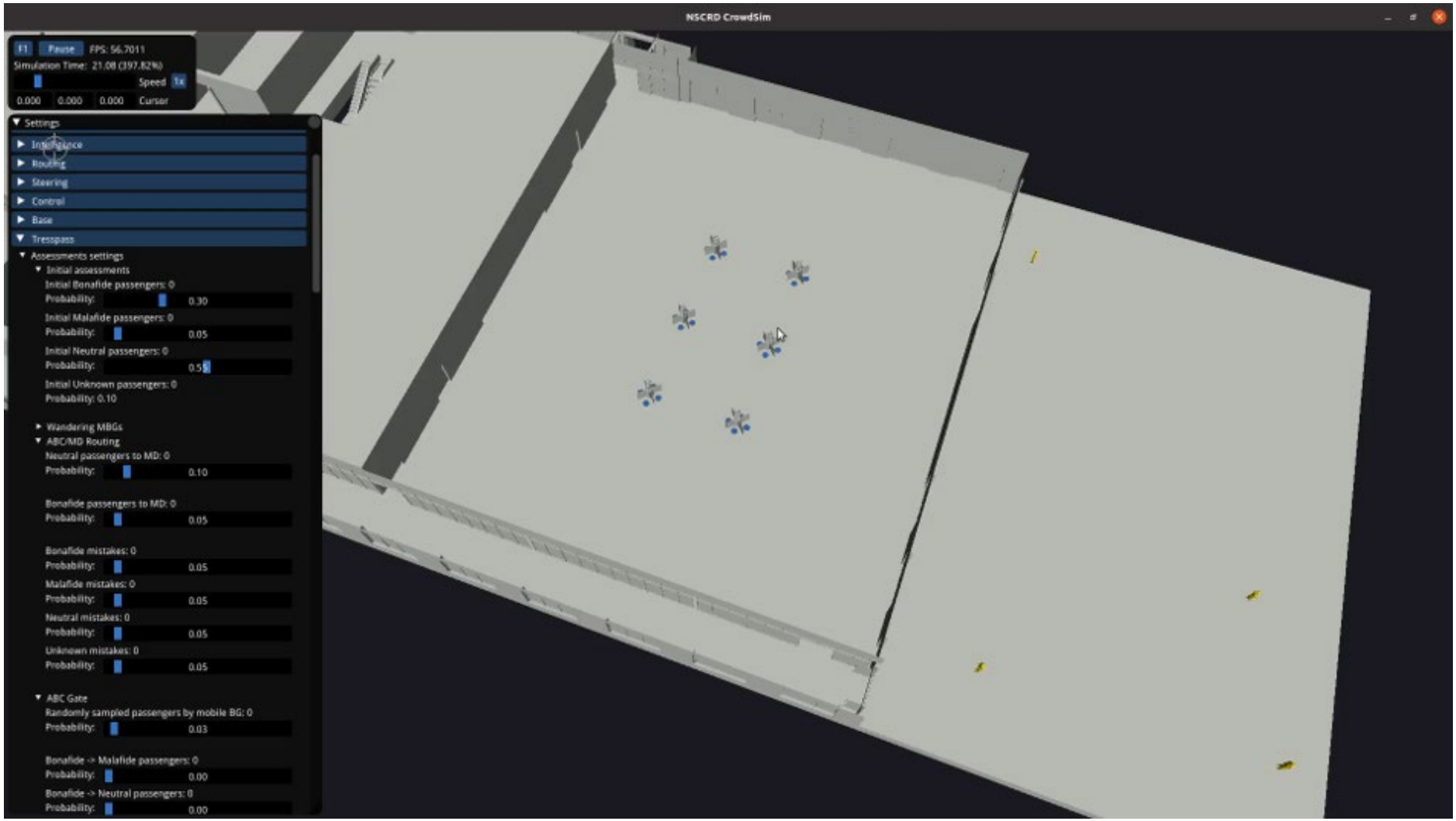
	Low performance	Medium performance	High performance
Bonafide	15%	40%	80%
Neutral	55%	45%	13%
Malafide	5%	5%	2%
Unknown	25%	10%	5%



Arrival rate per hour	Total number of travellers	EU/non-EU (tresspass)	EU (direct ABC gate)
Busy	1100	550	550
Regular	400	200	200
Quiet	120	60	60



Risk-BS vs Rule-BS iCrowd simulation: Airport Arrivals BCP testbed



Benchmarking Risk-based vs Rule-based Security for Airport BCP using iCrowd

- Allowed to compare the performance of *risk-based security* by benchmarking it **against** *rule-based security policies* at BCPs

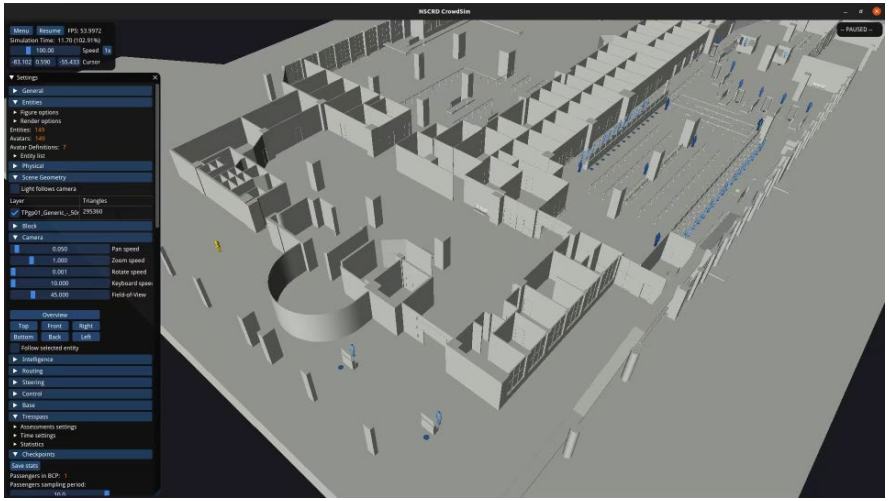
- **Performance Comparison**:
  - *Within allowing accumulating queues up to 100 per hour with fixed # of border guards*,

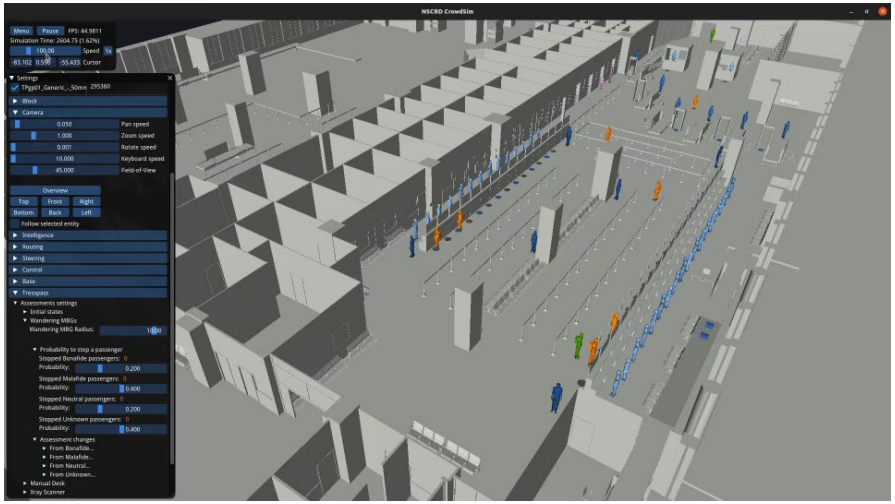
  ➔ **RBBM can handle 1 (LP) to 3 (HP) times higher flowrate than the current rule-based situation**.
  - *Without allowing any queues and varying the number of borderguards for that,*

  ➔ In case of a ***low performance system*** the **same number of borderguards are needed**, but

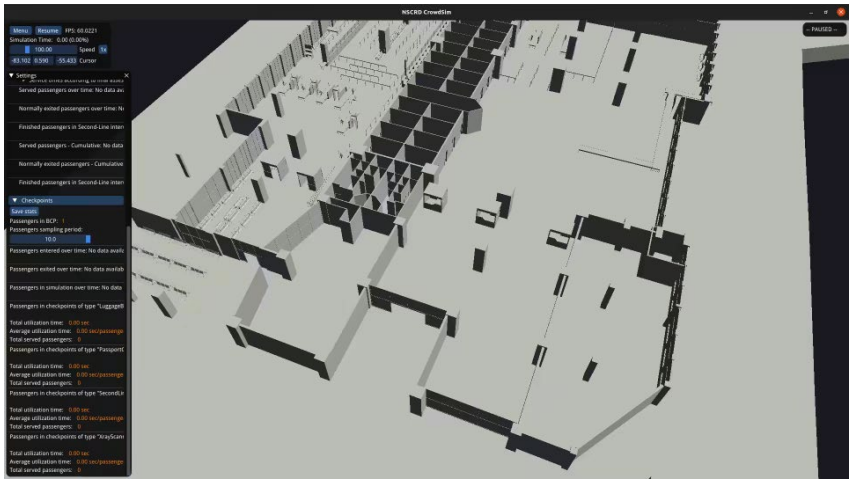
  ➔ **1/3** in case of a **high-performance system**

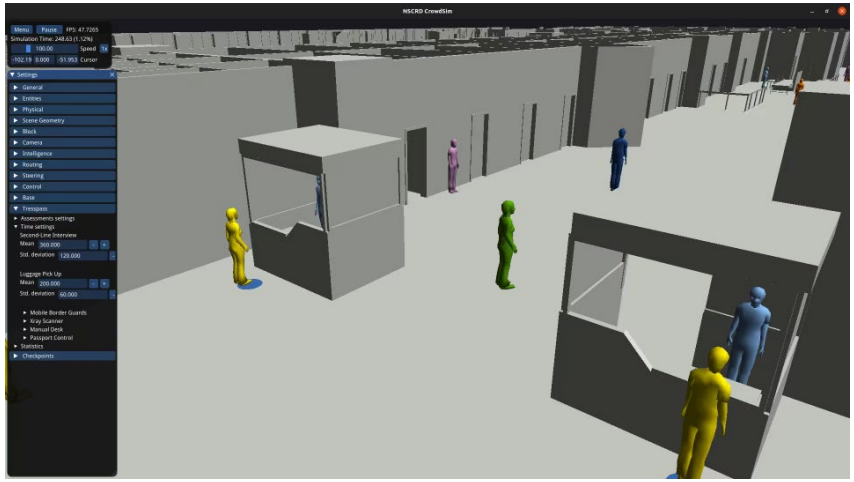
Risk-based Security Assessment at Sea Port BCP using iCrowd: Departures





Sea Port Greek Pilot using iCrowd Simulator: Arrivals Terminal



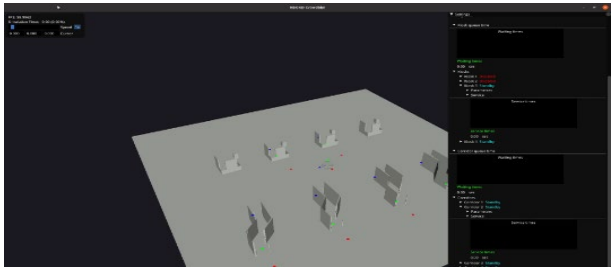


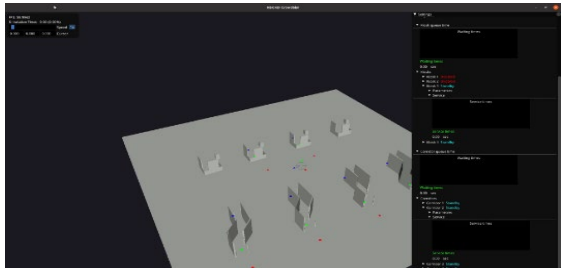
Seaport RBS BCP KPI's using iCrowd Simulator

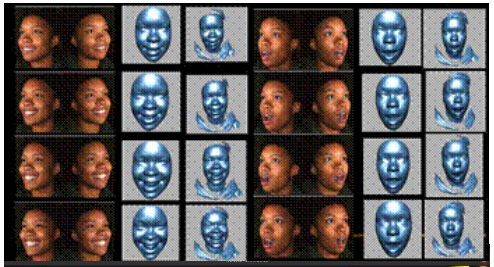
BCP PERFORMANCE INDICATORS

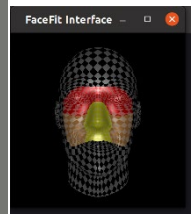
Indicators	Description
Effectiveness	Success-rate of stopping unauthorised travellers when they attempt to cross the border at the BCP
Flow-rate	Speed of the flow of travellers as they approach and cross the border at the BCP
Efficiency	Number of resources required at the BCP to achieve a certain degree of effectiveness and/or certain minimal flow-rate
Level of ethical compliance	Extent to which a BCP mitigates negative ethical impact on the travelling public and on the public in general

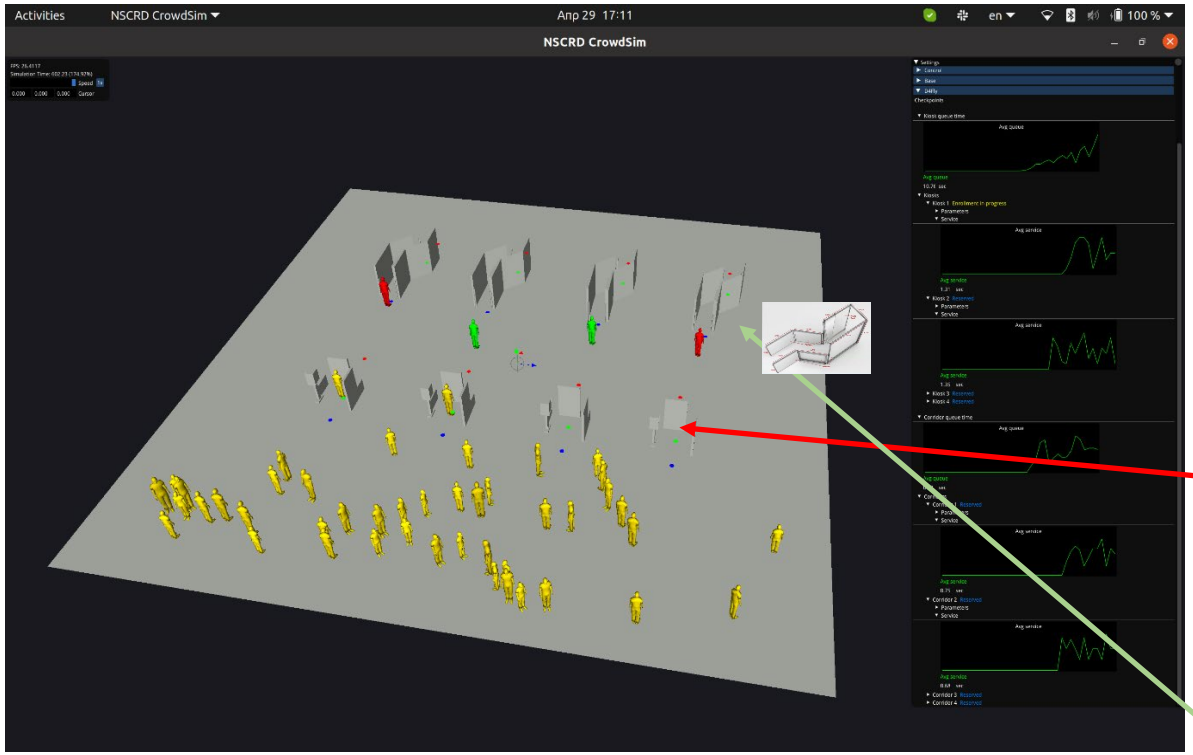
Biometrics flow simulation with iCrowd





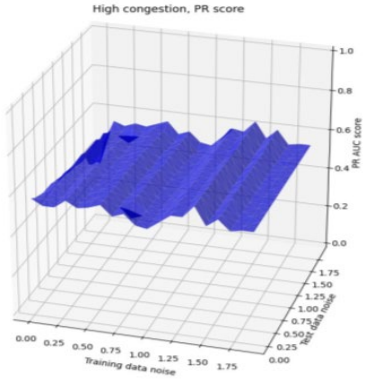


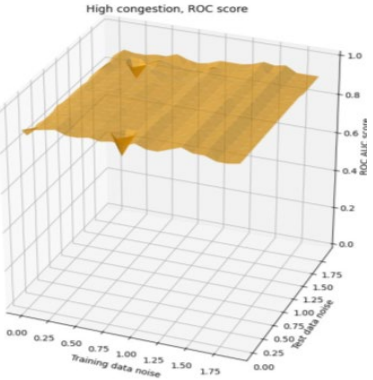


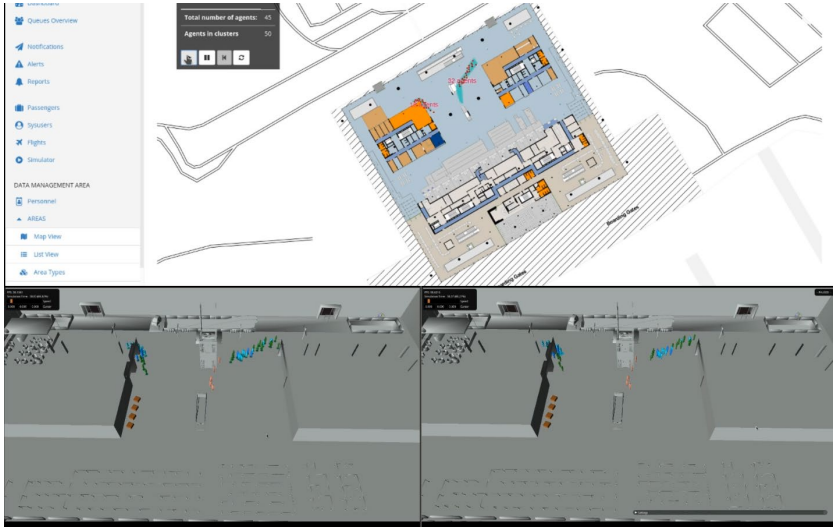


- 3D Faces from BU-3DFE db are associated with iCrowd agent mannequins
- **2-Stage Process**
- **Stage 1**: **Enrollment** & **Match** against criminal 3Df db
- **Enrollment**: Faces are “scanned” and converted to 3D face biometric templates
- **Matching**: Agent 3Df template matched against known criminal 3Df templates db
  - Negative id ➔ **Green**
  - Positive id ➔ **Red**
- **Stage 2**: Biometric corridor verification – functional and adaptable to the functional specs of each pilot.

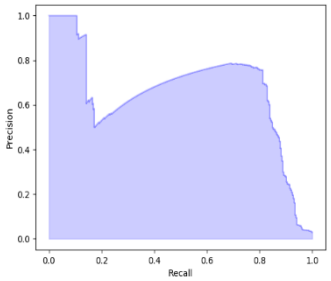
Anomaly detection using RNN and iCrowd



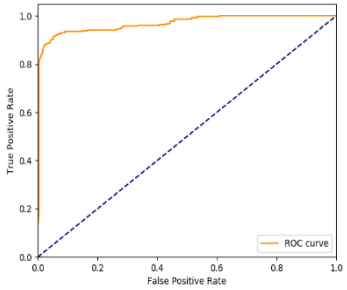




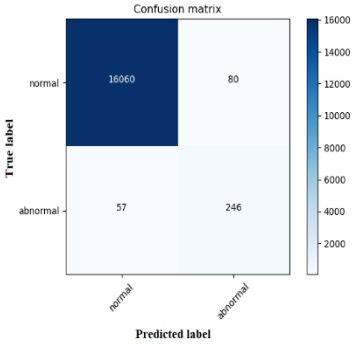
Training with high congestion data and different noise levels.
Testing with low-to-medium congestion data



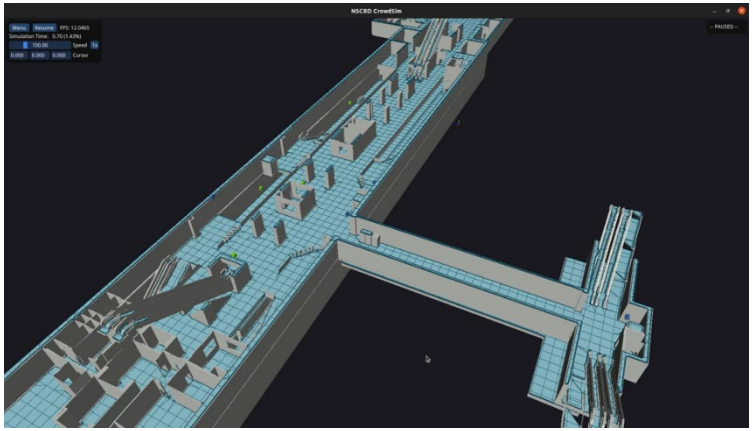
Precision-Recall Diagram



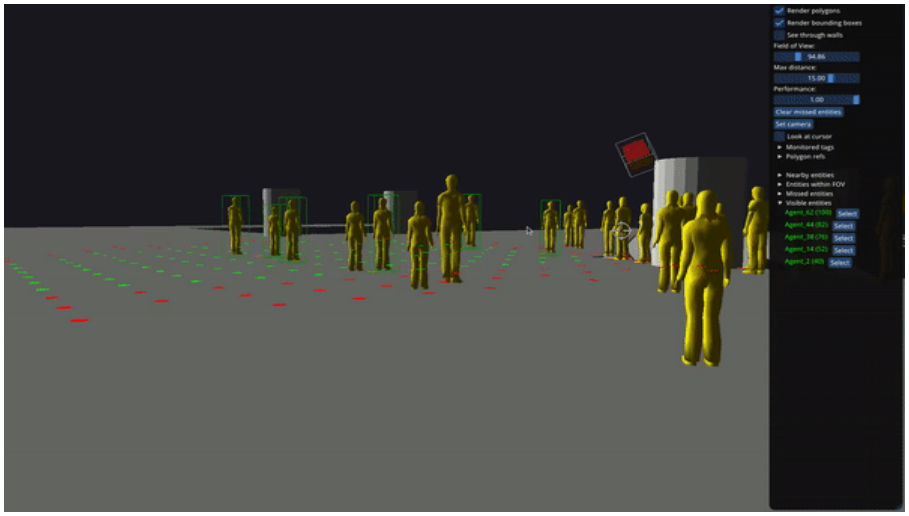
ROC Curve

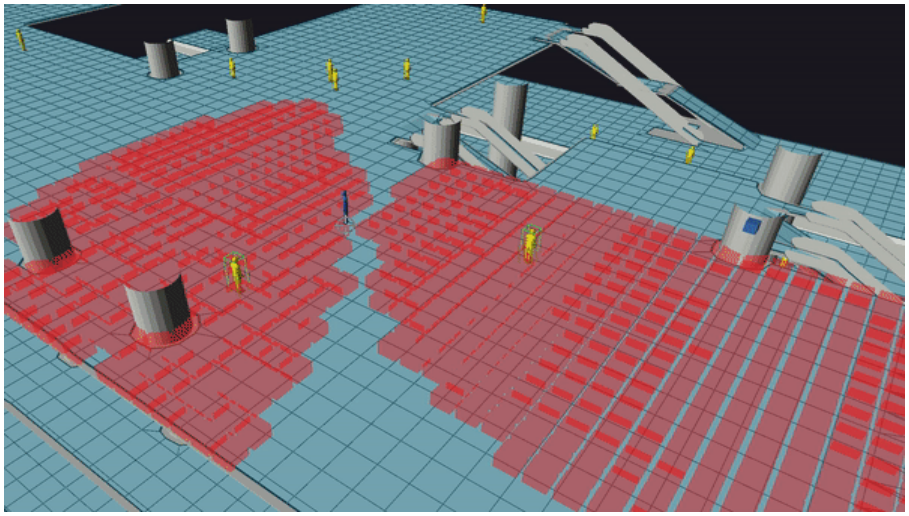


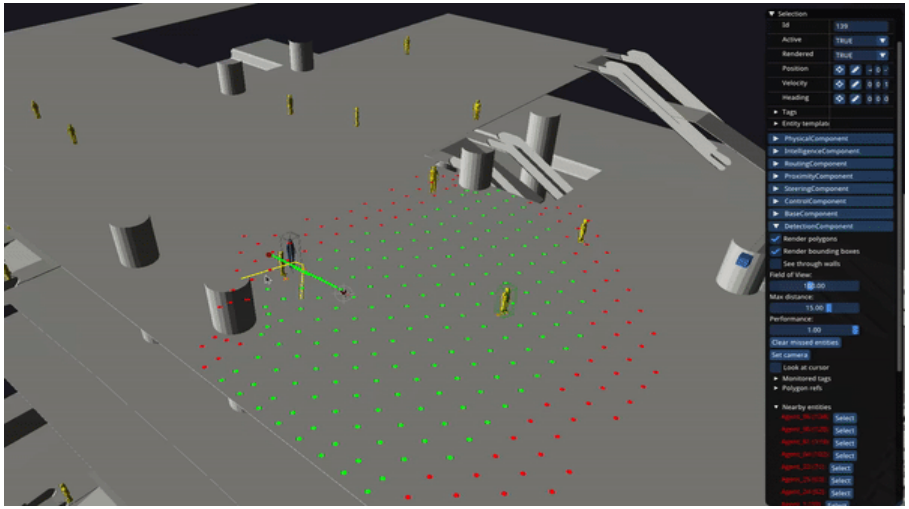
Confusion Matrix

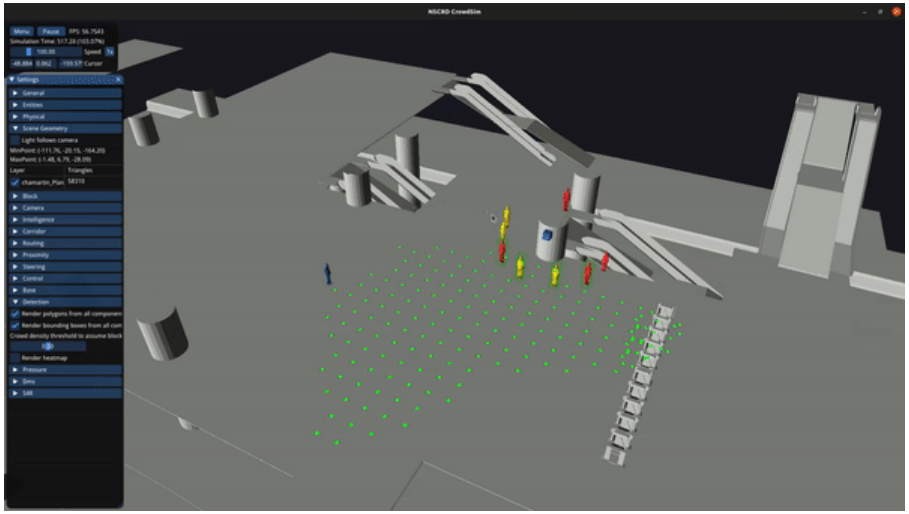


Assessing Surveillance Infrastructure Effectiveness and Cost Effectiveness with iCrowd Simulator









Conclusions

- Risk-based security (RBS) is a promising concept for providing security with convenience to passengers
- Risk Assessment is a complex process and should adhere to GDPR rules
- RBS can increase effectiveness but delay must be controlled as well
- Realistic testing is a challenging task and requires an integrated C2I and Simulation environment to test algorithms, protocols, procedures and technologies associated with risk assessment
- OCULUS C2I and the embedded iCrowd Simulator offer such a comprehensive implementation and testing environment for RBS
- Extensive simulation and field pilot tests used in TRESSPASS to test the risk assessment provided strongly supported evidence that RBS increases effectiveness and efficiency at security check points.
- A multi-biometrics corridor can be an effective means for on-the-fly ID testing
- A Robust anomaly detection RNN algorithm in conjunction with well designed and tested via simulation video surveillance system can detect suspicious behaviours and justify investment in video infrastructure & analytics.

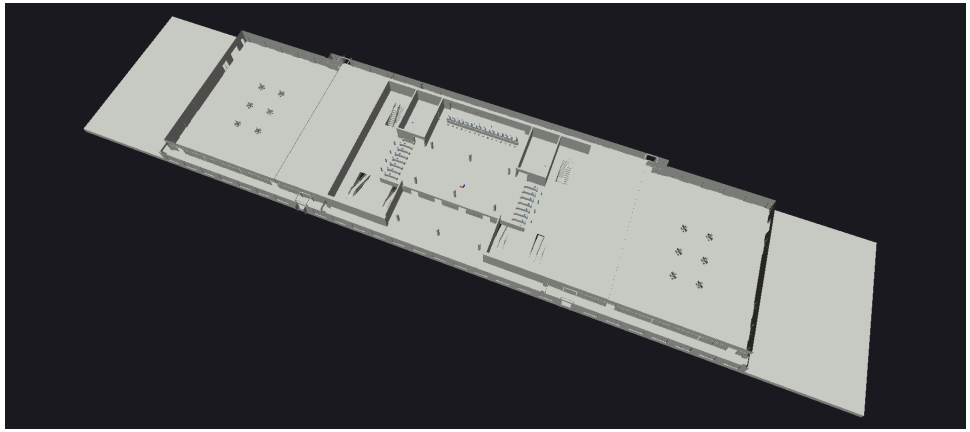
Contact information

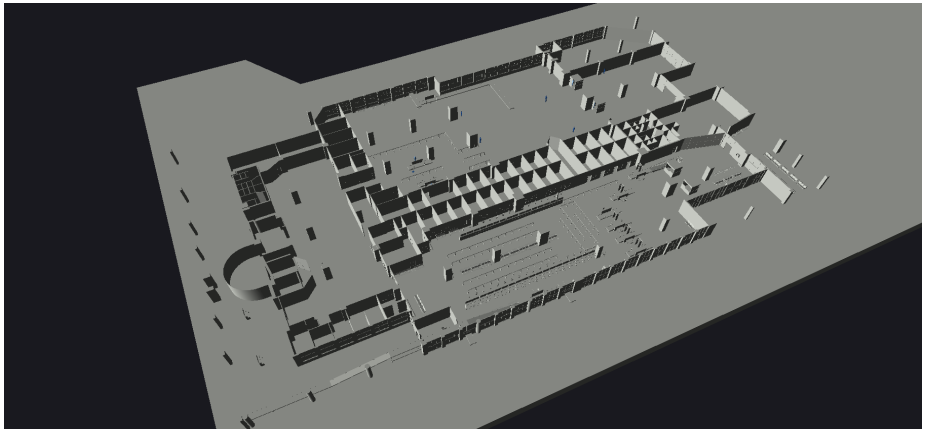
Dr. Stelios C. A. Thomopoulos
Director of Research & Head of Integrated Systems Laboratory
email: scat@iit.demokritos.gr

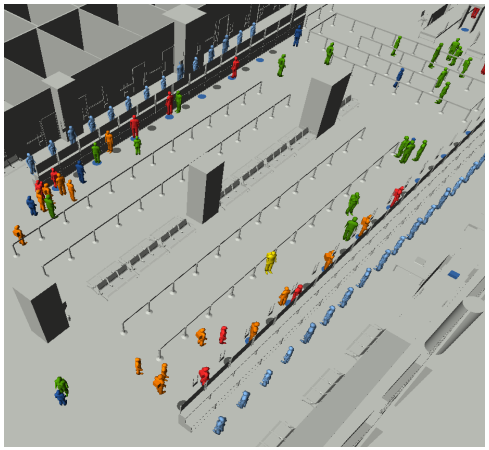
Integrated Systems Laboratory
http://isl.iit.demokritos.gr/
Institute of Informatics & Telecommunications
National Center for Scientific Research «Demokritos»
Patr. Gregoriou E' & Neapoleos 27, Aghia Paraskevi, Athens 15341, Greece
tel: +30 210 650 3155 – mob. +30 6944 986699
fax: +301-6532175

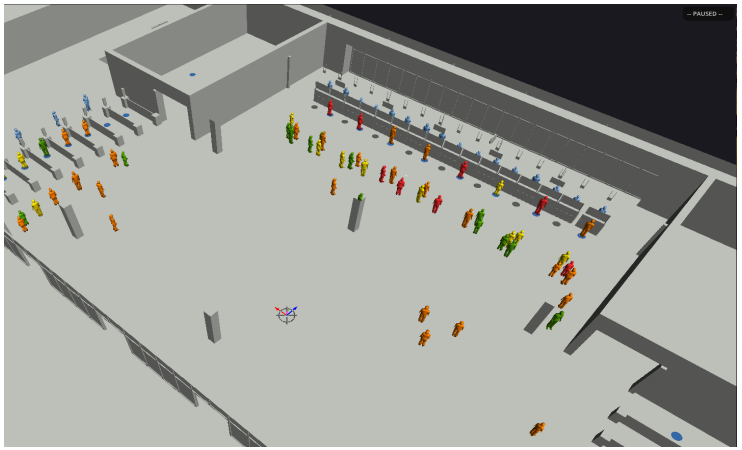
ISL video channel on vimeo:
https://vimeo.com/isldemokritos/videos/page:1

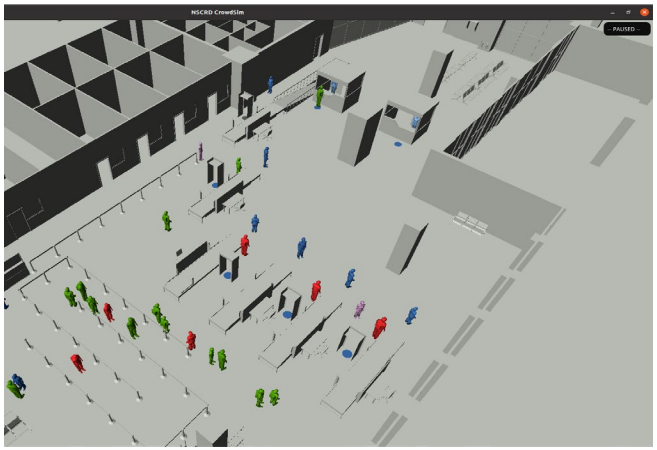
Development of detailed 3D models for iCrowd Simulations









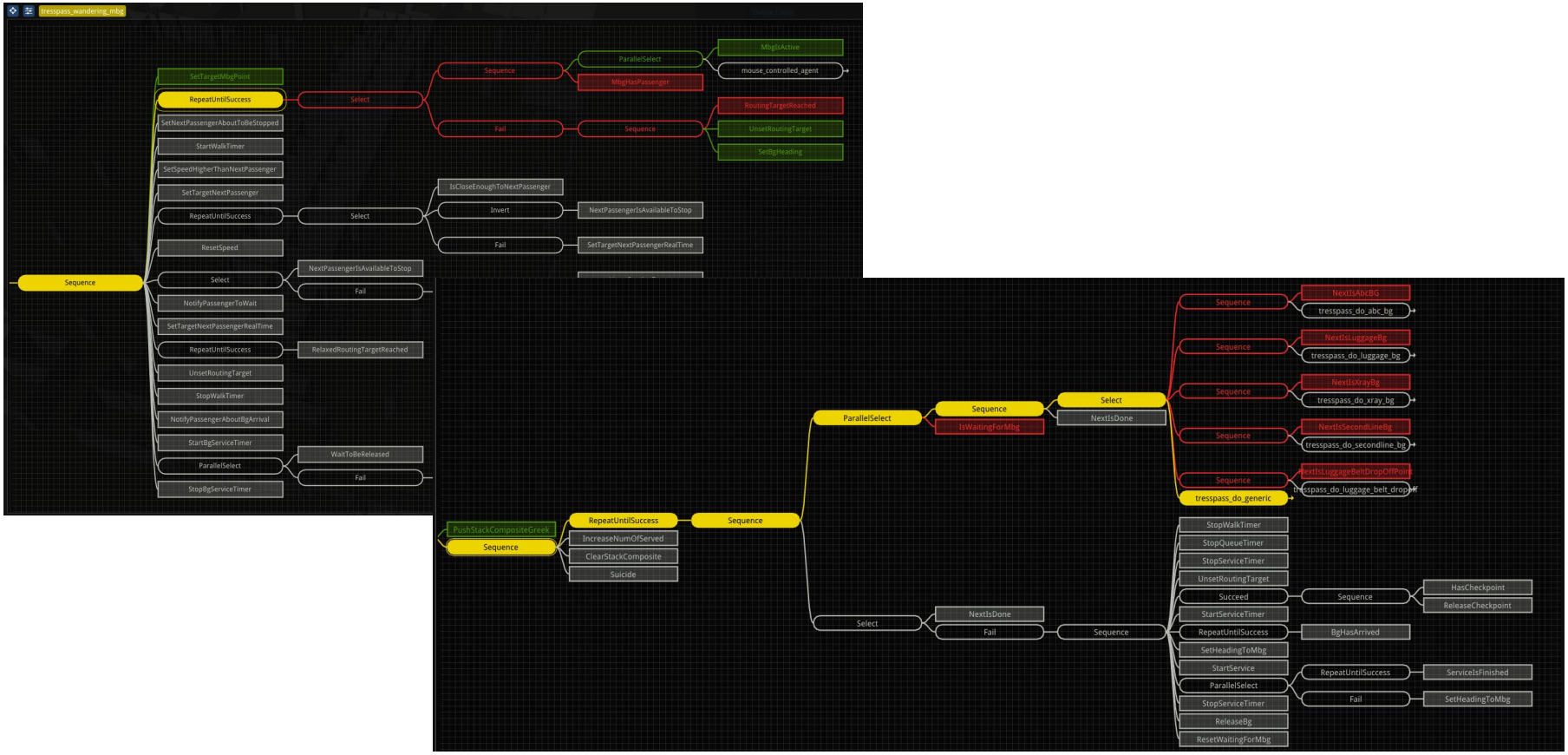


Integrated simulation environment

- Development of the integrated TRS Simulation Environment

iCrowd complex behavioral models

- Development of new and complex behavioral models of passengers and border guards in iCrowd Simulator



iCrowd Simulation-as-a-Service (SaaS)

Simulation Phase: iCrowd Simulation-as-a-Service (SaaS) Environment

- The end-users were given access to a VM prepared with their submitted configurations.
- Training was done remotely using the **TRS e-learning platform** that consisted of a teleconference platform for teaching and a secure VPN connection providing each end user trainee direct access to the iCrowd simulator on a separate and private VM under the supervision of the instructor/trainer.
- The end-users had the opportunity to execute **remotely & securely** their scenarios, adjust them and run them again, and extract the results in .csv files, until the results were acceptable.
- The end-user, as the operator of the simulator, can observe the execution of the simulation in real time, get metrics of the desired indicators, and manipulate checkpoints and agents.