White paper on standardisation for risk based border crossing points

Dissemination, Exploitation, Communication Activities - WP10

Document Date: 28 January 2022
Dissemination Level: Public

TRESSPASS
robus**T** **R**isk bas**Ed** **S**creening and alert **S**ystem for **PASS**engers and luggage
is funded by the Horizon 2020 Framework Programme of the EU for Research and Innovation.
Grant Agreement number: 787120 — TRESSPASS

Abstract

The goal of TRESSPASS is to develop a comprehensive concept for risk-based border control, and to explore the feasibility and usefulness of this concept. This white paper describes the necessity and opportunities for standardisation based on this concept.

Risk-based border control is about using information per traveller to make the border checks more proportional. This information per traveller can be obtained from a wide range of existing and potential new and innovative systems. Standards are required to make these systems interoperable with each other. Many relevant standards already exist, but not all interoperability aspects seem to be covered.

Altering border checks raises questions about quality and trust. Identifying, describing, assessing, comparing, maintaining and raising quality indicators of (risk-based) border control is another function of standards. Again, relevant standards exist, but there is room for improvement.
The approach for this white paper consisted of four steps:

Step 1: Determine structure: to determine a generic format in which the proposed standards can be presented in a coherent manner.

Step 2: Assess need for standardisation per TRESSPASS element: to assess each TRESSPASS deliverable for elements that might be improved when standardised.

Step 3: Assess consistency and uniformity: to check the resulting structure for internal consistency and uniformity.

Step 4: External validation: to confront the resulting structure with a set of policy options of TRESSPASS sustainability report (roadmap):

> ***The current situation: "Rule-based + more stopping power".*** *Member states can opt for rule-based ('systematic') checks determined centrally (by DG HOME), or for risk-based-but-only-more-stringent ('thorough').*
>
> ***The next step: "Uniform residual risk".*** *DG HOME determines a uniform level of output criterium in the form of maximum accepted residual risk (per threat) that each member state must realise for relevant border related threats. It creates options for member states to find alternative (more efficient, less intrusive, better flowing) risk-based manners to obtain the same residual risk as can be achieved with the rule based approach. A mandatory method for assessing the actual security effectiveness level of border control operations is defined.*
>
> ***A possible state: "Pluriform residual risk".*** *DG HOME determines a framework for international cooperation based on RBBM with mandatory communication between MSs and EC, but refrain from setting a uniform level of accepted residual risk. Individual member states determine the desired level of accepted residual risk for all or for a subset of relevant border related threats. Other MSs adapt where necessary at national BCPs.*

Table 1 describes per element whether it is merely **beneficial, strongly advised** or even **required** to standardise it for each policy option. Even though RBBM is currently already possible, it would still be beneficial to standardise the elements.

For the policy option "the next step" a lot more standardisation is required. For the policy option "a possible state" an **extended level** of standardisation is required for the element "coordinate operations".

TABLE 1 NEED FOR STANDARDISATION PER HIGH LEVEL POLICY OPTION: BENEFICIAL OR REQUIRED. * SOME RECOMMENDATIONS DEPEND ON THE CONDITION THAT THE RESPECTIVE DATA SOURCE IS NEEDED FOR A PARTICULAR INDICATOR TYPE, SUCH AS INDICATORS BASED ON WEB INTELLIGENCE.

System Group: Risk based border control point Methods	The current situation	The next step	A possible state
Risk identification: Design basis threat	Beneficial	Required	Required
Border control ethics	Beneficial	Required	Required
Design risk-based BCP	Strongly advised	Required	Required
Evaluate BCP	Beneficial	Strongly advised	Strongly advised
Profiling and risk indicators	Strongly advised	Required	Required
Operate risk-based BCP	Beneficial	Required	Required
Coordinate operations	Beneficial	Required	Extended standardisation required
Systems	**The current situation**	**The next step**	**A possible state**
Data fusion	Strongly advised	Strongly advised	Strongly advised
Screening	Strongly advised	Required	Required
Detection through human observation	Strongly advised*	Strongly advised*	Strongly advised*
Detection in human physical behaviour	Strongly advised*	Strongly advised*	Strongly advised*
Detection in luggage related behaviour	Beneficial	Strongly advised*	Strongly advised*
Analytics for tracks based on physical behaviour	Strongly advised*	Strongly advised*	Strongly advised*
Detection in online open sources	Strongly advised*	Strongly advised*	Strongly advised*
Detection of biometric face presentation attacks	No	No	No

Detection of indicators of mental constructs in interviews	Strongly advised*	Strongly advised*	Strongly advised*
Simulation	Strongly advised	Required	Required

The policy option “current situation” does not require standardisation. However, TRESSPASS has identified several areas where standardisation would benefit this option.

The policy options “The next step” and “A possible state” do require standardisation, predominantly to provide more certainty about the quality of RBBM, and to a smaller degree also for interoperability purposes.

This work was done as part of the TRESSPASS task 10.1 on “Exploitation strategy and activities”.

Project Information

Project Name	robusT Risk basEd Screening and alert System for PASSengers and luggage
Project Acronym	TRESSPASS
Project Coordinator	National Centre 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 Title	TRESSPASS White paper on standardisation for risk based border crossing points
Work Package reference	WP10 "Dissemination, Exploitation, Communication Activities"
Dissemination Level	Public
Author(s)	Jeroen van Rest (TNO), Naomi Alexander (ICTS), Dirk Stolk (TNO), Manolis Kermitsis (KEMEA), Georgia Lavranou (NUIM), Elisa Orru (ALU-FR), Slavtcho Groshev (CASRA), Aishvarya Kumar Jain (FHG), Enno Geissler (ICTS), Shaike Rozanski (ICTS), Paola Fratantoni (Z&P), Dimitris Kyriazanos (NCSRD)

Table of Contents

1 INTRODUCTION

The goal of TRESSPASS is to develop a comprehensive concept for risk-based border control, and to explore the feasibility and usefulness of this concept. This white paper describes the necessity and opportunities for standardisation based on this concept.

1.1 Background

Risk-based border control is about using information per traveller to make the border checks more proportional. This information per traveller can be obtained from a wide range of existing and potential new and innovative systems. Standards are required to make these systems interoperable with each other. Many relevant standards already exist, but not all interoperability aspects seem to be covered.

Altering border checks raises questions about quality and trust. Identifying, describing, assessing, comparing, maintaining and raising quality indicators of (risk-based) border control is another function of standards. Again, relevant standards exist, but there is room for improvement.

The ability to alter checks based on information per traveller, allows for border control policy options to differ between border control points (BCPs), between member states, and between any combinations of them. For example, if (a collection of) member states face different border-related threats and / or a different flow of travellers, then it may be useful to assess the threat posed by their travellers in a different manner from other member states. This kind of diversification expands on the earlier mentioned questions about quality and trust, and may require additional standards.

1.2 Aim of this document

The aim of this document is to inform TRESSPASS stakeholders about the opportunities that standardisation can create for risk-based border control. By submitting this document to the attention of standardisation groups, policy makers on EU and on national level and of industry groups, the TRESSPASS consortium expects that interest will be raised in the matter of standardisation for risk-based border control.

Standardisation is sometimes seen as an activity strictly done by, or for, industry. This document takes a more generic perspective. Standardisation can also be done for, and by public entities such as border guards or passenger information units and their (public) partners.

The scope of this white paper is strictly related to risk-based border control, i.e. to the use of pre-border information for assessing the risk posed by a traveller in a screening, and to use this assessment to alter the respective check (either first line or second line).

Out of scope are matters strictly related to border surveillance, object (e.g. (air)port) security, front-line policing (at transport hubs), transport (e.g. aviation or rail) security, forensics and to crisis management. However, it is acknowledged that risk-based border control should have interfaces to each of those other domains. For example, data retention should facilitate the a posteriori forensic investigation of crimes occurring at the border.

1.3 Approach

This work was done as part of the TRESSPASS task 10.1 on "Exploitation strategy and activities".

Step 1: Determine structure

The approach for obtaining the contents of this white paper is first to determine a generic format in which the proposed standards can be presented in a coherent manner. Risk-based border control typically requires a system-of-systems approach, and accordingly, the TRESSPASS concept is also of that nature. For standardisation, the implication is that multiple (types of) standards are required.

In 2018, the CEN and the FP7 HECTOS project published a CEN Workshop Agreement (CWA) with guidelines on evaluation systems and schemes for physical security products (CEN, 2018). In this CWA, a generic structure was presented for a collection of standards within a common area (Figure 1). This layered structure enables common aspects to be defined once only – avoiding duplicated effort and potential variations which inhibit mutual acceptance.

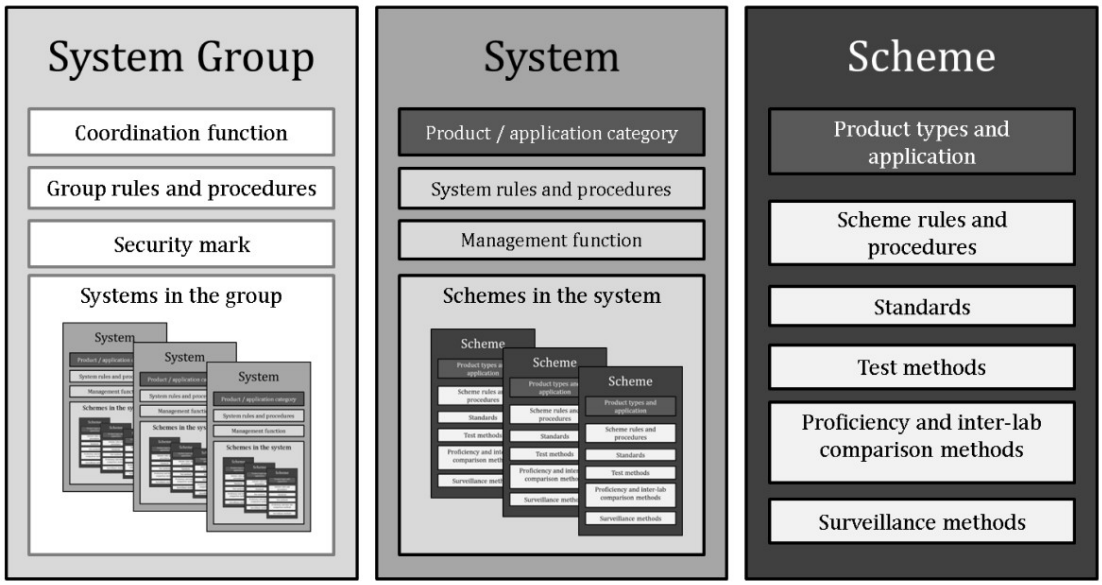

FIGURE 1 CERTIFICATION SYSTEMS AND SCHEMES, KEY BUILDING BLOCKS (CEN, 2018)

A disadvantage of this structure is that it does not have a clear placeholder for the standardisation of *methods*. For example, the method of designing a BCP or of evaluating the stopping power or flowrate of a BCP. These methods are not limited to one system, but rather cover (the use of) multiple or even all systems. Second, the level of Schemes is too much detail for the purpose of this white paper, so that level can be omitted.

Therefore, an adapted version will be used in this white paper as the structuring mechanism for a collection of standards for risk-based border control.

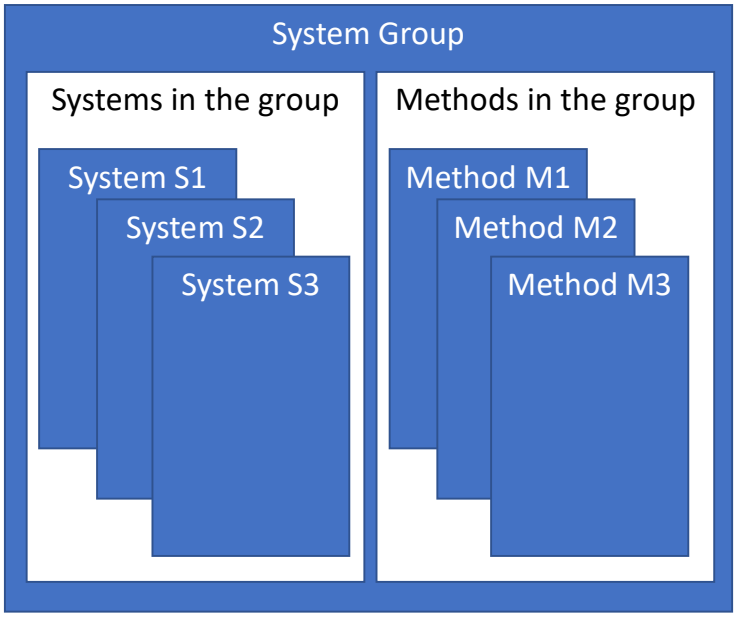

FIGURE 2 STRUCTURING MECHANISM FOR A COLLECTION OF STANDARDS FOR RISK-BASED BORDER CONTROL

The System Group is the top level, which will be focused on a risk-based border crossing point. The System is the level of main (TRESSPASS) components, and the Methods are the main methods that are required during the lifetime of a BCP, and which typically describe how multiple systems are used. Examples are the development of a BCP, or the ethical assessment of a (risk based) BCP.

Step 2: Assess need for standardisation per TRESSPASS element

Second, to assess each TRESSPASS deliverable for elements that might be improved when standardised. The result of this assessment is a projection of TRESSPASS core risk-based capabilities on the structure of Figure 1, and a brief textual description of the potential purpose of the respective aspect-as-a-standard.

Step 3: Assess consistency and uniformity

Third, by checking the resulting structure for internal consistency and uniformity.

Step 4: Confront the resulting structure with a set of policy options

Fourth, by confronting it with a set of policy options, described in the TRESSPASS roadmap (D10.6 from T10.3). This confrontation validates that the proposed standardisation is fulfilling a potential demand (pull) which is grounded in coherent policy options.

The result of this four-step approach is a concept System Group containing multiple Systems and Methods. Standardisation efforts can use that as a starting point for an actual standardisation process.

2 STANDARDISATION IN RISK-BASED BORDER CONTROL

This chapter describes the current situation regarding standardisation in risk-based border control.

2.1 The need for standardisation for risk-based border control

Border control is a specific domain which is typically grouped in the more generic security domain. In 2011 DG ENTR commissioned the SECERCA studies describing the challenges and policy options for improving standardisation in this security domain. Border control was included in this study, and a border-control related example was given of the Regulatory situation at the time:

> *Currently* [2011]*, each of the four automated border control projects in the EU*[1] *has its own requirements, standards and time line. Importantly, interoperability is not asked for, since automated border control is considered as a strategy to achieve a [competitive] advantage for airports. This model is seen to contribute to fragmentation: no EU Regulation; no EU technical specifications but rather proprietary solutions; no published information on the requirements set by the operators; no prescriptions for the need of conformity assessment; and no facilitating role of the EU.* (ECORYS, 2011)

This example illustrates that standardisation is merely a means to an end. If there is no desire for harmonisation or for a minimum quality level, than there may be no need for standardisation. The same study also describes another border control related example where standardisation was indeed applied: biometric identity cards based on an EU norm (based on an ICAO standard) that can be read electronically across all EU countries.

The SECERCA study proceeds by describing two types of security products. Type-1 is for products for which standards exist, albeit different and national levels including national testing centres. Type-2 is for products for which …

> *… the range of policy challenges is wider, since there is often a direct link to issues of EU Internal Security, including ensuring minimum security performance levels (and promoting higher ones) and speeding-up the deployment of new technologies and solutions.* (ECORYS, 2011)

TRESSPASS consortium believes that systems for risk-based border control are clear examples of Type-2 security products, where EU member states would benefit from a common approach to standardisation.

However, noting that borders are a defining aspect of a state, it should be expected that from the point of view of a (member) state, there may be a significant need for differences on the national level.

2.2 Proposed structure of standardisation for risk-based border control

Following the templates offered by (CEN, 2018), this section presents a high level structure for standardisation for risk-based border control. This structure is composed of a set of

[1] The 'Iris' programme in Heathrow, UK; The 'Mysense' project in Schiphol, the Netherlands; The HBG at Fraport, Germany; and The 'Pegase' programme in CDG, France.

Methods which are required during the lifetime of a risk-based BCP, and a set of Systems which provide operational capabilities.

TABLE 2 HIGH LEVEL STRUCTURE FOR STANDARDISATION FOR RISK-BASED BORDER CONTROL

System Group: Risk based border control point
Methods
Risk identification
Assess BCP Ethics
Design risk-based BCP
Evaluate BCP
Profiling and risk indicators
Operate risk-based BCP
Coordinate operations
Systems
Data fusion
Screening
Detection through human observation
Detection in online open sources
Detection in human physical behaviour
Detection in luggage related behaviour
Analytics for tracks based on physical behaviour
Detection of biometric face presentation attacks
Detection of indicators of mental constructs in interviews
Simulation

Chapters 4 and 5 describe these methods and systems respectively. Each of the subsections of those chapters start with a description of the element specifically in relation to RBBM. Then they proceed to describe the following aspects:

- (How) does the element rely on noteworthy pre-existing standards?
- Are there hard requirements for RBBM in standardising this element?
- Are there other benefits for RBBM in standardising this element?

Together, this should give a good starting point for any party that is interested in standardisation of RBBM.

2.3 High level policy options for RBBM

TRESSPASS D10.6 proposed three high level policy options. These options are used to establish the need for standardisation. The three high level policy options are:

The current situation: "Rule-based + more stopping power". *Member states can opt for rule-based ('systematic') checks determined centrally (by DG HOME), or for risk-based-but-only-more-stringent ('thorough').*

The next step: "Uniform residual risk". *DG HOME determines a uniform level of output criterium in the form of maximum accepted residual risk (per threat) that each member state must realise for relevant border related threats. It creates options for member states to find alternative (more efficient, less intrusive, better flowing) risk-based manners to obtain the same residual risk as can be achieved with the rule based approach. A mandatory method for assessing the actual security effectiveness level of border control operations is defined.*

A possible state: "Pluriform residual risk". *DG HOME determines a framework for international cooperation based on RBBM with mandatory communication between MSs and EC, but refrain from setting a uniform level of accepted residual risk. Individual member states determine the desired level of accepted residual risk for all or for a subset of relevant border related threats. Other MSs adapt where necessary at national BCPs.*

In this deliverable, the need for standardisation is motivated per element by its contribution to one or more of these policy options.

3 SYSTEM GROUP "RISK BASED BORDER CONTROL POINT"

The system group level provides an overall common structure and a security mark - a security-specific quality mark indicating that a BCP has been certified according to the Risk based border control point framework.

3.1 Terminology

Proper terminology is the basis for any kind of standardisation. This is described in TRESSPASS D1.2.

A first example of the relevance of proper terminology for risk-based border control, concerns the term "risk-based border control" itself. Risk-based as an adjective can be applied to all sorts of operations, including (air)port control and transport (e.g. aviation) security. Risk-based border control is a very specific type of operations, with a specific legal and societal context, which is different for other (although related) domains.

TRESSPASS D1.2 continues with adopting relevant terminology from pre-existing underlying frameworks, such as ISO 31.000 and CIRAM. ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk. It can be used by any organization regardless of its size, activity or sector. The objective of the Common Integrated Risk Analysis Model (CIRAM) is to establish a conceptual framework to assist Frontex and Member States in the preparation of risk analyses. It promotes a common understanding of risk analysis while simultaneously explaining how this tool can contribute to greater coherence in the management of the external borders. TRESSPASS D1.2 applies the key concepts threat, vulnerability, impact and risk owner to the risk-based border control domain:

> *… a threat is determined by the pressure generated by illegitimate travellers to cross the border at a BCP, including legitimate travellers who illegitimately bring certain goods with them. This means that anything surrounding that traveller, such as his travel group, may be relevant context.* (TRESSPASS D1.2)
>
> *… the vulnerability of a BCP is the lack of quality of the check (the ability of refusing and stopping unauthorised travellers to cross the border at the BCP).* (TRESSPASS D1.2)
>
> *… the impact of a risk is determined by the effects of the pressure generated by illegitimate travellers on the internal security after border checks have been conducted at the external borders.* (TRESSPASS D1.2)
>
> *… the risk owner is the state that owns the BCP, or a collective of states (such as the EU) for its external borders. For the sake of simplicity, this deliverable focusses on the state as risk owner. In concrete risk-based concepts, this will be more refined.* (TRESSPASS D1.2)

TRESSPASS D1.2 also positions risk-based border control vis-à-vis rule based border control. And it specifies the relation between screening, checking, a filter and a border control point.

3.2 Conceptual framework of RBBM

Chapter 5 of D1.2 describes a generic conceptual framework for RBBM. Understanding this framework is essential for understanding the relevance of (standardising) more specific elements. It describes how different organisational capabilities cooperate to create a risk-based BCP (Figure 3).

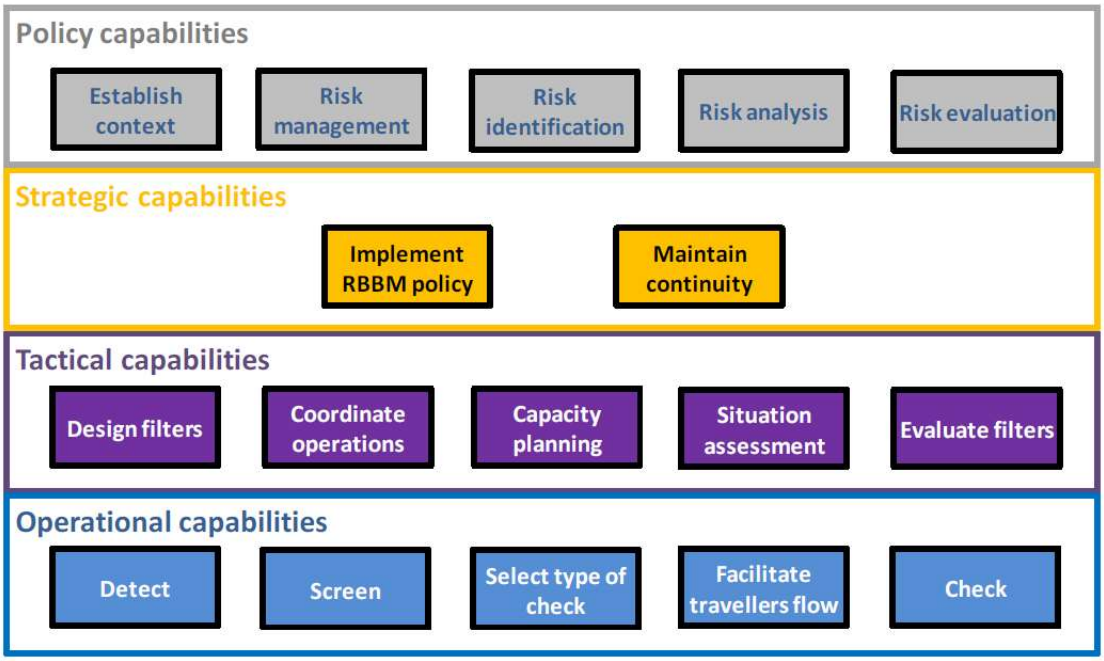

FIGURE 3 RBBM - OVERVIEW OF REQUIRED CAPABILITIES

The top level, grey row with policy capabilities are based on CIRAM and on ISO 31.000. Those are pre-existing standards, so in this white paper there is only limited elaboration on those capabilities. The capability that requires specific attention – and perhaps standardisation, is Risk identification:

> *identifying and describing the various types of threats, and risks caused by travellers who passed the border but should have been refused or stopped at the BCP.*

The second, orange level with strategic capabilities are typical organisational capabilities which can be supported with regular organisation management standards such as ISO 9001 "Quality management systems". Given the generic nature and the existence of these pre-existing standards, this white paper does not elaborate on these capabilities.

The third, purple level with tactical capabilities contain several capabilities that are highly specific for risk-based border control:

- Design filters: *Elaborate the MS's guidelines and instructions for RBBM (e.g. the risks that should be mitigated by border control) into filters (see Section 2.4.10) that should be established for screening, profiling and checking flows of travellers at the various BCPs.*
- Coordinate operations: *Coordinate border control operations between organisations at tactical level within the state and with similar organisations in other countries with respect to the implementation of RBBM at BCPs.*
- Evaluate filters: *Evaluate the results of border control operations at the BCPs and reporting the evaluated results to the strategic level, and* [thereby initiating] *re-designing border control operations and filters if needed*

3.3 Suggestions for marks

The standardisation of a risk-based BCP could be done according to several grades, levels or "marks". For example, a BCP could be marked as "moderate against terrorism – based on situational profiling" based on conformity with relevant elements from this standard.

Inspirated on the TRESSPASS work, several types of marks can be suggested, which are described in the following subsections.

3.3.1 Ethical invasiveness marks

From the ethics side, D9.7 proposes three types of profiling that are increasingly invasive: risk profiling, behavioral analysis and situational checks.

1. Situational risk assessment: this approach means that the intensity and the amount of resources used for checks depends on the situation and "contextual factors that do not relate to individual travellers"[2]. In case of a potentially threatening situation authorities would collect information about a specific situation but not about identifiable individuals.
2. Behavioural analytics: this type is based on behavioural data which is collected during the border checks procedures.
3. Risk profiling: Risk profiling aims to differentiate travellers into risk categories by collecting and analysing [personal] background information.

These three levels could be used as inspiration for marks of BCPs – distinguishing on the basis of these three types of information that they process.

3.3.2 Information domain marks

TRESSPASS D1.2 introduced the concept of the BCP-record and the online-record to complement the PNR-record. In the same manner that the PNR record describes travel legs, the BCP record would describe the traveller's behaviour at a BCP, and the online record would describe his behaviour online. The idea is that information collected from different domains should be named according their source domain which should facilitate transparency and accountability.

These information domains could also be used as inspiration for marks for BCPs – distinguishing on the basis of which domains they would process information from.

3.3.3 Threat marks

Marks could be defined related to specific threats. A BCP could be rated as secure against a certain threat. This could be expanded to also cover bona fide traveller streams.

An obvious and more refined version of this type of mark would relate it to a level of resistance against the threat. For example, a BCP could be marked as "strong against terrorism" based on conformity to relevant elements of this standard.

[2] TRESSPASS D9.7, Framework for assessing direct ethical, legal and societal impact of risk based border screening concepts, November, 2019.

4 METHODS

In the next subsections, each of the methodological elements will be assessed for needs for standardisation. That assessment is structured in three aspects. The last two aspects are directly derived from the three policy options introduced in section 2.3 and described in more detail in TRESSPASS D10.6.

- **Standards used in this element**: A brief description of standards that TRESSPASS used to realise this element, and / or that industry typically uses for this element.
- **Current situation**: Regarding the first policy option "*current situation: Rule-based + more stopping power*", what would be **beneficial** to standardise for the policy option, or perhaps would even be **strongly advised**?
- **Next steps**: Regarding the policy options "*Uniform residual risk*" and "*Pluriform residual risk*", what would be **beneficial**, **strongly advised**, **required** for this element, or is – for this element - even an **extended level of standardisation** required?

4.1 Method: Risk identification

Existing laws and policy documents describe high level threats for which borders must offer protection. The function of this method is to describe these threats in sufficient specific detail so that indicators can be defined in another method.

Standards used in this element: The TRESSPASS DBT method is derived from the DBT method for preventing nuclear proliferation, designed and required by IAEA. It is now a stand-alone method.

Current situation: The capability to specify the threat in sufficient detail must be present, but it does not strictly require standardisation. However, composing a quality DBT is complex. A good standard might help to support trust in border guards being able to do this.

Next steps: Member states need to be able to trust other states to be able to design their threats. Standards provide verifiable processes that generate required trust.

4.2 Method: Assess BCP ethics

The function of this method is to assess the ethical impact of a BCP design. Both of a rule-based BCP design, and of a risk-based BCP design. This facilitates expressing the ethical impact of transitioning from a rule based BCP to a risk-based BCP.

Standards used in this element: A first version of the methodology was presented in TRESSAPASS D9.6,[3] which "identified ethical, legal and societal aspects (ELSA) considered as unintended negative impact of introducing risk based border management. Twelve types of such potential, ELSA related negative impact were specified and grouped in three categories. The classification suggested in D9.6 was lately modified to reflect recent developments at EU level and to incorporate the Guidelines for trustworthy AI, issued in 2019 by the High-Level Expert Group on AI.

Current situation: The capability to assess the ethical impact of BCPs must be present, but it does not strictly require standardisation. On the other hand, the increased complexity of RBBM over rule-based border controls and the different way information is processed for

[3] TRESSPASS D9.6, Framework for assessing direct ethical, legal and societal impact of risk based border screening concepts, November, 2018.

border control, warrant an effort that maintains and generates trust in the ability to assess the ethical impact. Standardisation of this element is therefore strongly advised. Suggestions are described in "Annex B Assess BCP ethics"

Next steps: When member states have the option to relax checks or even to have different risk acceptance levels, the ethical impact becomes more complex to assess. Standardisation will be required for this element.

4.3 Method: Design Risk-based BCP

The function of this method is to be able to design a risk-based BCP according to (among others) specified risk-based performance criteria.

Standards used in this element: Although all BCPs have certain features in common (e.g. aiming at fluid traffic flows while fulfilling access/egress control effectiveness objectives), there is no prototypical BCP and no universally applicable design solution (UNECE & OSCE, 2012).

The Handbook of Best Practices at Border Crossings (UNECE & OSCE, 2012) states that the design goals of a BCP must be derived from national strategy and gives reference principles (UNECE & OSCE, 2012, pp. 142-143, 151).

Risk-based BCPs have been described as having to fulfil conditions related to alignment with Guidelines for Integrated Border Management (IBM), reflection of different modalities, flexibility and adaptiveness to trends and threats, respect for human rights and privacy and assessment of trustworthiness of data (sources).

TRESSPASS holistic risk-based BCP design builds upon the methodology described in XP-DITE D3.10 Airport Checkpoint Design Guide. The application of the XP-DITE methodology within (and beyond) TRESSPASS has, amongst others, the objective of facilitating the leveraging of simulation capabilities for holistic RBBCP evaluation.

Current situation: Obviously, the capability to design a risk-based BCP must be present, but it does not strictly require standardisation. However, the increased complexity of RBBM over rule-based border controls, warrants a coordinated effort that generates trust in the ability to design risk-based BCPs. Standardisation of this element is therefore **strongly advised**.

The overall target of the RBBCP design must be seen in relation to the drivers of the risk management decision-making process, namely meeting performance goals in the areas of effectiveness, flow-rate, efficiency and level of ethical compliance. These goals can be (re-)grouped into performance areas (PA) as main categories of stakeholder interest that consist of specific, measurable (key) performance indicators.

- **Access/Egress Control Effectiveness (ACE):** Requirements related to effectiveness objectives regarding access and egress control of persons and their belongings crossing the border
- **Flow-Related Performance (FRP):** Requirements related to the flow of travellers as they go through the RBBCP
- **Resource Use Efficiency (RUE):** Requirements related to operational resource use and efficiency of the entire RBBCP, including costs and working conditions
- **Traveller Experience and Ethics (TEE):** Requirements related to traveller experience and the mitigation of negative impact on the travelling and non-travelling public from an ethical and legal perspective

A **taxonomy for the relationship between performance area (PA) and key performance indicator (KPI) is proposed**, noting that KPIs in turn consist of more detailed performance

indicators (PIs) that could be defined/measured on component, subsystem and/or system level.

- **Access/Egress Control Effectiveness (PA)**
  - Terrorism detection probability (KPI)
  - Public health hazard detection probability (KPI)
  - Irregular migration detection probability (KPI)
  - Cross-border crime detection probability (KPI)
- **Flow-Related Performance (PA)**
  - Checking time per traveller (KPI)
  - Number of travellers per unit of time (KPI)
  - Waiting time per traveller (KPI)
  - False alarm probability (KPI)
- **Resource Use Efficiency (PA)**
  - Average cost per traveller (KPI)
  - Work conditions (KPI)
- **Traveller Experience and Ethics (PA)**
  - Privacy and data protection (data parsimony) (KPI)
  - Unfair distribution of impact across different social groups (KPI)
  - Restrictions of societal freedoms and liberties (KPI)

The Handbook of Best Practices at Border Crossings (UNECE & OSCE, 2012) states that the design goals of a BCP must be derived from national strategy and gives **reference principles** (UNECE & OSCE, 2012, pp. 142-143, 151):

- Act early
- Target efforts
- Manage bottlenecks
- Maximise depth and breadth of border protection
- Reassure and deter
- Balance security and safety with the need for trade facilitation (secure BCP buildings and zones, single window system, BCP building and ground design conducive to a fast flow of export and import traffic, risk management using fast-track lanes for pre-alerted/pre-declared commercial vehicles and buses, space for bonded warehousing)
- Manage functional and operational aspects (smooth operations, accommodation of long-term growth potential, clear circulation patterns, signs and visibility, minimal uncontrolled areas, simple export and import traffic lanes with constant-flow design)
- Manage productivity (high-quality working conditions for staff, promotion of health and well-being, possibilities for variations in work execution, effective technology integration and working space reliability)
- Manage sustainability (equipment meeting highest industry standards and needing little maintenance, energy-efficient and environmentally responsible facilities)
- Manage BCP image (welcoming public areas reflecting official status and law enforcement function, compatible with regional/local styles, architectural aspects, and existing historic structures and environment, respecting BCP social role for border communities)
- Facilitate joint BCP policy and inspections for customs, immigration and other relevant agencies
- Facilitate regular analysis of BCP performance indicators

While these design principles are arguably equally useful for RBBCPs, the following additional principles gain relevance for RBBCPs:

- Design RBBCP such that it can focus on the four main performance areas (ensuring that the BCP can quickly adapt in case of an incident of any type)

- Compare all travellers against mala fide profiles and only those that do not fit a mala fide profile against bona fide profiles (ensuring that no mala fide traveller can escape a check by mimicking a bona fide traveller and that no capacity is wasted on mala fide travellers).
- Apply invasive screenings and profiles only on travellers that have failed a previous less invasive profile (ensuring that invasive screening is applied selectively and transparently)
- Design RBBCP in such a way that it can be converted easily to a rule-based BCP (ensuring that a fall-back option is readily available)

Next steps: When member states have the option to relax checks or even to have different risk acceptance levels, the quality of a BCP becomes more important, and more important also for partner states. Standardisation will be required for this element.

4.4 Method: Evaluate BCP

The function of this method is to evaluate a BCP design against target performance criteria. Evaluation can be done on different maturity levels[4], expressed in TRL (used by the EC in H2020) or more holistically in Concept Maturity Levels.

Standards used in this element: The methodology that TRESSPASS used was adapted from the Trials Guidance Methodology (TGM), which was designed for crisis management and used in the Driver+ EU project.

Current situation: With a poor evaluation, important weak spots in a BCP design can remain hidden. This undermines confidence and trust in the quality of the BCP. Standardising this element might help to plan and execute high quality evaluations.

There is no strict requirement for the standardisation of this element. However, TRESSPASS collected, tried and validated many "good practices for evaluation" during its three pilots. The TGM methodology has already (before TRESSPASS) been offered to standardisation bodies, which can benefit from the experiences in TRESSPASS.

The PGM method has also been applied by KEMEA in many EU projects and topics (COPKIT, ROXANNE, WELCOME etc.) with the appropriate variations and adjustments made to fit each project's needs and requirements. "Annex C Pilots Guidance Methodology " provides more information about the PGM.

Next steps: The next steps do not create additional needs for standardising this element beyond what is already described for the current situation.

4.5 Method: Profiling and Indicators

The purpose of this method is to specify the mala fide and bona fide indicators and profiles that can be used in a risk-based BCP. In TRESSPASS, this method is called the TRESSPASS Risk Assessment Method (TRAM).

The assessment of the threat level per traveller based on his characteristics, is by definition a type of profiling. There is an intense societal debate about the ethical, societal and legal aspects of profiling, which are all closely related to topics such as data exchange (and thus interoperability) and to effectiveness (and thus to quality). There should be standards for

[4] The TRESSPASS project evaluated the pilots on TRL7 – with real border guards but outside of an operational setting.

profiling, but TRESSPASS found none. Profiling is not specific for risk-based border control. Profiling is applied in forensics, object security, customs, close protection and many domains outside the security domain.

Standards used in this element: There were no existing standards identified that could be used here. The TRAM method is developed from scratch.

Current situation: The capability to specify the risk indicators and profiles in sufficient detail must be present, and given the societal debate about profiling, it is **strongly advised** to standardise exiting good practices.

Next steps: When member states have the option to relax checks or even to have different risk acceptance levels, the ability to do professional profiling becomes more important, and more important also for partner states. Standardisation will be required for this element.

4.6 Method: Operate a Risk Based BCP

TRESSPASS WP6 is concerned with the analysis of operational processes and organisational systems involved in BCP management particularly from the perspective of human factors, but including the interaction between people, technology, rules, resources, and structures, in the context of the overall objectives and motivation for border control operations. These objectives and motivational factors include security, but also economic as well as human rights, and the role that border control plays in the context of societal values.

Standards used in this element: The primary aim of creating a TRESSPASS CONOPS is to provide "*a user-oriented document that describes system characteristics for a proposed system from the users' viewpoint*" (IEEE 2007). In accordance with the original IEEE CONOPS (IEEE, 1998) template format, an 'as-is' baseline system is initially described for the TRESSPASS system, then the desired system changes and justifications for these changes were explained, including any system restrictions or risks. The approach taken to CONOPS within TRESSPASS has also been influenced by the activity system framework developed by Engeström (Engeström, 1987).

Current situation: Operating a risk-based BCP does require a CONOPS which is more flexible and more suited to taking responsibility for design-changes. Standards that support those aspects would be useful but are not strictly required. "Annex D Operate a risk-based BCP" describes the TRESSPASS input for such standards.

Next steps: When member states have the option to relax checks or even to have different risk acceptance levels, the ability to operate a risk-based BCP becomes more important, and more important also for partner states. Standardisation will be required for this element.

4.7 Method: Coordinate operations

An important pre-condition for RBBM is information exchange at various management levels between all involved organisations, which can be considered as one of the core principles of RBBM.

Standards used in this element: TRESSPASS D2.5 describes multinational risk-based cooperation and the standards that this is based on.

Current situation: Standardisation for (inter)national coordination is already being done for the current situation. For example for interoperability by EU-LISA.

Next steps: The policy option “a possible state” requires the coordination between member states per traveller (group) on their checks and residual risk. This is a large step in coordinating operations and would require a large standardisation effort.

5 SYSTEMS

In the next subsections, each of the technical elements will be assessed for needs for standardisation. The structure of these subsections is identical as that of the subsections of the previous chapter.

Most systems rely on existing standards such as for technical communication and interoperability, and for information security. D10.9 chapter 5 contains a detailed overview, and the respective deliverables per component provide all information related to use standards. The sections in this chapter only provide generic and / or particularly relevant information related to (the use of) pre-existing standards to help put the suggestions for new standards into some context.

5.1 System: Data fusion

The function of data fusion for a risk-based BCP is to combine different data sources into risk indicators per traveller. In TRESSPASS, this functionality is provided by the component Data Fusion & Analytics (DFA).

Standards used in this element: Data sources are typically other systems / components, so besides the actual fusion itself, such a component typically relies heavily on low(er) level interoperability standards.

Current situation: For quality purposes, it may be **beneficial** to standardise the type of fusion. For example, certain identifiers such as names are written with different spelling conventions or in shorthand. The name “Alexander” can be abbreviated to Sacha, Alex, Sander and Alexis. It is relevant for the owner of a risk-based BCP to be able to trust that the Data Fusion component is able to fuse data correctly even with such variations.

In addition, with stronger privacy, data protection and information security laws in place, the ability to securely process data from disjunct data sources becomes more relevant. For example, it is useful to be able to compare traveller data to a profile, without having to reveal the traveller data to the owner of the profile. This may become possible using *multi-party computation*. In order for this kind of technology to be scalable, it typically requires a level of standardisation of the underlying data formats.

Data fusion is a type of functionality that is broadly applicable, so any standardisation may benefit multiple application domains.

Next steps: The next steps do not create additional needs for standardising this element beyond what is already described for the current situation.

5.2 System: Screening

The function of the screening system is to assess a risk per traveller (i.e. screening), based on the similarity with predetermined profiles. This includes both similarity with mala fide profiles and with bona fide profiles. In TRESSPASS, this functionality is provided by the Dynamic Risk Assessment System (DRAS).

Standards used in this element: For the DRAS TRESSPASS used generic technical communication and interoperability standards and standards for information security.

Current situation: The risk assessment is a core system for a risk-based BCP. Although there is no hard technical requirement to standardise the screening, the quality of this system is essential for trust that travellers, states and the general population will have in risk-based BCPs. This includes quality aspects such as accuracy, and also aspects such as the prohibition of unethical indicators. It should also include aspects related to transparency, reproducibility, usability and flexibility. It is therefore **strongly advised** to standardise this element.

Standardising the screening would also allow for interoperability between BCPs of one member state, and even between multiple member states. Profiles that are designed for application to outbound travellers of member state A, can then also be applied to outbound traveller of member state B. This in turn improves accountability and learning over multiple member states.

Screening is not specific for RBBM. Standardisation of this system for RBBM can also have benefits for other domains where natural persons are the subject of screening, such as object security, critical infrastructure protection, and travel security.

Next steps: For the policy options were checks are relaxed based on the outcome of screenings, it is **required** that this element is standardised.

5.3 System: Detection of physical traveller behaviour through human observation

Human professional observations of traveller behaviour at a risk-based BCP can contain relevant information for their screening. This information can be manually entered by border guard professionals through GUIs. In TRESSPASS, this functionality was considered for the Security Personnel App (SPA) and Command & Control (C2) application.

Standards used in this element: The TRESSPASS SPA and C2 used generic technical communication and information security standards.

Current situation: If indicators need this data source, then it is **strongly advised** to standardise this element. Of particular attention is (1) that this information is syntactically and semantically interoperable with the screening systems, and (2) the quality of this information in relation to potential biases that may be present in human professionals. Any GUI, including the SPA and the C2, is a potential “backdoor” for unethical and / or ineffective indicators if border guards are allowed to make up (free text) new indicators ad hoc. The SPA and C2 should only offer indicators from a carefully curated set of predefined indicators.

The SPA and C2 could also be useful for facilitating the entry of indicators for other locally relevant operational processes. Such as for customs, for object security of the BCP, for frontline policing (such as pickpocketing), etc.

Next steps: The next steps do not create additional needs for standardising this element beyond what is already described for the current situation.

5.4 System: Detection of physical traveller behaviour through tracking

The physical behaviour of travellers, specifically their walking patterns, can reveal information related to specific indicators. Behavioural patterns that stretches over larger areas or longer periods of time are more difficult and time consuming for human observers to assess. This system therefore uses video footage (e.g. from video surveillance systems) to create tracks from individual persons. In TRESSPASS, the detection of this behaviour is provided by the Visual Tracking Component (VTC).

Standards used in this element: The TRESSPASS VTC used generic video processing, technical communication and information security standards.

Current situation: If indicators based on this data source are needed, then it is **strongly advised** to standardise this element. In particular to standardise the quality parameters to obtain high quality tracks (e.g. resolution, lighting, camera position and orientation), and the processes to keep these parameters in valid technical and operational margins during day to day operations. Specifically the method of *managed analytics* should be proposed as input for a standardisation effort (Den Hollander, 2017).

This element, and related standardisation, would also be useful for other application domains.

Next steps: The next steps do not create additional needs for standardising this element beyond what is already described for the current situation.

5.5 System: Detection in luggage related behaviour

The way travellers handle their luggage can reveal information related to specific indicators. The function of this system is to create tracks from tagged pieces of luggage, thereby also creating tracks from people that carry that luggage. In TRESSPASS, this functionality is provided by the component Travellers and Luggage Tracking Component (TLTC).

Standards used in this element: Several low level communication standards are used for this element. A strategic choice in line with a near future global standard adoption was the use of passive UHF RFID for luggage tracking.

Current situation: Risk model integration include detecting the location of the carry-on luggage for purposes of (i) abnormal movement correlation and inconsistencies at security checkpoints and (ii) unattended luggage automated recognition alert. In favour of the exploitation potential are standardisation developments, IATA announced in 2019 its formal support to the global deployment of RFID for baggage tracking. The IATA Annual General Meeting also called for the implementation of modern baggage messaging standards to more accurately track passengers' baggage in real time across key points in the journey. Towards this global standard RFID-embedded, tamper-resistant luggage items (referred also as Smart Baggage in IATA's 2017 report) already exist and are expected to be more widely deployed in the near future.

Next steps: Monitoring and adopting Smart Baggage and RFID-embedded global standard luggage developments.

5.6 System: Analytics for tracks based on physical behaviour

The two systems "Detection in human physical behaviour", and "Detection in luggage related behaviour" generate tracks, which contain a specific kind of useful information, but which are by themselves not indicators. The function of the Real Time Behaviour Analytics (RTBA)[5] is to detect relevant information in these tracks.

Standards used in this element: No standards have been used for this element.

[5] In TRESSPASS, the RTBA focused only on the tracks created by the VTC. Luggage related tracks can be analysed in the same manner, and by combining the two types of tracks, more functionality can be obtained.

Current situation: For useful risk indicators, a minimum quality level of tracks may be required. The definition of tracks may also be standardised, which allows for interoperability between tracking components such as the VTC and TLTS and the RTBA.

Tracks can contain information that is not relevant for the purpose of RBBM. In principle, this concern should be covered by existing laws, such as the LED and the GDPR. Standardisation may be useful to address these concerns more direct and specifically for tracking.

This element, and related standardisation, would also be useful for other application domains.

Next steps: The next steps do not create additional needs for standardising this element beyond what is already described for the current situation.

5.7 System: Detection in online open sources

Travellers can publish relevant information on online open sources, such as social media. The function of this system is to detect relevant information in such sources. In TRESSPASS, this functionality is provided by the component Web Intelligence (WI).

Standards used in this element: Large social media platforms are de facto standards, which have to be followed in order to efficiently extract information.

Current situation: If indicators based on this data source are needed, then it is **strongly advised** to standardise this element. Personal open source data, such as social media, is semi-structured data. It is difficult to obtain relevant information from such data. In addition, this kind of analysis is ethically sensitive. Public acceptance of this kind of analysis may rely on standardisation of the analysis such that sufficient quality and (privacy preserving) controls can be built-in.

This system, and related standardisation, would also be useful for other application domains.

Next steps: The next steps do not create additional needs for standardising this element beyond what is already described for the current situation.

5.8 System: Detection of biometric face presentation attacks

RBBM relies on linking information to the proper traveller. Any attacks that frustrate this, such as through presentation attacks in face recognition, must be mitigated. The function of this system is to detect presentation attacks in facial biometrics. In TRESSPASS, this functionality is provided by the component Thermal Counter Spoofing Sensor (TCSS).

RBBM requires a level of certainty that a traveller is recognized between different screening and checking steps. Note: it does *not* require the actual identity of the traveller. In other words, RBBM can also be used to screen for, and check for identity fraud.

Standards used in this element: The TCSS used generic technical communication, video processing and information security standards.

Current situation: No additional standardisation is required.

Next steps: The next steps do not create additional needs for standardising this element beyond what is already described for the current situation.

5.9 System: Detection of indicators of mental constructs in interviews

Just like in rule-based BCPs, travellers that may pose a risk will be led to a check. This check can take the form of an interview with a human professional border guard. They can happen

directly at the border in a kiosk or desk ("1st line"), or in a separate office ("2nd line"). In RBBM these checks are altered based on the outcome of screenings.

This system supports the use of the actual information obtained during screenings in such interviews, and also to detect additional indicators during the interview itself. In TRESSPASS, the second part of this functionality is provided by the component Interview Support System (ISS)[6].

In that interview, the human security/authority officer ('Interviewer') applies interviewing techniques. Some of these existing techniques currently rely on the human assessment of behavioural clues. The application of these techniques can be biased, tiresome and selective. It is also less traceable if only done by humans.

TRESSPASS developed an interview support system (ISS) that helps registering and presenting selected clues in a transparent and consistent manner. It is meant to be used in line with the concept of operations and training that border guards have for conducting interviews. It would typically be used in conjunction with a view on the information that caused the traveller to be led to the interview, so that alternative explanations for mala fide indicators can be easily verified. The Interviewer uses this information to choose lines of questioning. For example by helping him in his assessment if a traveller is telling the truth. A difference from the other TRESSPASS components is that ISS is not connected to the DRAS, so it does not contribute to the classification of travellers or their behaviours into threats.

Standards used in this element: The TCSS used generic technical communication, video processing and information security standards. Border guard operational staff is trained in conducting 1st and 2nd line interviews. The existence of these trainings – not their contents – were taken as starting point for TRESSPASS. There do not appear to be international formal standards for these interviews that can be used as basis for the registration of behaviour cues.

Current situation: In a BCP -risk-based or not- all mala fide travellers will be directed towards interviews, with the expectation that the interview provides a more thorough revelatory function. Because of quality and ethical concerns, it is **strongly advised** to standardise this element. The quality of this system is essential for trust that travellers, states and the general population will have in risk-based BCPs. This includes quality aspects such as accuracy, and also aspects such as the prohibition of unethical indicators. It should also include aspects related to transparency, reproducibility, usability and flexibility. In particular, there should be standardisation covering:

- the information protection and privacy preserving aspects of an interview support system
- the link between
    - mental constructs (emotions, cognitive load, etc.),
    - observable physiological, communication and behavioural cues, and
    - their relevance for modern interview strategies.

This system, and related standardisation, would also be useful for other application domains.

Next steps:

The next steps do not create additional needs for standardising this element beyond what is already described for the current situation.

[6] The initial name for the Interview Support System was the Multimodal Communication Analysis Tool (MMCAT). The Interview Support System (ISS) is later added as a more descriptive name.

5.10 System: Simulation

Simulation of (elements of) a risk-based BCP allows for evaluating alternative scenarios and configurations. This fulfils different functions in the context of a risk-based BCP:

- To evaluate the effects of a potential (risk-based) BCP. For example vis a vis an (equivalent) rule based BCP.
- To evaluate the effects of alternative travel flows. Such as an increase in (irregular) migration.
- To evaluate the effects of a new data source / technology (e.g. the contribution of physical behaviour detection, or of web intelligence)
- To generate training material (e.g. effects of different configuration) for end users.

Simulation is essential for generating and maintain trust in RBBM. In TRESSPASS, this functionality is provided by the components iCrowd and the FHG Simulator.

Simulation is a very important tool to evaluate the ex-situ performance of a risk-based BCP. Given that the RBBM concept of TRESSPASS could sometimes pose complex understanding challenges to the stakeholders, simulation is a tool that could be used for the training. On the other hand, it is also a tool that takes the data input from stakeholders and provides a relevant performance output. Since the data belong to the stakeholders, it is natural that they understand it, and the output is provided in the format (for example, queue length, waiting time, service time, effectiveness, false alarm rates, etc.) which is understandable to the stakeholders. This whole process decorrelates the need for the stakeholders to completely understand the RBBM concept (still a basic understanding is needed) and rely on the simulator to evaluate the BCP performance.

The Simulator developed by Fraunhofer (MCBCCS+MCBCEP) is fundamentally different than the simulator developed by NCSRD (iCrowd). Fraunhofer's simulator implements all the core functionalities of TRESSPASS (screening and checking components, data fusion, TRAM, traveller's profile, and decision mechanism). Essentially it duplicates the whole process of RBBM. Another important function of this simulator is that it has a very steep learning curve, and with very minimal training stakeholders can use this simulator to design their own BCP without the involvement of any developer. To keep all these functionalities at the core, some statistical approximations were taken to keep the design process simple and computation time low. At the moment simulation of a simple BCP takes around 1-2 minutes.

Standards used in this element: Both TRESSPASS simulators used generic communication protocols. The FHG simulator uses existing standard programming libraries to simulate the traveller flow. It uses the discrete event simulation method along with Monte Carlo techniques to simulate the flow process. The FHG simulator simulates all the core functionalities of TRESSPASS. If those elements change (due to standardisation), it will become essential to change their corresponding models in the simulation.

Current situation: It is strongly advised to standardise the simulator's inputs, processing and outputs in order to raise trust in the outcome of simulators.

(MCBCCS+MCBCP)'s output quality relies on the quality of the input data. Standardisation of the input data will drastically increase the quality of the generated performance output. One of the most essential data for the RBBM is the traveller profiles. Having standard traveller profiles for each kind of threat is not only essential for the RBBM but also for the accuracy of the simulator.

Standardising the way specific types of components are simulated, allows for certainty about the quality (e.g. representativeness) of the simulation for reality. It also allows for

interoperability between simulators, e.g. that focus on different performance areas. For example, the iCrowd simulator focusses on visualising in 3D flow-related performance indicators. The FHG simulator focusses (in a more abstract manner) on all four performance areas. Making these two components interoperable, e.g. in input parameters and in the KPI's that they calculate, it becomes more feasible to validate their results against each other.

This system, and related standardisation, would also be useful for other application domains. In fact, both simulators in TRESSPASS have their origin in other domains: iCrowd in airport security, and the FHG simulator in aviation security. To simulate the flow at a BCP it is essential to couple simulators with all the other process which precedes and proceeds the border control process. FHG's simulator could be used to design an isolated border control process and can also integrate with all the other processes like check-in, luggage screening, aviation security, waiting, random selection process, etc. All these were for example already taken into account during the modelling of Maritime BCP. So, the standardisation of the data collection process and flow modelling of the whole traveller process could drastically increase the performance measure to all the other application domains.

Next steps: For the next steps, simulation is essential. In a situation where member states have the liberty to opt for risk-based BCPs, they need high quality simulation tools to assess the quality of their risk-based BCPs and show how they compare to equivalent rule based BCPs under various circumstances.

6 CONCLUSIONS AND REFLECTION

This white paper describes the TRESSPASS results that may be useful for risk-based border control when standardised. Table 3 describes per element whether it is merely **beneficial, strongly advised** or even **required** to standardise it for each policy option. Even though RBBM is currently already possible, it would still be beneficial to standardise the elements.

For the policy option "the next step" a lot more standardisation is required. For the policy option "a possible state" an **extended level** of standardisation is required for the element "coordinate operations".

TABLE 3 NEED FOR STANDARDISATION PER HIGH LEVEL POLICY OPTION: BENEFICIAL OR REQUIRED. * SOME RECOMMENDATIONS DEPEND ON THE CONDITION THAT THE RESPECTIVE DATA SOURCE IS NEEDED FOR A PARTICULAR INDICATOR TYPE, SUCH AS INDICATORS BASED ON WEB INTELLIGENCE.

System Group: Risk based border control point Methods	The current situation	The next step	A possible state
Risk identification: Design basis threat	Beneficial	Required	Required
Border control ethics	Beneficial	Required	Required
Design risk-based BCP	Strongly advised	Required	Required
Evaluate BCP	Beneficial	Strongly advised	Strongly advised
Profiling and risk indicators	Strongly advised	Required	Required
Operate risk-based BCP	Beneficial	Required	Required
Coordinate operations	Beneficial	Required	Extended standardisation required
Systems	**The current situation**	**The next step**	**A possible state**
Data fusion	Strongly advised	Strongly advised	Strongly advised
Screening	Strongly advised	Required	Required
Detection through human observation	Strongly advised*	Strongly advised*	Strongly advised*
Detection in human physical behaviour	Strongly advised*	Strongly advised*	Strongly advised*
Detection in luggage related behaviour	Beneficial	Strongly advised*	Strongly advised*
Analytics for tracks based on physical behaviour	Strongly advised*	Strongly advised*	Strongly advised*
Detection in online open sources	Strongly advised*	Strongly advised*	Strongly advised*

Detection of biometric face presentation attacks	No	No	No
Detection of indicators of mental constructs in interviews	Strongly advised*	Strongly advised*	Strongly advised*
Simulation	Strongly advised	Required	Required

The policy option “current situation” does not require standardisation. However, TRESSPASS has identified several areas where standardisation would benefit this option.

The policy options “The next step” and “A possible state” do require standardisation, predominantly to provide more certainty about the quality of RBBM, and to a smaller degree also for interoperability purposes.

REFERENCES

CEN, 2018, CEN Workshop Agreement CWA 17260

den Hollander, R. J., Bouma, H., van Rest, J. H., ten Hove, J. M., ter Haar, F. B., & Burghouts, G. J. (2017, October). Automatically assessing properties of dynamic cameras for camera selection and rapid deployment of video content analysis tasks in large-scale ad-hoc networks. In Counterterrorism, Crime Fighting, Forensics, and Surveillance Technologies (Vol. 10441, p. 1044108). International Society for Optics and Photonics.

ECORYS, 2011, Security Regulation, Conformity Assessment & Certification (SECERCA) Final Report – Volume I: Main Report

Engeström Y. 1987. Learning by expanding: An activity-theoretical approach to developmental research (Helsinki: Orienta-Konsultit)

European Commission. (2016). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL (COM(2016) 205 final) - Stronger and Smarter Information Systems for Borders and Security. https://www.eulisa.europa.eu/Newsroom/News/Documents/SB-EES/communication_on_stronger_and_smart_borders_20160406_en.pdf

EU INFORMATION SYSTEMS Security and Borders. (2019). https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171212_eu_information_systems_security_and_borders_en.pdf

EUCISE2020. (n.d.). Retrieved July 6, 2020, from http://www.eucise2020.eu/

IEEE Computer Society, March 19, 1998, IEEE Guide for Information Technology—System Definition—Concept of Operations (ConOps) Document (IEEE Std 1362-1998).

Institute for Electrical and Electronics Engineers, IEEE Guide for Information Technology (2007). System Definition — Concept of Operations (ConOps) Document, Software Engineering Standards Committee of the IEEE Computer Society.

UNECE & OSCE (2012). Handbook of Best Practices at Border Crossing -- A Trade and Transport Facilitation Perspective. Retrieved from http://www.unece.org/fileadmin/DAM/trans/bcf/publications/OSCE-UNECE_Handbook.pdf

Voogd, J., Janssen, H. (2016). Airport Checkpoint Design Guide, XP-DITE ("*Accelerated Checkpoint Design Integration Test and Evaluation"*)

LIST OF FIGURES

LIST OF TABLES

ANNEX A RISK IDENTIFICATION: DESIGN BASIS THREAT

Existing laws and policy documents describe high level threats for which borders must offer protection. These threats must be described in sufficient specific detail so that indicators can be defined in a next step. These threats can be described by applying the so-called Design Basis Threat at BCPs (DBT@BCP method) which has been developed in TRESSPASS. In this method threat scenarios are defined to enable risk-based border control of travellers, including their luggage and/or vehicles, at border crossing points.

For the development and the use of the DBT@BCP it is required that:

- All relevant stakeholders are involved in its development and maintenance ensuring a sound basis and trust.
- Consensus is reached among the stakeholders on the risks to be mitigated.
- It does not violate legal or ethical constraints.
- The set of discriminating characteristics of the various actors and their modi operandi is as complete as reasonably possible.
- It is flexible with respect to changes in (types of) risks, the various characteristics of threat scenarios, and changes in modi operandi.
- It can be applied and maintained at any (type of) BCP of the EU Member States for travellers entering or leaving the EU area.
- The results can be exchanged with other BCPs.

In the context of RBBM at a BCP, a threat is considered as an external phenomenon that endangers one or more objectives of the EU and/or individual Member States. To attain these objectives, BCPs are established to manage EU's external borders. In respect to the mitigation of threats, the goal of border management is the "protection of internal security and management of migration flows to prevent irregular migration, related crime and other cross-border crime" (European Commission, 2010, p.20). Hence, the overall threats that should be mitigated by the BCPs are: (1) irregular migration, (2) cross-border crime, and (3) other threats that endanger internal security. In the TRESSPASS DBT-Method, these kind of threats are formulated at (inter)national policy level (i.e. EU-level and/or MS-level). Therefore, these can be regarded as societal threat categories that are partially mitigated by the border management practices of BCPs. Within each of the societal threat categories so-called threat scenarios can be formulated. Threat scenarios are plausible events at individual BCPs that (potentially) can lead to endangering one of the objectives of the EU and/or individual MS. Hence, these threat scenarios contain the elements of risks, which are defined as the result of the likelihood of a certain event to occur and its impact on the risk-owner (i.e. the state that owns the BCP). The ways in which threat scenarios will unfold, depend on the modi operandi (MO) that are used by malicious or illegitimate persons in their attempt to circumvent border control at a BCP. The selection of a certain MO concerns more or less deliberate decisions with respect to documentation, way of travelling, possessions and predetermined behaviour. Table 4 provides an overview of the above mentioned aspects in relation to a DBT, including an example to illustrate the relationship between these aspects.

TABLE 4 KEY ASPECTS IN RELATION TO TRESSPASS DBT

Key aspect	Description	Example
Societal threat category	Threat that the EU and/or individual MSs want to mitigate by means of effective border management	Cross-border crime
Threat scenario	Event that possibly leads to societal threats and therefore needs to be mitigated by border control at BCPs	Drugs smugglers entering the EU by crossing the external border at a BCP
Modus operandi	The way in which a malicious traveller attempts to cross the border at a BCP	A drugs smuggler hides drugs in his luggage in some inventive way and uses falsified travel documents when he arrives at the BCP

The development of the DBT@BCP within the RBBM concept consists of seven steps.

Step 1 – Assessment of stakeholders

This step should be coordinated at (inter)national policy and strategic level and conducted in close cooperation with the tactical and operational level of the involved BCP. It has to result in an overview of stakeholders that should be involved, including a description of their roles and responsibilities in developing and maintaining the DBT@BCP. These roles and responsibilities should be in alignment with international and national legislation.

Aspects that should be considered are for instance:

- The existing legal and regulatory framework;
- The responsibilities regarding the coordination of the DBT@BCP development;
- The responsibilities for formalisation of the DBT@BCP;
- The responsibilities for implementation of the DBT@BCP;
- The responsibilities for maintenance of the DBT@BCP;
- Provision of intelligence, information, and data to support the development;
- Threat assessment; and
- Facilitating, supporting activities.

Step 2 – Assessment of societal threat (sub-)categories

In this step it is assessed which kind of societal threat categories should be mitigated by border control at BCPs. This is a broad outline of relevant threats without much details: it is a general description of the societal threats including the description of the sub-categories.

This step is typically taken at (inter)national policy level, while decisions will be communicated to the other governance levels. This governance level is identified as the 'risk owner' for border management and therefore is obliged and accountable for formulating the societal threat categories that should be addressed at the BCPs. The resulting overview of threats that should be mitigated will be quite general and invariable.

In support of this step it is necessary to identify what information is required to determine what the societal trends are inside and outside the EU to make a grounded judgement about the threat categories that are worthwhile to mitigate. This can be done by identifying and making use of proper data sources (e.g. those from trusted partners, but also from open

sources). Consequently, the collected information can be analysed before final decision on what the relevant threat categories are.

To illustrate, the current objectives of Border Management (based on the Schengen Border Code) can be regarded as threat categories – or can be used as starting-point for discussion of assessing societal threats – that should currently be accounted for:

- Preventing threats to national internal security (and safety); e.g. crisis situations caused by terrorist attacks (security) or a pandemic outbreak caused by infected people from abroad (public health).
- Preventing irregular migration.
- Preventing cross-border crime: Human trafficking, Drug trafficking, Firearm trafficking, etc.

Step 3 – Assessment of threat scenarios

In this step for each of the relevant threat categories, specific threat scenarios are determined. In fact, this step concerns a more detailed specification of the sub-categories determined in step 2. This is achieved by identifying plausible threat scenarios that concern illegitimate entry or leave of Europe of persons and their goods/vehicles at the BCP.

Step 4 – Assessment of the relevance of the identified scenarios

Three criteria can be applied to assess the relevance of the threat scenarios that have been identified in the previous step:

1. The likelihood that the specific threat scenario occurs at the BCP;
   - *Scored on a 5-point scale: 1 = (almost) never, 2 = yearly, 3 = monthly, 4 = weekly, and 5 = daily.*
2. The severity of the threat scenario from the perspective of the EU/MS (i.e. from a national/societal perspective);
   - *Scored on a 5-point scale: 1 = very low, 2 = low, 3 = medium, 4 = high, and 5=very high; when scoring one can think of aspects such as (potential): number of victims or wounded people, economic loss/costs, Europe's or the country's reputation and social unrest.*
3. The expectations about the relevance of the threat scenario in the (near) future;
   - *options are: rising, constant and declining.*

Based on these criteria it can be determined what the relevance of the threat scenario is within the context of the BCP. This concerns an expert judgement through which it is argued to what extent the scenario is applicable within the context of the BCP. It can also be regarded as input for the (risk-based) decision concerning the mitigation measures that should be taken to address the threat scenario. This involves a weighing of the different elements of a risk (i.e. likelihood and effect of the threat), and an estimation of the extent in which these elements are expected to alter in the (near) future.

Step 5 – Determination of the desired detection rate of threat scenarios

There are several factors that determine the desired detection rate of the BCP's filter[7]. In generic terms, these are the initial risk, the (expected) performance of existing check performance, the consequential current residual risk, and the risk acceptance of a risk owner

[7] The filter of a BCP is the combination of screening and checks of travellers, including their goods and/or vehicle, to cross the external border at the BCP. The detection rate is the probability that an attempt to illegitimately cross the border, is detected.

(i.e. the MS). The current residual risk, as expressed by the likelihood and the severity in the previous step, is the consequence of the initial risk which is mitigated by existing filters.

To make this desired detection rate explicit, it can be scored on a 5-point scale: *1 = small deterioration is admitted, 2 = no improvement needed, 3 = small improvement needed, 4 = moderate improvement needed, and 5 = big improvement needed.*

Step 6 – Expressing the information needs

Once the threat scenarios have been identified, it is important to express the information needs to recognise certain threat scenarios at the respective BCP. In practice, this task will be carried out in close collaboration with the tactical and operational level as they are responsible for construing the risk profiles of malicious travellers. However, this is already a strategic choice in respect to the type of information that border officials want to collect systematically, and therefore beneficial to already identify in the DBT@BCP.

In deliverable D1.2 has been described that there are four travellers' aspects that should be assessed and for which information needs to be collected information. These are: the travellers' *identity, (online) behaviour, mental state and capabilities*. On these categories, indicators can be distilled (see deliverable 2.2), which can be regarded as the information that should be collected on the traveller to determine the risk profiles. When these information needs are expressed, it is possible to determine what data of travellers then should be collected, and what sources are needed to gain access to this data.

Step 7 – Formalisation of the initial DBT@BCP

The final step of the TRESSPASS DBT-Method is to formalise the results of the previous steps in a DBT@BCP by competent authorities, and to distribute it to all stakeholders involved in RBBM at the concerning BCP. Taking this step is beyond the scope of the TRESSPASS project.

ANNEX B ASSESS BCP ETHICS

"In order to meet the goal within the TRESSPASS approach of a risk-based border management concept for air, maritime and land border crossing points, WP9 follows an "Ethics and Data Protection by Design (EDPbD) approach"[8].

A first version of the methodology was presented in TRESSAPASS D9.6, [9] which "identified ethical, legal and societal aspects (ELSA) considered as unintended negative impact of introducing risk based border management. Twelve types of such potential, ELSA related negative impact were specified and grouped in three categories. These categories are:

- ELSA category A: privacy and data protection issues;
- ELSA category B: unfair distribution of impact across different social groups;
- ELSA category C: restrictions of societal freedoms and liberties.

The conceptualization of these impact types enabled us to draft qualitative scales for assessment which is part of the ethical evaluation framework. It is also consistent with the concept of operations (CONOPS) framework."[10]

The assessed impacts provide designers and decision makers with tools "to evaluate the impact of introducing risk-based border checks and make ethically informed and well-balanced design decisions"[11].

The classification suggested in D9.6 was lately modified[12] to reflect recent developments at EU level and to incorporate the Guidelines for trustworthy AI, issued in 2019 by the High-Level Expert Group on AI.

"The Guidelines for trustworthy AI are addressed to all groups of stakeholders and involved personnel designing and developing, implementing, using or being affected by AI. They are designed not only to hand a list of ethical principles but to provide guidance on the operationalization of these principles in socio-technical systems by the stakeholders."[13]

To specify and assist the process of analysis and evaluation in the context of development, deployment or use of AI systems the Guidelines for Trustworthy AI contain an *Assessment List for Trustworthy AI* (ALTAI) which is "intended for self-evaluation purposes. It provides an initial approach for the evaluation of Trustworthy AI"[14]. The list names seven requirements of Trustworthy AI:

1. Human Agency and Oversight;

2. Technical Robustness and Safety;

---

[8] TRESSPASS D9.8, Updated Framework for assessing direct ethical, legal and societal impact of risk based border screening concepts, November 2021.

[9] TRESSPASS D9.6, Framework for assessing direct ethical, legal and societal impact of risk based border screening concepts, November, 2018.

[10] TRESSPASS D9.8, Updated Framework for assessing direct ethical, legal and societal impact of risk based border screening concepts, November 2021

[11] TRESSPASS D9.6, Framework for assessing direct ethical, legal and societal impact of risk based border screening concepts, November, 2018.

[12] Only a few technologies developed in TRRESSPASS actually make use of AI.

[13] TRESSPASS D9.8

[14] Ethics Guidelines for Trustworthy AI. High-Level Expert Group on Artificial Intelligence, April 2019.

3. Privacy and Data Governance;

4. Transparency;

5. Diversity, Non-discrimination and Fairness;

6. Societal and Environmental Well-being;

7. Accountability.[15]

Following this list, D9.8 provided an assessment of the ethical risks of each TRESSPASS component and suggested mitigation measures to reduce them.

[15] Ethics Guidelines for Trustworthy AI. High-Level Expert Group on Artificial Intelligence, April 2019.

ANNEX C PILOTS GUIDANCE METHODOLOGY

The pilots' preparation and the plan for executing, testing, validating and assessing the TRESSPASS system was guided by the Pilots Guidance Methodology (PGM), a new methodology introduced by KEMEA, the leader of the Pilots of the TRESSPASS project.

The methodology was adapted from the Trials Guidance Methodology (TGM), which was designed for crisis management and used in the Driver+ EU project.

The figure below shows the PGM wheel as an outcome after the transformation, enrichment, and customisation of the TGM, and how it was tailored to the TRESSPASS pilots' needs and requirements.

The PGM consists of three main phases: Planning, Execution and Evaluation, with various steps in each phase. Each phase ends with the submission of one or more reports (project's deliverables).

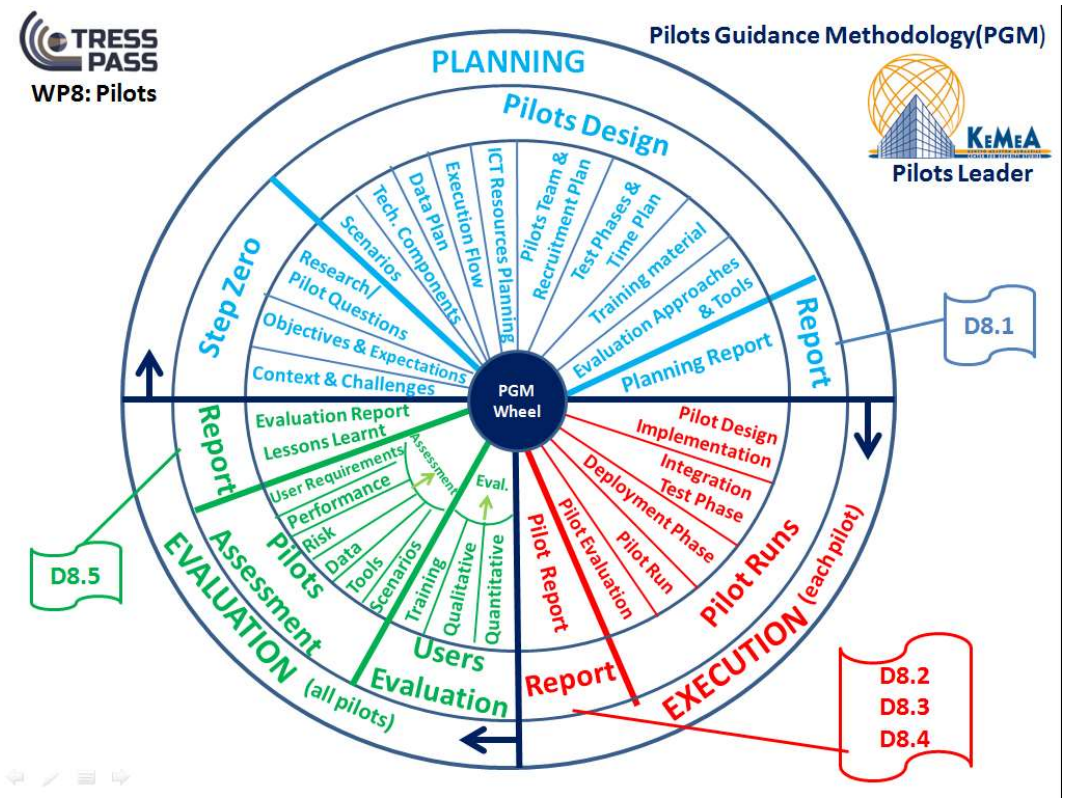

FIGURE 4 - OVERVIEW OF TRESSPASS PILOTS GUIDANCE METHODOLOGY (PGM)

Planning Phase

During the Preparation-Planning phase, the end users, technical and research partners, who were involved in the development of the Risk Based Border Management (RBBM) concept and the development of the associated components, recorded an overview of the **current context**, the stakeholders involved, **the existing challenges, the research questions**, and the gaps to be filled, in order to set the **objectives and the expectations** for filling those gaps and enabling the TRESSPASS system to provide differentiation and added value to the current strategic, tactical and operational Border Crossing environments in three different modalities (air, land, sea) and EU countries (NL, PL, GR).

- The first step of the Pilots' Design involved the selection and design of the most appropriate use cases and the high-level and detailed **scenarios** to be used in the pilots.
- As a next step, a list of the **technical components** and sensors were prepared describing for each component in detail the different functionalities, the interdependencies and their inputs and outputs that contribute to the RBBM system.
- Based on the selected use cases and scenarios and the functionality of each selected component in the previous steps, the partners were then able to list the input/output **data** handled by each component and the datasets to be collected and prepared from various data sources and used during the pilots. Through this procedure, they were able to determine a pool of data used in the project, in order to be able to address early on potential data protection, ethical, legal and privacy issues arising from the development of the tools.
- Having selected the appropriate scenarios, the components and the associated data, the **pilot's execution flow** in the different travel phases was designed for each pilot.
- Different **ICT Infrastructure and Resources** and the pilot team and **participants' recruitment** process were defined for each pilot to run the test phases securely and in a scheduled **time plan** prepared for the different pilot **test phases** (integration, deployment/dry runs and final pilot).
- The development of **Training process and material** and the **Evaluation approaches and tools** which would be used for the assessment of TRESSPASS system after the pilots, were the two last steps of the Pilots' Design phase.

Execution Phase

- This phase included the actual **planning implementation** for each pilot of all the above steps in the Pilots Design phase.
- The technical team, the end user partners, and the ethical/legal team organized several regular **integration and dry run tests** to execute trial-outs prior to the actual final pilot events.
- After the integration, the deployment and the dry run test phases, each **pilot run** was performed by the end users at their local sites to test, validate and evaluate the RBBM concept and the technology involved.
- The system and all its components tested during each pilot were evaluated by the end users providing quantitative and qualitative feedback with the aid of the **evaluation** tools designed in the planning phase (score and text-based questionnaires, interviews, comments etc)
- Finally, a **report** [16]was produced for each pilot.

[16] The report should be protected from dissemination to readers not having the proper security screening level or need to know, and be classified accordingly.

Evaluation Phase

- The final phase of this methodology involves the overall end user evaluations from all pilots and the overall assessment of the system and the project in general, including the scenarios, the tools, the data, the training, the performance indicators as well as the fulfilment of the initial end user requirements in all pilots.
- Finally, a report[17] is produced with the lessons learnt and the experience gained from each and all pilots.

[17] The report should be protected from dissemination to readers not having the proper security screening level or need to know, and be classified accordingly.

ANNEX D OPERATE A RISK-BASED BCP

TRESSPASS WP6 is concerned with the analysis of operational processes and organisational systems involved in BCP management particularly from the perspective of human factors, but including the interaction between people, technology, rules, resources, and structures, in the context of the overall objectives and motivation for border control operations. These objectives and motivational factors include security, but also economic as well as human rights, and the role that border control plays in the context of societal values.

As such, within TRESSPASS, WP6 deals with the operational processes and societal acceptability of the TRESSPASS risk-based border management (RBBM) solution. Viewing the RBBM system from a human factors perspective, anticipated changes, best practises and potential issues are highlighted for end-users and other system stakeholders, when planning to adopt the RBBM solution, through the establishment of a unique Concept of Operations (CONOPS) user guide and future framework for implementation.

Concept of Operations Framework

A CONOPS is a conceptual design approach that is mainly concerned with highlighting and describing the human role in operational systems in the context of planned change, such as that involving technological and procedural innovation. The primary aim of creating a TRESSPASS CONOPS is to provide "*a user-oriented document that describes system characteristics for a proposed system from the users' viewpoint*" (IEEE 2007). In accordance with the original IEEE CONOPS (IEEE, 1998) template format, an 'as-is' baseline system is initially described for the TRESSPASS system, then the desired system changes and justifications for these changes were explained, including any system restrictions or risks. Succeeding this, the proposed system is described, with an emphasis placed on anticipating the operational and process changes that may occur with these given modifications. The first "as is" sweep of operational processes and systems allows for analysis of the relative importance of system components, such as software, hardware, environment, and liveware, including liveware-to-liveware interactions. This then allows for the identification of gaps and opportunities for innovation and the further detailing and elaboration of requirements.

The second sweep involving layering over a proposed solution's system architecture is to attempt to anticipate collaboratively with end-users what the impact of each component may be from the point of view of the actors involved and in so doing try to reduce the risk of implementation and foster a more participatory approach thus enhancing acceptance.

Activity System Framework

The approach taken to CONOPS within TRESSPASS has been influenced by the activity system framework developed by Engeström (Engeström, 1987). The activity system emphasises the role that technology plays in mediating (facilitating or obstructing) human activity defined in terms of goal orientation. Working back from the planned or intended outcome of an operational process, or its KPIs, it is possible in principle to trace the relative contribution that various system components make towards that outcome. However, within this approach it is acknowledged that each component's value exists in its interaction with other component, such as the relationship between people and the tools they use, or the interdependencies between people performing difference complementary roles.

CONOPS development

Below we list the methodological steps that were followed, offering this as a foundation for establishing a proposed standard for creating a CONOPS for risk-based border control management (RBBM).

1. Using activity theory, a CONOPs heuristic was established. This heuristic acts as a baseline for structuring the operational questions from a human factors' perspective. These operational questions are initiated as the RBBM system is first developed and are then continually referenced throughout the lifecycle of the system development as the CONOP framework evolves.

a) **Who** are the stakeholders involved in the system? Who is the system intended for? How are human roles structured and articulated? What do human actors contribute to and receive from the system?
b) **Why** are the system changes being initiated? For what purpose? What does the current system lack that the changes with fulfil?
c) **What** are the known elements and high-level capabilities of the system?
d) **When** are the activities of the system to be performed? At what phases/time sequences will the technical components be initiated?
e) **Where** are the system changes taking place? Geographical and physical location of the system in space.
f) **How** will the changes take place? How will the system components be integrated and used? What resources are required, e.g., technical, personnel, manpower, to carry out these changes?

2. The baseline 'as-is' system is established through observational data collection including stakeholder interviews, field observation and walkthroughs. Using the operational questions as a framework, current BCP system processes and challenges were established from the perspective of end-users via a collaborative workshop. Applying the activity-centred CONOPS methodology permitted end-users to identify the key personnel, goals, tools & technologies, task distribution, organisational context, and rules currently in operation in their BCP and highlighted the interdependence of all these elements.

Following on from this, empirical fieldwork visits to each BCP modality were conducted to study, refine and detail the baseline system processes.

To best structure the TRESSPASS CONOPs, the operational processes were divided into three phases, illustrated by visual swim-lane graphics for each case modality.

a) Pre-travel Phase – This phase entails all system activity that takes place prior to presentation at the BCP.
b) Approaching BCP Phase – This phase includes all activity that takes place within the BCP area but prior to presentation and the actual BCP.
c) BCP Phase – This stage of the RBBM system consists of the activity that occurs at the BCP.

3. Once the baseline system is established, the proposed future system is described using the operational questions and across the three temporal phases outlined above. The proposed system changes were described under the following subsections:

a) **System architecture/technological components** – a description of the new system components and their intended purpose within the system was first described.
b) **Travel process changes** – description of the changes that will occur to the travel process with the initiation of the new system architecture.
c) **Anticipated Operational Process Changes –** a description of the changes that could potentially occur to BCP operations with the new technical components in place.

Establishing the TRESSPASS CONOPS in this dialogical manner, that is, adapting Activity Theory from a human factors' perspective, allows ethical, sociotechnical and organisational constraints to be brought to the surface for discussion and problem-solving. Therefore, the TRESSPASS CONOPS guide is an evolving document, which has three iterations, as things are clarified and expanded upon through the system design development, before arriving at a final Concept of Operations user guide.

4. Final Evolving Concept of Operations

The final Concept of Operations follows the structure of the two previous iterations, describing the operational processes across the three phases and under the process categories of the travel, operational and technological changes, however this version layers the information, insights and answers garnered from the piloting phase of the project onto the CONOPS to develop the final user guide. The piloting phase, under the management of WP8, carries out test studies at each of the three BCP case modality sites, air, maritime and land, respectively. Using scenarios devised by BCP end-users for both defined benevolent and malevolent passengers, testing of the system takes place with the use of actors. In this manner, any shortcomings, missing information, or overlooked processes of the system will then be brought to light and subsequently integrated into the final evolving CONOPs guide.

5. Key Performance Indicators and Future Implementation

Once the final TRESSPASS CONOPS guide has been established, operational validation can then be evaluated in a participatory manner and subsequently future system implications can be highlighted and discussed. This stage of the process occurs post piloting the system and in collaboration with end-users, in order to provide a detailed system standard, where RBBM functionalities can be described in full. This evaluation stage permits the TRESSPASS system to be adopted and tailored to future and alternative operational and system processes.

The operational effectiveness of the future TRESSPASS platform is evaluated in with reference to the four main TRESSPASS system KPIs (listed below) along with other relevant operational KPIs as uncovered in collaboration with end-users and potentially during the piloting phase. This is carried out in a way that is sustainable beyond the lifespan of the project through the provision of guidance on how to assess the suitability of the KPIs.

- Effectiveness – as determined by measures of success in identifying passengers, luggage and cargo as safe or unsafe and the reduction of false positives and false negatives.
- Efficiency – by examining the level of resources required at the BCP to achieve a specified degree of effectiveness and/or certain minimal flowrate.
- Flowrate - This refers to the speed of the flow of travellers as they approach and cross the border at the BCP. This may include the amount of travellers crossing the BCP per hour or may be measured through decreases in bottlenecks or queues.

- Ethical compliance level – This could be considered as the degree to which the BCP mitigates negative ethical impact on the traveling public and on the public in general, regardless of if they travel.
- Traveller satisfaction and societal acceptance – the extent to which passengers report that the BCP operation is not perceived as an inconvenience and that the benefits are recognized as worthwhile. Also, the acceptance by the general public that the risk-based method is fair and reasonable.
- Cost – including both capital investment and operating/maintenance costs.

WP6 provides an evolving CONOPS user guide, the three iterations describe the methodology and operational processes for each BCP through the progression of the project. Once this CONOPS has been fully established, post-piloting phase, KPIs can be looked in conjunction with end-users, to determine, measure and reflect upon the successful performance of the system. That is, if the original goal and intentions of the system changes have been met. Critical reflection on the performance of the system at this point provides valuable information for those wishing to replicate or initiate a future RBBM system and hence we offer this TRESSPASS WP6 summary as a standard for managing and structuring the operational processes of an RBBM system.

TRESSPASS and Operational Standards

The remaining deliverables in TRESSPASS WP6 include D6.6 Evolving CONOPS framework (final), and D6.4 “Framework for future implementation and validation of the TRESPASS solution including post project” will deliver a proposed concept of operations for the three BCP modalities incorporating the TRESSPASS system integrated with operational processes and systems. This will inevitably mean some modification of existing operating procedures and the elimination of some parts of the current process while upstreaming much of the screening. Therefore, the final CONOPS can be read as an initial proposal towards a standardised approach to BCP system design and operation incorporating the risk-based approach enabled by TRESSPASS. Along with this, D6.4 will stand as a guide for the implementation of the CONOPS approach to analysing and preparing for the integration of TRESSPASS within new operational contexts and allowing for new sensors and other innovations to be incorporated smoothly in the future. The CONOPS approach as employed within TRESSPASS can also be considered an adaptation of and refinement of the IEEE CONOPS standard.

ANNEX E COORDINATE OPERATIONS

A central aspect of RBBM is screening of travellers in support of risk assessments that allow for more proportional checks for each traveller. RBBM requires threat definition and residual risk acceptance on a (inter-)national policy level to be followed by national strategic formulations of threat scenarios, associated risk profiles and risk indicators. An important pre-condition for RBBM is information exchange at various management levels between all involved organisations, which can be considered as one of the core principles of RBBM. General risk-based concepts, residual risk acceptance, distinguishing features between illegitimate and legitimate travellers as well as information on a traveller's passage through a BCP become central information units to be exchanged.

In the following Table 7 an overview of information flows with relevance for RBBM is provided. It summarises what kind of information the different border management stakeholder levels receive from whom at what stage of a traveller journey, and why. Current challenges for such an information exchange are equally noted.

TABLE 5: OVERVIEW OF MULTI-NATIONAL, MULTI-LEVEL AND MULTI-STAGE RBBM INFORMATION FLOWS

Recipient	Information Type	Sender	Time / Travel Stage	Reason	Challenges
EU/National level policy entity	Risk-based concept inputs	Other EU/national level policy entity	Periodically	Collaboration on risk-based concept implementation	Mandate, common understanding
	Threat and risk acceptance inputs	Other EU/national level policy entity	Periodically	Collaboration on risk-based concept implementation	Risk appetite divergence
	Threat and risk acceptance inputs	Strategic level border management entity	Regular intervals	Aid in threat mitigation and residual risk achievement decision making	Mandate, common understanding
Strategic level border management entity	Definition of threats and risk acceptance	EU/national level policy entity	Precondition	Threat mitigation and residual risk achievement	Mandate, common understanding
	Threat scenario and risk profile and indicator detail and trend inputs	Tactical level border management entity	Regular intervals	Aid to define, update and assess threats and risks	Mandate, common understanding
Tactical level border management entity	Definition of threat scenarios, initial risk profiles and indicators and risk acceptance details	Strategic border management entity	Precondition	Creating lists of risk indicators and thresholds specific for a BCP	Mandate, common understanding

	Threat scenario and risk profile and indicator detail and trend inputs	Other tactical level border management entity	Periodically	Sharing risk profiles that have proven to be valuable	Mandate, common understanding
	BCP records of travellers and alerts	Other tactical level border management entity	On demand	Cross-border collaboration	Mandate, data privacy, interoperability
Operational level border management entity	Risk indicator lists, weights and decision rules	Tactical level border management entity	Precondition	Allowing for execution of risk-based screening and checks	Mandate, data privacy, interoperability
	Behavioural indicators	RBBM technology (sensors)	Traveller approaching and at BCP	Risk assessment	Mandate, data privacy, interoperability
	Indicators of intent	RBBM technology (e.g. Internet search)	Pre-travel, traveller approaching and at BCP	Risk assessment	Mandate, data privacy, interoperability
	Personal travel information	RBBM technology (pre-travel information)	Pre-travel	Risk assessment	Mandate, data privacy, interoperability
	Information from existing information systems	Database providers	Pre-travel, traveller approaching and at BCP	Risk assessment	Mandate, data privacy, interoperability

The TRESSPASS information exchange approach describes how information exchange and interoperability on a tactical (where command, control and coordination at BCPs takes place) and operational level (where border control is effectively executed) can be realised. TRESSPASS builds upon existing and planned information exchange structures (European Commission (2016, 2019), EUCISE2020) and adds the ability to exchange information with relevance for traveller risk assessment between BCPs in Europe and even third country BCPs within a specified exchange protocol (Figure 8).

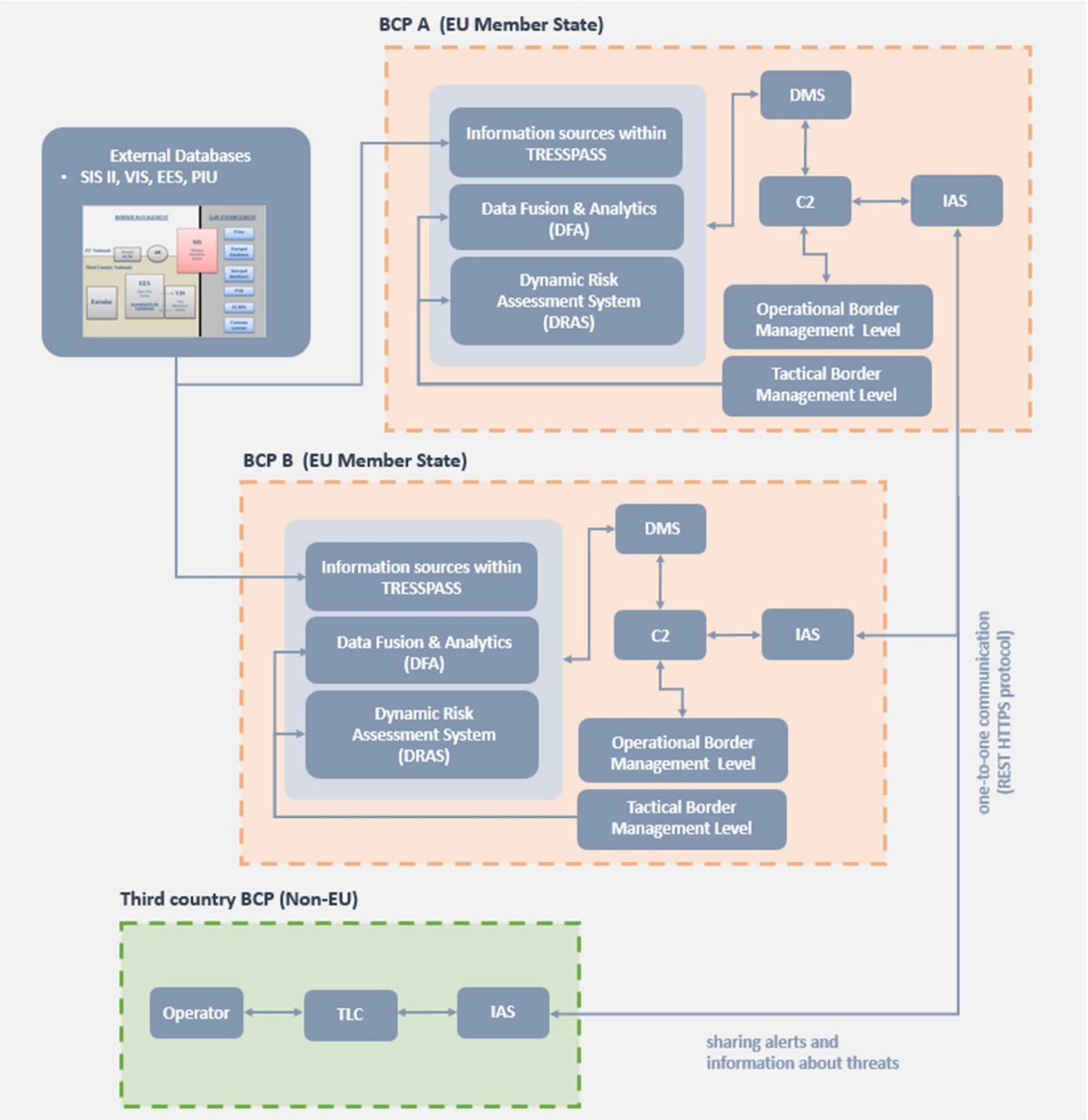

FIGURE 5 TRESSPASS FUNCTIONAL INFORMATION EXCHANGE

Central components span TRESSPASS Information Sources, a Distributed Messaging System, an International Alert System, a Command & Control component and the TRESSPASS Light Client. Risk assessments are facilitated via the combination of a Data Fusion & Analytics component and a Dynamic Risk Assessment System. Central features are rigorous authentication and authorisation schemes that give users access only to information that they are authorised to see, while adhering to privacy by design principles.

While the TRESSPASS system does not directly provide functionalities for the policy and strategic levels, inputs from and to these levels are essential for the realisation of RBBM (Figure 9) and a substantial benefit can arguably be expected from the realisation of a standardised tactical and operational RBBM framework like the one proposed by TRESSPASS. Maintaining integrity and public trust in the risk-based mechanisms is a crucial element to that end.

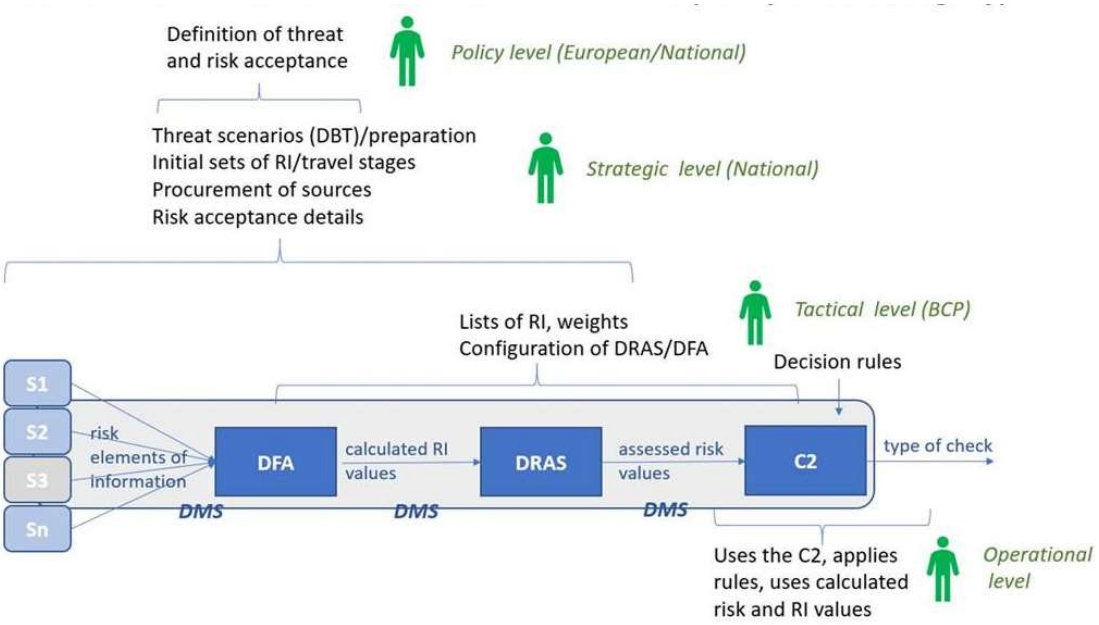

FIGURE 6 VERTICAL INFORMATION FLOW BETWEEN STAKEHOLDERS WITHIN THE TRESSPASS CONCEPT

However, extensive legislative changes at the EU level will have to occur to facilitate true multi-level, multi-stage and multi-national RBBM collaboration. A relaxation of requirements to apply the same minimum checks to all travellers will be needed, conditional on checks being executed in correspondence with clearly defined risk profiles addressing agreed upon threat scenarios and supported by active risk acceptance. More extensive traveller screening and associated cross-border and cross-agency information exchange will be necessary to support the verification of traveller matching against risk profiles. These changes will have to be justified, at the minimum, through positive answers to central research questions addressed by the TRESSPASS pilots and to stand on rigorous and transparent ethical foundations as described by deliverables from TRESSPASS WP9 - Ethics and Data Protection.