D1.3 High-Level Scenarios

Document Submission Date: 08/07/2019

Work Package 1: End-user requirements and needs

Document Dissemination Level: Public

TRESSPASS - robusT Risk basEd Screening and alert System for Passengers and luggage
Funded by the Horizon H2020 Framework Programme of the European Union for Research and Innovation, Grant Agreement number: 787120

Abstract

Within the scope of TRESSPASS, a new so-called risk-based concept has been developed to perform security checks at border crossing points at Europe's external borders. This deliverable (D1.3) develops scenarios illustrating how future border management could take place according to the TRESSPASS concept. In order to lay the groundwork for the design of realistic scenarios, a gap analysis has been carried out identifying the key gaps between the current state of the art and possible future risk-based border control. A set of exploratory scenarios are presented here, highlighting how the TRESSPASS concept could be implemented at three different European Union border crossing points namely air, land and sea. For each border-crossing point, there is a focus on the range of threats considered most relevant.

Following an introductory chapter and a chapter articulating some key definitions associated with border control, Chapter 3 delivers a high-level border crossing point gap analysis. After some explanation of the key aspects of International Border Management, some of the more present day approaches to border control are considered such as rule-based and intelligence-based approaches. Some of the key developments and associated European Union projects concerning border control are highlighted before the introduction of a risk-based approach to border management. The lack of an integrated system of systems approach is identified as the key gap between the current state of the art and possible future risk-based border control. Many of the recent developments in border control have focused on either: limited threats; single modalities (i.e. either solely air, land or sea focused); or only on Tier 3 (Border Control) of the four Tier model as described in the European Commission's International Border Management Guidelines. This limitation in scope and the 'stove-pipe' nature of border control developments and enhancements invariably limit the potential to maximise the effectiveness as well as the efficiency of border control.

Chapters 4, 5 and 6 then take each of the air, land and sea border crossing points in turn and articulate a high-level scenario for each. After a short introduction, details are provided for traffic and travellers using the border crossing and the challenges that arise. Three vignettes for each border crossing type is then developed which details the emerging concept of operations and critically the threats that pertain to that border crossing. The current infrastructure of the crossing point is then discussed in order to frame the context of how border control is conducted in the present day. The infrastructure and processes ascribed here to each of the three border types is intended to provide an overview of the facilities and procedures that could be employed at a particular crossing. It is not the intention of this high-level report to replicate the full border control procedural detail. Detail regarding a potential approach to border control in a TRESSPASS context is then provided, including a brief assessment of the anticipated benefits that would arise from adopting such an approach. The final part of these chapters briefly introduces the concept of swim-lanes. To assist with understanding the passenger 'flow' through a particular border-type, the concept of 'swim-lanes' is being developed as part of TRESSPASS Work Package 6 (Operational Methods and Acceptability). This method will assist the development of a risk-based border management concept.

This reports concludes, in Chapter 7, with an initial visualisation of the land border TRESSPASS scenario. The visualisation here is in a series of screen shots from animations, developed with Unity software, to bring the land BCP threat scenario and TRESSPASS approach 'to life'. This visualisation is only at a preliminary stage and could be adapted and developed as necessary as the TRESSPASS project continues.

Project Information

Project Name	robusT Risk basEd Screening and alert System for PASSengers and luggage
Project Acronym	TRESSPASS
Project Coordinator	National Center for Scientific Research "Demokritos", EL
Project Funded by	European Commission
Under the Programme	Horizon 2020 Secure Societies
Call	H2020-SEC-2016-2017(SECURITY)
Topic	SEC-15-BES-2017"Risk-based screening at border crossing"
Funding Instrument	Innovation Action
Grant Agreement No.	787120

Document Information

Document reference	**D1.3**
Document Title	**High Level Scenarios**
Work Package reference	WP1
Delivery due date	M12
Actual submission date	8 July 19
Dissemination Level	PU
Author(s)	**Andy Howard - RINA**
Contributor(s)	**Manuele Barbieri– RINA. Plus input from: PBG; WAT; KEMEA; PPA; NUIM; CASRA; TNO; Z&P.**
Document Review Status	☒ Consortium ☒ WP leader ☒ Technical Manager ☒ Quality and Risk Manager ☐ Ethical Advisory Board ☐ Security Advisory Committee ☒ Project Coordinator

List of Acronyms and Abbreviations

ACRONYM	EXPLANATION
ANPR	Automatic Number Plate Recognition
API	Advance Passenger Information
BCP	Border Crossing Point
CCD	Diplomatic and Consular Corps
CD	*Corps Diplomatique* (Diplomatic Corps)
CH	(Country Code for) Switzerland
CONOPS	Concept of Operations
EC	European Commission
ECRIS	European Criminal Records Information System
ECRIS-TCN	European Criminal Records Information System – Third Country National
EEA	European Economic Area
EES	Entry-Exit System
eGates	Electronic (Passport) Gates
ESP	European Search Portal
ETIAS	European Travel Information and Authorisation System
EU	European Union
FLYSEC	Optimising time-to-FLY and enhancing airport SECurity
GDPR	General Data Protection Regulations
H2020	Horizon 2020
IBM	Integrated Border Management
iBorderCtrl	Intelligent Portable Control System
ID	Identification
IMO	International Maritime Organization
ISO	International Organization for Standardization
ISPS	International Ship and Port Facility Security (Code)
MS	Member States
PERSONA	Privacy, Ethical, Regulatory and SOcial, No-gate crossing-point solutions Acceptance
PNR	Passenger Name Record
RBBM	Risk-based Border Management
RNM	Royal Netherlands Marechaussee (Dutch Border Guard)
RTP	Registered Traveller Programme
SEABILLA	SEA Border surveiLLAnce
TCN	Third Country National

TEU	Twenty-foot Equivalent Units (cargo container)
TIEN	TRESSPASS Information Exchange Network
TRESSPASS	robusT Risk basEd Screening and alert System for PASSengers and luggage
WP	Work Package
XP-DITE	Accelerated Checkpoint Design Integration Test and Evaluation

Table of Contents

1 INTRODUCTION

1.1 Background

TRESSPASS Work Package (WP) 1 'End-user requirements and needs' animates the TRESSPASS user community to foster pro-active involvement of stakeholders following a user-centric approach in the TRESSPASS design. WP1 anticipates the current and future end-user needs and requirements for Borders/Customs authorities with respect to the development of a new risk-based border management concept. Within WP1, high-level scenarios will be developed illustrating the implementation of the TRESSPASS concept in the three pilots with three different crossing points (air, land, sea).

1.2 Aim of this document

The aim of T1.3 is defined in the TRESSPASS Grant Agreement [Reference 1]. The aim is to develop scenarios illustrating how future border management could take place according to the TRESSPASS concept. In order to lay the groundwork for the design of realistic scenarios, a gap analysis has been carried out which identifies the key gaps between the current state of the art and possible future risk-based border control. A set of exploratory scenarios are presented here, highlighting how the TRESSPASS concept could be implemented at three different EU border crossing points (BCPs) namely air, land and sea. For each border-crossing point, there is a focus on the range of threats considered most relevant. In WP8, the proposed scenarios will be further developed and consolidated into an integrated set of scenarios to be used during piloting activities in order to test the effectiveness of the TRESSPASS concept and solutions.

1.3 Inputs to this deliverable

The primary inputs taken into account for preparing this deliverable are as follows:

1.3.1 ***Task 1.1*** *End user requirements.*

1.3.2 ***Task 1.2*** *Developing a new risk-based border management concept**.***

1.3.3 ***Task 1.4*** *Legal and regulatory framework.*

1.3.4 ***Task 2.2*** *Inputs on Risk Indication.*

1.3.5 ***Task T6.1*** *{Draft} Operational observation studies for validating and support CONOPS definition.*

1.3.6 ***Task T8.1*** *{Draft} Planning and End User Training.*

It will be noted that some of the inputs, considered in the development of this deliverable, has been from other partners' preliminary planning for subsequent work packages most notably from WP8: Pilots.

1.4 Anticipated output (dependencies)

Given the fundamental importance of the high-level scenarios to the overall project, it is anticipated that all subsequent WP (2 – 11) will draw upon this deliverable to a lesser or greater extent. However, the WP that have the greatest dependencies on this deliverable are anticipated to be:

1.4.1 ***WP2*** *Risk based border crossing points.*

1.4.2 ***WP3*** *Sensors & Information gathering.*

1.4.3 ***WP5*** *Dynamic Risk Assessment and Alert System.*

1.4.4 ***WP6*** *Operational Methods and Acceptability.*

1.4.5 ***WP7*** *Simulation, Evaluation and Training Tools.*

1.4.6 ***WP8*** *Pilots.*

2 DEFINITIONS

2.1 Establishing a Base Line

In developing these high level scenarios, it is critical to have a common understanding of terms (and the scope of those terms) used. In particular, it is necessary to define what exactly is meant by the terms: BCP, Concept of Operations (CONOPS), 'scenario', 'vignette' and 'use case'; it is vital that there is a common understanding of terms. It should also be recognized that this deliverable describes the TRESSPASS scenarios in 'high-level' terms. Clearly, as the project progresses, the detail pertaining to each of the three scenarios will increase. In addition, as the project develops and the TRESSPASS concept (along with its constituent elements) matures, so the scenarios for the three BCP types may also be refined and further developed.

2.2 Source of Definitions

The definition of 'border' is taken from EU Guidelines for Integrated Border Management [Reference 2] and the definition of CONOPS is taken from the draft of Deliverable 6.1 to the TRESSPASS project. To maintain consistency with other EU-funded (and border-related projects), the high level definitions for the key terms 'scenario', 'vignette' and 'use case' have used the 2010 SEABILLA project on Sea Border Surveillance [Reference 3] as a starting reference point. These form a hierarchy of terms from which elements of one can be derived (in a hierarchical context) from another.

2.3 Border Crossing Point (BCP)

A BCP is described as:

'any crossing point at land, sea, river, lake or air borders, authorised by the competent authorities for crossing a state border'.[1]

In total there are approximately 1,800 BCPs at EUs external borders of the Schengen area.[2]In fact there exist three types of BCPs: land BCPs, seaports and international airports.

2.4 CONOPS

A CONOPS is not a detailed user-requirements document but functions as a high-level description of the proposed end-state which helps to guide the technology development and implementation process. It is not a static representation of the ultimate state of the system as it can reciprocally change as the development process requires based on user-requirements changes or technical limitations but nonetheless provides a conceptual reference for the direction of the technological development. The TRESSPASS approach to CONOPS places particular emphasis on the needs of end-users and the operational realities of their working

[1] European Commission: Guidelines for Integrated Border Management in European Commission External Cooperation, November 2010.

[2]Quoted in Deliverable 1.2 (D1.2 Conceptual Model) from the presentation on smart borders by Anna Herrera de la Casa (DG Home, Unit C3 – TransEuropean Networks for Freedom and Security & relations with eu-LISA), Madrid, 25 June 2014.

environment. It advocates for a process of iterative system development and close consultation with end-users and system stakeholders. A CONOPS therefore is used to support the process of system development or system change. It provides a consensus document that communicates the vision for change from the current system to the prospective system to all system actors and stakeholders.

2.5 Scenario

A scenario is:

'*a generic description of an operational mission in a given context*'.[3]

In the context of TRESSPASS, this consists of a description of the geographical area of the BCP including environmental condition, operational theatres, actors, and security threats.

2.6 Vignette

A vignette is:

'*a specific narrative of a particular materialisation of a scenario, where time, actors, weather, etc. are determined and when the actors behave as expected from the current modes of operation and available capabilities'*.[4]

Vignettes do not consider the potential benefit of future capabilities. By their nature, numerous vignettes can be derived from any one particular scenario. In each of the three BCP types described in this paper, an indication of the type of threats pertaining to the border type is given. A threat, in the context of border control, can be defined as:

'*a force or pressure acting on the external borders*'.[5]

However, more specifically, a threat:

'is anything that leads to a violation or disruption of the border control regime or has a potential negative impact either directly or indirectly'.[6]

With respect to border control, these threats can be external or internal. For example, in the case of the air border (Schiphol Airport) described in Chapter 4, the top two threats identified are one external (the use of counterfeited documents by imposters) and one internal (the lack of skilled/experienced border staff).The issue of threats are discussed in more detail in Deliverable 1.2.[7] Related to threats, are risks, with a risk described as:

[3] SEABILLA Project: Sea Border Surveillance, Seventh Framework Programme, Theme 10 – Security, Deliverable Number D11.1, Analysis of maritime surveillance scenarios, gaps and enhancement requirements, page 6/45, dated 28/10/2010.

[4] Ibid.

[5] Frontex. (2012) 'Common Integrated Risk Analysis Model a comprehensive update (version 2.0)'. Reference 4.

[6] European Commission: Guidelines for Integrated Border Management in European Commission External Cooperation, November 2010. Page 91.

[7] TRESSPASS Deliverable 1.2 Conceptual Model. 03/04/2019.

'the likelihood or probability of that threat being realised'.[8]

The level of risk is always determined in the context of the national and international priorities set for the relevant border management agencies.

2.7 Use case

A use case is:

'a projection of the capabilities possibly developed in the future to alter the course of a vignette'.[9]

Use cases will reflect assumptions on the project developments and expected performance, and will result from an iterative work between the 'technologists' and the 'operators'. The use cases descriptions are essential to guiding the improvement requirement. As with the relationship between scenarios and vignettes, numerous use cases can be derived from a vignette. They should preferably consider a graduated technological and operational complexity and draw upon associated cost benefit analysis in order to set priorities.

2.8 TRESSPASS High-Level Scenarios

In the context of the TRESSPASS project, three scenarios will be developed (land, sea, air). For the purposes of this deliverable, these will remain at a high-level and will focus on the generic threats to each type of BCP, drawing from the analysis undertaken as part of: T1.1 *End-user requirements*; and T1.2 *Developing a new risk-based border management concept*. These high-level scenarios introduce a basic series of three vignettes for each BCP type. These vignettes outline the CONOPS work (being undertaken as part of TRESPASS WP6) for each BCP type as well as identify broad groups of actors against a specific threat.

It will be noted that the vignette's outlined in this report (for air, land and sea) describe different possible cases for both arrival (inbound) and departure cases (outbound). Different checks may apply in each case as well as other different checks that may be applicable depending on the destination or on the country of origin (i.e. where passengers come from, e.g. a Schengen or Non-Schengen country). As such, the infrastructure and processes ascribed here to each of the three BCP types is intended to provide an overview of the facilities and procedures that *could* be employed at the particular BCP. It is not the intention of this high-level report to replicate the full border control procedural detail (as applicable to each of the BCP vignettes) which will be described fully in WP8: TRESSPASS Pilots.

The high-level scenarios presented here do not introduce detailed use cases. Such use cases will be the preserve of later elements of the TRESSPASS Project. However, for each of the three BCP types a potential TRESSPASS approach is described with some of the key processes and techniques that could be applied at the particular border crossing. This includes an articulation of some of the anticipated benefits that TRESSPASS could deliver.

2.9 TRESSPASS Pilots

As part of WP8, different use case scenarios will be defined to test and validate the TRESSPASS technology in the different trial configurations, with the aim to provide validated

[8] European Commission: Guidelines for Integrated Border Management in European Commission External Cooperation, November 2010. Page 91.

[9] Ibid.

configurations for the pilots' execution. A detailed plan will be developed for each of the three pilot demonstrations, which will take place in Netherlands, Poland and Greece covering the three use case scenarios air, land and sea respectively. The Border Guards and Customs Staff in all three pilot sites will need to be trained to become accustomed to any new technology introduced as part of the TRESSPASS project. Appropriate training material will be developed and delivered in preparation for the pilot demonstrations. This training material will build upon the simulations developed in individual and system tests performed as part of WP7 (Simulation, Evaluation and Training Tools). The broad objectives of the TRESSPASS pilots are:

- To test the TRESSPASS risked based screening technology under a variety of different environments, conditions and procedures in order to cover as many as possible use case scenarios and travelling types which vary from one country's BCPs to the other;
- To establish shared and effective demonstration procedures with the appropriate end user training and guidelines, taking into account interoperability with legacy systems and between the competent authorities that will use the system;
- To validate the performance and functionality of the total system and to collect and organise the evaluation feedback from the end-users, in order to report the lessons learnt identifying strengths, weaknesses and refinement suggestions for TRESSPASS.

2.10 Visualisation of TRESSPASS Scenarios

Chapter 7 of this report presents a series of screen shots from an animation developed to illustrate the application of the TRESSPASS concepts at the land BCP. It illustratively combines the three threats considered to be the most significant at the land BCP. This visualisation does not, however, represent the pilot process. This visualisation is preliminary in nature and may be developed, as necessary, through the TRESSPASS project (including the potential development of one for each of the air and sea BCPs).

3 HIGH-LEVEL BCP GAP ANALYSIS

3.1 International Guidelines for Border Management

The European *Guidelines for Integrated Border Management* [10]*(IBM)* describes a four-tier access control model; a set of complementary measures to be implemented, based on the need for both inter-agency and international cooperation. The four tiers are: Tier 1 – Measures in Third Countries; Tier 2 – Cooperation with Neighbouring Countries; Tier 3 – Border Control (at the external border); and Tier 4 – Control Measures within the Area of Free Movement. With respect to the TRESSPASS project, all four tiers are in scope. However, with respect to the descriptions of the three BCP types (provided in Chapters 4 to 6), the focus is primarily on Tier 3 Border Control, which:

> *'guarantees systematic border checks for every person entering or exiting the Schengen area…it also ensures an adequate level for exposing illegal border crossings in areas between border crossing points or via sea, using false documents or hiding inside various modes of transport…border control is part of national crime prevention, as it detects and reveals human smuggling, stolen property and other cross-border and border-related crimes as well as contributing to the detection of serious crime.'*[11]

3.2 Border Management Objectives

According to the IBM Guidelines, border management must meet three objectives[12], which are equally indispensable and fully compatible with each other. These objectives are:

- Protection of internal security and management of migration flows to prevent irregular migration, related crime and other cross-border crime;
- Smooth and fast border crossings for the vast majority of travellers who do meet the conditions laid down in relevant Regulations; and
- Full respect of fundamental rights, including treating each individual with full respect for human dignity and allowing access to international protection to those in need thereof.

3.3 Data Protection

Whilst not an objective of border management in its own right, data protection nonetheless forms a fundamental consideration in this arena. The IBM Guidelines highlight that issues of personal data protection arise at all levels of border management where a balance between the human right for privacy and the use of personal data or databases to fight crime and related unlawful activities needs to be found. Natural persons have the right to legal protection of their personal data. Consequently the use, allocation, sharing and storage of personal data have to be regulated by national data protection laws.[13]In addition to the

[10] European Commission: *Guidelines for Integrated Border Management in European Commission External Cooperation*, November 2010.

[11]Ibid. Page 21.

[12]Ibid. Page 20.

[13]Ibid. Page 96.

national law on data protection, the laws regulating the tasks of the border management agencies should identify the following:

- The types of data that the agency may collect;
- The purpose for which data might be used;
- The accuracy and up-to-date nature of the data;
- The time limits for the erasure of personal data;
- Rules regarding how data may be forwarded to a third party (both internally and internationally);
- Access to data by other authorities; and
- Any specific rules concerning law enforcement issues on data processing, which differ from the general data protection regulations.

3.4 Present Day Border Control – Rule-based Decision Making

In implementing border control, BCPs can be categorised – in a general manner – as making decisions on passengers transiting the border according to a series of rules. Initially, an individual attempting to cross a border is subject to a minimum identification check which will also:

- Verify that the individual has valid travel documentation;
- Cross-check the individual against an issued 'watch list'; and
- For Third Country Nationals (TCNs) additional checks may be carried out. This will depend on the specific border being crossed and will vary from country to country.

Closer inspections may then be carried out on individuals; such inspections could be targeted, random or unexpected in nature. It is the physical nature of the checking / inspection process which will begin to introduce delays at BCPs. The greater the level of inspection, the greater the impact to the 'flow' of personnel through a BCP. The flow-rate is the average speed of travellers when they cross the border at the BCP. It is, of course, the volume of people transiting BCPs which possesses the greatest challenge to flow-rates, especially through the air and sea BCPs.

As indicated in Chapter 4 below, Schiphol Airport – as but one example of an EU BCP – dealt with more than 70 million passengers (including those in transit) in 2018. At 67 million and 65 million seaborne passengers, respectively, Italian and Greek ports handled a combined share of more than 33% of the total number of passengers embarking and disembarking in EU ports in 2016. Denmark was third in this list with recording nearly 42 million passengers in the same year.[14]

3.5 Present Day Border Control – Intelligence-based Decision Making

Rule-based decision making is often enhanced by intelligence-based decision making (an approach adopted at many air or sea BCPs, for instance). This introduces the collection and screening of passenger data before these individuals present at the BCP. With respect to EU air BCPs, for instance, carriers must transmit information concerning the passengers they will

[14] Source: *Eurostat statistics explained: Maritime ports, freight and passenger statistics. Ec.europa.eu.* (Reference 5) Care must be exercised with these figures since most EU seaborne passenger transport is within national borders. However, with cruise passengers making up over 3% of the total number of passengers embarking and disembarking in EU ports (estimated at more than 200 million passengers), the scale is nonetheless significant.

carry to an authorised BCP, and through which these persons will enter the territory of a Member State (MS).With respect to sea BCPs, the submission of International Maritime Organization (IMO) crew-passenger lists is required. Carriers which, as a result of fault, have not transmitted data or have transmitted incomplete or false data are subject to sanctions or even confiscation of the means of transport, temporary suspension or withdrawal of the operating licence. The information submitted by the carriers to border control agencies comprises:

- Number and type of travel document used;
- Nationality
- Full names;
- Date of birth;
- BCP of entry into the territory of the EU;
- Code of transport;
- Departure and arrival time of the transportation;
- Total number of passengers carried on that transport; and
- The initial point of embarkation.

Deploying intelligence-based decision making will therefore increase the ability for agencies to undertake targeted checks, based on the information received and analysed prior to arrival at the BCP. Due to increasing air traffic and enhanced security checks, however, the processing of such information can cause significant delays – this, of course, runs counter to the overall goal to minimise delays at borders. In order to ensure that the flow-rate of individuals processing through a BCP adopting an intelligence-based approach, is generally higher than for BCPs solely relying on a rule-based approach, various tools and techniques have been developed. These include:

- Profiling[15];
- Information systems;
- API (Advance Passenger Information) / Passenger Name Record (PNR) (at air BCPs);
- IMO crew passenger list (at sea BCP); and
- Various other national systems.

However, whilst such tools and techniques have undoubtedly been of value in enhancing overall border control efficacy and especially improving flow rates, they are invariably 'standalone' in nature and little, if any, integration of systems especially between nations exists. For example, at present it is not permitted for information to be exchanged outside the European Economic Area (EEA) if there are no appropriate safeguards in place. Even within the EEA, not all countries are connected to all existing information sharing systems and these systems are in turn not all interconnected with each other. This is discussed in more detail at paragraph 3.12.7 below.

3.6 Developments in Border Control

Whilst the paragraphs above have described rule-based and intelligence based approaches to border control, the overall picture is not as binary as this. Numerous significant – either incremental or innovative – developments have taken place (or are planned) in the arena of

[15] Profiling is considered as an extrapolation of a certain characteristic of a person, a group or a situation based on other information of the respective subject (Van Rest, J.H.C., Roelofs, M., Van Nunen, A., and Don, S.B., 2014, quoted in TRESSPASS Deliverable 1.2, Chapter 2). Profiling can be used to draw attention to suspicious patterns (or the absence of normal patterns).

border control which inevitably blur the boundaries with respect to approaches taken. These include several EU Horizon 2020 (H2020) projects related to border control or security. A number of developments are discussed in more detail in TRESSPASS Deliverables 1.1 and 1.2. These developments include the following initiatives and projects summarised below.

3.6.1 *The European Criminal Records Information System (ECRIS)*

ECRIS provides criminal record information on convictions of EU nationals. ECRIS-TCN is an extension of ECRIS and will enable the exchange of information on criminal activities committed by TCNs or stateless persons.

3.6.2 *The European Travel Information and Authorisation System (ETIAS)*

ETIAS keeps track of visitors from countries who do not need a visa to enter the Schengen Zone for up to 90 days.

3.6.3 *The Entry-Exit System (EES)*

EES registers dates and places of entry and exit, and calculates the maximum length that visa holders and visa exempted TCNs are authorised to stay. Furthermore, the EES provides information on refusals of entry.

3.6.4 *Registered Traveller Programme (RTP)*

The purpose of the European initiative for an RTP is to speed up, facilitate and reinforce border check procedures by using smart technologies that give frequent TCN travellers the option of pre-screening, so that they would be able to use the automated border control systems.

3.6.5 *Exploitation of Biometrics*

An example of the exploitation of biometrics in the arena of border control is the 'Seamless Flow' initiative being developed at Schiphol Airport to '*enable a smooth passenger process whereby the required checkpoints can be passed easily, quickly and document-free*'.[16]

3.6.6 *Exploitation of Data Analytics*

Significant recent technological developments in the use of data analytics is allowing support to enhanced screening through the creation of risk profiles based on data that is collected from multiple public and private stakeholders.

3.6.7 *iBorderCtrl (Intelligent Portable Control System)*[17]

iBorderCtrl is a H2020 project combining state-of-the-art technologies for biometric verification, automated deception detection, and document authentication with a tool for risk assessment.

[16] Van Dijk, W. (2017) *Passenger experience: Enabling a seamless flow* [Online]. Available at: https://www.internationalairportreview.com/article/75108/seamles-pass-flow/ (Reference 6).

[17] iBorderCtrl: Intelligent Portable Border Control System, EU H2020 project, 01/09/2016 - 31/08/2019.Available athttp://www.iborderctrl.eu/ (Reference 7).

3.6.8 *PERSONA (Privacy, Ethical, Regulatory and SOcial, No-gate crossing-point solutions Acceptance)*[18]

PERSONA is a H2020 project which aims to fulfil the need for processing an increasing amount of border crossings and decreasing the pressure on border control systems by developing flexible, automated and scalable border security solutions.

3.6.9 *FLYSEC* (*Optimising time-to-FLY and enhancing airport SECurity)*[19]

FLYSEC – another H2020 project – developed an innovative integrated and end-to-end airport security process for passengers that enabled a guided and streamlined procedure from the landside to airside and into the boarding gates.

3.6.10 *XP-DITE (Accelerated Checkpoint Design Integration Test and Evaluation)*[20]

This H2020 project developed a comprehensive, passenger-centred, outcome-focused, system-level approach to the design and evaluation of airport security checkpoints.

3.7 Risk Analysis

Central to effective border control is the identification and management of threats. In Chapters 4, 5 and 6 each of the BCPs (air, sea and land) are considered in turn with a key focus on the range of threats most relevant to each border type. As described in paragraph 2.6 above, the concepts of threats and risks are intrinsically linked: a threat is anything that leads to a violation or disruption of the border control regime (with an associated negative impact); with a risk being the likelihood or probability of that threat being realised.

The probability of a threat being realised needs to be determined as well as a consideration of the possible resulting consequences – the impact – of a risk being realised. This requires a careful balancing of how each factor could influence the level of risk either positively or negatively, in order to determine whether or not the identified change in circumstances may lead to the potential risk to the border being realised. In the context of border control, the impact of risks may be wide ranging and varied but could include: disruption to the overall border service; delays to passengers / travellers; damage to infrastructure; or – in extremis – closure of border. The probability of risk realisation is achieved through a structured process of risk analysis.

3.8 Risk Management

Risk management is concerned with systematically taking all measures necessary to prevent or limit the likelihood of risks being realised or, if the risk is realised, measures to limit the impact. In effect, to neutralise the identified threat or threats through the implementation of appropriate measures, procedures or processes. Clearly a balance must be struck between the costs of implementing necessary solutions and the benefits that will accrue. As can be

[18] PERSONA: Privacy, Ethical, Regulatory and SOcial, No-gate crossing-point solutions Acceptance. Available at http://persona-project.eecs.qmul.ac.uk/ (Reference 8).

[19] FLYSEC: Optimising time-to-FLY and enhancing airport SECurity, H2020-SEC-2015-Project contract: 653879, Innovation Action. Available at http://www.fly-sec.eu/. (Reference 9).

[20] XP-DITE: Accelerated Checkpoint Design Integration Test and Evaluation, EU FP7 project, 01/09/2012 - 31/07/2017. Available at http://www.xp-dite.eu/. (Reference 10).

inferred from a consideration of the threats detailed in the following chapters, it will not be cost effective to address all risks equally. Criteria are needed to decide what constitutes an acceptable or unacceptable level of risk. According to the IBM Guidelines, the choices available fall into one of four categories:

- The threat can be removed;
- The threat can be avoided;
- The threat can be reduced; or
- The threat can be accepted.

3.9 Risk Profiling

Profiling of risks is often considered the most important application of risk analysis in day-to-day border management. A relatively simple, but very effective, method of targeting resources, profiling uses existing knowledge and operational information available to the range of agencies concerned with border control.[21] In this way, scarce or niche resources can be targeted against identified or predicted threats through the exploitation of risk profiles at BCPs. Such profiles are based on risk indicators, which are trends or patterns that have common distinguishing features. These indicators relate to issues that can be measured or observed, such as time, frequency and age.[22]

3.10 The Future of Border Control – Risk-based Border Management (RBBM)

Paragraphs 3.4 and 3.5 above summarise what could be termed as more traditional approaches to border control. However, from the discussion of the developments in border control and a short consideration of risk, it is clear that a more focused or targeted approach is required to enhance the overall effectiveness of a BCP and to improve the flow-rate. One such approach is a focus on the risks pertaining to border control through the adoption of RBBM. Whilst the heading of this section refers to 'future' border control, it is acknowledged that there are many existing approaches to border control which fundamentally apply a risk-based approach (or elements of), including many of the developments in the arena of border control, described in paragraph 3.6 above. The TRESSPASS Project has defined a risk-based border crossing point concept by the following elements:[23]

- The type of travellers (target group) for which the concept is meant for, defined by aspects such as: entering or leaving Europe, crew member or passenger, nationality, being a registered traveller or not, etc.;
- A risk acceptance statement that describes which risk is accepted (tolerated) for travellers who belong to the target group;
- Changes in the risk reduction of border control for the target group;
- Changes in the screening capabilities and capacities;
- Changes in the checking capabilities and capacities;
- Changes in flow-rate;
- The legal base;
- The applicability of the concept.

[21] Additional detail with respect to risk profiling is given in TRESSPASS Deliverable 1.2, paragraph 4.6.2.

[22] European Commission: Guidelines for Integrated Border Management in European Commission External Cooperation, November 2010. Page 93.

[23] TRESSPASS Deliverable 1.2, paragraph 4.8.1.

3.11 The Fundamental Gap in Effective Border Management

The introduction of RBBM, in itself, does not equate to the panacea for all border control issues. Border control is a complex issue and whilst generalisations can be made with respect to rule-based, intelligence-based or risk-based approaches, it is obvious that most of the border management concepts and developments (such as those described above) are limited in scope and relative insular in nature. It is the limitations of scope and the 'stove-piping' of capability that represents the fundamental gap that still exists today in border management (despite many recent and numerous developments in this arena) – i.e. the lack of an integrated, system of systems approach.

Many of the developments in border control focus on either: limited threats; single modalities (i.e. either solely air, land or sea focused); or only on Tier 3 (Border Control) of the four Tier model as described in the IBM Guidelines. This limitation in scope and the 'stove-pipe' nature of border control developments and enhancements invariably limit the potential to maximise the effectiveness as well as the efficiency of border control. This, in turn, impacts on the costs and resources required to deliver effective border control as well as negatively impacting on the overall 'passenger / traveller' experience. More fundamentally, however, the confidence to deliver the maximum level of security to passengers / travellers and border agency / security employees is also diminished.

3.12 Closing the Gap – the TRESSPASS Concept

It is the fundamental gap described above which, at its heart, the TRESSPASS project aims to address and ultimately close. TRESPASS proposes a new approach that links existing risk-based approaches into a multi-threat, multi-modality and four tier risk-based border management system-of-systems. As such, this integrated approach will cover: air, land and sea BCPs; the full range of threats[24] applicable to such BCPs; and all of the four tiers as described by the IBM Guidelines. In addition, TRESSPASS also intends to exploit concepts developed from previous or ongoing related H2020 projects.[25] The objectives of the TRESSPASS project are summed up as follows:

3.12.1 *Develop a single cohesive risk-based border management concept*

This concept will be a four-tier trans-national, multi-modal security tunnel, including the accompanying CONOPS.

3.12.2 *Apply an ethics and data protection 'by design' approach*

This is to ensure legal and ethical compliance of the solutions and provide ethical guidelines for decision makers regarding the planning and implementation of risk-based screening at borders. This addresses the data protection issues raised in paragraph 3.3 above.

[24] Less those threats posed by state-actors and threats to bulk cargo.

[25] In particular, this applies to the iBorderCtrl, FLYSEC, and XP-DITE projects summarised in paragraph 3.5. All of these projects have been coordinated by member organisations of the TRESSPASS Consortium.

3.12.3 *Include passenger trust in the risk management model*

The aim is to achieve this by taking into consideration a trustful passenger as a proactive and trustworthy source of voluntary information. Benefits will be determined from the development of such trust-based interaction between security system and passenger in order to optimise the performance of the system in terms of efficiency, cost reduction, and increased security.

3.12.4 *Develop three pivoting pilot demonstrators*

These pilots will practically demonstrate key conceptual, operational and technical aspects of the TRESSPASS concept using multiple threat scenarios, including terrorism activities at air borders, cross-border crime at land borders and irregular immigration via sea (port) borders. Chapters 4, 5 and 6 below set the context for these pilots by a consideration of air, land and sea BCPs including a focus on the threats faced by each border type and the potential application of the TRESSPASS capability with respect to each BCP.

3.12.5 *Demonstrate the validity of the single cohesive RBBM concept*

This will be achieved through the use and exploitation of the developed pilot demonstrators as well as red teaming and the use of appropriate simulation.

3.12.6 *Prepare for the further development of this concept*

This is a key element of the project in order to achieve a level of integration of border management approaches not seen today. Such integration will be achieved through articulating and developing appropriate links to other known risk-based border management projects and describing how their results contribute to a single cohesive risk-based border management concept. This will give all stakeholders a perspective for their respective further development.

3.12.7 *Information Exchange Considerations*

As introduced in paragraph 3.3 above, the management of information (especially with respect to data protection) is a fundamental element of effective and, more importantly legal border control. This aspect is no less critical to the overall TRESSPASS concept which involves the use of an information exchange network (TIEN) to enable efficient and reliable, risk-based passenger checks through:

- The application of biometric technologies;
- The use of sensing technologies (passport/ID readers, CCTV systems, body/cargo scanners);
- The design and development of a RBBM system and relevant models to assess:
    - **Identity** (of travellers);
    - **Possession** (of assets that can/cannot be used to generate a threat);
    - **Capability** (specific skills of people with which they can/cannot impose threat); and
    - **Intent** (from which the presence or absence of a threat can be derived).
- Links to legacy systems and external databases.

An international alert system that offers the capability to exchange and receive information to operational entities with links from the TIEN to legacy systems and external databases (such as PNR) through the TRESSPASS node is envisaged. Currently, however, it is not permitted for information to be exchanged outside the EEA if there are no appropriate safeguards in place. Even within the EEA, not all countries are connected to all existing information sharing systems and these systems are in turn not all interconnected with each other. Furthermore, different authorities have different access to data.

As part of increasing interoperability at the EU level, it is planned to establish the European Search Portal (ESP), through which all information systems could be searched simultaneously; legislative changes at the EU level will be necessary to enable this. Possible changes in law regarding PNR (pending decision of the EU Court of Justice) will also have to be taken into account. Access to any existing databases will require authorisation by legal departments of the appropriate agencies and a clear and transparent definition of access and data processing rules within the information flow of the TIEN will most likely be a prerequisite.[26]

[26] For full detail see TRESSPASS Deliverable 1.4, Chapter 4.

4 BCP TYPE 1 – AIR (AMSTERDAM SCHIPHOL AIRPORT)

4.1 Introduction

The air BCP is located in the Netherlands. For the purposes of the pilot, it will the Amsterdam Airport Schiphol. Schiphol Airport is the main international airport of the Netherlands. It is located 9 kilometres southwest of Amsterdam, in the municipality of Haarlemmermeer, North Holland. It is the third busiest airport in Europe in terms of passenger volume.

The airport is built as one large terminal (a single-terminal concept), split into three large departure halls, which connect again once airside. The most recent of these was completed in 1994 and expanded in 2007 with a new section, called Terminal 4, although it is not considered a separate building. A new pier is to be opened in 2019 with a terminal extension planned to be operational by 2023. Plans for further terminal and gate expansion exist, including the construction of a separate new terminal between the Zwanenburgbaan and Polderbaan runways that would end the one-terminal concept.[27]An aerial view of the airport is shown in the photograph in Figure 4-1.

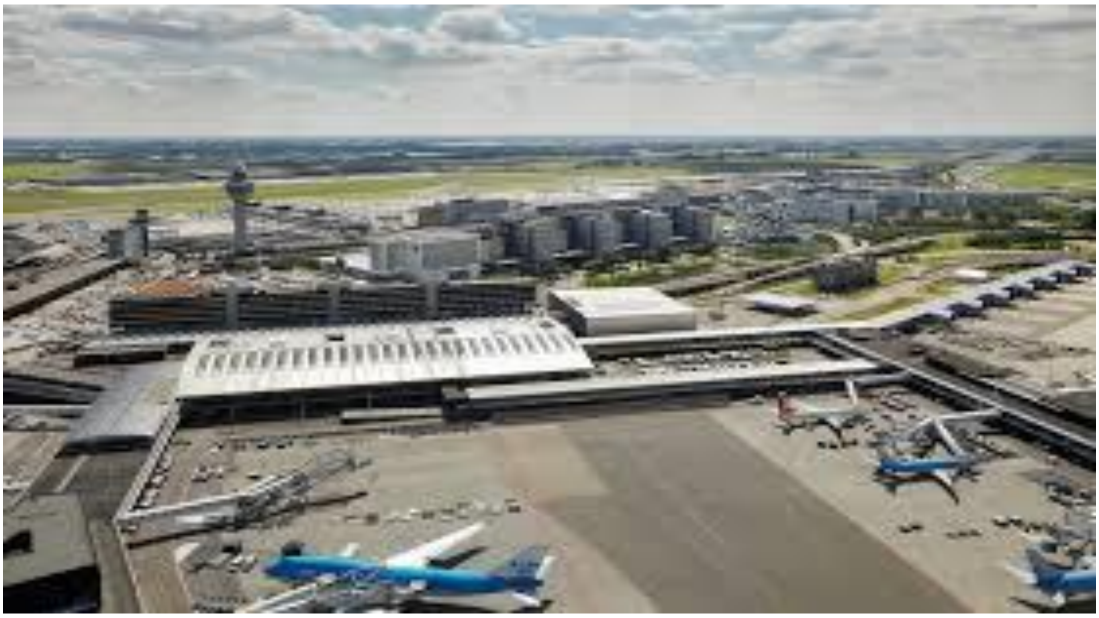


FIGURE 4-1. AERIAL VIEW OF AMSTERDAM SCHIPHOL AIRPORT

4.2 Scenario

4.2.1 *Traffic / Travellers*

Schiphol Airport is a large scale airport, which has strongly grown in the recent years and is expected to grow up to the (provisionally established) maximum number of movements of 500,000. In 2018 the passenger flow was 71.1 million passengers (including those in transit);

[27]https://en.wikipedia.org/wiki/Amsterdam_Airport_Schiphol. (Reference 11).

this was an increase of 3.7% from the previous year. About 40% of the passenger population crossed the Netherlands border, about 38% consisted of transfer passengers (outside of the Schengen area) and about 22% travelled intra-Schengen.[28]

4.2.2 *Challenges*

The main challenge, for the RNM Border Guard, associated with this BCP lies within the balance between mobility and security:

- People are more mobile, travel more and farther than before. This growth of mobility leads to increased pressure on the border control process; more people are crossing the border which results in longer queues. The challenge is to spend less time in average per passenger without compromising the quality of the border check process.

- Attacks in the EU show that national security is threatened by terrorism, with terrorists travelling via border crossing points. After terrorist attacks in Paris (November 2015) and Brussels (March 2016), legislation in this area became more stringent. This is at odds with the need for more mobility of individuals using BCPs;

- Processes on the airport, including the border process, are becoming more digitised. Examples are the EES and ETIAS systems described in paragraph 3.6 above. In this context Schiphol Airport authorities and RNM have taken initiative to further streamline the passenger flow process and developed the 'seamless flow' concept. In this concept the passenger is identified with a biometric token, by which he or she can move through all the airport processes. For RNM this means that the information provided through biometrics will enable passengers to avoid unnecessary border controls wherever possible.

4.3 Vignettes

4.3.1 *CONOPS*

The detailed CONOPS is one of the main outputs of WP6 (Operational Methods and Acceptability). However, preliminary work has been undertaken with partners and end-users to develop initial CONOPS for each of the border types – air, land and sea. It is anticipated that this preliminary work will be developed and refined as the TRESSPASS project progresses. A first draft of the air CONOPS[29] is shown in Figure 4-2 below.

[28] Schiphol Traffic Review 2018 (Reference 12).

[29] The draft CONOPS here (and the subsequent ones for the Land and Sea BCPs) were drawn from the preliminary work undertaken at the TRESSPASS End-Users Workshop (held in Dublin on the 11th of December 2018). These CONOPS will be refined through the TRESSPASS project (Work Package 6: Operational Methods and Acceptability).

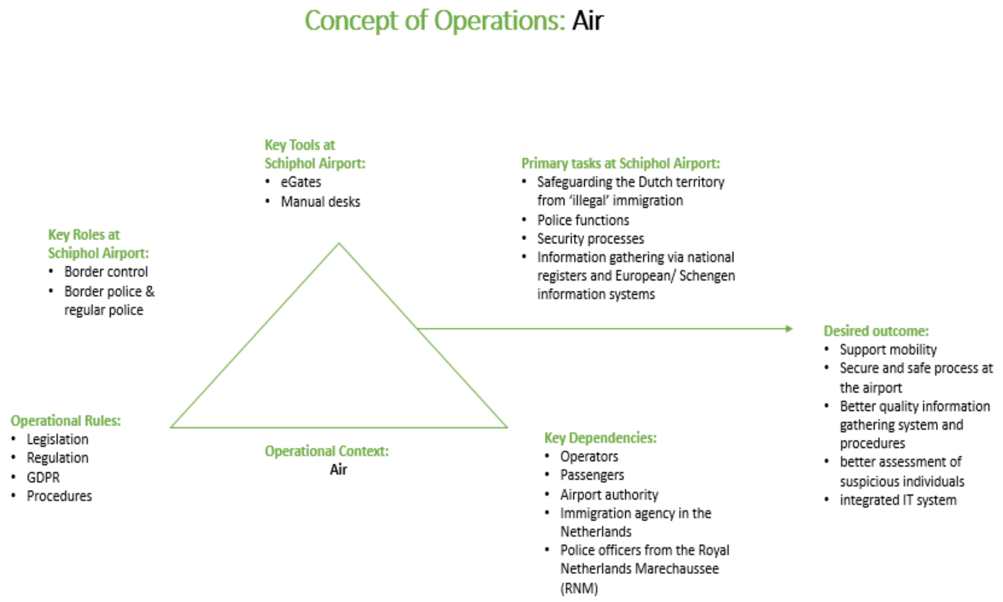

Concept of Operations: Air
Key Tools at Schiphol Airport:
• eGates
• Manual desks
Primary tasks at Schiphol Airport:
• Safeguarding the Dutch territory from 'illegal' immigration
• Police functions
• Security processes
• Information gathering via national registers and European/ Schengen information systems
Key Roles at Schiphol Airport:
• Border control
• Border police & regular police
Desired outcome:
• Support mobility
• Secure and safe process at the airport
• Better quality information gathering system and procedures
• better assessment of suspicious individuals
• integrated IT system
Operational Rules:
• Legislation
• Regulation
• GDPR
• Procedures
Operational Context:
Air
Key Dependencies:
• Operators
• Passengers
• Airport authority
• Immigration agency in the Netherlands
• Police officers from the Royal Netherlands Marechaussee (RNM)

FIGURE 4-2. DRAFT CONOPS AIR BCP

4.3.2 *Threats*

The initial challenges identified for this type of BCP are outlined in paragraph 4.2.2 above. However, further work in this area was conducted as part of TRESSPASS Task 1.1 as well as this Task 1.3. Fuller detail on threats can, therefore, be found in Deliverable 1.1.[30] As part of a survey of end-users, the following main challenges encountered (as pertaining to an air border) during day-to-day activities were expressed as follows:

- Counterfeited documents / Impostors: 17.46 %
- Lack of (skilled/experienced) staff: 17.46 %
- Threat identification and management: 15.88 %
- Lack of information on new regulations / Changes in legislation: 14.28 %
- Increasing volume of passengers: 9,52 %
- Time management: 6.35 %
- Difficulty to use / adopt new technologies: 6.35 %
- Potential threatening passengers: 4.76 %
- Balance between quality assurance and compliance to regulations: 4.76 %
- Cooperation/Exchange of information with other authorities: 3.18 %

WP2 of the TRESSPASS project (ongoing) is concerned with the development of the RBBM concept specifically with regards to BCPs. The first element of this WP is to deliver a method to specify the threat scenarios that the risk-based border management should be weighted and evaluated. Building on the threats described above, three specific air BCP threats are being developed, as shown in Figure 4-3 below:

[30] *TRESSPASS: robusT Risk basEd Screening and alert System for PASSengers*. D1.1 End-user requirements and needs.

Air BCP Threat	Inbound / Outbound	Actors	Modus Operandi
Return from a conflict area	Inbound	Terrorists, jihadists, insurgents	Act as a regular and legal border crosser
Human Trafficking	Outbound	Smugglers, criminal organisations	Unaccompanied minor trafficking: deviated routes (e.g. Ecuador – Netherlands – Spain).
Illegal Entry	Inbound	Third country citizen	Expired / false / stolen documentation; pseudo aircrew

FIGURE 4-3. WP2 AIR BCP THREATS

The three broad air BCP vignettes, derived from the threats identified above, are summarised as follows:

- **Vignette 1**. This vignette considers the return of individuals from a war-torn / conflict area somewhere in the world. As such, the actors are inbound (in this scenario) to the Netherlands. The actors are terrorists, jihadists, insurgents or similar and will tend to be individuals or small groups (not necessarily travelling together). They are likely to be residents of Holland or Dutch nationals and as such are likely to have transited in and out of the country on a regular or semi-regular basis as legal border crossers who have genuine (or at least seemingly genuine) travel documentation (passports) and identification cards / papers.

- **Vignette 2**.Vignette 2 is concerned with human trafficking. For the purposes of this vignette, the actors will be considered as outbound i.e. leaving Holland or transiting through from other countries. Naturally, the actors could also be considered from an inbound perspective as necessary. The actors will be smugglers or criminal organisations, generally operating on an organised or semi-organised basis. However, opportunistic examples of human trafficking – by an individual or small group of individuals on a one-off or occasional basis – cannot be discounted. The *modus operandi* will vary but could consist of (seemingly) unaccompanied minors.

- **Vignette 3**.This vignette is focused on the illegal entry, through Schiphol Airport, of individuals. As such, the actors are inbound to the Netherlands. For a large part, such individuals may be from third-world countries (as their point of origin or nationality) but not exclusively so. Given the complex and convoluted routes that many of these people may have travelled, it is not possible to predict from which country they may be travelling from to enter the Netherlands. It is likely that such actors will be travelling on either expired, stolen or forged documents (passports and identification cards / papers). There is a small risk that such actors could attempt to enter the Netherlands as (pseudo) aircrew.

4.4 Current Air BCP Infrastructure

API-data is received by the Royal Netherlands Marechaussee (RNM) for all incoming flights from outside the EU. The data is automatically compared to watch-lists and profiles, with the hits becoming alerts (improved hit) which are directed to the operations team. Follow-up takes place, for example by means of a Dedicated Gate Control if the risk assessment is judged as high. All border crossing points at the airport have e-gates (78 in total), besides the manual control booths (Figure 4-4). The airport is monitored by surveillance cameras.

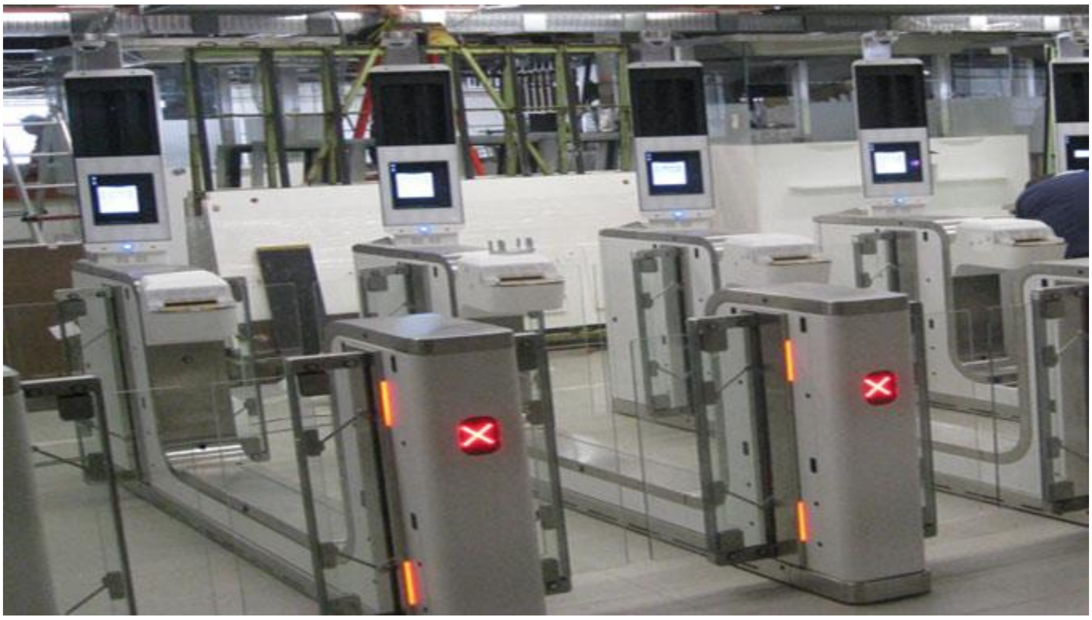


FIGURE 4-4. SCHIPHOL AIRPORT E-GATES

4.5 A Potential TRESSPASS Approach at the Air BCP

As described in paragraph 3.6.5 above, Schiphol Airport is already developing biometrics to improve flow-rates and the efficiency and effectiveness of its air BCP; indeed the overall goal is to achieve a 'seamless flow' of travellers through the identification of individual passengers by means of a biometric token. Developing the TRESSPASS concept further, the intention is to shape risk-based border control by exploiting both traveller information in advance and subsequent traveller behaviour at the BCP itself. The elements of a TRESSPASS approach may include the following:

4.5.1.1 Classification of the Travellers

Travellers can be categorised, on the basis of advance information (received prior to arrival at the BCP) in three categories. These are: 'no or acceptable risk' (green); 'unknown risk' (orange) and 'known risk' (red).

4.5.1.2 Recognition of abnormal behaviour

TRESSPASS should enable the recognition of abnormal behaviour (either by individuals or groups of individuals) when at the BCP. This could be achieved through identifying certain noteworthy physical characteristics such as displaying excessive nervousness or anxiety. Alternatively this may be manifested by obvious contradictions in individual traveller statements to border agencies.

4.5.1.3 Improved exploitation of information

TRESSPASS should enable much more effective integration and exploitation of information to enable border agencies to react more quickly or appropriately. This is especially important in the processing of updated information in order to inform any potential re-classification of passengers e.g. a traveller previously considered as ‘no risk’ being re-categorised as ‘known’ or ‘unknown’ risk based on updated intelligence received or as a result of abnormal behaviour displayed by individuals at the BCP and noted by the border agencies. It is essential that information as well as the classification of travellers is passed as effectively and in as timely a manner as possible to the border guards to allow for appropriate decisions to be made and action taken.

4.5.1.4 Expected Benefits of a TRESPASS Approach

One direct benefit of the implementation of a TRESSPASS approach is the improved exploitation of information described in the paragraph above. The exploitation of traveller information in advance and subsequent traveller behaviour at the BCP itself should allow bona fide travellers – in a ‘no risk’ category – to pass through the BCP as swiftly as possible (with minimum or ultimately no delay). Travellers categorised as ‘known’ or ‘unknown’ (see below), however, can be identified in advance and allow the border authorities to either act proactively (through the deployment of relevant and suitable agencies) or reactively i.e. wait for the arrival of such travellers at the BCP and then act accordingly.

4.6 Air BCP – Swim-lanes

To assist with understanding the passenger ‘flow’ through a particular border-type, the concept of ‘swim-lanes’ is being developed as part of WP6 (Operational Methods and Acceptability). This method will assist the development of a risk-based border management concept. A swim-lane represent interactions among actors / systems / data.[31] The first iteration of a swim-lane for the air BCP is shown in Figure 4-5 below. It should be noted, that for the purposes of this deliverable – the high-level scenarios – the swim-lanes broadly describe the ‘as is’ situation pertaining to border control. They do not, at this stage, attempt to fully describe the future risk-based border control processes. These will be developed later on in the TRESSPASS project.

[31] Due to the Public Dissemination Level of this document, only extracts from passenger-experienced flows / interactions are shown here. There are, clearly, many more interactions (for instance with border control agencies or the police) which will take place in the border control process.

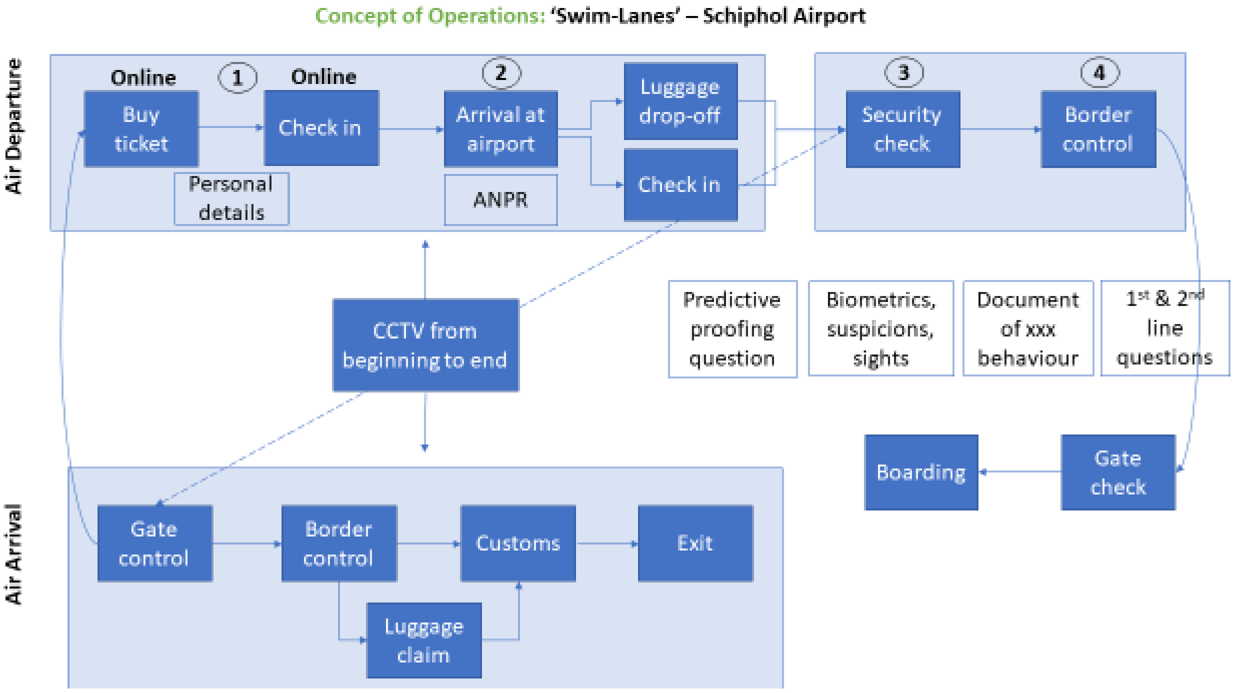


FIGURE 4-5.WP6 EXTRACT OF DRAFT AIR BCP SWIM-LANES – SCHIPHOL AIRPORT

5 BCP TYPE 2 – LAND (POLISH BORDER GUARD)

5.1 Introduction

The land BCP is located in Poland. For the purposes of the pilot, it will be one of the border crossing points within Nadbużański Regional Unit of Polish Border Guard, i.e. Dorohusk or Terespol BCPs. The specific BCP will be selected in line with geo-political situation and project requirements. The border type is an external land border consisting of vehicle (freight, buses, cars etc.), rail and pedestrian traffic. The operators of land BCPs and border/custom authorities wish to better utilise their existing infrastructure and facilities and ultimately increase the capacity and throughput of individual BCPs.

During last several years, the statistics show a steady increase in the number of travellers crossing Polish border. Most of the travellers are citizens of Ukraine, Russian Federation and Belarus and approximately 80% of all border crossings is made by frequent travellers. The frequent travellers are considered as low risk travellers. The BCPs at Terespol and Dorohusk are shown below in Figures 5-1 to 5-3:

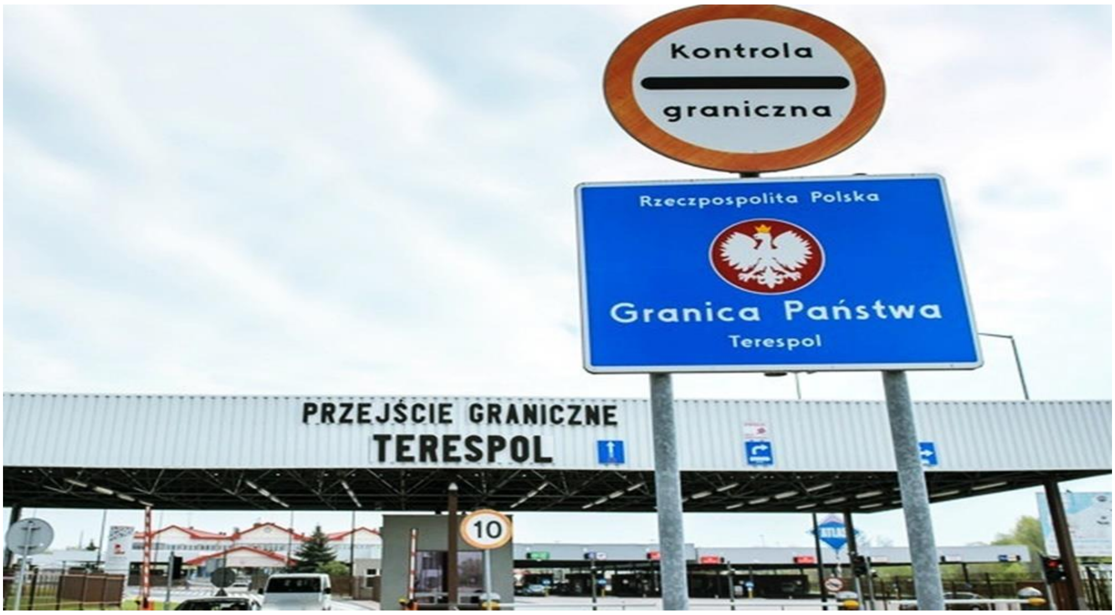


FIGURE 5-1.BORDER CROSSING POINT IN TERESPOL

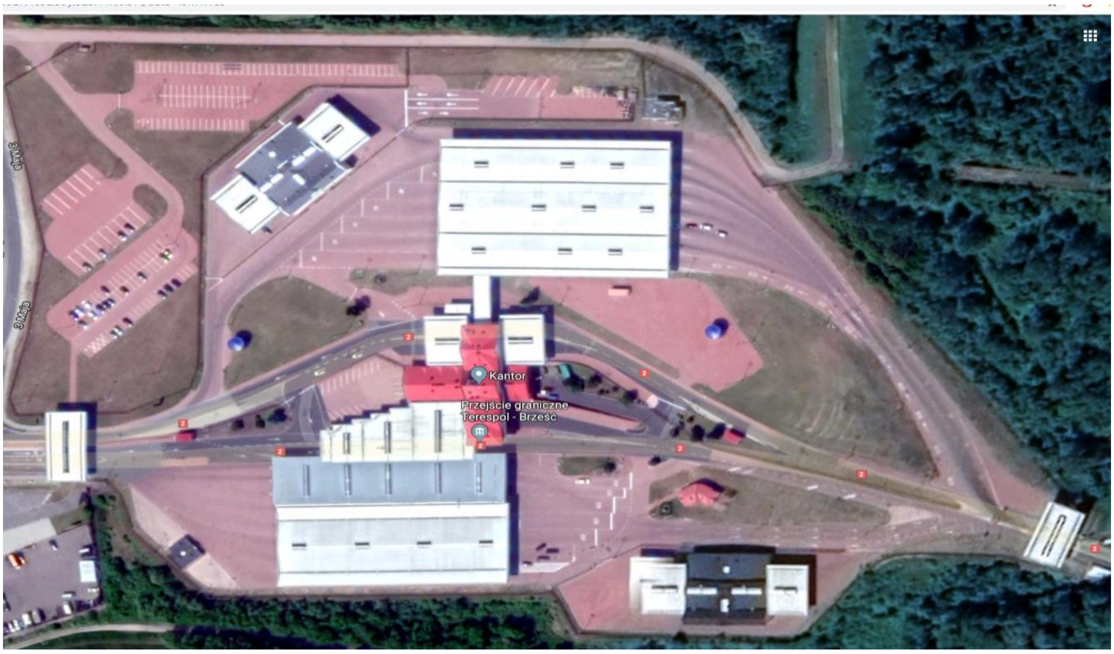


FIGURE 5-2.AERIAL VIEW OF BORDER CROSSING POINT IN TERESPOL

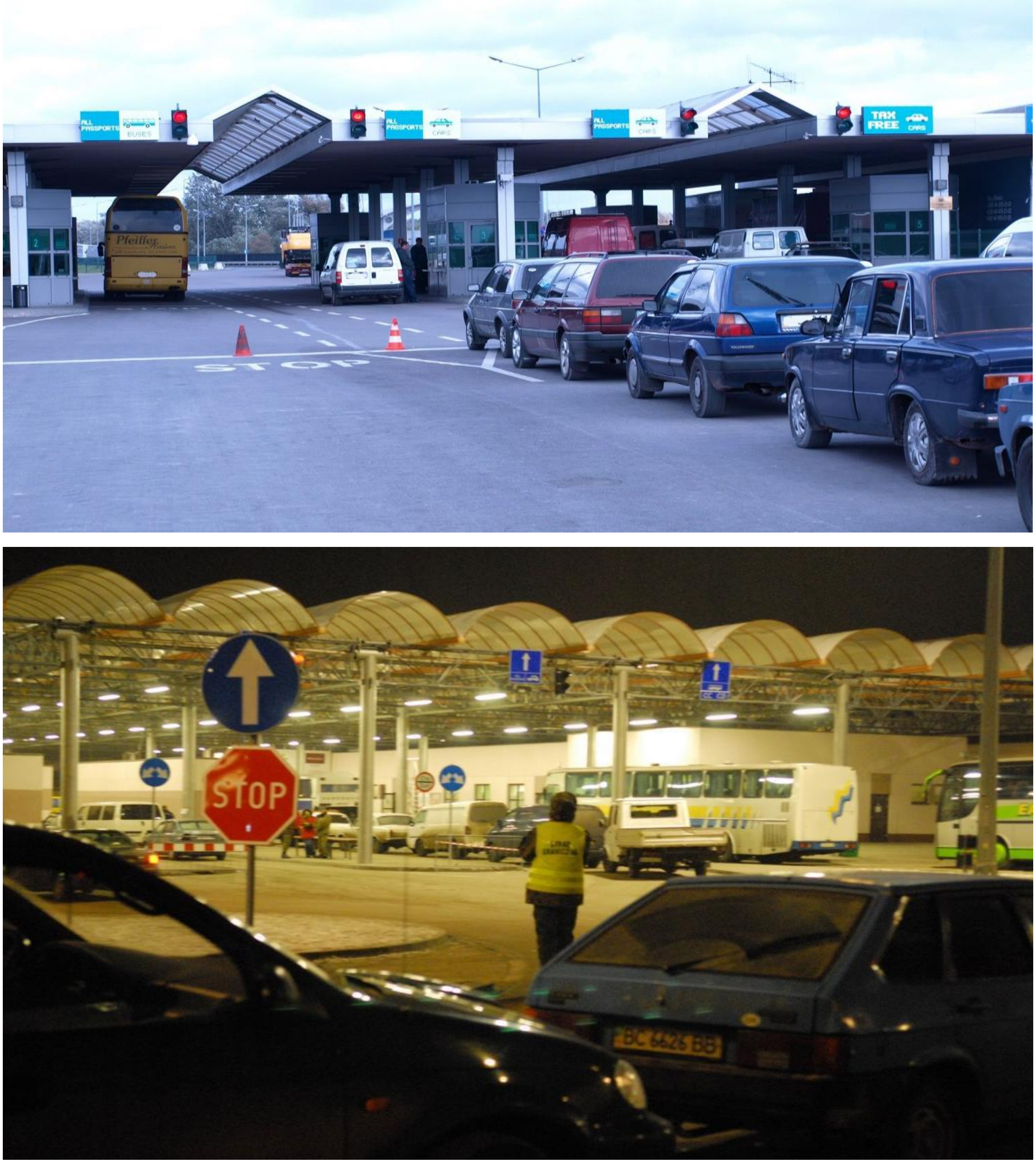


FIGURE 5-3. BORDER CROSSING POINT IN DOROHUSK

5.2 Scenario

5.2.1 *Traffic/Travellers*

Statistics show a steady increase in the number of travellers crossing Polish border.[32] Whilst the nationalities of travellers vary, the majority of travellers are citizens of Ukraine, Russian Federation and Belarus; all of them are third country nationals and in respect of the Schengen

[32] Data from the PBG quoted in Reference 1.

arrangements require visas[33] in order to travel into the European Union. There is a high percentage of frequent travellers, a group which constitutes approximately 80% of all border crossings. These frequent travellers are considered as low risk travellers.

5.2.2 ***Challenges***

The challenges, for the Polish Border Guard and other agencies, associated with this BCP are as follows:

- High volumes of traffic.
- Cross-border smuggling (especially alcohol, cigarettes and drugs). The routine detection of smuggling is particularly difficult due to constantly changing smuggling patterns and means of hiding the illicit goods.
- Document forgeries. This especially applies to: freight transport and lorry drivers' attempts to forge the certificates allowing them to transport hazardous materials; and a growing tendency to forge passport stamps, on the basis of which border officers are able to establish how long a given individual stayed on the territory of European Union/Schengen zone.
- Customs control, which is conducted separately after passport control, becoming a 'bottleneck'.

5.3 Vignettes

5.3.1 ***CONOPS***

The detailed CONOPS is one of the main outputs of WP6 (Operational Methods and Acceptability). However, preliminary work has been undertaken with partners and end-users to develop initial CONOPS for each of the border types – air, land and sea. It is anticipated that this preliminary work will be developed and refined as the project progresses. A first draft of the land CONOPS[34] is shown in Figure 5-4 below.

[33] Ukrainian citizens possessing biometric passports do not need visas for short trips to the EU (90 days in every 180 days period).

[34] See footnote 8 above.

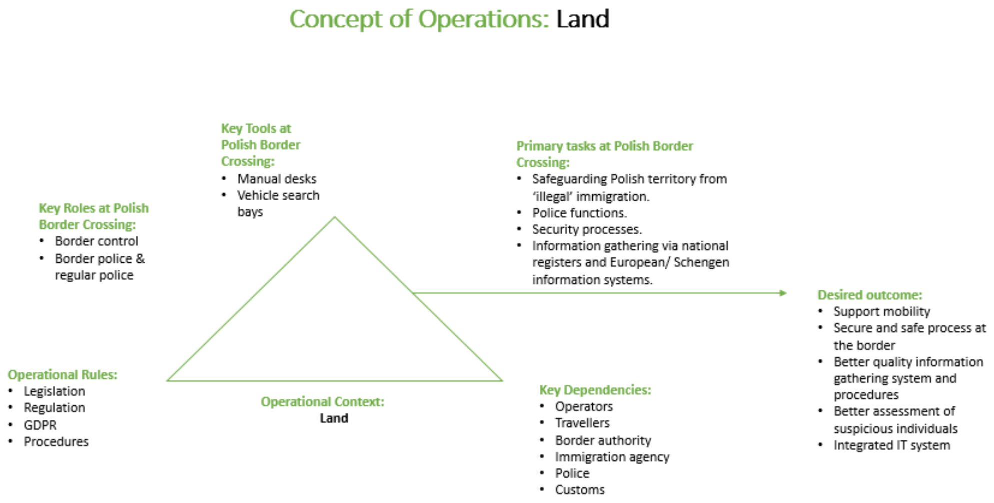

Concept of Operations: Land
Key Tools at Polish Border Crossing:
• Manual desks
• Vehicle search bays
Primary tasks at Polish Border Crossing:
• Safeguarding Polish territory from 'illegal' immigration.
• Police functions.
• Security processes.
• Information gathering via national registers and European/ Schengen information systems.
Key Roles at Polish Border Crossing:
• Border control
• Border police & regular police
Desired outcome:
• Support mobility
• Secure and safe process at the border
• Better quality information gathering system and procedures
• Better assessment of suspicious individuals
• Integrated IT system
Operational Rules:
• Legislation
• Regulation
• GDPR
• Procedures
Operational Context:
Land
Key Dependencies:
• Operators
• Travellers
• Border authority
• Immigration agency
• Police
• Customs

FIGURE 5-4. DRAFT CONOPS LAND BCP

5.3.2 *Threats*

The initial challenges identified for this type of BCP are outlined in paragraph 5.2.2 above. However, further work in this area was conducted as part of TRESSPASS Task 1.1 as well as this Task 1.3. Fuller detail on threats can be found at Deliverable 1.1.[35]As part of a survey of end-users, the following main challenges encountered (as pertaining to a land border) during day-to-day activities were expressed as follows:

- Lack of (skilled/experienced) staff: 22.22 %
- Threat identification and management: 22.22 %
- Smuggling of excise goods / drugs: 13.88 %
- Lack of information on new regulations / changes in legislation: 13.88 %
- Difficulty to use / adopt new technologies: 8.34 %
- Illegal border crossings: 8.34 %
- Cooperation/Exchange of information with other authorities: 5.56 %
- Counterfeited documents / Impostors: 2.78 %
- Potential threatening passengers: 2.78 %

WP2 of the TRESSPASS project (ongoing) is concerned with the development of the risk-based border management concept specifically with regards to BCPs. The first element of this WP is to deliver a method to specify the threat scenarios that the risk-based border management should be weighted and evaluated. Building on the threats described above, three specific land BCP threats are being developed, as shown in Figure 5-5 below:

[35] *TRESSPASS: robusT Risk basEd Screening and alert System for PASSengers*. D1.1 End-user requirements and needs.

Land BCP Threats	Inbound / Outbound	Actors	Modus Operandi
Disclosure of national sensitive information or goods	Outbound	EU citizens involved in espionage	Posing as a student etc. (valid travel documentation and visa); concealment of goods
Smuggling of cigarettes	Inbound	Drug smugglers	Concealment in vehicles or luggage
Trafficking illegal economic migrants	Inbound	People smugglers, criminal organisations	Concealment

FIGURE 5-5. WP2 LAND BCP THREATS

The three broad land BCP vignettes, derived from the threats identified above, are summarised as follows:

- **Vignette 1**. This vignette considers the cross-border carriage (for subsequent disclosure / exploitation e.g. to other governments, criminal organisations or even corrupt businesses) of national and EU sensitive information or goods. The actors will vary but could involve EU (or non-EU citizens) involved in governmental, criminal or commercial espionage. Actors may pose as individuals from groups considered generally to be of low threat (such as students) and invariably may be travelling on genuine documentation (both passports and identification cards / documents). For the transportation of sensitive goods, it is likely that these will be concealed within the vehicle the actor is travelling in to cross the border. In the case of this vignette the actors will be considered outbound – either to Belarus (if crossing at Terespol) or to Ukraine (if using the Dorohusk BCP).

- **Vignette 2**. Vignette 2 is concerned with the smuggling of cigarettes, on a scale large enough to be of commercial value to the actor concerned. The actors are considered to be inbound i.e. travelling across the relevant land border to enter Poland where they will (at an undefined location / locations) sell their cargo of cigarettes for profit. The actors are likely to be part of a larger organised criminal gang (although smaller scale operations could not be discounted) and potentially be involved with wider drug smuggling activities. In this vignette, the concealment of such illicit cargo is paramount and invariably the actors will go to great (and imaginative) lengths to conceal their cargo within the vehicles they are transiting the border in.

- **Vignette 3**. This vignette is focused on the trafficking of illegal migrants seeking to gain entry into Poland, either as a final destination or as a transit route to a third country. Once again, the actors are considered inbound to Poland (either from Belarus or Ukraine (although the journeys of the actors and their human cargo are unlikely to have started from these destinations). Invariably, this will be generally organised activity with the actors being associated with wider criminal gangs / organisations or larger-scale experienced smuggling / trafficking gangs. Concealment of the cargo (in this case, people) is essential but the vehicles / spaces used clearly must be large enough to accommodate one or more person.

5.4 Current Land BCP Infrastructure

The following sections detail the key components of the border crossing infrastructure at the land BCP (Terespol and Dorohusk respectively).

5.4.1 *Terespol BCP at the Polish-Belarusian Border*

The BCP in Terespol has two road border crossings in:

- Terespol - for cars up to 3.5 tons and buses:
  - On the entry direction to Poland, there are eight (8) lines (1 x EU/EEA/CH citizens; 5 x All passports, 1 x bus, 1 x CD/CCD[36]);
  - Ten (10) lines on the exit direction (1 x EU/EEA/CH citizens; 7 x All passports, 1 x bus, 1 x CD);
  - On average 120 buses undergo border control at Terespol BCP daily.

- Kukuryki - for trucks; as a part of international road freight transport, connected by a 5.2-kilometre customs road with a car terminal in Koroszczyn:
  - On the entry direction to Poland, there are four (4) lines (1 x EU/EEA/CH citizens; 3 x All passports);
  - Five (5) lines on the exit direction (1 x EU/EEA/CH citizens; 4 x All passports);

On average the daily number of travellers crossing the border at Terespol is 10,000.About 8% of the vehicles crossing the border are directed to more detailed control. This is usually caused by border officer's suspicions of smuggling. Photographs of the Terespol land BCP are presented in Figures 5-1 and 5-2 above with a photograph of the Border Guard internal infrastructure at Figure 5-6 below:

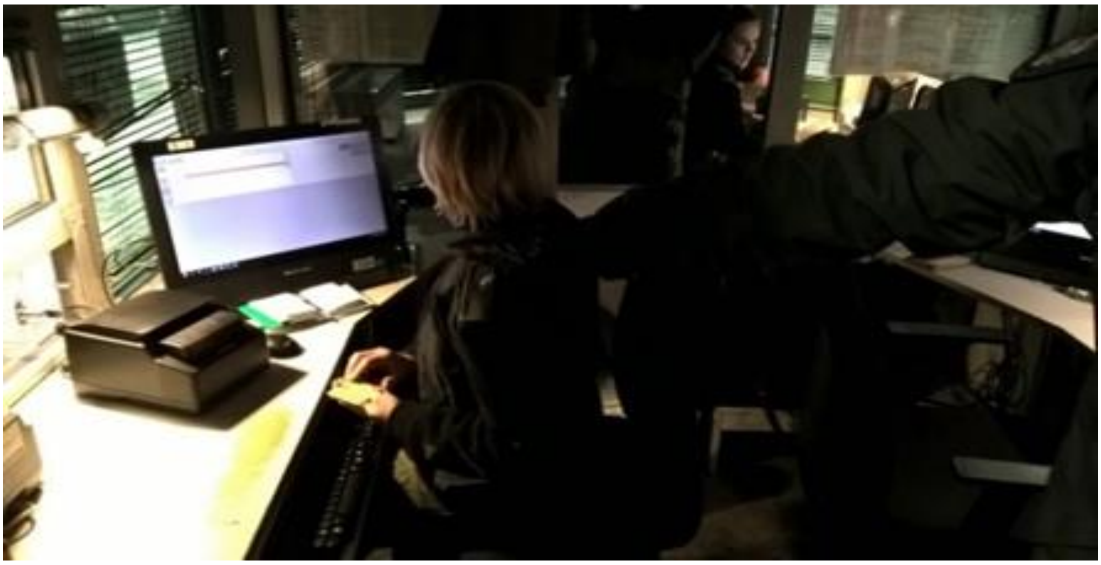


FIGURE 5-6.INTERNAL INFRASTRUCTURE AT THE BORDER CROSSING POINT IN TERESPOL

[36] CCD: Diplomatic and Consular Corps and CD: Diplomatic Corps. Diplomatic vehicles in most countries have distinctive diplomatic licence plates, often with the prefix or suffix *CD,* the abbreviation for the French *corps diplomatique.* Such travellers are afforded certain privileges when transiting through border control between countries.

5.4.2 *Dorohusk BCP at the Polish-Ukrainian Border*

The road border crossing in Dorohusk has the status of international passage for passenger and freight traffic without restrictions. It operates on a 24-hour system. Border checks on entry and exit directions are made on Polish territory by Polish border services according to the order: entry/exit Border Guard, Customs Service. Border checks are carried out on 25 lanes:

- On the entry direction to Poland, there are 14 lines in total:
  - Six (6) border control lines for traveller traffic (1 x EU/EEA/CH citizens; 4 x All Passports; 1 x buses);
  - Eight (8) border control lines for freight traffic (2 x EU/EEA/CH citizens; 5 x All passports and 1 manoeuvring line).

- With regard to the exit direction from Poland, there are 11 lanes in total:
  - Six (6) border control lines for traveller traffic (1 x EU/EEA/CH citizens; 1 x CD/CCD and buses; 4 x All Passports);
  - Five (5) lines for trucks (1 x EU/EEA/CH citizens, 3 x All Passports 1 x manoeuvring line).

A photograph of the Dorohusk land BCP is at Figure 5-3 above with a photograph of the Border Guard internal infrastructure at Figure 5-7 below:

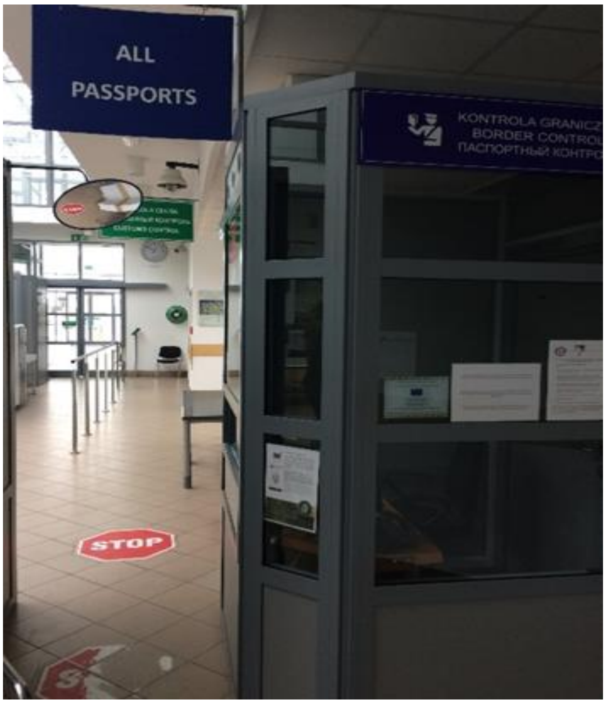


FIGURE 5-7. INTERNAL INFRASTRUCTURE AT THE BORDER CROSSING POINT IN DOROHUSK

5.5 A Potential TRESSPASS Approach at the Land BCP

In this potential TRESSPASS approach, there is a particular focus on validating web intelligence information and undertaking behavioural analysis of walking travellers (inside bus or train terminals). In addition, there is the integration of data obtained from different databases (Interpol and law enforcement agencies, third countries etc.) and information from sensors located at the crossing and the nearby vicinity (i.e. access roads). There is also a focus on checking authenticity of documents as well as preliminary checking of cars and trucks approaching the crossings. The elements of a TRESSPASS approach may include the following:

5.5.1.1 Pre-checking

Competent authorities, based on analysis of web-intelligence data and appropriate databases as well as other sources, start the risk-based processing in order to identify whether a traveller poses a threat to the internal security of the EU. This is primarily achieved through a profiling process for each passenger applying various sets of rules used by various competent authorities such as border control and customs authorities as well as comparing their data against a set of databases and open source data (social media etc.). With respect to border control authorities, profiling is presently focused on travellers or passengers at various stages of their transit to or through the border. Three broad types of current profiles include:

- **'Business-as-usual'**. This type of profile describes normal travellers / passengers and is based on experiences of border authorities gained over time. Perceived abnormalities to expected patterns of behaviour, that cannot easily be explained, will result in a further inspection.
- **'Known modus operandi'**. This type of profile describes the observable aspects, by the border authorities, of known modus operandi of suspicious / potentially threatening behaviour. This will lead to closer / further inspection to verify or allay suspicions.
- **'Specialist profile'**. This type of profile is based on the individual expertise of experienced specialists supporting, or integral to, border authorities. The purpose of this type of profiling is to ensure that even unknown types of threatening modus operandi, which include those of well-prepared adversaries, can be identified. Identification will always result in further inspection.

5.5.1.2 Checking at the border

The TRESSPASS systems will be employed to check whether a traveller is of increased risk level based on the analysis of 'at the border' systems (including, for instance, baggage scanners and behavioural analysis). Similar scenario considers freight transport and lorry drivers. Detailed checks of freight will be performed using TRESPASS systems. All documents will be the subject of thorough checking.

5.5.1.3 Profile Alerting/Notification

After the pre-checking and checking at the border is completed, the alerting system is initiated for all competent authorities including Border Guards who shall be notified in the case that a particular traveller or group of travellers poses a threat. This is in order to proceed to the corresponding further actions required. At this stage the processing result could be transmitted to other MS or third countries.

5.5.1.4 Identity verification

At the land BCP, all travellers will be verified based on ID and biometric verification. 'On-the-move' capability will be used wherever possible. Interoperability concepts with simulated legacy systems, shall be introduced at this stage, for biometric matching.

5.5.1.5 Web intelligence

By closely observing the trends on specific related keywords about illicit goods purchases in blogs or discussion forums it is possible to identify potentially threatening developments of imminent smuggling incidents. These threats will need to be dealt with by immediate action in order to avoid probable large-scale cross border flows of illicit goods.

5.5.1.6 Expected Benefits of a TRESPASS Approach

The operators of land BCPs and the relevant border/custom authorities are expecting to utilise better the existing border control infrastructure and facilities. Most of the travellers, in this land border case, are citizens of Ukraine, Russian Federation and Belarus and approximately 80% of all border crossings is made by frequent travellers. These frequent travellers are considered as low risk travellers. Through the application of TRESSPASS it should be possible to eliminate the dependencies based on the types of travellers, their origins, entries or exit types and improve existing border and customs control processes. The result should be an improved flow-rate of travellers with much reduced queues. It is anticipated that the deployment of a TRESSPASS capability will also improve the detection rates of cross-border smuggling as well as the use of document forgeries by travellers.

5.6 Land BCP – Swim-lanes

To assist with understanding the passenger 'flow' through a particular border-type, the concept of 'swim-lanes' is being developed as part of WP6 (Operational Methods and Acceptability). This is discussed in full at paragraph 4.6 above. The first iteration of a swim-lane for the land BCP is shown in Figure 5-8 below:

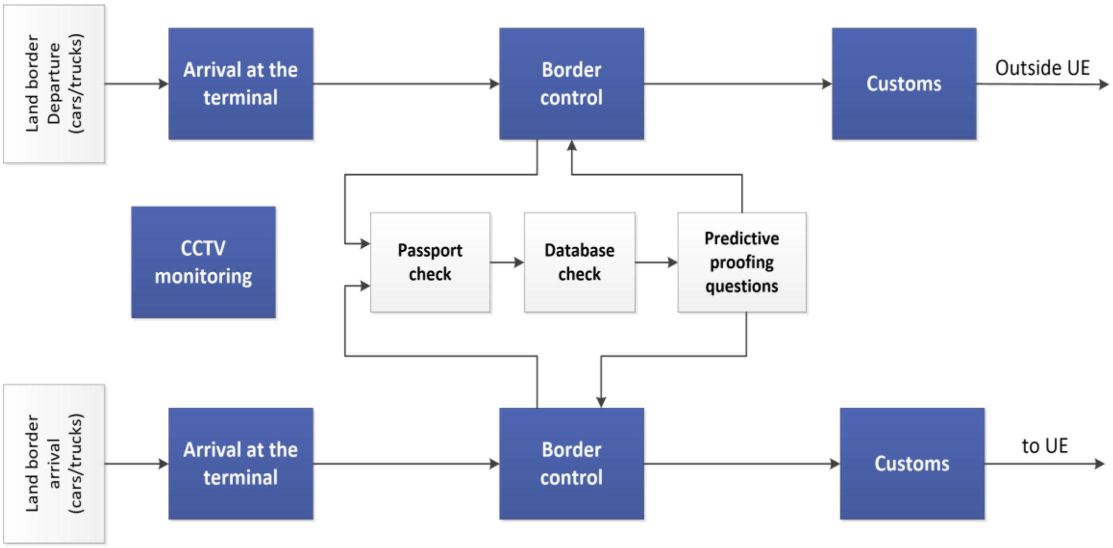


FIGURE 5-8. DRAFT LAND BCP SWIM-LANES – POLISH BORDER CROSSINGS

6 BCP TYPE 3 – SEA (PIRAEUS PORT)

6.1 Introduction

The sea BCP is located in Greece. For the purposes of the TRESSPASS pilot, it will be the Piraeus Cruise Port. Piraeus is a city port in the region of Attica, Greece. It is located within the Athens urban area, 12 kilometres southwest from its city centre (municipality of Athens) and lies along the east coast of the Saronic Gulf.

The port of Piraeus is the major and biggest port in Greece, the largest passenger port in Europe and the second largest in the world, servicing about 20 million passengers annually. With a throughput of 1.4 million Twenty-foot Equivalent Units (TEUs)[37], Piraeus is placed among the top ten ports in container traffic in Europe and the top container port in the Eastern Mediterranean.[38]An aerial photograph of the port is in Figure 6-1 with a map at Figure 6-2 below.

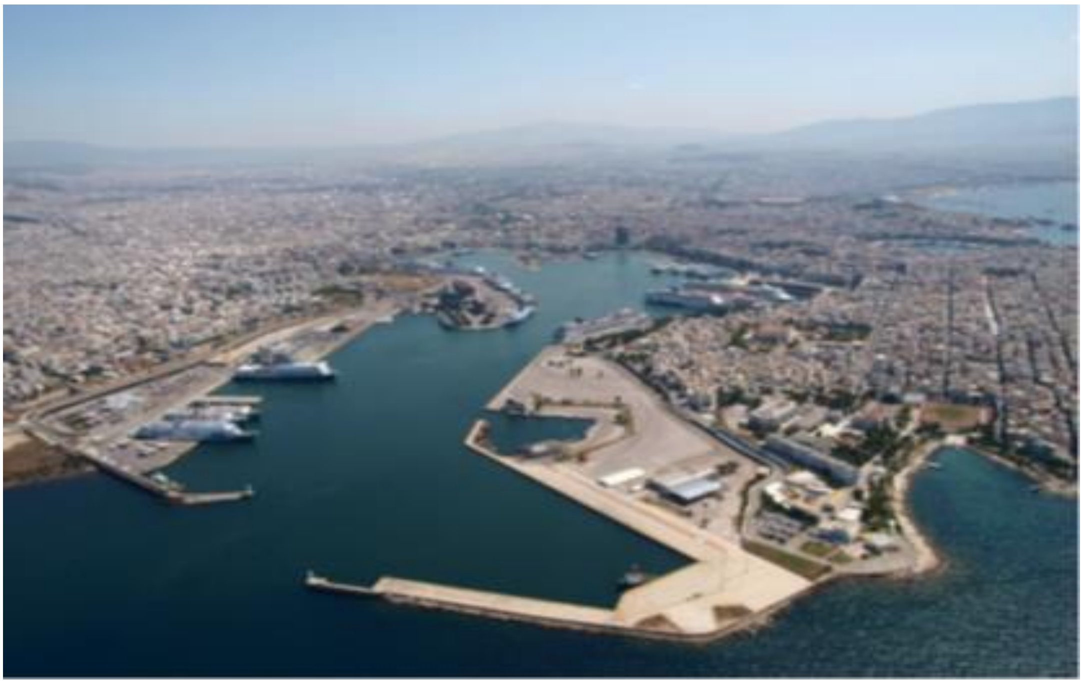


FIGURE 6-1. AERIAL VIEW OF THE CENTRAL PORT OF PIRAEUS

[37]A TEU is an inexact unit of cargo capacity often used to describe the capacity of container ships and container terminals. It is based on the volume of a 20-foot-long (6.1m) intermodal container, a standard-sized metal box which can easily be transferred between different modes of transportation, such as ships, trains and trucks. These are also widely referred to as ISO (International Organization for Standardization) containers.

[38]https://en.wikipedia.org/wiki/Piraeus (Reference 13).

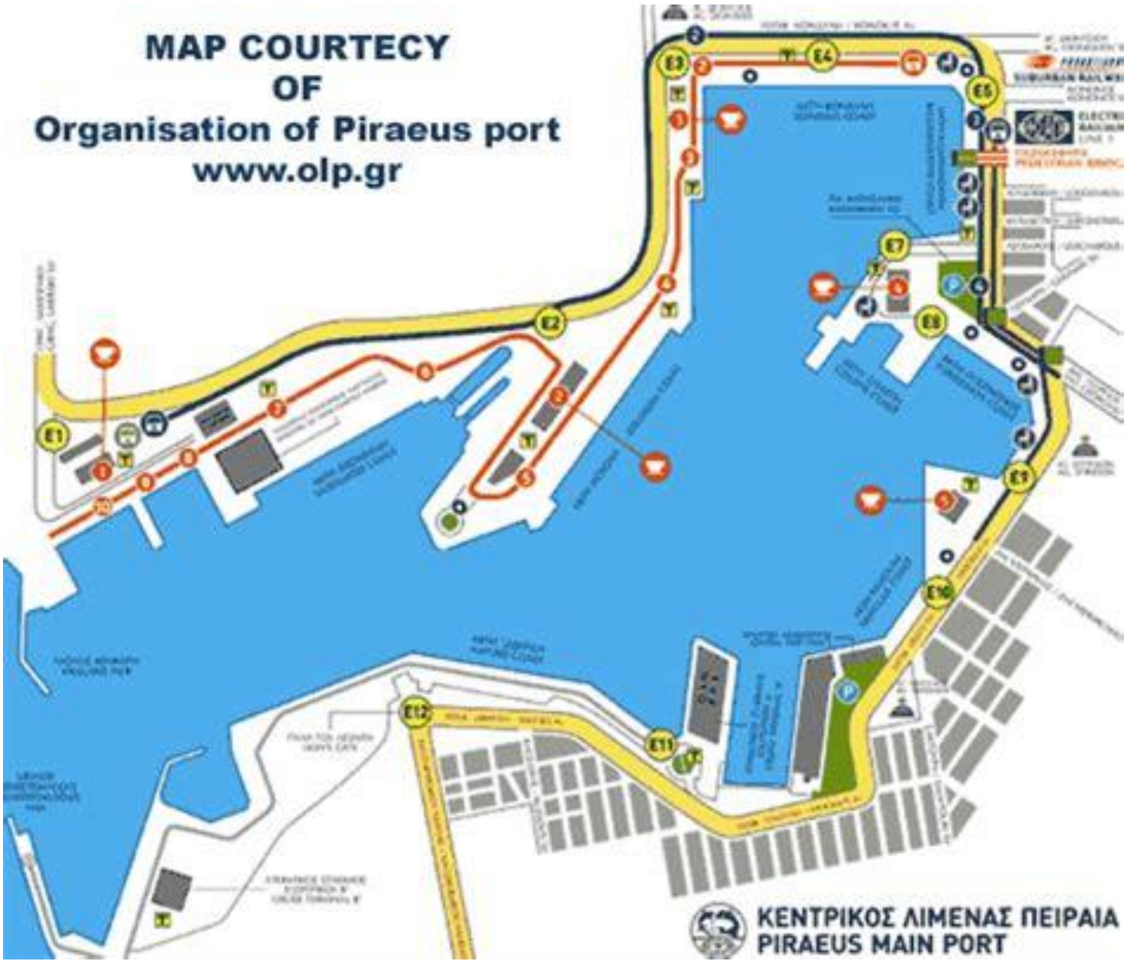


FIGURE 6-2. MAP OF THE CENTRAL PORT OF PIRAEUS

6.2 Scenario

6.2.1 *Traffic / Travellers*

Cruise travelling is a relatively new, emerging and developing form of transportation and tourism especially in the Mediterranean. Statistics show that the number of cruise travellers crossing the Piraeus Port can reach up to 20,000 per day (home/transit)[39]. The majority of travellers arrange their travels by first visiting Greece or other European or Mediterranean countries by plane or other means and then take a cruise visiting places around various ports of Schengen or non-Schengen countries.

Two types of passengers, home and transit, are identified in the process depending on whether they exit permanently from the ship to the destination country or they exit the ship, visit the country and come back to the ship to continue their cruise. The cruise ships conduct their own security checks on board, such as X-rays and magnetic doors.Transit passengers hold a special ship boarding card ID which is provided by the cruise company. For non-

[39] Data from the PPA quoted in Reference 1.

Schengen passengers control is done in first Greek or other EU port, then Schengen applies for the rest of the visiting ports.

6.2.2 *Challenges*

The main challenge, for the Border Guard, associated with this BCP is a large flow of disembarking passengers which creates bottlenecks and delays in the control procedures at BCPs. This compounded by the conduct of city visits for significant numbers of passengers in a very compressed period of time. Some critical issues to be considered mainly related with the port infrastructure include:

- Hosting the embarking and disembarking services of many cruise ships in parallel.
- Separating and directing non-Schengen arrivals to a specific terminal which has the appropriate infrastructure and facilities required.
- Implementing the appropriate border controls to the large number of cruise passengers crossing the BCPs simultaneously. Due to resources and time restrictions and limitations to cover the large amount of passengers' traffic, it is not feasible to perform all the border and customs controls on all cruise passengers. Customs and Passport control often happens on a basic ad hoc risk analysis approach or following a specific tip/alert.

Figure 6-3 below presents a 'snapshot' of a day in the Piraeus Port cruise terminal:

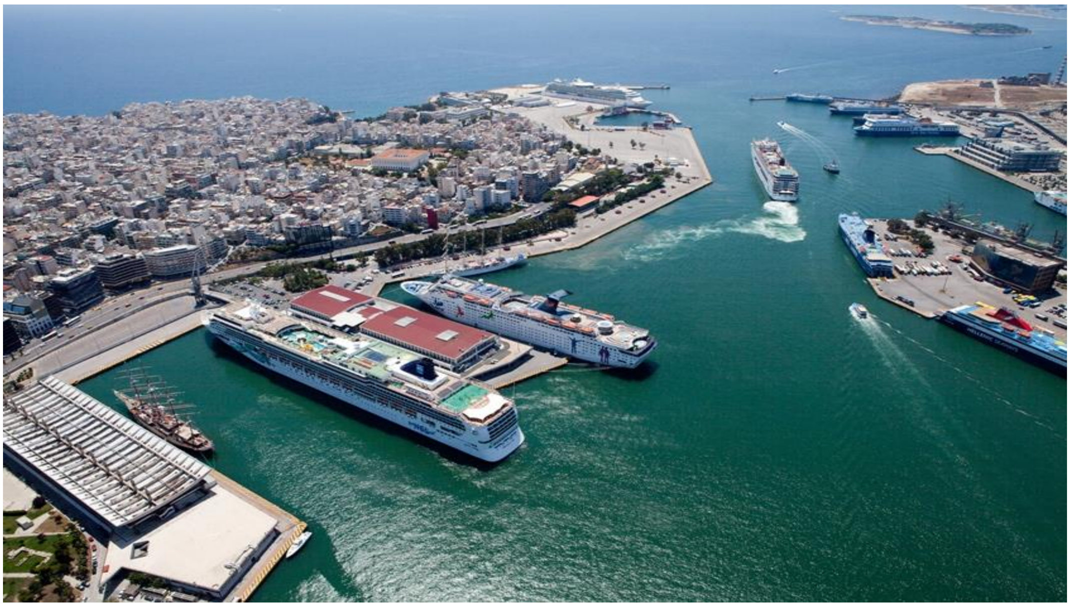


FIGURE 6-3. CRUISE TERMINAL

6.3 Vignettes

6.3.1 *CONOPS*

The detailed CONOPS is one of the main outputs of WP6 (Operational Methods and Acceptability). However, preliminary work has been undertaken with partners and end-users to develop initial CONOPS for each of the border types – air, land and sea. It is anticipated that this preliminary work will be developed and refined as the project progresses. A first draft of the sea CONOPS[40] is shown in Figure 6-4 below:

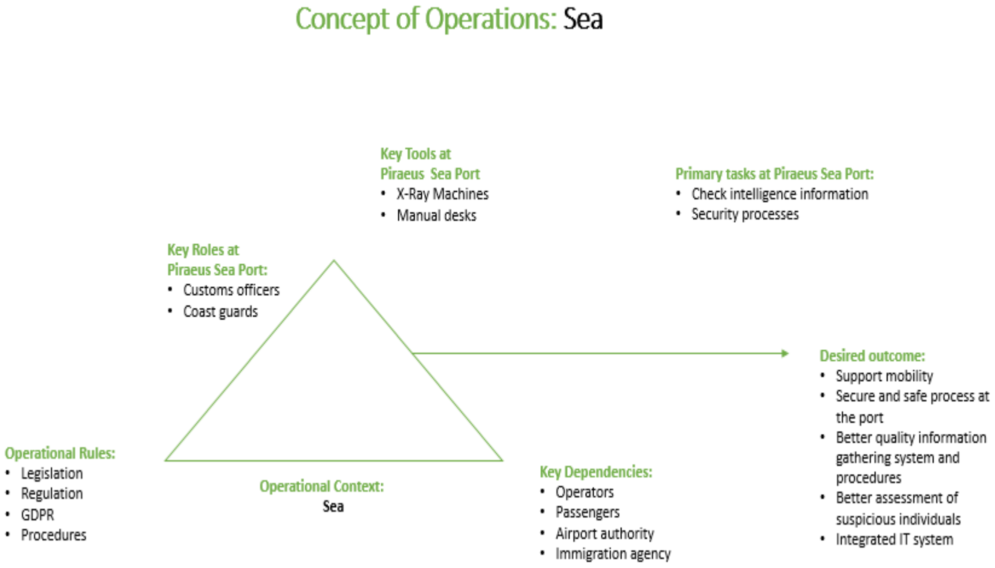


FIGURE 6-4.DRAFT CONOPS SEA BCP

6.3.2 *Threats*

The initial challenges identified for this type of BCP are outlined in paragraph 6.2.2 above. However, further work in this area was conducted as part of TRESSPASS Task 1.1 as well as this Task 1.3. Fuller detail on threats can be found in Deliverable 1.1.[41]As part of a survey of end-users, the following main challenges encountered (as pertaining to a sea border) during day-to-day activities were expressed as follows:

- Lack of (skilled/experienced) staff: 23.53 %
- Time management: 23.53 %
- Lack of information on new regulations / changes in legislation: 17.65 %
- Difficulty to use / adopt new technologies: 11.77 %
- Increasing volume of passengers: 5.88 %
- Threat identification and management: 5.88 %
- Information position: 5.88 %
- Balance between quality assurance and compliance to regulations: 5.88 %

WP2 of the TRESSPASS project (ongoing) is concerned with the development of the risk-based border management concept specifically with regards to BCPs. The first element of this WP is to deliver a method to specify the threat scenarios that the risk-based border management

[40] See footnote 8 above.

[41] *TRESSPASS: robusT Risk basEd Screening and alert System for PASSengers*. D1.1 End-user requirements and needs.

should be weighted and evaluated. Building on the threats described above, three specific sea BCP threats are being developed, as shown in Figure 6-5 below:

Sea BCP Threats	Inbound / Outbound	Actors	Modus Operandi
Entry to country of a potential terrorist acting as a cruise passenger	Inbound	Terrorists / individuals supporting terrorism	Stolen or counterfeit travel documents
Entry of drugs or substances that can be used to make illicit drugs (e.g. precursors)	Inbound	Drugs dealers and drugs mules	Carrying drugs on person, ingesting drugs or concealing in luggage
Illegal entry of a non-European through a Sea BCP	Inbound	Third country citizen	Stolen or counterfeit documents

Figure 6-5. WP2 Sea BCP Threats

The three broad sea BCP vignettes, derived from the threats identified above, are summarised as follows:

- **Vignette 1**. This vignette considers the entry into a country (in this case Greece) of a potential (or actual) terrorist acting as a legitimate cruise passenger. As such, the vignette is similar (although not identical) to Vignette 1 of the air BCP. The actors are, therefore, inbound (in this case) to Greece. The actors are either terrorists, jihadists, insurgents or similar (potentially linked to specific terrorist organisations) or are individuals that are sympathetic to the aims and ideals of such groups. However, unlike Vignette 1 of the air BCP, these actors are not those who are returning 'home' from an area of conflict but are potentially intent on committing an act of terror in Greece. As such, it is likely that these actors will be travelling on stolen or forged documentation (primarily passports and identification cards / papers).

- **Vignette 2**. Vignette 2 is concerned with the entry of drugs or substances that can be used to make illicit drugs (e.g. precursors rather than actual illegal drugs at this stage). For the purposes of this vignette, the actors will be considered as inbound into Greece. It is likely that the actors will be drug smugglers or so-called 'mules'[42] but perhaps operating on a much smaller scale (in terms of quantity of material carried) than, say, cigarette (or drug) smuggling operations across a land border (see Vignette 2 of the land BCP). Given the route of entry into Greece (i.e. via a cruise ship) the illicit goods will only be able to be carried on an individual (including having been ingested) or in accompanying luggage. As such, the quantities of illicit material could be quite small-scale in nature.

[42] A mule or courier is someone who personally smuggles contraband across a border (as opposed to sending by mail, etc.) for a smuggling organization. The organizers employ mules to reduce the risk of getting caught themselves. Methods of smuggling include hiding the goods in vehicles or carried items, attaching them to one's body, or using the body as a container. In the case of transporting illegal drugs, the term drug mule applies. https://en.wikipedia.org/wiki/Mule_(smuggling) (Reference 14).

- **Vignette 3**. This vignette is focused on the illegal entry of a non-EU citizen through the sea BCP, in this case Piraeus Port. As such, the actors are inbound to Greece. This vignette is very similar to the case considered under Vignette 3 of the air BCP. For a large part, such individuals are likely to be from third-world countries (as their point of origin or nationality) but not exclusively so. Given the complex and convoluted routes that many of these people may have travelled, it is not possible to predict from which country they may be travelling from to enter Greece (although it must be assumed that joined the cruise ship from one of the formal post destinations along the cruise ship's route). It is likely that such actors will be travelling on expired, stolen or forged documents (passports and identification cards / papers). There is a small risk that such actors could attempt to enter Greece as (pseudo) ship's crew. Given the large number of crew on a cruise ship (and the wide variety of nationalities making up a particular crew) this is considered to be more likely than individuals posing as aircrew in Vignette 3 of the air BCP.

6.4 Current Sea BCP Infrastructure

6.4.1 *Terminals*

Piraeus cruise port covers an area of 210 acres. At the port there are 11 vessel berths in total; some of them hosting new generation cruise ships of total length more than 300-400m each. There are three air conditioned passenger terminals (Figures 6-6 and 6-7) of 16,000 m2. Within the terminals, facilities and services include: check-in desks; arrivals and departures halls; police and immigration services; customs office; and security services compliant with ISPS[43] code. The details for each terminal are as follows:

- **Terminal A (Miaoulis-Main Terminal)**: Covering some 8000m^2 of ground space, it is less than 50m from the quays serving 2 ships with up to 2000 passengers to check-in simultaneously. The check-in area consists of 36 x check-in counters, 4 x immigration desks and 5x X-ray machines.
- **Terminal B (Themistocles)**: Covering some 6000m^2 of ground space, it has 2 quays of 11m depth, 50m from the terminal which is designed to operate home port calls of mega-cruise ships (4500+ passengers). The check-in area consists of 36 check-in counters, 4 x immigration desks, 6 x X-Ray machines and 2 x luggage belts in the arrival hall-luggage of 1700m^2. There is also an additional check-in / waiting area with 60 x check-in counters which can serve 1500 passengers per hour.
- **Terminal C (Alkimos)**: Covering 2100m^2 of ground space, 20m from the quay it has a capacity up to 3000 passengers and is able to serve 700 passengers per hour with 20 x check-in counters and 3 x X-Ray machines.

[43] The International Maritime Organization (IMO) states that "The International Ship and Port Facility Security Code (ISPS Code) is a comprehensive set of measures to enhance the security of ships and port facilities, developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States". https://en.wikipedia.org/wiki/International_Ship_and_Port_Facility_Security_Code (Reference 15).

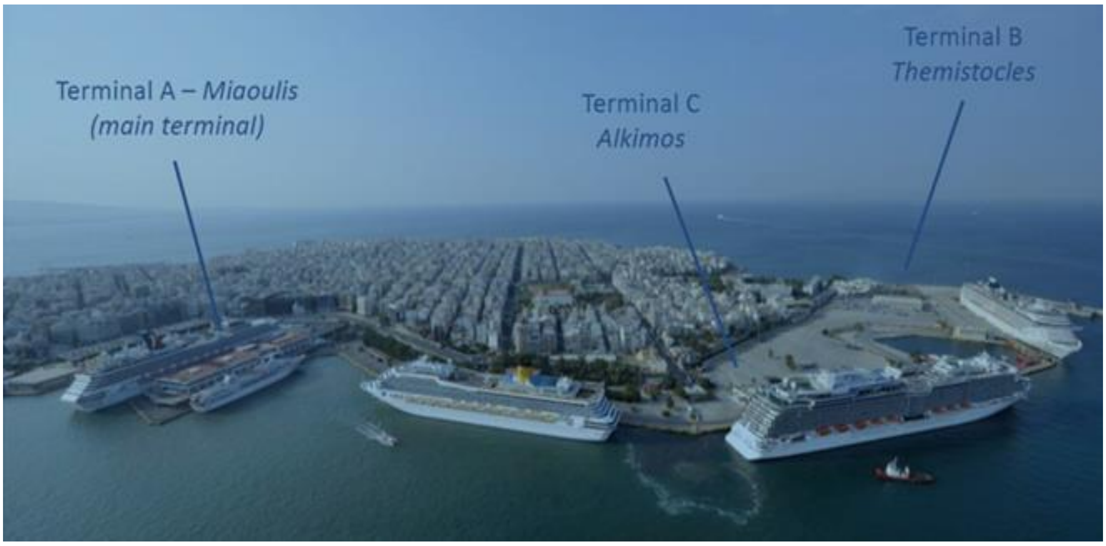


FIGURE 6-6. THE THREE TERMINALS AT THE SEA BCP, PIRAEUS PORT

FIGURE 6-7. TERMINAL B ARRIVAL HALL AT THE SEA BCP, PIRAEUS PORT

6.4.2 *Passengers Arrival to the Terminal*

Passengers arrive at cruise terminal either by buses of travel/ship agents, taxis or their own other means. The luggage arrives at terminal area either by agents' / carriers' trucks (already tagged) or brought by the passengers themselves. All luggage is then submitted to the luggage reception desk where it is tagged on the spot by the receptionist. All tagged luggage is placed on the rolling path by the port's reception staff.

While check-in for the passengers is in progress, luggage items are rolled to the check-in room for X-ray checks before being loaded onto the ship (Figure 6-8).In the case of any suspicious findings, the security officer of the ship is called to decide the next actions. After passing the checks, all cleared luggage is loaded to the ship.

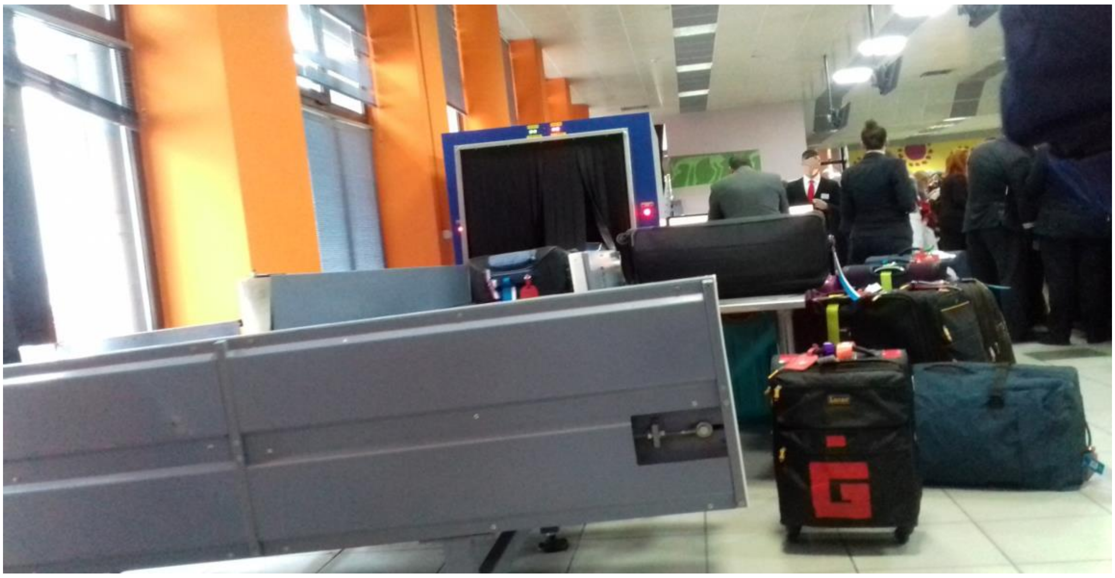


FIGURE 6-8. LUGGAGE SCREENING

6.4.3 *Check-In and Screening*

Passengers, having submitted their luggage to the reception desk or to the rolling bar, then enter the departure area for check-in, carrying only their hand-baggage. Passengers wait for check-in from the point of entrance up to the check-in departure area. A full passengers' list is made available by the shipping carrier, to check-in staff and the police, 48 hrs in advance. Boarding passes for passengers are pre-printed. Check-in staff use mobile devices to scan passengers' passports and check passenger identification and travel information against the pre-loaded passengers' list. Passengers' boarding passes are then issued to passengers.

In cases where no photos of passengers are presented at check-in, these are taken at this stage. Having completed check-in, passengers then queue up for hand-baggage and body x-ray checks (Figure 6-9). These are undertaken for each passenger and any incidents are dealt with by the Coast Guard and the Port Security Officer and recoded in a log book. Having completed the necessary X-ray checks, passengers subsequently pass through passport control procedures carried out by Police Border Authority. Passport control is undertaken for all 'Extra-Schengen' departures. For 'Intra-Schengen' departures, however, only random checks take place or if it is felt required by the authorities.

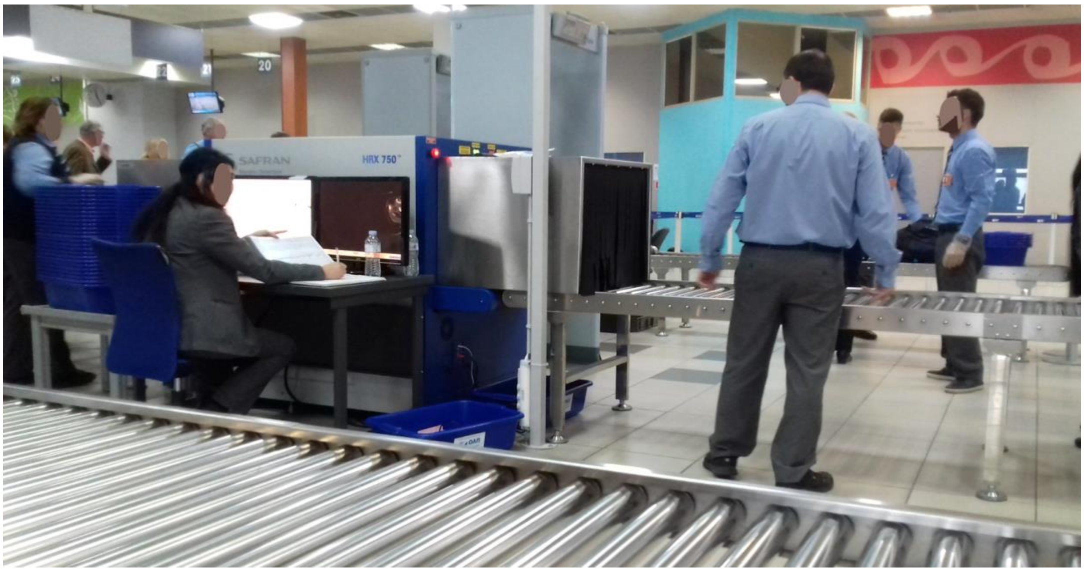


FIGURE 6-9. PASSENGER SCREENING

6.4.4 *Boarding*

Passengers are then cleared to board the ship. Boarding passes for each and every passenger are shown to the ship's security staff, photos are taken and these crossed-check with the check-in information for each passenger. Check-in and boarding is now complete. For an average departure, the whole process from the passengers' arrival at the port until the ship boarding stage, takes less than an hour for the whole group. The time, will however vary depending on the size of the group undertaking these check-in and boarding procedures.

6.5 A Potential TRESSPASS Approach at the Sea BCP

In this potential TRESSPASS approach, the focus is on the introduction of a Maritime-PNR. This should be integrated as well as inter-operated with Airline-PNR, in order to provide a common operating picture based on a shared risk-based screening. It is also intended to employ 'on-the-move' identification and verification technology within the logic of non-disruptive no-gate border crossing. The elements of a TRESSPASS approach may include the following:

6.5.1.1 Passengers Registration

In the first phase, prior to passengers' departures or arrivals from/to a Schengen-port, the cruise liners need to send a PNR-based list of all passengers and crew to the competent authorities both for the outbound and inbound traffic, 24 to 48 hours in advance. In the second phase, after passengers' boarding is completed, cruise liners need to count and weigh the goods and transmit the data together with the facial images taken, either at check-in points in the port or on-board, to the departure or destination Schengen-country's competent authorities. In accordance to the PNR-approach used in the airports, passengers' data related to their luggage information will also be included for further security processing.

6.5.1.2 Risk-based Profile Processing

Competent authorities, exploiting the PNR-data of travelling passengers received from the cruise liner, start the risk-based processing in order to identify whether a traveller poses a threat to the internal security of the EU. This is achieved primarily through a profiling process for each passenger applying various sets of rules used by various competent authorities such as border control and customs authorities as well as comparing their data against a set of databases and open source data (social media etc.).

6.5.1.3 *Profile Alerting/Notification*

Once the profile processing is completed, the alerting system is initiated for all competent authorities including Border and Customs which shall be notified in the case where a traveller poses a threat. The processing result could be transmitted to other MS or third countries at this stage.

6.5.1.4 *Identity verification*

At the border crossing point, all travellers shall be verified based on a non-disruptive facial matching technology, 'on-the-'move. Interoperability concepts with simulated legacy systems, such as ETIAS and EES, will be introduced at this stage, for the biometric matching.

6.5.1.5 *Web Intelligence*

By closely observing the trends on specific related keywords about illicit goods purchases and financial transactions in blogs or discussion forums it is possible to identify threatening developments of imminent smuggling incidents or illegal cash flows. Immediate action is required to avoid probable large scale cross border flows of illicit goods or travellers associated with criminal / terrorist activities.

6.5.1.6 *Expected Benefits of a TRESPASS Approach*

The port operators and border authorities are expecting to utilise better their existing infrastructure and facilities, and improve the overall flow-rate experienced at the sea BCP. Since cruising (compared with other transportation means) is generally considered as a low-risk form of travelling and tourism and the traffic generated at the sea BCP is high (following the docking of a cruise ship), one expected impact of the TRESSPASS approach is the implementation of a non-stop point control for security and border control. The aim is to ensure that no delay is imposed on passengers, similar to the seamless flow concept discussed with respect to the Schiphol Airport. It is also anticipated that the lessons learnt from TRESSPASS will provide a valuable insight into how to handle security issues and design a risk-based passenger checking security design for the new terminal which is within the short-term expansion plans for Piraeus Port.

6.6 Sea BCP – Swim-lanes

To assist with understanding the passenger 'flow' through a particular border-type, the concept of 'swim-lanes' is being developed as part of WP6 (Operational Methods and Acceptability). This is discussed in full at paragraph 4.6 above. An extract of the passenger element of the border crossing (in this case including the interaction with customs) is shown in a swim-lane at Figure 6-10 below:

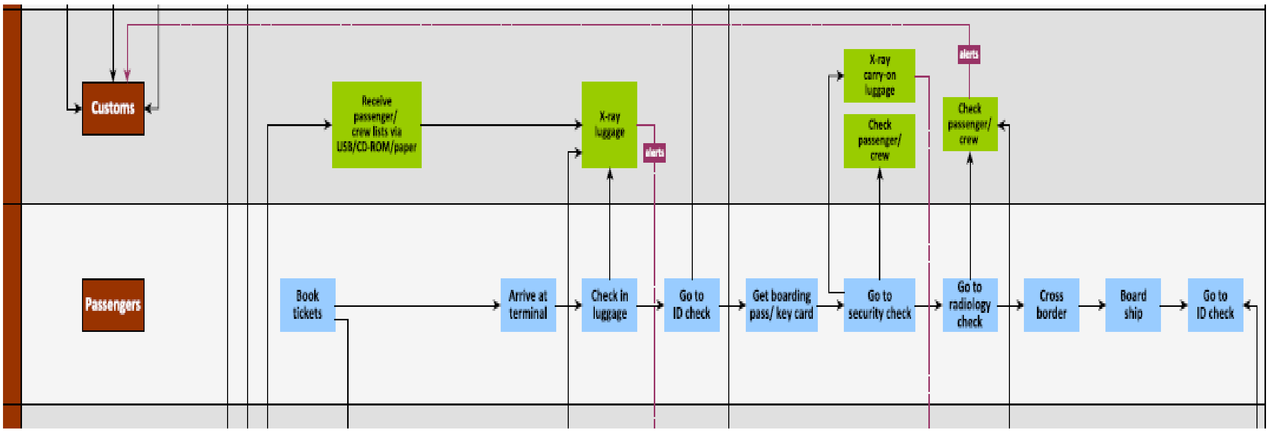


FIGURE 6-10. WP6 EXTRACT OF DRAFT SEA SWIM-LANES – PIRAEUS PORT

7 LAND BCP – VISUALISATION

7.1 Visualisation Concept

The visualisation shown below is a series of screen shots from animations, developed with Unity software[44], to bring the land BCP threats and TRESSPASS approach 'to life'. The scenes depict a combination of the three vignettes (and the associated threats) described in the land BCP scenario (paragraph 5.3 above). The three threats in this case are: the disclosure of national sensitive information or goods; the illegal smuggling of cigarettes; and the illegal trafficking of economic migrants.

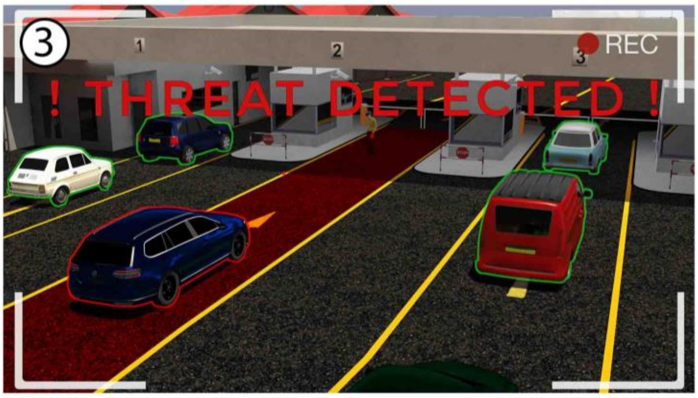
The key element depicted at the beginning of the visualisation is the detection, by the BCP authorities, of the particular threat before the arrival of the vehicle at the BCP. As discussed in paragraph 5.5, such identification could be based on analysis of web-intelligence data and appropriate databases as well as other sources. Such analysis will aim to determine whether a traveller – yet to arrive at the BCP – poses a threat to the internal security of the EU. It is envisaged that this will primarily be achieved through a profiling process for each passenger applying various sets of rules used by various competent authorities such as border control and customs authorities as well as comparing their data against a set of databases and open source data (social media etc.).

The first element of the visualisation storyboard (scenes 1 to 8) deals with the discovery of a traveller attempting to move sensitive information across the border. The second element (scenes 9 to 12) then deals with the smuggling of cigarettes with the third (scenes 13 to 16) depicting human trafficking, with people concealed with in a large commercial vehicle.

[44] Unity is a cross-platform game engine developed by Unity Technologies. The engine can be used to create three-dimensional, two-dimensional, virtual reality and augmented reality games, as well as simulations. The visualisations shown here have been created by RINA Consulting Defence Ltd. digital developers.

1

2
1
2
3


3
1
2
3
REC
! THREAT DETECTED !

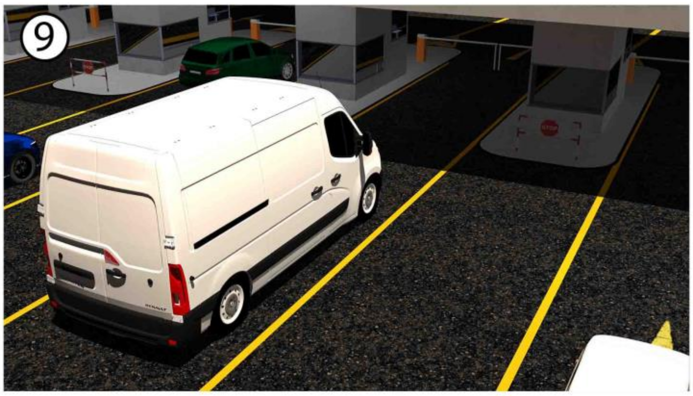
4

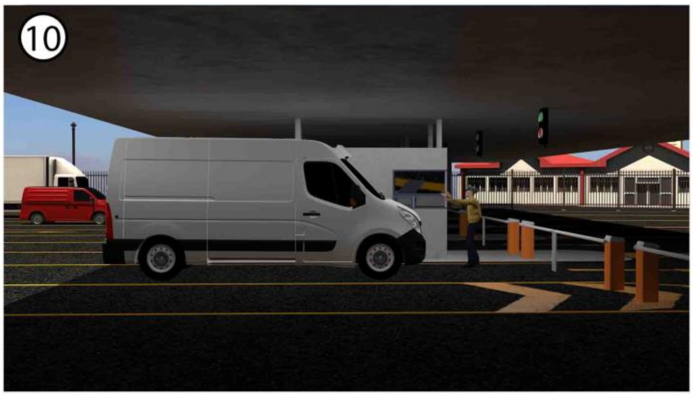
5

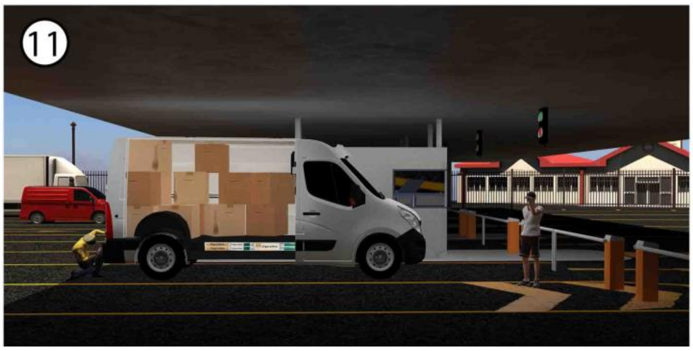
6

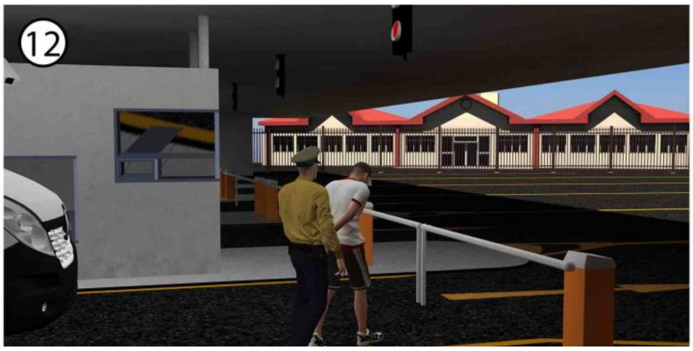
7

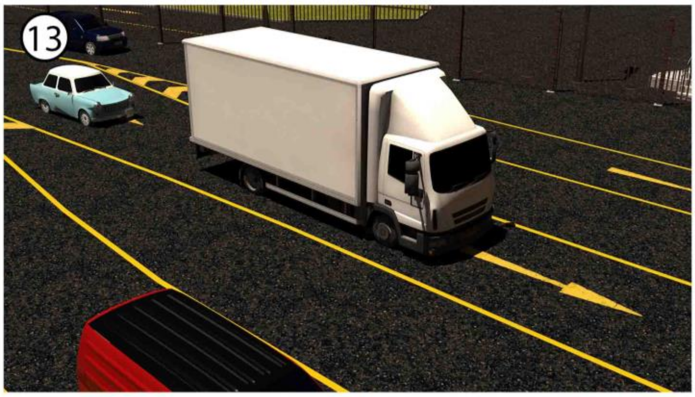
8

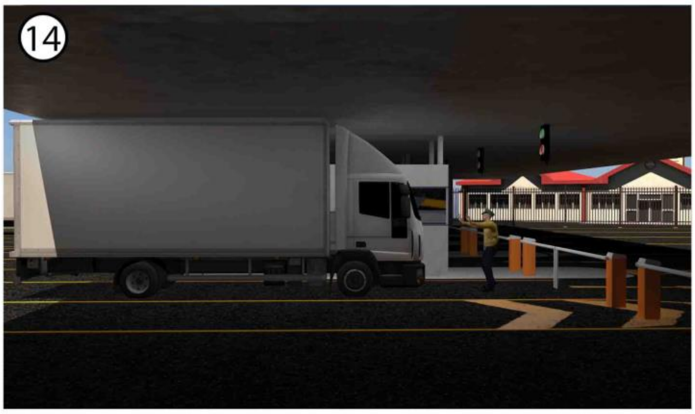

9

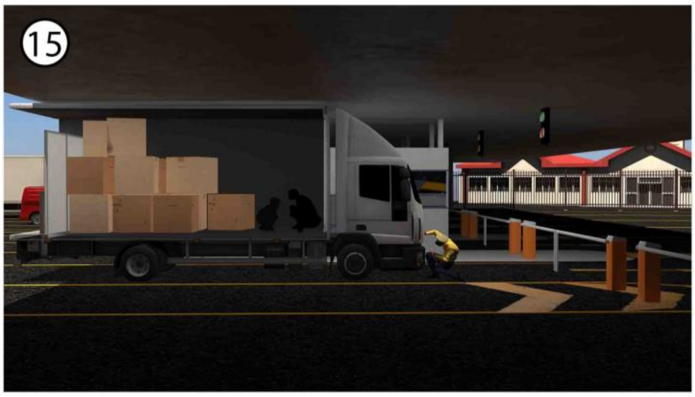

10

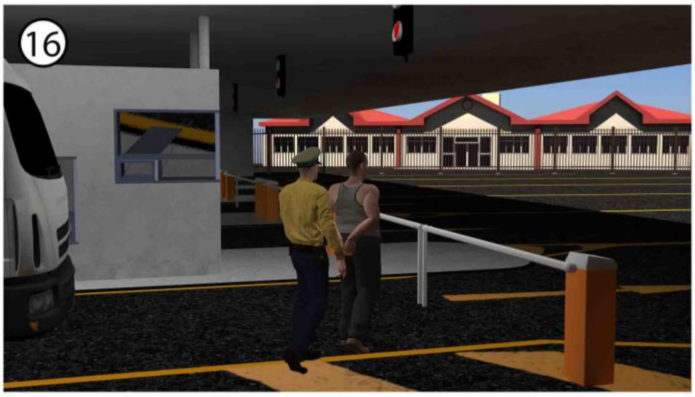

11


12


13


14


15


16

7.2 Visualisation Development

The visualisation shown here is only at a preliminary stage and could be adapted and developed as necessary as the TRESSPASS project continues. This could include the development of visualisations for the air and sea BCP if required. The visualisations could be used, for instance, to complement training aids developed as part of TRESSPASS WP7.

8 References

[1] European Commission. Research Executive Agency. Grant Agreement number: 787120 – TRESSPASS – H2020-SEC-2016-2017/H2020-SEC-2016-2017-2.

[2] European Commission. (2010) *Guidelines for Integrated Border Management in European Commission External Cooperation* [Online]. Available at: https://europa.eu/capacity4dev/ibm-eap/document/1-guidelines-integrated-border-management-european-commission-external-cooperation-european.Accessed April 2019.

[3] SEABILLA Project: *Sea Border Surveillance, Seventh Framework Programme*, Theme 10 – Security, Deliverable Number D11.1, Analysis of maritime surveillance scenarios, gaps and enhancement requirements, dated 28/10/2010.

[4] Frontex. (2012) '*Common Integrated Risk Analysis Model a comprehensive update* (version 2.0)'.

[5] Eurostat statistics explained: *Maritime ports, freight and passenger statistics*. Available at: https://Ec.europa.eu. Accessed May 2019.

[6] Van Dijk, W. (2017) *Passenger experience: Enabling a seamless flow* [Online]. Available at: https://www.internationalairportreview.com/article/75108/seamles-pass-flow/. Accessed March 2019).

[7] iBorderCtrl: *Intelligent Portable Border Control System*, EU H2020 project, 01/09/2016 - 31/08/2019. Available at http://www.iborderctrl.eu/. Accessed April 2019.

[8] PERSONA: *Privacy, Ethical, Regulatory and SOcial, No-gate crossing-point solutions Acceptance*. Available at http://persona-project.eecs.qmul.ac.uk/. Accessed April 2019.

[9] FLYSEC: *Optimising time-to-FLY and enhancing airport SECurity*, H2020-SEC-2015-Project contract: 653879, Innovation Action. Available at http://www.fly-sec.eu/. Accessed April 2019.

[10] XP-DITE: *Accelerated Checkpoint Design Integration Test and Evaluation*, EU FP7 project, 01/09/2012 - 31/07/2017. Available at http://www.xp-dite.eu/. Accessed April 2019.

[11] https://en.wikipedia.org/wiki/Amsterdam_Airport_Schiphol. Accessed January 2019.

[12] Schiphol Traffic Review 2018. Available at http://trafficreview2018.schiphol.tangelo.nl/passengers. Accessed April 2019.

[13] https://en.wikipedia.org/wiki/Piraeus. Accessed January 2019.

[14] https://en.wikipedia.org/wiki/Mule_(smuggling). Accessed January 2019.

[15] The International Ship and Port Facility Security Code (ISPS Code). Available at: https://en.wikipedia.org/wiki/International_Ship_and_Port_Facility_Security_Code. Accessed January 2019.