# Analysis of Risks and Trends in Automated Border Control

*Final Report*

Dmitry O. Gorodnichy
Canada Border Services Agency

Prepared By:
Canada Border Services Agency
Science and Engineering Directorate
Suite 210, 14 Colonnade Rd
Ottawa, ON  K1A 0L8

Project Number: 2013-CSSP-CFP-1020
Technical Authority: Paul Hubbard, 613-992-0595



Contract Report
DRDC-RDDC-2016-C324
July 2015

Canada Border Services Agency | Agence des services frontaliers du Canada

# Science and Engineering Directorate

# Border Technology Division

## Division Report 2015 – 11 (TR)
## July 2015

## ART in ABC:
## Analysis of Risks and Trends in Automated Border Control

### CSSP-2013-CP-1020 study
### Final Report

**Dmitry O. Gorodnichy**

PROTECTION • SERVICE • INTEGRITY

Canada

| Version #: 1.0 | | |
|---|---|---|
| **Action** | **Name** | **Date** |
| Prepared By | Dmitry Gorodnichy | 2015-05-06 |
| Reviewed By | David Bissessar | 2015-05-25 |
| Revised By | Dmitry Gorodnichy | 2015-06-08 |
| Reviewed By | Phil Lightfoot | 2015-07-03 |
| Revised By | Dmitry Gorodnichy | 2015-08-14 |
| Reviewed By | Phil Lightfoot | 2015-08-19 |
| Final Version | Dmitry Gorodnichy | 2015-09-17 |

# Abstract

This report presents the outcomes of the "Risk analysis of face and iris biometrics in border/access control applications" (CSSP-2013-CP-1020) study conducted by the Canada Border Services Agency in partnership with the University of Calgary through support from the Defence Research and Development Canada, Canadian Safety and Security Program (CSSP). This study relates directly to the technologies that apply to e-passport-based gate systems and iris-recognition-based registered traveller programs such as NEXUS. It also contributes to the development of a new generation of automated border control (ABC) systems and processes that are currently being developed by many countries, including Canada. The summarized outcomes include: establishing the terminology, metrics and tools for describing and analyzing ABC systems, analysis of issues with currently deployed systems, and investigation into further development of ABC and other traveller screening technologies within a larger e-border process that deals with automation of traveller clearance at the border.

**Keywords:** Border modernization, air traveller continuum, automated border control, biometric authentication, e-gates, e-passport, face recognition, iris, semi-automated systems, vulnerability, risk assessment, behavioural indicators, standards, performance evaluation, cost-benefit analysis, complex systems.

**CSSP Communities of Practice:** Biometrics and Identity Management (BIOM), Border and Transportation Security (BTS).

**CSSP investment priorities:**

1. Capability area: P1.6 – Border and critical infrastructure perimeter screening technologies/ protocols for rapidly detecting and identifying threats.
2. Specific Objectives: O1 – Enhance efficient and comprehensive screening of people and cargo (identify threats as early as possible) so as to improve the free flow of legitimate goods and travellers across borders, and to align/coordinate security systems for goods, cargo and baggage;
3. Cross-Cutting Objectives CO1 – Engage in rapid assessment, transition and deployment of innovative technologies for public safety and security practitioners to achieve specific objectives;
4. Threats/Hazards F – Major trans-border criminal activity – e.g. smuggling people/ material

# Disclaimer

In no way do the results presented in this paper imply recommendation or endorsement by the Canada Border Services Agency (CBSA), nor do they imply that the products and equipment identified are necessarily the best available for the purpose.

For the purpose of this study, the term ABC *does not* refer to the CBSA's Automated Border Clearance program and is used solely in reference to a general automated border control system that performs automated clearance of travellers at the border.

# Acknowledgments

This work was done under funding from the Canadian Safety and Security Program (CSSP) managed by the Defence Research and Development Canada, Centre for Security Science (DRDC-CSS).

A large portion of this report is based on the information provided by the researchers from the Biometric Technologies Laboratory of the University of Calgary: Vlad Shmerko, Svetlana Yanushkevich and Shawn Eastwood, and the comments and information provided by Ignacio Zozaya, a researcher with European Agency for the Management of Operational Cooperation at the External Borders (Frontex). Additional valuable feedback was provided by Markus Nuppeney (BSI), John Campbell (Biom Biometrics), Norman Poh (University of Surrey), Tony Mansfield (NPL), Monica Gariup (Frontex), Michael Petrov (Vision-Box), Glen Wimbury (UK Border Force), Judee Burgoon (University of Arizona), Paul Hubbard (DRDC-CSS), Michael Chumakov (CBSA), Tony Mungham (CSBA), David Bissessar (CBSA) and other colleagues from the Advanced Analytics section and Port of Entry Transformation / Air Traveller Strategy group. The author is most grateful to all mentioned individuals and organizations for their contribution to this study and the report.

# Release Notes

**Context:** The CSSP-2013-CP-1020 study was conducted from October 2013 to March 2015. Most work on this report was done prior to December 2014 and may not reflect technology development after that date.

**Appendices:** This report is accompanied by the appendices that include additional information summarized from other study reports which provides more detail on the topics discussed in this report.

**Typesetting:** The report contains automatically generated hyper-link references and table of contents for easier navigation and reading online.

**Call for contributions:** This report has produced a number of concepts, recommendations and roadmaps related to the development and deployment of ABC and other e-border systems, the further discussion of which with the international community is welcomed.

**Contact:** Correspondence regarding the CSSP-2013-CP-1020 study and the reports associated with this study should be directed to: DMITRY dot GORODNICHY at CBSA dot GC dot CA.

# Contents

# List of Figures

# List of Tables

# Abbreviations

| | |
|---|---|
| **ABC** | 1. Automated Border Control (used in EU and this report), see BE-ABC |
| **ABC** | 2. Automated Border Clearance program/kiosks (used by CBSA), see APC |
| APC | Automated Passport Control kiosks, see also ABC (Abbreviation 2) |
| API | Advance Passenger Information |
| ATC | Air Traveller Continuum |
| AVATAR | Automated Virtual Agent for Truth Assessments in Real-Time |
| BE-ABC | Biometric-Enabled Automated Border Control, see also ABC (Abbreviation 1) |
| BWT | Border Wait Time |
| CAPPS | Computer-Assisted Passenger Pre-screening System |
| CATSA | Canadian Air Transportation Security Agency |
| CIC | Canada Immigration and Citizenship |
| CBSA | Canada Border Service Agency |
| DHS | Department of Homeland Security |
| EUROSUR | European External Border Surveillance System |
| FAST | Future Attribute Screening Technology |
| FNMR/FMR | False Non-Match Rate / False Match Rate |
| FRR/FAR | False Reject Rate / False Accept Rate |
| IATA | International Air Transport Association |
| ICAO | International Civil Aviation Organization |
| IDENT | Automatic Biometric Identification System |
| ISO | International Standards Organization, International Organization for Standardization |
| MRTD | Machine Readable Travel Document |
| NIST | National Institute of Standards and Technology |
| ORR | Operational Reject Rate |
| PIL | Primary Inspection Line |
| POE | Port of Entry |
| PNR | Passenger Name Record |
| RAIC | Restricted Access Identity Card |
| RFID | Radio Frequency Identification |
| RTP | Registered Traveller Program, see also TTP |
| SITA | Société Internationale de Télécommunications Aéronautiques |
| SPOT | Screening Passengers by Observation Technique program |
| TSA | Transportation Security Administration |
| TRBP | Temporary Resident Biometrics Program |
| TRL | Technology Readiness Level |
| TTP | Trusted Traveller Program, see also RTP |
| SIS | Schengen Information System |
| VIS | The EU Visa Information System |

# Study overview

In 2013 the Canada Border Services Agency (CBSA), through support from the Defence Research and Development Canada (DRDC) Canadian Safety and Security Program (CSSP) and partnership with the Biometric Technology Laboratory of the University of Calgary, established the "Risk analysis of face and iris biometrics in border/access control applications" (CSSP-2013-CP-1020) study, later re-named the "*ART in ABC*" study.

This study is directly related to automated border control (ABC) technologies that enable seamless and fully automated authentication, screening and clearance of travellers at the border, in particular, the technologies that apply to e-passport-based gate systems and iris-based registered traveller programs such as NEXUS.

The study also contributes to the development of a new generation of ABC systems and processes that are currently being developed by many countries, including Canada. The study name (*"ART in ABC"*) is thus crafted to signify both the state of **art** and **a**nalysis of **r**isks in **t**rends in ABC.

## Study reports

The outcomes of the research conducted by the *"ART in ABC"* study are presented in this report, which extends and refines the results presented in earlier study publications [1]-[6] and Contractor Reports from the University of Calgary [9, 10].

A shorter version of this report, summarizing the study outcomes, is published as a separate report, entitled "ART in ABC: Analysis of Risks and Trends in Automated Border Control. CSSP-2013-CP-1020 study Executive Summary" (Division Report 2015–17). Additionally, a slide presentation of the key study outcomes is also prepared and provided in Appendix H.

# Linkages with previous studies

This study is an extension of the ongoing work of the Science and Engineering Directorate of the Canada Border Services Agency (CBSA-S&E) supported through the funding from DRDC Center for Security Sciences on analyzing and developing Biometrics and Video Surveillance technologies for the use in border control applications. The previous work performed by the directorate in this area funded by DRDC is listed below:

- Faces on the Move: Multi-Camera Watchlist Screening (CSSP-2014-CP-2000), 2014-2016. In process.
- Accelerated Evidence Search project (CSSP-2013-CD-1063), 2013-2014. Ref: Bergeron, J-P.; Bissessar, D. "Accelerated Evidence Search Report", DRDC-RDDC-2014-C166. Online: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc159/p800470_A1b.pdf
- Architecture and Assessment: Privacy Preserving Biometrically Secured Electronic Documents (CSSP-2013-CD-1064), 2013-2014. Ref: D. Bissessar, D. Liu, S. Nahmias, J. Harvey, Technical Report DRDC-RDDC-2015-C055.
- PROVE-IT(VA) study: Video Analytics for Border and Transportation Security: Indoor and Outdoor Environments (PSTP03-402BTS), 2011-2013. Ref. : D. Bissessar, E. Choy, D. Gorodnichy, T. Mungham, "Face Recognition and Event Detection in Video: An Overview of PROVE-IT Projects", Technical Report DRDC-RDDC-2014-C167, Online: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc157/p800402_A1b.pdf

- PROVE-IT (FRiV) study: Real-time Face Recognition Technologies for Video-surveillance Applications (PSTP03-401BIOM), 2011-2013. Ref.: Gorodnichy, D.O.; Granger, E.; Radtke, P. Survey of commercial technologies for face recognition in Video, Technical Report DRDC-RDDC-2014-C245, Online: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc159/p800510_A1b.pdf

- VT4NS: Video Technology for National Security, inter-departmental workshops and portal, 2007-2013. https://partners.drdc-rddc.gc.ca/css/Portfolios/Biometrics/VT4NS (available to DRDC partners). Ref: Gorodnichy, D.O.; Bergeron, J.-P.; Bissessar, D.; Choy, E.; Sciandra, J. Video Analytics technology: The foundations, market analysis and demonstrations, Technical Report DRDC-RDDC-2014-C251, Online: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc167/p801081_A1b.pdf.

- Biometric Data Safeguarding Technologies: Analysis and Best Practices, in partnership with Indiana University-Purdue University Indianapolis and International Biometrics Group (PSTP-02-351-BIOM), 2009-2010. Ref: David Bissessar, Dmitry Gorodnichy, Alex Stoianov and Michael Thieme. Assessment of Privacy Enhancing Technologies for Biometrics, Proc. 2012 IEEE Symposium on Computational Intelligence for Security and Defence Applications (CISDA 2012), Ottawa, 2012.

- C-BET: Comprehensive Biometrics Evaluation Toolkit and Portal, 2009-2010. https://partners.drdc-rddc.gc.ca/css/Portfolios/Biometrics/CBET (available to DRDC partners). Ref.: Dmitry O. Gorodnichy. Multi-order biometric score analysis framework and its application to designing and evaluating biometric systems for access and border control. Proceedings of IEEE SSCI Workshop on Computational Intelligence in Biometrics and Identity Management (CIBIM), April 2011, Paris.

- Comprehensive Evaluation of Stand-Off Biometrics Techniques for Enhanced Surveillance during Major Events (PSTP08-0109BIOM), in partnership with RCMP and International Biometrics Group, 2008-2009. Ref.: Dmitry O. Gorodnichy, Michael Thieme, David Bissessar, Jessica Chung, Elan Dubrofsky, Jonathon Lee. C-BET evaluation of voice biometrics. Proceedings of SPIE Defence, Security & Sensing Conference, Special Track on Biometric Technology for Human Identification VIII (DS108), Orlando, April 25-29, 2011.

- Biometric Border Security Evaluation Framework (PSTP08-0110BIOM), in partnership with International Biometrics Group, 2008-2009.

## The "*ART in ABC*" study in numbers

240,000: ($) Funding provided by DRDC-CSS over two years
Over 200,000: ($) In-kind contribution in term of additional labour hours from all projects partners
Over 500: Publications reviewed
Over 50 terms reviewed and revised
16: Publications produced, including 7 memos for internal clients ([1]-[10])
9: Advantages of iris modality identified (p. 44)
8: Distinct zones in the Air Traveller Continuum recognized for deploying traveller screening technologies (p. 9)
7: Critical differences between biometric-enabled access control and border control (p. 22)
6: Key properties defining the ABC (Gen-3 ABC) machine of the future (p. 25)
6: Biometric-capable technologies and programs used in Canada identified (p. 6)
5: Pillars (key traveller screening technologies) of e-border defined (p. 47)
5: Potential development roadmaps suggested – on APC kiosks (p. 57), AVATAR-like technologies (p. 50), ABC systems (p. 58), iris biometrics (p. 44), ABC Standards (p. 113)
4: Types of tools recommended for ABC analysis – life-cycle degraded performance metric (p. 61), simulation/modeling tools (p. 65), generic criteria for automated personal identification mechanisms (p. 66), PROVE-IT($x$) TRL assessment framework (p. 134)
3: Generations of biometric-enabled ABC (p. 24): RTP-based, eID-based, eBorder-based
3: Levels of ABC modeling defined (p. 65) – basic illustrative, complex point models, complex continuum models
3: Packages of standards for ABC established (p. 110) – on life-cycle of general large-scale systems, biometric components of ABC, and life-cycle of ABC systems, 11 strategic directions for which are introduced
3: ABC top level metrics (p. 59) – operational reject rate, throughput, wait time; and over 35 low level metrics for system specifications (p. 61)
3: ABC performance optimization areas (p. 60) – facilitation, security resources, cost resources

# Chapter 1

# Border control context

## 1.1 Global context

The International Air Transport Association (IATA) estimates that the volume of international air travel passengers will grow at around 6% per year. It will result in nearly 1.4 billion passengers in 2015 compared to just 1 billion in 2010 [47]. Similar estimates have ben obtained by the International Civil Aviation Organization (ICAO), according to whom global air passenger traffic is expected to more than double by 2030, from 2.7 billion in 2011 to 6 billion annually, with the corresponding number of flights increasing from 30 million to 60 million. Traditional border processing systems and procedures will not be able to cope with the increase in volume, yet travellers will still expect to be processed quickly and with minimum inconvenience. Governments are in the difficult position of balancing the economic benefit of cross-border travel with the need to ensure traveller safety, and at a time when spending reductions are the norm.

Additionally, the human factor has also been regarded as a highly vulnerable element of the border screening system [13, 175]. Reference [13] provides analysis of the checkpoints in the U.S. airports. It states, in particular, that "*. . . Passenger checkpoint screening activities at all passenger airports are carried out by about 30,000 screeners who make up about 60-65% of the total TSA screener workforce. . . . A variety of factors may contribute to these human performance limitations, including inadequate training, lack of motivation and job satisfaction, fatigue, and workplace conditions, as well as general human perception and performance limitations.*"

To address these challenges, many governments are in the process of developing strategies for border modernization [72, 13, 36, 84, 65], the key component of which is seen in automating and improving the traveller authentication and clearance process. The costs of modernization have been reported in many documents, in particular, the costs of USA border modernization are given in [17]. According to the e-border roadmap created by the ICAO for the short-term perspective (2017), e-gates and e-passport/e-ID will be deployed in most airports. In a long-term perspective (2020+), e-border systems will be able to communicate globally [27, 35, 44].

The global market for ABC systems, including kiosks will exceed $1.2 billion in annual revenue by 2020 according to [11]. Over the forecasted period the total number of deployed ABC systems is projected to reach over 6,000 and border clearance kiosks are forecasted to reach deployment numbers of 33,000. Europe will have a massive chunk of this market, making $2 billion during the period, which represents the projected 47% market share.

Vancouver, Atlanta Hartsfield-Jackson and Chicago O'Hare were the first airports in North America to announce the introduction of biometric APC/ABC kiosks. Now there are 400 APC/ABC kiosks deployed in 13 airports in North America, including the three largest Canadian Airports: Vancouver, Montreal and Toronto. This in addition to over 60 Nexus kiosks installed in Canada for processing Nexus trusted travellers program members!

As indicated in [11], "*APC kiosks offer a cost effective and rapidly deployable means of reducing congestion*

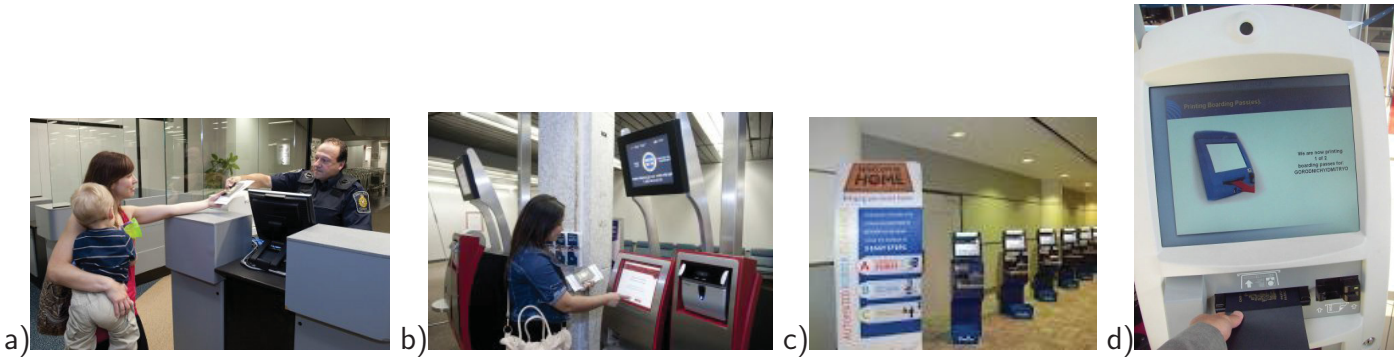



Figure 1.1: Technologies used for air travel: manual processing at PIL (a), iris scanners for Nexus members (b), ABC/APC self-service custom declaration kiosks (c), airline check-in kiosk (d).

*at international arrivals. These announcements reflect a decisive global trend towards expediting international airport passengers through rapid adoption of automated border control technology*". In the same reference it is predicted that "*European airports will drive global APC Kiosk market expansion to nearly 8,000 units and more than $550 million in revenues by 2018, reflecting a 22% Compound Annual Growth Rate over five years.*" The first generation of APC kiosks did not include biometrics and were available only to US and Canadian passport holders. The second generation of biometric-capable APC kiosks extends this service to international travelers from 38 visa-waiver countries including Australia, Japan, Germany and the United Kingdom. Their design has improved significantly towards user-centric systems that make operation easier for travellers and biometric capture more reliable. Shown in Figure 5.5, the second generation of APC kiosks installed in the USA automatically adjusts the screen and camera to the eye level of the travellers and can potentially capture ICAO-compliant[1] e-passport quality traveller facial image. More analysis of APC further development is presented in Section 5.4.

As the complexity of automated border control grows, so does the need for further research in this area. Various intensive research programs have been launched to provide research support for current and future border control technologies, such as "ABC4EU" (2014-2017, 17 millions EUR) [151] and FASTPASS (2013-2016, 15 million EUR) [152] projects funded by the European Commission. More detail about these and other related projects funded by the European Commission are provided in Appendix B.

## 1.2 Biometric-capable technologies in Canada

Traditionally, travellers arriving to Canada are processed at the *Primary Inspection Line* (*PIL*) by *Border Services Officers* (BSOs). A BSO validates traveller documents, verifies travellers' identity and makes the admissibility decision for the traveller based on the information available about him or her (Figure 1.1-a). When required, a traveller and the accompanying family members are sent to *Secondary Inspection* (*Secondary*). In contrast to the EU and many other countries, in addition to clearing the travellers, the responsibilities of the Canadian BSOs include performing customs control and collecting excise duties and taxes. In addition to BSOs working at PIL and Secondary, there are also BSOs who work with CATSA and airport employees to monitor travellers for suspicious behaviours and various behaviour indicators. Finally, there are also BSOs working with trained dogs and trace detection equipment searching for illegal products or food.

In an effort to automate and expedite processing (i.e., authentication and clearance) of travellers, a number of technologies and programs have been introduced to the airport environment over the last decade in Canada, summarized in Table 1.1 and shown in Figure 1.1. Six similar technologies are used in most other developed

[1] The ICAO has defined the requirements for biometric passports, which includes the requirements for the quality of facial images stored in passports [32, 33]. The facial images that meet these requirements are referred to as ICAO-compliant.

Table 1.1: Biometric-capable technologies in Canada.

| |
|---|
| 1. **Nexus Trusted Traveller Program (TTP).** This program uses iris biometrics kiosks installed in all major Canadian airports to identify pre-cleared low-risk frequent travellers. It was introduced by the CBSA for Canadian and US citizen and counts over a million registered members. A new generation of Nexus kiosks was deployed in 2014. The earlier Canadian-only version of the program, known as Canpass is gradually winding down due to lower interest from Canadian citizens. The program is managed by the CBSA. Biometric data (iris photo images) are also stored by the CBSA.<br>2. **Temporary Resident Biometrics Program (TRBP).** This program, introduced by the Citizenship and Immigration Canada (CIC) in partnership with the CBSA in 2013, performs verification of all residents requiring visas in the Secondary inspection area using fingerprint scanners (the so called "Live-scan" device). The program is managed by the CIC. Biometric Data is stored and managed by the RCMP.<br>3. **Automated Border Clearance self-service kiosks.** These kiosks allow travellers to scan their travel documents and customs declaration cards (E311 paper forms), and pay duties online. These programs were introduced by the Vancouver International Airport for Vancouver 2010 Olympics and have been since extended in partnership with the CBSA to Toronto and then Montreal International airports. They are very similar to Automated Passport Control kiosks being installed in many US airports and are managed by the corresponding airport authorities. They do not perform any biometric authentication or screening of travellers, which is still performed in a traditional manner manually by a BSO later in the process.<br>4. **Biometric-enabled e-passports**, with ICAO-compliant facial images stored in a protected chip inside the passport, are being issued by Passport Canada since summer 2013 and will soon replace all old non-biometric passports in Canada. Such passports are sufficient for the use with biometric-enabled border control e-gate systems, many of which are increasingly deployed in the EU and many other countries.<br>5. **Airline self-service check-in kiosks.** In additional to all of the above, airlines offer self-service check-in kiosks with passport readers. Many of these kiosks are also equipped with a camera on top the kiosk, which is used (or can be used) to capture the traveller's face for manual verification by an airline agent at the time of boarding a plane.<br>6. **Video surveillance cameras**. All airports are equipped with high-quality mega-pixel video-surveillance cameras (Figure 1.2), which potentially can be used for face recognition of travellers, particularly in controlled settings such as in front of a kiosk or passport booth. |

countries.

All of these technologies/programs use common infrastructure, contribute to the same two-fold mandate of the CBSA (facilitate travel, while securing the border) and are seen as potentially conflicting with each other in future. A kiosk of one program may potentially perform the tasks performed by other programs. Equally, travellers have an increasing number of options to be processed at the border. The use (or potential use) of traveller biometrics in all of these technologies is also clearly seen.

In an effort to seek cost-effective solutions that can deal with the growing traffic of travellers and increasing security threats, the Canadian government, and specifically the CBSA, jointly with other countries are exploring the options for border modernization and "the airport border of the future".

More information about border challenges and border modernization initiatives in different countries, including Entry-Exit programs and the IATA future checkpoint roadmap, is provided in Appendix B.

## 1.3 Schematic of Air Traveller Continuum

The development of automated border solutions is most recognized for the air mode of transportation or within the so-called *Air Traveller Continuum*.

Through the course of this study the architectural schematic of the Air Traveller Continuum is developed, extended from the original travel continuum schematics introduced by Frontex [34] (Figure 1.3) to include the

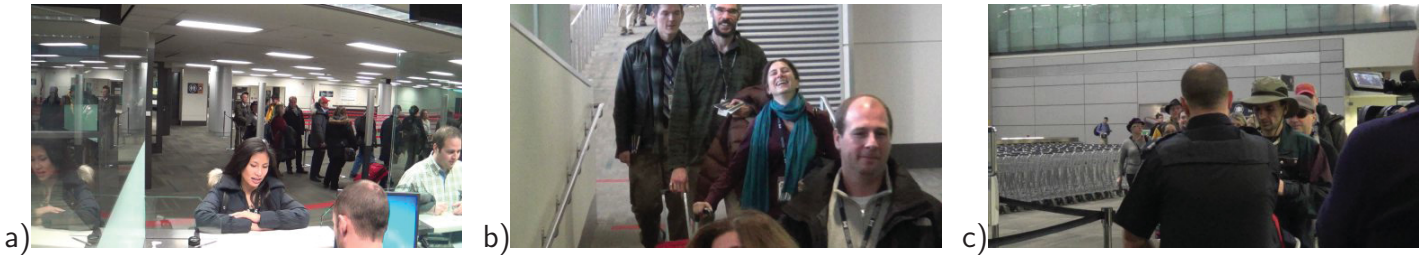



Figure 1.2: Video surveillance is one of the technologies that supports automated border control. The figure shows three airport setups (zones) of increasing complexity defined in [135] where faces can be captured for identification purpose: a) at PIL, b) in one-way corridors, c) in luggage area (see also Figure 1.3).

**Critical Observation**

*A number of technologies employing (or capable of employing) traveller's biometric data are already used in Canadian airports: Nexus kiosks, fingerprint scanners, self-service ABC kiosks, e-passports, airline check-in kiosks, video-cameras. While having overlapping functions and using common infrastructure, these technologies are not yet working in concord with each other. Combining them in one unit is seen as an opportunity for the optimization of the border control process, with benefits for both travellers and border agencies.*

specifics related to the travel by plane within the Canadian border control context. This schematic, described below and shown in Figure 1.3, becomes the starting point for the discussion and analysis of the study.

The following four main Air Traveller Continuum stages are recognized, *Pre-border (prior to departure)*, *Pre-border (en route)*, *At border (entry)*, and *At border (exit)*, which are further divided into smaller distinct sub-stages, or "zones", each with its own layout and capacity for for deploying e-border technologies, *eight* zones in total, with the first three of which being outside and the last five of which being inside the port of entry.

The e-border technologies that can be deployed in these zones aim at accumulating information about a traveller related to two main traveller clearance tasks (traveller authentication and risk assessment), as he or she moves along the continuum: from the time he/she buys the ticket or applies for visa until the final admissibility decision is made, either allowing or denying him/her an entry to the country.

### 1.3.1 Pre-border (prior to departure)" stage

The "Pre-border (prior to departure)" stage starts from the time when a traveller purchases a ticket or applies for a visa (for visa-required travellers). At this stage, *pre-screening technologies* are engaged aimed at assigning the initial risk score **Risk(0)** to a traveller prior to his/her arrival at an airport, based on his/her biographic data and criminal / travel history associated with his or her name. *Screening technologies*, the key five of which are identified by the study (Chapter 5), are engaged at later stages, aimed at further refining the traveller's risk score while the traveller progresses through different stages of the air continuum, with more information about the traveller being accumulated at each stage.

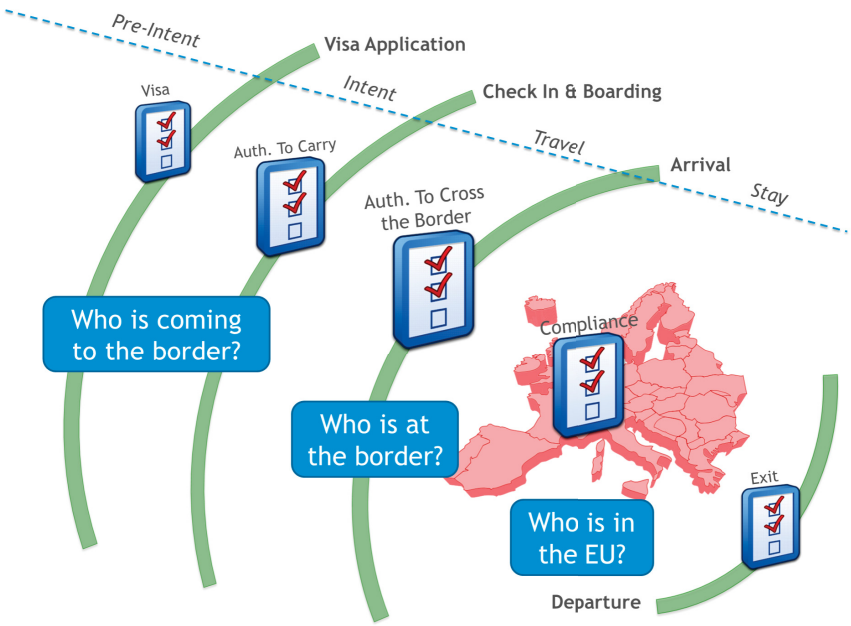



Figure 1.3: Traveller Continuum: schematic introduced by Frontex (from [34]).

### 1.3.2 "Pre-border (en route)" stage

The "Pre-border (en route)" stage consists of two main zones. In the first zone located within the premises of the airport of departure, new information about the luggage of the traveller and accompanying persons is obtained. Additionally, his/her behaviour can be captured by the airport cameras and his facial image can be captured for additional authentication of his/her identity. In the second zone, happening during the flight, closer interaction and behaviour of the traveller can be observed and reported to the border agents at the destination airport, should there be any abnormalities detected by a flight attendant or other travellers.

### 1.3.3 "At border (entry)" stage

The "At border (entry)" stage is divided into five zones, each with its own capacity for traveller screening and risk assessment technology. For example, as a traveller moves from the plane to primary inspection ("Upon arrival" zone), his/her behaviour can be monitored through the video cameras by the border officers. Prior to the interaction with the officer or a biometric-enabled e-gate/kiosk (which happens at "Primary Inspection Line (PIL)" zone) the traveller goes through the *"upstream border control"* zone (marked as "In queue" zone in the figure), where automated queuing technologies (e-border Component #4 according to the definitions introduced in Chapter 5 can be employed such as self-service APC kiosks or manual redirection of traveller's traffic (or particular travellers) by the officer.

Then the traveller goes through the "Luggage pick-up" zone, should he/she have any checked-in luggage, at which point he/she can be observed through cameras and by roving officers, while his luggage can be additionally screened by dogs or trace detection technologies, and then through "Secondary Inspection" zone, if he/she has any immigration or customs (duty/taxes) related procedures to perform.

### 1.3.4 "At border (exit)"stage

Finally, at the last "At border (exit)" stage, the final admissibility decision about the traveller is made, based on all intelligence accumulated about him/her and the final risk score **Risk(final)** associated with him/her based

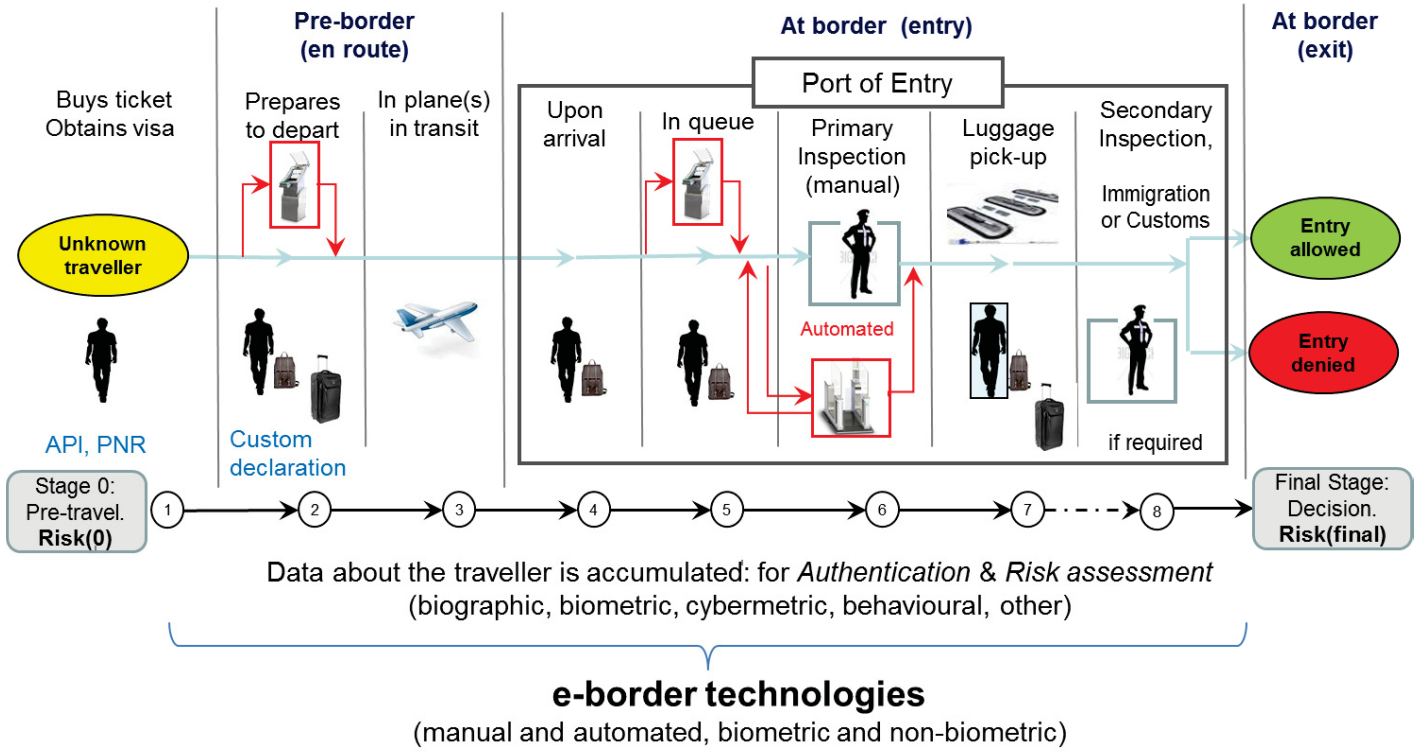



Figure 1.4: Air Traveller Continuum: schematic developed in this study. Eight zones are defined, each with its own layout and capacity for deploying e-border technologies, aimed at accumulating the information about a traveller related to two main traveller clearance tasks (traveller authentication and risk assessment), as he or she moves along the continuum. Already deployed e-border technologies are shown in red: self-service APC/ABC kiosks in zone (5), biometric-enabled gates in zone (6), and Entry-Exit kiosks in zone (2). It is only after zone (6) that travellers' identity is assumed known (marked blue). Prior to that it is unknown.

there on.

### 1.3.5 Use of ABC technologies along the Air Traveller Continuum

As further discussed in Chapter 5, a number of traveller screening technologies can be deployed at different zones of the Air Traveller Continuum. Specifically, shown in red in Figure 1.3 are the automated traveller screening technologies that are already being deployed at the border. This includes: Self-service APC kiosks deployed in the "In queue" zone (zone 5), e-gates deployed in the PIL zone (zone 6), and Entry-Exit kiosks being deployed in the airports of departure in the "Prepares to depart" zone (zone 2). Eventually, as highlighted in the next three chapters, it is envisaged that all automated traveller screening systems can be combined in single units, called *Gen-3 ABC machines*, one at each airport, which are interconnected and perform all traveller screening functions: from data collection and transfer to final admissibility decisions.

Finally, it is important to note that in addition to the zones related to traveller screening, the Air Traveller Continuum has also zones related to screening of travellers' goods and luggage, which allow for the deployment of additional technological solutions along the travel continuum, such as metal detectors, sampling for drug traces etc. These are not shown in the Air Traveller Continuum schematics, yet can be further explored for the additional level of intelligence gathered about the traveller.

## 1.4 Conclusions

The analysis of the international and Canadian context with respect to the use of current and future traveller clearance technologies clearly demonstrates high interest and need in ABC technologies on a global and local scale. Automated border control solutions and e-border supporting technologies are being actively introduced along the Air Traveller Continuum. The prime purpose of these solutions/technologies is to gather information about travellers as they travel to another country for the purpose of improving and expediting their authentication and risk assessment. More analysis of biometric-enabled ABC systems and other e-border technologies that can be deployed at different zones of the Air Traveller Continuum is provided in the next chapters.

In conclusion, it is noted that a strategic vision for automation of border crossing has been developed by the IATA, ICAO, and Frontex. For organizations developing border modernization initiatives, the partnership with Frontex, who has accumulated to date the strongest research knowledge related to e-border and ABC, is recommended.

**Critical Observation**

*Many countries, including Canada, are actively working on modernizing their borders through the use of automated border control and other e-border traveller screening technologies. To assist countries in these efforts, IATA, ICAO and Frontex have developed a strategic vision for border crossing automation, the rationality of which is confirmed and leveraged in this study. For agencies seeking knowledge-driven decisions related to border modernization, partnership with Frontex is recommended.*

# Chapter 2

# Concepts and definitions

As a relatively young area of science and technology, the area of border control automation requires establishing relevant terminology and definitions. While a variety of concepts have been used to describe various components of e-border, there are formal definitions yet to be developed specifically for ABC. This study addresses this gap by identifying and bringing together the concepts from *five* different technical domains that are important for the analysis of ABC solutions within a larger e-border infrastructure and management [9]. They are:

i e-border technologies (ABC machine[1], components of e-border, supporting technologies, e-passport, e-gate, kiosks, databases, logistics),

ii biometrics (modalities, faces / iris recognition, aging, decision making, biometric performance metrics, biometric evaluation, standards),

iii traveller risk assessment (statistical surveillance, data-mining, decision making under uncertainty and risks, large-scale applications), and

iv complex systems management (large-scale systems, technological risks, system vulnerabilities, cost and benefit analysis, system modeling),

v training of personnel (training facilities, training automation, automation bias, skill degradation, training scenarios, and training efficiency metrics).

In the following, key concepts and definitions from these areas are summarized, further refined from definitions presented by the University of Calgary researchers [9], with emphasis on those of them that refine and extend the existing technical vocabulary.

## 2.1 Concepts related to e-border technologies

The term "e-border" (or eBorder) does not refer to any particular border program, but is used solely as in reference to the infrastructure for **automated border control and management**. Formal definitions related to this term and its key functionalities are presented below.

**Definition 2.1.1 Border management** *is understood as the unity of the following operations: pre-arrival, arrival, stay management, departure, and database reconciliation/management* [170].

[1] Throughout this study, the term "ABC machine" is frequently used instead of the terms "ABC systems" / "ABC technology" to refer to the formalized conceptual definition of the system as in "Turing Machine", "Authentication Machine" or "evidence-accumulating machine" used later in this report. The term "machine" is also used as a counterpart to "human", as in "machine-human interaction" vs. "human-to-human interaction" when a traveller communicates with an ABC system rather than with an border officer. In other work [229, 230] the term "authentication/identification mechanism" is also used to signify both the concept and an actual device used for authenticating individuals at the border.

## Critical Observation

*The term "***e-border***" refers to the infrastructure for* **automated border control and management***, specifically for the air mode of transportation, or within the* **Air Traveller Continuum** *(Figure 1.3). The key task of the e-border is to expedite the traveller's passage and improve border security through automation of the* **traveller clearance** *process, which includes the automation of two traveller clearance functions :*

- **traveller authentication** *(answers the question "Who are you?"), and*
- **traveller risk assessment** *(answers the question "What is your risk factor?")*

*Additionally, the e-border may also deal with automation of other border control processes, such as data collection, luggage screening, customs declaration and duty/tax payments.*

**Definition 2.1.2** **Border checks** *are the checks carried out at a border crossing point which is understood as any crossing-point authorized by the competent authorities for the crossing of external borders* [36].

Checkpoints may be operated by governments, airports or subcontracted to private security companies. Screening regulations may vary from one country to another.

**Definition 2.1.3** *The* **e-border** *is the infrastructure for border control and management aimed at automation of traveller clearance, specifically for the air mode of transportation or within the so called* **Air Traveller Continuum** *(Figure 1.3).*

In addition to dealing with automation of traveller clearance, the e-border may include various tools for automating data-collection and traveller service, such as:

- luggage screening,
- health screening
- customs declaration (duty/tax payments), and
- e-service, such as e-shop
- other forms of service, such as support to travellers with disabilities.

These automated tools are not directly related to traveller clearance. However they affect the Air Travel Continuum flow thus indirectly affecting the traveller risk assessment process.

The key and final top-level component of the e-border is the ABC machine, which performs automated (biometric-enabled) authentication and clearance of travellers.

Four other main components of e-border, as further established in Chapter 5 are: "Three-lane" risk-based processing; Non-automated behavior screening; Automated behavior screening technologies; and Self-service kiosks (also known as ABC or APC kiosks).

The term "ABC" is also used to signify the environment in which ABC machines are used. Two areas of applications for an ABC are distinguished:

- *Closed-set applications* [2] , which work with limited group of pre-enrolled users such as "trusted/registered travellers" and rely on local security infrastructure, and

[2] The meaning of terms "closed-set" and "open-set" applications in the ABC context is further discussed in Conclusions of this chapter and Appendix D.

**Critical Observation**

*In the context of this study,* **Automated Border Clearance (ABC) kiosks** *used by the CBSA, also known as* **Automated Passport Control (APC)** *kiosks in the USA,* **are not called ABC machines**, *since they do not perform authentication of travellers. Instead they are classified as* **Automated queuing and self-service technology** *(e-border component #IV). They however are critical to the e-border infrastructure, as they provide the foundation for further build-up of automated technology, including: dialogues and behaviour screening technology (e-border component #III) and biometric-based traveller authentication, thus becoming a true ABC machine (e-border component #V). - See Chapter 5 for definition of all e-border components.*

- *Open-set applications*, which work with users who are not pre-enrolled or known to the system, and which rely on national and international IT security infrastructure.

This is further discussed in Chapter 3, which establishes three main types, or generations, of the ABC machines.

ABC is a logistic system, meaning that it relies on number of resources, policies and procedures.

**Definition 2.1.4 Logistics** *of ABC is a set of rules and regulations used for the automated border crossing.*

Main logistical components of ABC are

- signs in the airport that divide travellers into separate groups according to nationality, passport type, etc;
- border service signs and procedures that divide travellers into streams according to their risks using "three-lane" concept, described in Chapter 5;
- system **design** and **topology**, further described below.

Two key ABC system designs are (see Figure 2.1):

- **kiosks**, which are gate-less open space systems interacting with the travellers in order to authenticate their identity and optionally printing a ticket confirming their identity and/or instruction code, and
- **e-gates**, which are defined as a physical barrier controlled electronically and manually.

Two key ABC topologies are: **two-stage topology**, in which the traveller initiates the document verification and then, if successful, moves to a second stage where a biometric match and other applicable checks are carried out [36], and **one-stage topology**, in which the traveller completes the whole transaction in a single stage without the need to move to another stage.

The list of online resources for news on ABC deployments, topologies and traveller feedback on their use is provided in Appendix A.1.

### 2.1.1 Supporting technology

As is further discussed in Chapter 5, an ABC relies on a number of supporting technologies, the key of which are e-passport, MRTD, RFID and data-bases, which are described below.


Figure 2.1: Key ABC system designs: a) kiosks (Canada airports), b) e-gates (Portugal), c) combination of both (Australia).

**Definition 2.1.5** *The* **e-passport** *is an ID in the form of a machine-readable travel document (MRTD), which combines a booklet with a contactless chip capable of secure data storage. E-passports can store biometric data in the form of images and/or templates for biometric modalities, such as face, fingerprint and iris.*

The e-passport and e-ID are defined by the ICAO standard [43] and are the key components of the automated border control technologies . E-passport is defined as a machine readable passport (MRP) containing a contactless integrated circuit within which is stored data from the MRP data page, a biometric measure of the passport holder, and a security object to protect the data with cryptographic technology. In 2002, the face was recommended as the primary biometric, mandatory for global interoperability in passport inspection systems. Fingerprint and iris were recommended as secondary biometrics. The e-passport uses RFID technology.

**Definition 2.1.6 Radio Frequency Identification (RFID)** *is a form of automatic identification technology (auto ID). Auto ID is characterized by data forms that are machine readable* [124].

Current efforts in RFID technology aim at creating a so-called **RFID infrastructure** in which holders of e-passports will be associated with their baggage, e-visa, and statistical surveillance. The role of RFID infrastructure in ABC technologies will be increased [43, 30].

In RFID, less human intervention is required for data retrieval. For example, the e-passport is based on passive RFID technology. An e-passport does not have own source of energy and relies on the energy obtained by induction from the electromagnetic field of the reader[3].

[3]For example, the standard ISO 14443 uses the frequency 13.56 MHz and enables contactless communication over a distance of up to 10 cm at a speed of 106 kbps (up to 848 kbps is possible).

**Definition 2.1.7 Registered travellers** *or* **trusted travellers** *are passengers who undergo a rigorous risk assessment process and have submitted their biographic and biometric data such as iris, fingerprint, face etc. to a government.*

Registered Travellers Programs (RTP) / Trusted Travellers Programs (TTP) are the essential part of the e-border management, as they allow for more focused allocation of border control resources towards travellers whose risk is unknown.

**Definition 2.1.8 Electronic visa waiver** *is the approach to dismantle the paper visa system for nationalities that pose a low immigration risk.*

The electronic visa waiver is a source of early warning information such as that a certain person is coming to the country. This allows more time for assessment of potential risks [47]. The electronic visa waiver is a part of the Entry-Exit system.

**Definition 2.1.9 Entry-Exit system** *is the technology for detection and prevention of overstaying for foreign visitors.*

The main function of the Entry-Exit system is to match foreign visitors' arrival records to subsequent departure records. It is expected that the system will analyze all arrivals and all departures, and an immigration agency could determine whether and when a foreign traveller departs the country and identify those who overstay their period of admission.

An example of the Entry-Exit system is the US-Canada Entry-Exit system currently being developed by the CBSA and DHS [56, 57, 58]. The aim of this system is to facilitate exchanges of entry information between the two countries. In particular, an entry into one country will be paired with an exit from the other. Two phases for the implementation of this system are defined. The first phase of the US-Canada Entry-Exit system includes twelve personal data elements recommended by ICAO: first name, middle name, last name, date of birth, nationality, gender, document type (e.g., a passport), document number, document country of issuance, work location code / U.S. POE codes, date of entry, and time of entry, which are determined to be the minimum necessary in order to carry out the objectives of this phase, most notably reconciling entry and exit records. The second phase of this Entry-Exit system will extend these elements to include traveller's biometric data.

**Definition 2.1.10 Database** *is understood as any storage of biometric templates and related end-user information [43].*

Only ABC machines for service of trusted travellers collect and store personal data, including traveller's biometric templates. ABC machines that serve e-passport holders (including trusted travellers), operate with a database known as a **watchlist**. This database contains personal data of persons of interest. This data is gathered from various national and international agencies/databases. A sample list of databases used for border access in EU, populated by the University of Calgary researchers from [20], is provided in Table 2.1.

One of the challenges of the e-border is seen in keeping watchlist databases up-to-date [76].

## 2.2 Concepts related to traveller risk assessment

The aim of the *risk assessment* is to assign one of several available security classes to each traveller. This decision is made based on the traveller's perceived risk level which is calculated using statistical prediction and available information.

The initial source of information for risk assessment is **Advance Passenger Information (API)**; it is a pre-declaration of document information before departure; it contains information on the flight and personal information from the machine-readable zone of the traveller's passport. Real-time processing of API aims at ensuring that a traveller has the right clearance.

Risk assessment is performed using two technological components:

Table 2.1: Databases used in border control in the EU.

| Database | Purpose |
|---|---|
| Schengen Information System (SIS) | National security, border control and law enforcement purposes |
| EURODACE | Help identify asylum applicants and persons who have been apprehended in connection with an irregular crossing of an external border of the Union |
| Customs Information System (CIS) | Assist in combating customs related crime by facilitating co-operation between European customs authorities |
| EUROPOL Information System | Fight against cross-border crime |
| Visa Information System (VIS) | Facilitate the visa application procedure and the fight against fraud, checks at external border crossing points, and the examinations of asylum applications; assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States, contribute to the prevention of threats to the internal security of any of the Member States. |
| Advanced Passenger Information (API) | Improving border controls and combating illegal immigration by the transmission of advance passenger data by carriers to the competent national authorities. |
| Passenger Name Record (PNR) agreements with Canada, Australia and the United State | Preventing and combating terrorism and related crimes and other serious crimes that are transnational in nature, including organised crime. |
| EU-US TFTP (Terrorist Finance Tracking Programme) | Ensuring an effective instrument to prevent and to fight the financing of terrorism, and limiting personal data flow to third countries |

1. **Pre-screening** (also called statistical surveillance), which assigns each traveller a risk factor based on all available information about him/her from the time he/she initiates the travel arrangement (Stage 0 of the Air Traveller Continuum).
2. **Screening** (also called **risk profiling**), which is applied along all other stages of person's travel from the time he/she enters the airport with the purpose of further refining his/her risk factor as he/she moves along the Air Traveller Continuum.

More general sense of the term "risk profiling" means that information about the traveller *is accumulated* from the moment of buying tickets and providing required personal information (pre-screening). Having provided this information, the traveller enters airport with a predefined personal risk-factor which can be adjusted via the airport risk profiling infrastructure.

Another term that is closely related to risk assessment is *differentiation*, which is screening of different passengers in different ways, according to their risk. Differentiation does not mean screening based on race, gender or religious beliefs [27].

**Definition 2.2.1 Cybermetric** *is technology to identify a person from his/her interactions and circle of friends in social networks, such as Facebook or Google+, (adopted from [123]).*

This study highlights that in the context of an air traveller continuum, when person's social interactions can be tracked from the moment s/he purchases the ticket, person's cybermetric is becoming one of the most important pieces of information (evidence) that can be used for both traveller identification and his/her risk assessment.

Additionally, researchers from the University of Calgary introduced another concept called *social integration* or *social embedding*, which addresses the fact that ABC systems cannot operate without traveller risk assessment [9].

**Definition 2.2.2 Social integration** *of the ABC machine is defined as a phenomenon of its interaction with a local or global network of machines or components (such as databases), aiming at information gathering and exchange.*

**Definition 2.2.3** *The* **depth of social integration** *is defined as the number of national and international databases that support the ABC technologies in performing the travellers' risk assessment.*

The following example illustrated the application of social embedding for ABC applications. Among biometric modalities considered for ABC, iris has much better biometric false match/non-match rates compared to face and finger (See Appendix F). However, iris "snapshots" (images) are not left at a crime-scene (in contracts to latent finger-prints or facial images captured by video-surveillance cameras). They are also not used in social media (Facebook, Google, etc.). Hence, it is said that iris modality has minus one less *depth of social embedding*, compared to fingerprint, and minus two, compared to faces. As a result, iris by itself may not be used for ABC when the risk of a traveller is unknown and needs to be determined. However, when combined with other modalities, whenever it is available (as in pre-enrolled programs such as Nexus or in national ID-programs based on iris), it can greatly improve the reliability of biometric-based authentication. More discussion on the use of iris is provided in Chapter 4.

## 2.3 Concepts related to training of ABC operators

This category of concepts was introduced by University of Calgary researchers [9], the most important of which are mentioned below.

A training facility is defined as an environment for training personnel/operators for border crossing automation. There are two main approaches to training personnel for border crossing automation: (a) *Virtual training facility*, and (b) *Training ground environment*. Virtual training facility based on simulation techniques provides a safe and relatively inexpensive means to rigorously explore multiple dimensions of complex real-world scenarios including skills for working in a team. In contrast to virtual training, the training ground environment provides real-world conditions for training border officers/operator in critical scenarios. Examples of such an environment include the DHS testing area [64] and FAST facilities [65].

Another approach is known as covert testing which can be extended for training personnel for border crossing automation. The TSA has developed thousands of covert tests in an effort to identify vulnerabilities and take corrective action to improve checkpoint screening [13].

## 2.4 Concepts related to complex system management and anlysis

This category of concepts was also introduced by University of Calgary researchers [9], the most important of which are mentioned below.

**Definition 2.4.1 Modeling and simulation** *in ABC technologies assumes evaluation of the ABC machine and supporting technologies at all life-cycle phases, by replacing real-life processes by their appropriate mathematical models. The obtained information can be interpreted in terms of predicted, or potential, events, threats, and risks.*

**Definition 2.4.2 Biometric system life-cycle** *is defined as stages of biometric system design, prototyping, testing, deployment, degradation, and dismantling.*

For example, biometric-enabled ABC systems for trusted travellers based on iris recognition in UK were dismantled in 2013 [107]. The life-cycle of these machines including their development is more than 10 years. They were replaced by the next generation of biometric machines which implement border crossing technology based on biometric passports.

To further quantify the biometric system life-cycle performance, the concept of the *degraded life-time performance metric* is introduced in this study (Section 6.3), according to which three critical measuring points of the ABC life-cycle performance are recognized: (a) *theoretical* (reported in literature, corresponding to the performance of the chosen biometric modality), (b) *tested* (vendor claimed, obtained in laboratory or mock-up experiment), and (c) *operational* (real performance, observed in deployed system).

More analysis of metrics and tools that can be used for describing and analyzing ABC performance is provided in Chapter 6.

## 2.5 Conclusions

In conclusion, a number of discussions items are put forward related to the use of the terms "biometric", "authentication" and "automated border control" in the context of extending border control from a checkpoint to a traveller continuum.

### 2.5.1 Wider meaning of biometrics and authentication in the context of automated border control

Historically, the terms **"biometrics"** and **"biometric recognition"**, as used by industry and defined by ISO [4] , refer exclusively to the technology used for verification (1-to-1 matching) or identification (1-to-N matching) of individuals based on their "distinguishing, repeatable biometric features". Recognition of person's state (such as emotion, stress, health condition etc), which can be also estimated from biometric measurements (e.g., from heart rate, pupil dilation, facial images), does not fall under the current definition of biometrics, Similarly, recognition of person's types or classes (such as age, gender or race), which can can be estimated from facial images and other biometric features, is not covered by ISO Sub-Committee on Biometrics (SC 37) either.

Similarly, the term **"authentication"** is traditionally defined as an act of proving or showing to be of undisputed origin or veracity, which can be either biometric-based (using face recognition, for example) or non-biometric based (using documents, for example)

Through the course of this study, it has been realized that in open-set applications such as automated border control, when nothing is known about a biometric system user (traveller), it is suitable to extend the definitions of both of these terms, because the final admissibility decision about the traveller is not based solely on a single act or piece of information, but rather on all information that has been accumulated about the traveller through the entire course of his or her travel in Air Traveller Continuum.

The recommendation is made therefore to extend the definition of "biometrics" to include the technology for recognition of person's classes and states. Under this extended definition of biometrics, biometric-enabled ABC systems of the future generations are envisaged as machines that will use traveller biometric features

[4] ISO standards on "Biometrics" are developed Sub-committee on "Biometrics" (SC 37). The latest approved revisions of the following related documents are freely available at http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html: ISO/IEC 2382-37:2012, Information Technology "Vocabulary" Part 37: Biometrics. ISO/IEC TR 24741:2007 Information technology - "Biometrics Tutorial". ISO/IEC TR 24714-1:2008, Information technology – "Biometrics – Jurisdictional and societal considerations for commercial applications – Part 1: General guidance". Other key references on Biometric vocabulary include DoD Common Biometric Vocabulary developed by the Defense Forensics and Biometrics Agency (DFBA) Architecture Branch found at http://www.biometrics.dod.mil/Files/Documents/References/common%20biometric%20vocabulary.pdf and International Biometrics Industry Association (IBIA) Glossary developed by National Science & Technology Council's (NSTC) Subcommittee on Biometrics found at https://www.ibia.org/biometrics/glossary.

to perform both authentication of travellers (traditional definition of biometrics) and their risk assessment (extended definition of biometrics). In both cases, "biometric recognition" is understood in a broad sense as contributing to the decision related to the person's identity, which may or may not be correct. Biometric systems always recognize some level of error.

Similarly, authentication of the users in ABC can be considered as an *intelligence-gathering* or *evidence-accumulation* process that is performed throughout the entire Air Traveller Continuum, rather than at a single Checkpoint. It includes two components: 1) non-automated component – related to the extraction of information from all available sources (biometric sensors, responses during the interview, API / PNR, data bases, global search in social networks and security infrastructures, etc.), and 2) automated component – related to matching this accumulated information against the previously retrieved information about the individual.

Such an interpretation of authentication of travellers in ABC becomes useful when analyzing the performance of the ABC through simulation.

### 2.5.2 Wide meaning of automation in border control

One of the key observations of this study is that "automated border control" (ABC) does not only refer to automation in traveller authentication (as in e-gates in EU or NEXUS iris kiosks) and automation in custom declaration tasks (as in APC kiosks), but it also refers to automation in traveller screening and risk assessment. Furthermore, it is highlighted that all these automated technologies (1: traveller authentication, 2: traveller custom declarations, and 3: traveller screening / risk assessment) can be done at the same time, at the same location and at the same kiosk/gate, provided that such kiosk/gate is equipped with proper sensors and artificial intelligence (AI). In doing so, the same biometric sensors, such as video, audio, weight / temperature / heat sensors, can be used to perform two types of biometric recognition: 1) for traveller authentication - by matching his/her biometric measurements to those corresponding to a particular person (classic definition of biometrics), and 2) for traveller risk assessment - by matching his/her biometric measurements to those normally expressed by stressed individuals during an interview (extended definition of biometrics).

To further extend the above observation, one can state that ABC machine is an example of a large-scale biometrics-enabled system, in a wide definition of biometrics. It uses various biometric data captured from sensors and stored on e-passports/ID such as face, iris, and fingerprints to automate the recognition of person's identity. Other examples of biometrics-enabled systems are Integrated Automated Fingerprint Identification System (IAFIS), a national fingerprint and criminal history system that stores, searches, matches, and shares fingerprints; Automated Biometric Identification System (IDENT), a national fingerprints system with extension to irises and facial images, which is used for many purposes including border security, information on persons undergoing naturalization and visa processes, and in counter-terrorism efforts; and Automated Biometric Identification System (ABIS) that stores facial images [23]. In the ABC context however, these systems are defined as ABC **supporting technologies**.

Additionally, in the context of automated clearance of travellers, another type of *biometric technologies* is considered. These are the so-called *behaviour analysis* or *AVATAR-like* technologies that do not directly perform recognition of travellers but rather use their biometric measurements for other applications relevant to the border context such as stress, lie, emotion and disease detection. These applications can make use of such additional biometrics measurements as heart-beat, temperature, pupil dilation and saccadic motion, heat / perspiration detection, as well as facial expression already available from the cameras, to improve both authentication of a person and estimation of his or her risk. More analysis into behaviour analysis systems and their convergence with other automated border control systems is provided in Chapter 5. The future outlook of the entire ABC, with various types of biometric employed in it, is further presented in Chapter 7.

### 2.5.3 Contribution to the standards on biometric terminology

One of the key objectives of this study was to contribute to better standards, including vocabulary, related to the use of biometrics for automated border control. The outcome of this work, combined with the results from the preceding PROVE-IT() studies [137, 138], which dealt with another open-flow biometric application - that of people recognition in surveillance video, is being prepared as a separate report [5]. This report, the excerpts from which are presented in Appendix D, is designed to assist organizations in further improving and extending their biometric standards specifically to address the needs of such two growing biometric application areas as automated border control and video surveillance. Additionally, the full set of recommendations for improving and extending standards related to designing and analyzing automated border control systems through their life-cycle has been prepared in the University of Calgary report, the summary of which is presented in Appendix C.

**Critical Observation**

*The biometric terms were originally developed for applications such as physical security and forensics, where the number of processed subjects is limited and controlled. When applied to more complex applications, such as automated border control or video-surveillance, where the flow of subjects is very high and subjects themselves are not known in advance, these terms are found to be insufficient.*
*– "Authentication" is no longer a single checkpoint act, but rather a process of accumulating the evidence over the entire traveller continuum. "Biometric recognition" also includes recognition of person's state (emotion, stress, health condition) and type (gender, age, race). "Recognition" of a traveller in a traveller continuum is always coupled with his/her "risk assessment" and "trust". In addition to biometrics, "cybermetric" is critical for authentication of travellers.*

# Chapter 3

# Evolution and categorization of ABC

## 3.1 Border control vs. access control: key differences

Biometrics, as a technology for automated authentication of humans based on their measurable biological traits, was originally applied to access control. Physical and logical access control systems, enabled by the biometric recognition of fingerprints and iris, have become an essential part of the security and identity management infrastructure in many organizations. Several guidelines and standards have been developed to support these systems and evaluate their performance (such as those discussed in Appendix C).

Following the success of biometric-enabled access control systems, it appeared natural to extend the application of biometric systems from access control to border control. In the early 2000s, several countries introduced Registered (or Trusted) Traveller Programs (RTP/TTP) to expedite the border crossing for the pre-cleared pre-enrolled travellers through biometric-based verification of their identities. This was done by reusing the same framework that was already used for access control applications. In some cases, the same biometric components were deployed for both border and access control, as in the case of the NEXUS iris recognition program, which used the same iris biometric device as in the CATSA Restricted Access Identification Card (RAIC) access control system (shown in Figure 3.1). [1]

While seemingly very similar to biometric-enabled access control, biometric-enabled border control systems are significantly different from their earlier predecessor however. It is important to highlight these differences so that better methodologies and practices can be developed for ABC, while making use of those already developed for access control applications. These differences are highlighted in Table 3.1 in terms of changes, or shifts, in their functionality and the accepted human-machine interaction procedures.

In addition, unlike the earlier generations of the ABC machines, whose usage was voluntary albeit recommended, the ABC machines deployed today are deemed to be a mandatory component of the e-border. The ABC machine will process the majority of on-going traveller traffic. Therefore, it needs to work 24/7, becoming a critical infrastructure that needs to be constantly monitored and supported. In some cases, this support may have to be done by the border officers who have other critical duties, related to their border control mission-critical functions.

The evolution of biometric-enabled ABC systems is conceptualized in Figure 3.2 using two-dimensional space, in which one coordinate corresponds to the number of human-related factors and the other coordinate corresponds to the number of technology-related factors that influence the performance of the system. The figure shows that the number of technology-related factors (related to both biometric and non-biometric components of the ABC technology), and the number of human-related factors (controlled and uncontrolled) that influence the performance of the system increases with every ABC generation.

[1] *"Iris ID's iCAM 7 Series and IrisAccelerator backend matching engine are integral parts of the changes to the Nexus program... A similar system is also being used by Canadian Air Transport Security Authority (CATSA)"* (Charles Koo, CEO of Iris ID) - http://www.planetbiometrics.com/article-details/i/2745 (retrieved March 10, 2015)

Table 3.1: Key differences between biometrics-enabled access control and biometric-enabled border control systems, expressed in terms of shifts in system functionality and human-machine interaction procedures.

1. **Shift from habituated to non-habituated users:** The users of access control systems are *habituated* users. They are trained to use the system and use it on a regular basis. In contrast, the users of ABC systems are *non-habituated* users [164]. They may not know or may forget how to use the system, because they use it infrequently (only when travelling), and systems may look different in each airport.
2. **Shift towards additional human factors:** Travellers belong to a specific category of users, which are also preoccupied by other travel-related tasks and challenges (finding the way in unknown place, under time pressure, jet-lag, etc.) and be therefore under additional stress and fatigue. Introducing a technically advanced system and procedure to travellers may further contribute to their stress and complicate their travel. Therefore, it is important to conduct a usability study, which examines all human factors related to the interaction of travellers and the ABC machines, and to take the results of such study into account while implementing an advanced system.
3. **Shift from a limited set of known users to large flow of unknown users**, some of whom may belong to high risk travellers who will intentionally attempt to defeat the system (non-zero effort attack), and some may cause the system to malfunction due to misunderstanding or physiological condition (zero-effort attack);
4. **Shift from biometric component to a higher number of components and supporting technologies**: As discussed in Chapter 5.2, ABC systems rely on additional support from a number of e-border supporting technologies (e-document readers, RFID, pre-screening and watch-list databases), each of which may malfunction with certain degree of probability.
5. **Shift from fully-automated to semi-automated operation and need for personnel training:** As opposed to access control, in border control, the final decision is always made by a human. If the decision made by an ABC machine is not sufficient, the border officer will have to use his/her knowledge and expertise to arrive at the final admissibility decision. This highlights the need for developing ABC personnel training. It is costly and inefficient to develop special training systems for ABC personnel that would simulate all possible outcomes of the ABC system. Instead, an automated short-term intensive training can be developed based on a training mode of the ABC machine.
6. **Shift from controlled to semi-controlled environment:** The ABC systems operate in public spaces controlled by separate parties (airport authorities, transportation security, customs/border control), which have different and sometimes conflicting objectives of operating the ABC system. As a result, the positioning of the ABC system may not be the most optimal from the biometric performance perspective. Additional factors affecting performance are often present, such as light position and brightness.
7. **Shift from non-attended to attended users:** Users of ABC machines are referred to as *attended users* of the biometric devices. The latter are observed and guided by border officers, as opposed to unattended users, such as in unsupervised access control [173].

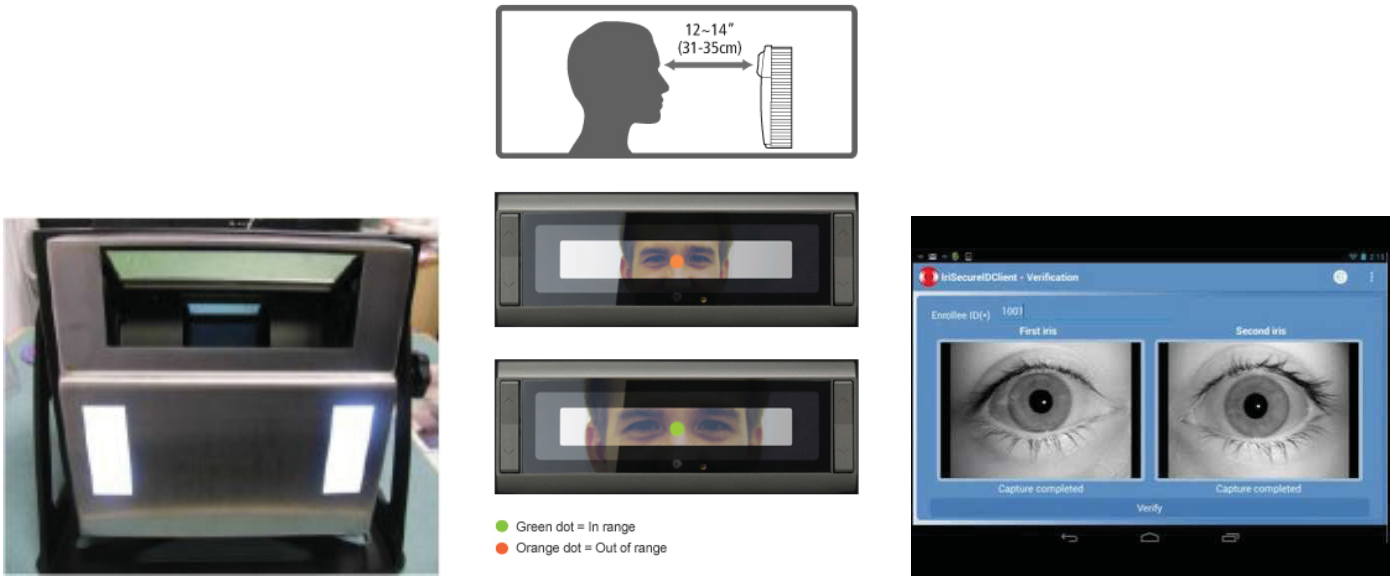



Figure 3.1: Iris recognition camera used for access control by CATSA and automated border control by CBSA NEXUS program (see also Figure 4.3).
(The image on the right shows iris images captured by the camera. Source: Google "Iris ID")

Following the deployment of biometric-based access control systems, which contain mainly biometric components and are operated by a known number of trained users, the first known ABC systems, embodied in the form of biometric-enabled RTP kiosks, are deployed to provide expedited passage to a small percentage of pre-cleared registered travellers (Gen-1 ABC). Next, biometric-enabled e-gates installed at checkpoints in various airports are capable of processing all travellers carrying an e-passport and eID biometric documents (Gen-2 ABC). Finally, future systems will process the entire flow of travellers arriving by air, with the information about them collected through their entire travel within the *Air Traveller Continuum* (Gen-3 ABC). The flow of system users also grows from a limited number of enrolled pre-cleared low-risk individuals (in access control and Gen-1 ABC systems) to a much larger flow of people whose risk score is not known, and many of whom are non-experienced users.

The following observations characterizing the evolution process of biometric-enabled systems can be made:

1. The contribution of non-biometric vs. biometric components is increasing drastically for ABC machines, compared to access control systems (the size dark blue vs. light blue boxes along the horizontal axis in the figure). These include components relate to document scanning and their authentication, traveller risk assessment, and gathering information about the traveller from available sources, the number of which grows with each ABC generation.
2. The value of uncontrolled human factors vs. controlled human factors is increasing rapidly (the size of the red box along the vertical axis in the figure). These factors relate to various social, logistical, psychological, geographical, ethnic, and business attributes, the value of which grows with the complexity of the system.
3. The sheer quantity of traveller traffic changes drastically with each new ABC generation: access control systems do not have any traffic outside of the limited and fixed quantity of access control employees; Gen-1 ABC systems deal only with a small percentage of travellers, who have enrolled to the system (less than 10% of traveller traffic); Gen-2 ABC systems open the technology to all travellers with e-passports or eID, although it is not yet required to use it, and the majority of travellers still do not use it (20%-50% of traffic). Finally, Gen-3 ABC systems are planned to handle close to 100% of all traveller traffic, which is also expected to grow compared to the traffic volume today.

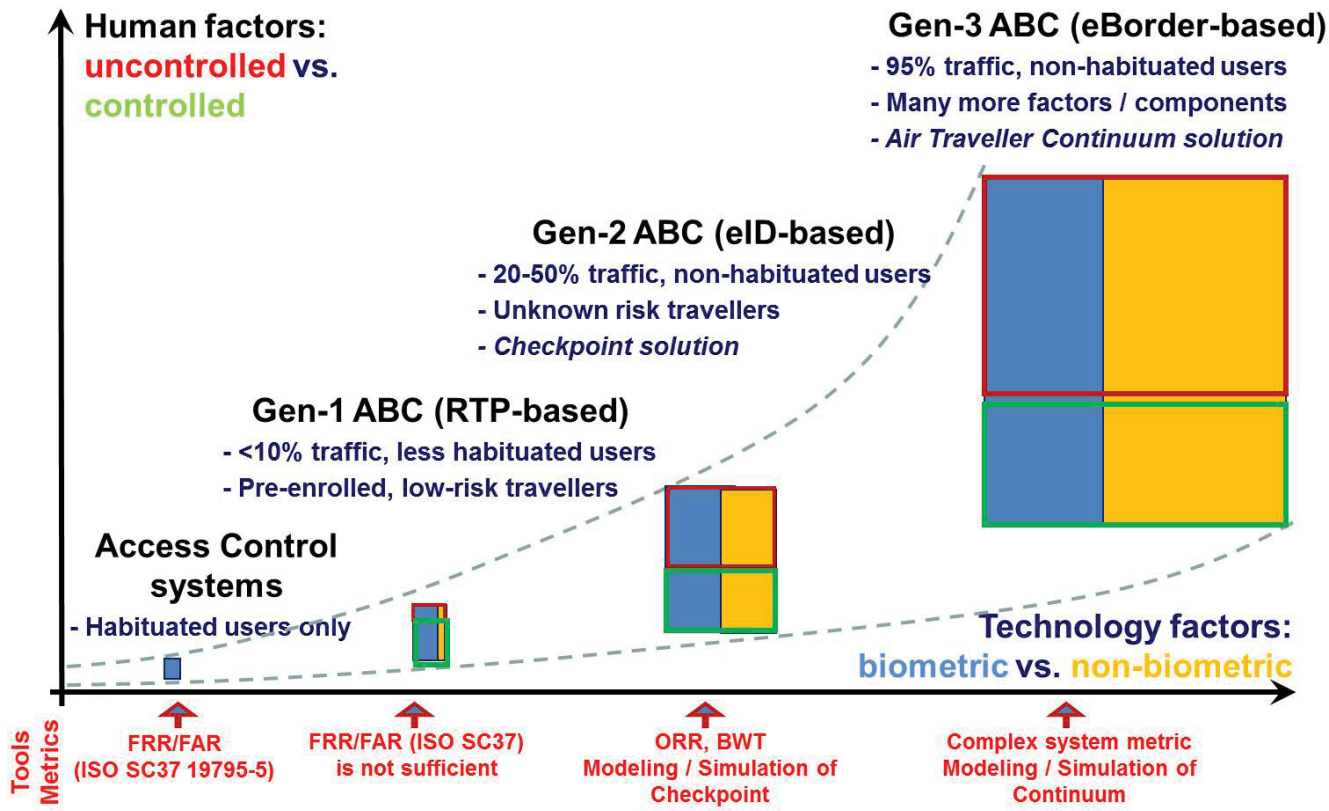



Figure 3.2: Conceptual diagram of the evolution of biometric-enabled ABC systems in the technology-vs-human factors space. The number of technology factors, those related to biometric (blue) and especially those related to non-biometric (yellow) ABC components, grows with every ABC generation. Similarly grows the number of human factors: controlled factors (green) and especially uncontrolled factors (red).

## 3.2 Three generations of ABC

Following the evolution of ABC deployment presented above, this study establishes *three* distinct types, or generations, of biometric-enabled ABC systems.

In the following, formal definitions of each ABC generation are presented, followed by the presentation of the conceptual architecture of the ABC machine in the next section and the analysis of issues of Gen-1 and Gen-2 ABC systems in the next chapter. Gen-3 ABC systems, which are based on the e-border concept, are the focus of Chapter 5.

### 3.2.1 Gen-1 ABC (RTP/TTP-based)

In the IATA Recommended Practice [31], ABC is distinguished with respect to the travellers' division into two groups: (a) regular and (b) registered travellers. ABC for registered travellers is defined as follows:

**Definition 3.2.1** ***ABC for registered travellers (Gen-1 ABC):*** ABC *is an automated border control system that either authenticates the travel documents, tokens or permits, or denies admission to a traveller according to some pre-established specifications. ABC may additionally verify a passenger biometric data against the travel document and/or token, or a pre-existing database, containing biometric data. It may also register the entry to or exit from the country* [31].

It follows from IATA's Definition and the Registered Traveller Scheme, that a *trusted traveller does not need to identify himself/herself*; it is only required that his/her travel documents are identified. Personal identification is considered as additional level of security but is not a mandatory requirement. That is, ABC for trusted travellers may or may not include biometric-enabled support. Generalization of the ABC concept to serve regular travellers is attributed to the ABC technology/machine.

### 3.2.2 Gen-2 ABC (eID/ePassport-based)

The IATA's definition above addresses the ABC process for the registered travellers. Frontex [36] provides definition of the ABC machine for the travellers who are holders of the e-passports/ID.

**Definition 3.2.2** ***ABC for e-passport/eID holders (Gen-2 ABC):*** *The ABC machine is an automated system which authenticates the e-MRTD, establishes whether the traveller is the rightful holder of the document, queries border control records and automatically determines eligibility for border crossing, according to certain pre-defined rules* [36].

### 3.2.3 Gen-3 ABC (eBorder-based)

A concept of the future, an ABC system, as established in this study , is defined theoretically as follows [2, 3]:

**Definition 3.2.3** ***Gen-3 ABC:*** *system is an ABC machine of the future that is defined by the following* six *properties:*

- *Property 1: It can operate only within the e-border infrastructure, supported by other e-border components and supporting technology.*
- *Property 2: It is a large-scale system that processes very large, possibly unlimited, flow of travellers.*
- *Property 3: It performs authentication of unknown travellers, who may or may not be in the database, using biometrics-based and non-biometric-based (such as cybermetric) techniques.*
- *Property 4: It is a semi-automated system that serves as a tool and operates under supervision of border officers, who need to be trained for the system to be efficient.*
- *Property 5: It is a risk assessment system that analyzes all available information about each traveller and assigns him/her a risk factor.*
- *Property 6: It is a machine that automatically communicates across the data network with other ABC machines and e-border components.*

**Critical Observation**

*In contrast to earlier generations, which were checkpoint solutions, next-generation ABC systems are traveller continuum solutions, which accumulate information about travellers as they advance through the Air Traveller Continuum, making the final admissibility decision based on all gathered intelligence.*

The last two properties differentiate ABC of the future from ABC of the present, and effectively extend ABC from a "Point solution" to an "Air Travel Continuum solution". The placement and key principles the operation of the ABC machine in the hierarchy of all e-border components, the main five of which are defined in this study, are further analyzed in Chapter 5.

## 3.3 Architecture of the ABC machine

As discussed in [3, 10] the ABC machine can be viewed as a decision support assistant (Fig. 3.3). It includes a *recognition assistant* tasked with identity verification using the biometric modalities specified by the e-passport, and a *risk assessment assistant* which performs the risk assessment function using all available sources, the key of which are i) **biometric**, ii) **biographic**, and iii) **cybermetric**.

The reports, provided by these assistants, are processed using the principles of consolidated clearance and decision-making. The output is a recommendation, which can be made final by default. This corresponds to the semi-automated principle of the border control.

If a traveller has been directed to a manual check, the officer can use an interviewing technique supported by a biometric-enabled *behavioral assistant*, which can be biometric-based (in the extended definition of biometrics, discussed in Section 2.5.1) or non-biometric (using expert system software that intelligently generates set of questions based on the received answers). This technology is further analyzed in Section 5.3). More details on the concept of decision support assistant are presented in [158, 159].

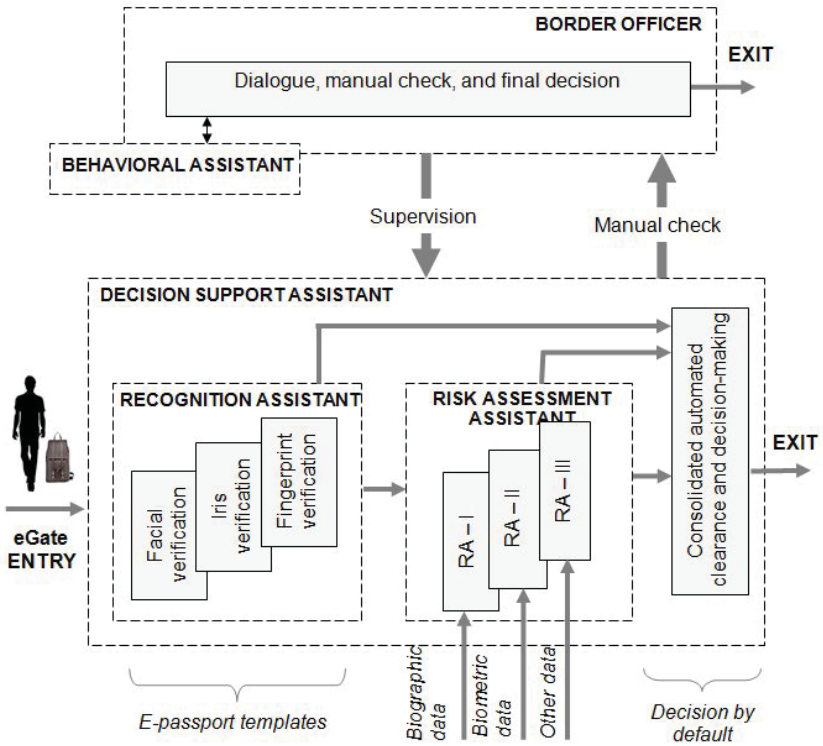



Figure 3.3: Architecture of the ABC machine consists of (a) the supervision facilities, and (b) the decision support assistant which includes both the verification assistant and the risk assessment assistant.

### 3.3.1 The ABC system as intelligence-gathering machine

ABC systems are complex systems that cannot be benchmarked the same way as are biometrics technologies or networks. One of the approaches for analyzing the performance of ABC machines is based on the generalized concept of the *evidence accumulation* or an *intelligence-gathering machine*.

Specifically, following its formalized definition, Gen-3 ABC system can be viewed as a multi-state intelligence-gathering machine [3, 10], which accumulates information about travellers as they advance in their travel through

the Air Traveller Continuum, the key states of which are shown in Table 3.2, following the schematics of the Air Traveller Continuum developed in Section 1.3 (Figure 1.3).

One of key efforts of the University of Calgary researchers was to show that, once formally defined as an evidence accumulation (or intelligence-gathering) machine, ABC system can be efficiently modeled using probabilistic techniques, which allows one to quantitatively describe and estimate all risks associated with ABC system performance, as discussed in [8] and their earlier work [154]-[162]. Additional information on modeling techniques and tools for ABC is provided in Chapter 6.

Table 3.2: The states of the ABC system as an intelligence-gathering machine.

| |
|---|
| *State 1:* Initialization of the ABC machine by providing personal data when buying a ticket. |
| *State 2:* Initial risk-factor estimation using the clearance technologies; information about the traveller is searched for and analyzed starting from the moment of the ticket purchase. |
| *State 3:* Risk factor correction using risk assessment technologies based on local surveillance facilities; information about the traveller's activity in the airport (logistics) is collected and analyzed. |
| *State 4:* Risk factor correction using verification technologies (e-passport) and additional risk assessment techniques (watchlists for the e-passport and its holder). Any decisions are made by default. |
| *State 5:* Risk factor correction by manual risk assessment (by border officer), if needed. The final decision is made. |

## 3.4 Alternative ABC categorizations

Several other approaches have been found in the literature related to the categorization of ABC technologies. In these approaches, different criteria for categorization are utilized, briefly summarized below in their relationship to the three generations of ABC developed in this study.

IATA and ICAO use the following groups of criteria in their approach to the ABC technology evaluation and prediction (roadmap 2020+) [44, 27]:

- Risk assessment and traveller differentiation,
- Technology and methodologies for implementation, and
- Operations.

In these terms, IATA and ICAO introduce today's checkpoints, as well as their vision of future checkpoints that correspond to the second and third generations of the ABC machines. In this classification, self-service kiosks, which are the supporting technologies for scanning the travellers' documents, are not considered. The IATA and ICAO approach is useful for development of the long-term strategy that has risk mitigation as the highest priority. The considered risks include potential cyber attacks, terrorism threats, pandemics/epidemics, and intentional appearance disguises.

Frontex uses a group of technological criteria, which results in the classification of ABC machines that distinguishes the machines of the first, second, and third generation [35]–[39]. Similarly to IATA and ICAO, Frontex uses this approach for strategic planning.

Finally, another categorization of ABC solutions has been presented by Acuity Market Intelligence [11], which defined the following five categories:

(a) ABC eGates: Automated Border Control Gates including Kiosks delivered as part of the configuration deployed at ARRIVALS or DEPARTURE that replace passport/border control agents seated at desks.

(b) ABC KIOSKS: Automated Border Control Kiosks at ARRIVALS (or for DEPARTURE preclearance) like those deployed in United States and Canadian airports for Global Entry and NEXUS programs. ABC KIOSKS provide essentially the same function as an ABC eGates but without an integrated physical barrier.

(c) APC KIOSKS: Automated Passport Control Kiosks like those currently deployed at United States and Canadian Airports that expedite ARRIVALS. APC Kiosks capture information prior to arrival at a border control agents desk significantly reducing processing time. Most APC Kiosks currently capture only a photo, though they are biometric capable. Some biometric APC Kiosks have been deployed to expedite foreign national arrivals from visa waiver nations.

(d) AIC KIOSKS: Automated Immigration Control Kiosks for DEPARTURE. There are currently no AIC KIOSKS deployed. These would be part of an integrated immigration processing program used to collect biometrics at check-in, bag drop, or security designed to integrate with DEPARTURE ABC eGates and AIB eGates.

(e) AIB eGates: Automated Immigration Boarding Gates for DEPARTURE designed to integrate with DEPARTURE AIC KIOSKS and ABC eGates and to confirm that an individual tied to a valid travel credential (e.g. e-passport) and a valid travel reservation via the AIC KIOSK and ABC eGate is the same individual that boards the aircraft.

Based on the definitions of the ABC machine and other e-border components introduced in this study, the following mapping between the categories proposed by Acuity Market Intelligence and ABC/e-border categories developed in this study is established:

(a) ABC eGates correspond to the ABC machines of the second generation (Gen-2 ABC).
(b) ABC KIOSKS correspond to the ABC machines of the first generation (Gen-1 ABC). These machines are demounted in EU, because their functions have been delegated to the Gen-2 ABC machines.
(c) APC KIOSKS do not satisfy definition of the ABC machine. They only check the traveller's document, and should be identified as an e-border component supporting the ABC, which is further discussed in Chapter 5.
(d) AIC KIOSKS is a part of the US-VISIT entry-exit system; this is a US national program. In the EU, these functions will be delegated to the ABC-machines.
(e) AIB eGates do not satisfy the definition of the ABC machine. They only check the traveller's documents and should be identified as the technology supporting the airport logistics.

At the same time, as highlighted by the University of Calgary researchers, the categories developed by Acuity Market Intelligence have certain limitations. Specifically, they do not reflect the actual evolution of the ABC and may result in the following erroneous interpretations:

- Forecasting regarding the dominance of the AIC kiosks, which are the components of the US-VISIT system deployed only in US, may not be true for the rest of the world. In EU and other countries, where the ABC machines are deployed, the AIC kiosk will be embedded into ABC machines.
- The APC kiosks are mainly used for domestic airlines in US. In other systems worldwide, this function is delegated to ABC machines.
- The ABC kiosks, such as NEXUS machines, serve only trusted travellers crossing the US-Canada border. The last similar systems deployed in UK (IRIS kiosks) have been demounted in 2012 and replaced by ABC machines.

## 3.5 Conclusions

Various approaches to the classification of ABC technologies exist. Choosing a particular approach depends of the specific needs and goals, such as vision of horizons and progress evaluation, comparisons of various

systems, deployment criterion, risk/cost estimations, vulnerability, etc. There is no uniform classification of ABC technologies which satisfy all the desired requirements.

The IATA and ICAO approach to categorization is based on three groups of criteria, such as: (a) risk assessment and differentiation, (b) technology, and (c) operations well suited for the strategic vision, as well for understanding details of functioning. Relations to other categorizations can be established using notions of risks/security, technological opportunities, as well as required specific-purpose operations.

In this report, classification of ABC technologies follows closely the IATA, ICAO, and Frontex approaches, however some novel extensions are proposed. Strategically, these approaches follow the classical paradigm in distinguishing the system using the notion "generation". In this study, the rigorous definitions and properties of the ABC machine, as a complex large-scale specific-purpose machine, provide new insights and predictions, regarding future ABC systems that will be based on a certain combination of various technologies. Simplification of the categorization such as that by Acuity Market Intelligence [11] may lead to false predictions in the market forecasting and incorrect understanding on the evolution of the technology development in general.

**Critical Observation**

*The categorization of ABC systems developed in this study, as belonging to one of three generations, the third generation of which makes use the entire e-border infrastructure, provides the holistic evolutionary point of view of the border modernization process and allows one to develop an ABC model that can be used for cost, benefit and risk analysis of the present and future ABC solutions.*

# Chapter 4

# Analysis of issues

This chapter provides a scan of issues with the already deployed biometric-enabled ABC systems, specifically those related to the Gen-1 ABC systems based on iris recognition of pre-cleared registered travellers and Gen-2 ABC systems based on face recognition of e-passport holders at e-gates. The lessons learnt from examining these issues are the key source of justification and inspiration for the work conducted in this study, specifically for the development of new approaches and concepts that allow border control stakeholders to deal with identified issues and plan for more efficient and secure automated border of the future.

## 4.1 RTP-based systems: UK IRIS.

The Iris Recognition Immigration System (IRIS) is a UK Home Office led program. It aimed at providing expedited automated clearance at the UK immigration for certain low-risk pre-enrolled travellers through the use of iris biometrics [70, 106]. The system worked by comparing live iris images, captured by the system, against the iris images stored in the database, involving all permanent residents of the UK and other people under special regulation.

### 4.1.1 Performance statistics

On May 2006, the IRIS Project Board considered performance over the period from 03/04/06 to 30/04/06, and the following performance was reported [106] as shown in Table 4.1.

Table 4.1: Performance of the IRIS system (from [106]).

- Failure to enrol rate (FTE): $< 2\%$
- Crossing Time (airside door open to barrier ready): $< 15$ sec
- Fixed enrolment time – standard enrolment: $< 4$ min 30 secs
- Enrolment false accept rate (FAR): $< 0.001\%$
- Barrier biometric false reject rate (FRR): $< 2\%$
- Barrier sensor false reject rate: $< 2\%$
- System availability – Arrivals: $> 99.8\%$ per port
- System availability – Enrolment: $> 99.5\%$ per port


Figure 4.1: UK IRIS system.
Source: http://www.airport-world.com/home/general-news/item/1227-blog-post-the-scaling-back-of-project-iris-

In 2012, there were 63 machines in various UK airports. In 2013 the system was dismantled in favour of using the ePassport-based gates [77].

### 4.1.2 Lessons learnt

Key factors leading to the closing of the IRIS program for trusted traveller are discussed in [107]. Originally heralded as a time-saving tool, the IRIS project has faced constant criticism since it was introduced. Many users complained that instead of saving time, going through an iris scanner could actually take longer than traditional passport control, not mentioning the cost incurred by deploying what was seen the most ambitious technology procurement of the time.

A report from the UK Border Agency criticizes the IRIS program and raises questions on progress in developing the e-borders and e-gates [70]. From press coverage[1] of the IRIS system, *six* key factors leading to the closing of the IRIS program are identified, as summarized in Table 4.2.

## 4.2 ePassport-based systems: EU EasyPASS

The ePassport-based automated border control systems (e-gates) are currently the fastest growing development project in the e-border business. The key questions are: How reliable are these systems? What is the percentage of travellers that still needs to be referred to manual examination? This percentage is measured by the Operational Reject Rate (ORR), which is analyzed below.

### 4.2.1 Performance statistics

Table 4.3 shows a representative sample of metrics that describe the performance of a typical e-gate (taken from [111]). The rejection of 12% of traveller is reported there: 5% due to face verification failure and 7% to other non-biometric-related factors, of which the following three reasons are noted:

1. Non compliant traveller behaviour, (not following or understanding the instructions)

[1] E.g. http://www.dailymail.co.uk/travel/article-2102489, https://aftermathnews.wordpress.com/2012/02/28. A wider set of quotes is provided in the University of Calgary report [9].

Table 4.2: Six key reported factors attributed to closing the UK IRIS program.

1 **Speed:** "*passengers often spent longer being scanned by the machines than when they went through traditional passport control*".
2 **False rejects:** "*it emerged that up to 1 in 10 travellers were wrongly rejected by the scanners, and then had to wait for manual checks to get through passport control*".
3 **Confusion:** "*an increasingly large number of people, who are clearly not registered for IRIS, try to use the gates and then fail*".
4 **Not in e-passports:** "*whilst iris images are a secure biometric, they are not included in e-passports, which contain face (and fingerprint) data*".
5 **Cost:** "*The money would be better spent employing more trained staff*".
6 **Limited lifetime:** "*Technologies have a finite lifetime*".


Figure 4.2: EU e-gate systems: a) first generation (Spain)– the camera is fixed, located on a side and b) second generation (Germany) – the camera automatically adjusts to eye level, located in the middle of the exit door.

Table 4.3: Sample of statistical data from the border control system EasyPass based on facial recognition from [111] (March 2012).

| Statistical parameter | Estimated value |
|---|---|
| Number of users per day | 500 |
| Success rate | 88%* |
| Rejection due to face verification failed | 5.0% (0.1% FAR) |
| Operational Rejection Rate | 12% |
| Period to pass the e-gate** | 18 seconds |

**Border crossing without manual interaction*
***Time from presenting the e-passport until the system is ready to serve the next traveller*

2. Document check failure, and
3. Hits from background database checks.

In a more recent analysis [112], it has been reported that, in general, the German Federal police is satisfied with the EasyPASS systems. Electronic document checks are very reliable (reject rate $< 0.1\%$). However, the ORR is still considered too high. Based on these results, in 2014 the German Federal police set the target objectives for future operation of EasyPASS systems as shown below in Table 4.4.

Table 4.4: 2014 target objectives for operation of e-gates by the German Federal police (from [112]).

To achieve total Operational Reject Rate (ORR) $< 10\%$, of which:

| | |
|---|---|
| 1st goal: | To achieve fraction to ORR from biometrics $< 5\%$, at a defined biometric security level (FAR $\geq 0.1\%$). |
| 2nd goal: | To achieve fraction to ORR from watch list and document checks $< 5\%$. |
| 3rd goal: | To optimize user guidance to avoid rejects due to traveller behavior. |

**Critical Observation**

*In UK IRIS kiosks, 1 in 10 ravellers were reportedly rejected by the system.*
*In Germany's EasyPASS system, 1 in 8 travellers were rejected.*
*More than half of these rejects were due to non-biometric reasons.*

### 4.2.2 Variation of system performance among subjects

An important observation about the performance of e-gates has been derived from the data reported in [108]. This paper describes the performance of the e-gates in two international airports in Spain, recorded for travellers coming from different EU countries over two testing periods (a four-month period during summer and a one-month period half a year later during winter).

By taking the data from this paper and converting it into a spreadsheet, the variation in Face Recognition performance, measured in terms of system's False Reject Rates (FRR), over different countries of origin and different testing periods has been computed, shown in Table 4.5, and is found to be significant. Specifically, the following observations are made:

- The best FRR, marked green in Table 4.5, was achieved with Portugese citizens (FRR$= 4.74\%$),
- The worst performance (FRR$> 15\%$), marked red in Table 4.5, was achieved for Belgian, Norwegian, Spanish, Italian and Danish citizens.
- For several countries, the performance varied substantially between two test periods.
- The countries marked blue in Table 4.5 provide statistically significant results, with data from over a thousand travellers collected. Among "poor-performing" countries, several did not have enough data to provide statistically significant confidence on the result.
- In total, during the best performing month, one in 10 travellers were directed to manual control because of facial verification failure (FRR$= 10.85\%$), among 18,884 travellers who used the gates.

Table 4.5: False Reject Rates (FRR) for travellers from different EU countries (computed from data reported in [108]).

| | Country of origin | Passages 06-09/2012 | Rejected | FRR | Passages 02/2013 | Rejected | FRR | Passages Total | Rejected Total | FRR Average | dFRR | . |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | BEL | 531 | 115 | 21.59% | 108 | 11 | 10.10% | 639 | 126 | 19.72% | ▲ | -11.49% |
| 2 | NOR | 97 | 16 | 16.49% | 25 | 4 | 16.00% | 122 | 20 | 16.39% | — | -0.49% |
| 4 | ITA | 2757 | 435 | 15.79% | 577 | 88 | 15.29% | 3334 | 523 | 15.69% | — | -0.50% |
| 5 | DNK | 152 | 20 | 13.16% | 22 | 4 | 18.18% | 174 | 24 | 13.79% | ▼ | 5.02% |
| 6 | NLD | 990 | 134 | 13.54% | 177 | 21 | 11.86% | 1167 | 155 | 13.28% | — | -1.68% |
| 3 | ESP | 67508 | 9006 | 13.34% | 13478 | 1648 | 12.23% | 80986 | 10654 | 13.16% | — | -1.11% |
| 7 | FRA | 2687 | 341 | 12.69% | 647 | 57 | 8.85% | 3334 | 398 | 11.94% | — | -3.84% |
| 8 | SVK | 49 | 7 | 14.29% | 11 | 0 | 0.00% | 60 | 7 | 11.67% | ▲ | -14.29% |
| 9 | SVN | 40 | 4 | 10.00% | 7 | 1 | 14.29% | 47 | 5 | 10.64% | ▼ | 4.29% |
| 10 | D | 1540 | 157 | 10.18% | 240 | 26 | 10.88% | 1780 | 183 | 10.28% | ▼ | 0.70% |
| 11 | POL | 214 | 22 | 10.33% | 30 | 3 | 10.00% | 244 | 25 | 10.25% | — | -0.33% |
| 12 | HUN | 70 | 6 | 8.57% | 28 | 3 | 11.54% | 98 | 9 | 9.18% | ▼ | 2.97% |
| 13 | MLT | 10 | 1 | 10.00% | 1 | 0 | 0.00% | 11 | 1 | 9.09% | ▲ | -10.00% |
| 14 | IRL | 749 | 64 | 8.58% | 173 | 17 | 9.64% | 922 | 81 | 8.79% | ▼ | 1.06% |
| 15 | CZE | 97 | 10 | 10.53% | 19 | 0 | 0.00% | 116 | 10 | 8.62% | ▲ | -10.53% |
| 16 | LTU | 56 | 5 | 8.93% | 14 | 1 | 7.14% | 70 | 6 | 8.57% | — | -1.79% |
| 17 | ROU | 367 | 27 | 7.42% | 94 | 10 | 10.99% | 461 | 37 | 8.03% | ▼ | 3.57% |
| 18 | EST | 15 | 1 | 7.14% | 11 | 1 | 9.09% | 26 | 2 | 7.69% | ▼ | 1.95% |
| 19 | GBR | 10914 | 823 | 7.54% | 2520 | 131 | 5.19% | 13434 | 954 | 7.10% | — | -2.35% |
| 20 | SWE | 397 | 30 | 7.61% | 64 | 1 | 1.59% | 461 | 31 | 6.72% | — | -6.02% |
| 21 | CHE | 217 | 11 | 5.09% | 55 | 7 | 12.96% | 272 | 18 | 6.62% | ▼ | 7.87% |
| 22 | AUT | 215 | 11 | 5.12% | 25 | 2 | 8.00% | 240 | 13 | 5.42% | ▼ | 2.88% |
| 23 | PRT | 2172 | 118 | 5.45% | 443 | 6 | 1.36% | 2615 | 124 | 4.74% | — | -4.09% |
| 24 | FIN | 155 | 7 | 4.52% | 28 | 1 | 3.57% | 183 | 8 | 4.37% | — | -0.95% |
| 25 | BGR | 135 | 5 | 3.73% | 26 | 1 | 4.00% | 161 | 6 | 3.73% | — | 0.27% |
| 26 | GRC | 187 | 5 | 2.67% | 37 | 3 | 8.11% | 224 | 8 | 3.57% | ▼ | 5.44% |
| 27 | LVA | 56 | 1 | 1.79% | 16 | 1 | 6.25% | 72 | 2 | 2.78% | ▼ | 4.46% |
| 28 | LUX | 13 | 0 | 0.00% | 4 | 0 | 0.00% | 17 | 0 | 0.00% | — | 0.00% |
| 29 | ISL | 10 | 0 | 0.00% | 3 | 0 | 0.00% | 13 | 0 | 0.00% | — | 0.00% |
| 30 | CYP | 5 | 0 | 0.00% | 1 | 0 | 0.00% | 6 | 0 | 0.00% | — | 0.00% |
| 31 | LIE | 1 | 0 | 0.00% | 0 | 0 | 0.00% | 1 | 0 | 0.00% | — | 0.00% |
| | **Total** | **92406** | **11382** | **12.32%** | **18884** | **2048** | **10.85%** | **111290** | **13430** | **12.07%** | | |

The table shows the data recorded from two international airports in Spain (Bajaras and El Prat), over two periods: 4-month period (left columns) and 1 month period, half a year later (middle columns). The total and variation in FRR – over different countries of origin and over two recording periods, are shown (right columns and bottom row). The system operated at False Accept Rate (FAR) of approximately 0.1%.

## Critical Observation

*False Accept Rates that are reported for ABC systems refer to the likelihood that a system will accidentally recognize a traveller as someone else (so called "zero-effort attack", as in a 1-to-N match against a watch-list database). They do not refer to the ability of the system to resist an intentional effort to defeat the system (so called "non-zero effort attack", as in spoofing by using a make-up or a face mask).*

The factors that have contributed to the variation in system performance are listed Table 4.6, the main of which is believed to be the poor quality of passports issued in some countries, based on the discussion with Frontex. More analysis of the factors affecting ABC performance is presented in the next section.

Table 4.6: Factors attributing to varying performance of e-gates in Table 4.5.

- Quality of biometric document (the main factor).
- User experience and difference in designs.
- "Biometric menagerie" phenomenon: intrinsic limitations of face recognition technology to recognize some types of facial images, e.g. with eye-glasses, long-hair, non-typical faces.
- Other factors related to travel: duration/complexity of travel, fatigue etc.

### 4.2.3 Policy-related issues

One of key challenges in ABC concerns optimizing and harmonizing the policies related to the use of ABC systems by people of different nationalities, ages and races. A number of projects have been launched in EU for this purpose, a survey of which is provided in Appendix A.

**Critical Observation**

*Having ICAO-compliant quality of facial images in e-passports (showing no smile or deviation from frontal view) is an important condition for successful operation of e-gates. However, enforcing it on young children and infants, who are not eligible to use e-gates anyway*, not only causes discontent among their parents, but also contributes to worsening the task of the border control officer – contrary to the original intent – who will need to match a live person (who is likely not fully frontal and smiling) to his/her picture in passport.*

* Most countries require travellers to be of 18 years or older to use the e-gate, except for Australia and New Zealand, where the age requirement for using e-gate has been recently lowered from 16 years to 12 years.

### 4.2.4 Lessons learnt

The lessons learnt from the analysis of the EU e-gates are summarized below. From the analysis of e-gate performance in Germany [109, 110], it is observed that the rejection rate is 12%. That is, *1 in 8 travellers* are re-sent to manual examination, of which only 5% are due to biometric failure, when live captured image does not match the image stored in the passport chip. Similar to IRIS-systems discussed earlier, likely reasons are:

- Traveller did not understand or missed logistical signs
- Traveller did not know or forgot what kind of passport they hold
- Traveller did not follow instructions of the document reading machine,
- Traveller was in some other way imperfect subject for database processing

Additionally, the performance may vary drastically for some travellers, exhibiting worse than 15% reject rate for some of them. The ways to improve the system performance are seen in using multi-biometric fusion and subject-based analysis discussed in the next section.

## 4.3 Use of multi-modal biometrics

Another observation from the study [108] discussed above, the data from which is used in Table 4.5, relates to the use of multi-modal biometric fusion. In fact, the original purpose of reporting the face FRR statistics in this paper, was not to examine the limitations or variations of face recognition performance, but rather to illustrate that FRR of the system can be significantly reduced by using multi-modal biometric recognition.

In the pilot described in [108], Spanish citizens, who in addition to an e-passport, have an e-ID document with encrypted fingerprint, were allowed to use this card, in cases when face recognition failed. Specifically, the face recognition system was configured so that it had two match thresholds. the lower threshold allows the system to undoubtly reject a person, the higher threshold allows the system to undoubtly accept a person. Only those travellers with matching score between the threholds would be required to undertake additional verification step with an e-ID. Using this fusion scheme[2], the FRR of Spanish citizens is decreased from 12.23% (shown in the table in the second testing period) to 3.72%. Of importance to note that this is also lower than when using with fingerprint alone (4.77%).

It is therefore envisaged that the use of multi-modal biometric in ABC systems (i.e., face combined with fingerprint and/or iris) will increase as the other two modalities (face and iris) become more prevalent in travel e-documents.

**Critical Observation**

*The false reject rate (FRR) of e-gates varies significantly: from 5% (for best performing countries) to almost 20% (for worst performing countries). Applying multi-modal biometrics (such as performing fingerprint recognition, when face recognition fails) will improve FRR significantly. In a pilot conducted in Spain [108], such multi-modal fusion is shown to reduce FRR from 12.23% to 3.72%.*

Figure 4.3: Nexus iris kiosks: used prior to 2006 (left), after 2006 (middle), new generation installed in 2014, which uses two camera positions: at high and low level (right).

## 4.4 Subject-based analysis to address the usability issues

As highlighted in Chapter 5, the majority of ABC users are not trained or habituated with the system. The critical point of the border system design therefore is the traveller's interaction with the system. For example,

[2]This is the so-called cascaded decision-level fusion technique further described in ISO TR 24722.

it is reported that some of the falsely rejected passengers were rejected purely because of the ergonomic issues of devices or ill-designed logistics of the ABC process [110, 109].

The characteristics of the subject population, their attitudes and level of cooperation, the deployment environment, and procedures for measuring performance can all affect the system performance and be the reason for the non-use of the ABC technology [114, 115]. Therefore, they must be properly addressed by the system designers [163].

**Critical Observation**

*Avoidance and non-use of ABC technologies by some travellers is seen as one of the key challenges that needs to be addressed by the border agencies and system designers [114, 115]. Analysis of human factors and system usability studies are therefore critical for the success of ABC.*

In addition to issues related to training and experience of users, there are other important user-specific issues such as those related to their physiology, health. A person who is very tall or very short, or is in a wheelchair may have problems being captured/recognized by the system (see Figure 4.1). This particular consideration was taken into account in the specifications of the second generation of Nexus kiosks installed in Canada in 2014 (see Figure 4.3), resulting in the overall improvement of their performance.

Similarly, a person with a missing eye, after face/eye surgery may also experience difficulty, as may a person

Table 4.7: The results from the subject-based performance analysis of the Nexus system shows that travellers who used the system many times perform much better than those who used it only a few times.

| Usages | Travellers | $HD \geq 0.20$ | $HD \geq 0.21$ | $HD \geq 0.22$ | $Atmp \geq 1.5$ | $Atmp \geq 1.7$ | $Atmp \geq 1.9$ |
|---|---|---|---|---|---|---|---|
| $> 2$ | 383463 | 4.2% | 2.9% | 1.8% | 3.4% | 1.7% | 1.1% |
| $> 4$ | 287472 | 2.4% | 1.5% | 0.8% | 2.4% | 1.5% | 1.0% |
| $> 8$ | 196573 | 1.3% | 0.7% | 0.4% | 1.3% | 0.7% | 0.4% |
| $> 16$ | 119538 | 0.8% | 0.4% | 0.2% | 0.6% | 0.3% | 0.2% |
| $> 32$ | 61332 | 0.6% | 0.3% | 0.1% | 0.3% | 0.14% | 0.08% |
| $> 64$ | 24383 | 0.3% | 0.1% | 0.05% | 0.12% | 0.04% | 0.01% |
| $> 128$ | 6530 | 0.2% | 0.09% | 0.01% | 0.06% | 0.00% | 0.00% |

The table shows the number of Nexus members who used the system more than 2,4,8,16,32,64,128 times, and percentage of those among them who consistently experienced difficulty in using the system, measured in terms of high average dissimilarity score ($HD$) and high average number of attempts ($Atmp$). The maximum allowed dissimilarity score $HD_{max}$ is 0.27. If travellers' dissimilarity score $HD$ is higher than $HD_{max}$, his/her iris is rejected. The maximum allowed number of attempts in a single session is three (3).

Note 1: When a traveller exceeds the maximum allowed number of attempts in a session, he/she can commence a new session (either with the same or different kiosk), in which case the information about the previous session is not recorded and is lost.

Note 2: Temporal information (i.e. whether a traveller used the systems over a short or long period of time) is not used.

Note 3: All transactions are considered factor-agnostic, meaning that no other information about the factors that could have affected the performance of the system is used. As examined separately in [4], some of these factors (in particular, the location of the kiosk) are shown to influence significantly the performance of the system. More details are provided in [4] and Appendix E.

with mental or other health or travel challenges who may not follow the instructions properly. Also, as mentioned earlier, the country of passport issuance is also a major factor effecting the quality of biometric recognition. Finally, the so-called "biometric menagerie" or "Doddington Zoo" phenomenon that some people are intrinsically much harder to recognize than others is a well known phenomenon, further discussed in Appendix E and comprehensively studied in literature [206]-[214].

To deal with all of these issues and ensure that ABC systems work well with groups of travellers, regardless of their physiology, origin or health, *subject-based system performance analysis* is highly recommended.

### 4.4.1 Analysis of Nexus performance

Using historical anonymized iris data recorded by the CBSA from 2003 till 2014, subject-based performance analysis of the Nexus system has been conducted. An outcome of this analysis is shown Table 4.7, which presents the statistics related to the number of travellers who experience difficulty using the the system. In particular, it is shown that there existed a small percentage of travellers ($< 5\%$), who consistently could not pass the system from a single attempt, having high dissimilarity score. While being relatively small, this percentage of travellers still needs to be taken into account in order to further improve the system performance and the reputation of the agency, because there is a risk that these travellers will be dissatisfied with the agency's service and may avoid using the system in the future.

Another important observation is made from this analysis that percentage of travellers who experience the difficulty is considerably smaller among those who used the system many times, compared to those who used it only a few times. This is an indication that many travellers may stop using the system, once experiencing the problem.

By detecting and focusing on the travellers who experience the problem with the system, the agency will be able to identify the factors that negatively affect the system performance and thus further improve it.

**Critical Observation**

*The performance of ABC systems may vary drastically from one traveller to another. Subject-based analysis needs to be conducted to categorize and control the factors that influence the performance of the system with respect to all travellers.*

## 4.5 Issues related to social integration of modalities

University of Calgary researchers [9] highlight that the relationship between the ABC system and social infrastructure is vital for traveler risk assessment. The term of "depth of social integration" is introduced (Section 2.2) to describe this relationship in terms of the number of databases that support the system.

Table 4.8, extended from [9], presents a summary on the use of various biometric modalities by largest national and international biometric databases. One can observe that:

- More than 70% of databases accept face biometric.
- More than 70% of databases accept fingerprint biometric.
- More than 60% of databases accept face and fingerprints.
- Less than 40% of databases accept iris biometric.

It is noted that Canada's trusted international partner countries, such as USA, UK, EU, Australia, and New Zealand, use databases of facial and fingerprint biometrics. For example, there are over 150 million fingerprints in the US-VISIT database alone, and the search time per person is approximately 8-10 seconds. This database handles over 200,000 transactions per day. This includes an average of 30,000 queries a day by the Departments of Defense, Justice and State; local and federal law enforcement; Interpol and intelligence agencies to verify identities for the purpose of immigration, law enforcement and national security [17, 21]. Other biometrics, such as face and iris can be added to US-VISIT.

The USA has required fingerprints and a photograph from all foreign nationals (except most Canadians) since 2004, Japan – since 2007, UK — since 2008, Australia – since 2010, and EU – since 2011 [63].

Table 4.8: Face, fingerprints, and iris biometric modalities in national and international databases.

| | Database | Face | Fingerprints | Iris |
|---|---|---|---|---|
| 1. | EUROSUR (European Border Surveillance/Entry-Exit System) | ✓ | ✓ | |
| 2. | EUROPOL (European Police Office) | ✓ | ✓ | |
| 3. | VIS (Visa Information System), EU | ✓ | ✓ | |
| 4. | SIS (Schengen Information System), EU | ✓ | | |
| 5. | SIS-II (Schengen Information System), EU | ✓ | ✓ | |
| 6. | US-VISIT (U.S.A.) | ✓ | ✓ | |
| 7. | IDENT (Automated Biometric Identification System), U.S.A. | ✓ | ✓ | |
| 8. | IAFIS (Integrated Automated Fingerprint Identification System), FBI, U.S.A. | | ✓ | |
| 9. | NGI (Next Generation Identification program) DHS, U.S.A. | ✓ | ✓ | ✓ |
| 10. | FLUX (Fast Low Risk Universal Crossing), U.S.A. - Netherlands | ✓ | ✓ | ✓ |
| 11. | Interpol | ✓ | ✓ | |
| 12. | Entry-exit database, Saudi Arabia, UAE | ✓ | ✓ | ✓ |
| 13. | Biometric database, military operations in Iraq and Afghanistan, U.S.A. | | | ✓ |
| 14. | NEXUS/CANPASS, Canada/U.S.A. | | | ✓ |
| 15. | UAE, India, Brasil (starting 2014) | | | ✓ |

The following observations can be made from Table 4.8 in the context of *open-set* ABC applications, where travellers are not known in advance to the system.

1. National and international resources of social infrastructure are concentrated around the interoperability of facial and fingerprint technologies, such as sharing this biometric data between databases, search for information, and collection of information.
2. The key technological component of the counter-terrorism, criminology, and forensics is a database of the respective data. These databases mostly rely on facial and fingerprint biometrics.
3. Iris modality can be used as supporting biometrics. For example, it applies to cases when fingerprints are not available. If available in e-passports as secondary modality, it can also be used to improve the performance of primary modality recognition, face, the performance of which is significantly worse than that of iris.

## 4.6 Modality specific issues

### 4.6.1 Stability over time: aging

#### Iris modality

In 2013, in co-authorship with CBSA, the National Institute of Standards and Technology (NIST) published the report "IREX VI: Temporal Stability of Iris Recognition Accuracy" [194], which examined the temporal stability of iris biometric features. Using iris scores recorded by the CBSA for its Nexus members who used the agency's iris kiosks for several (at least four and up to seven) years, it has been shown that there is practically no observed increase in the dissimilarity score (the so called Hemming Distance (HD)) for these travellers over those years, provided that proper computer vision techniques rectifying the variable dilation of the pupil are applied. Without computer vision techniques that take into account the variable dilation of the pupil, a slight increase in dissimilarity score is observed as indicated in earlier studies from the University of Notre Dame [192], which is attributed to weakening of the eye muscles that control the dilation of the pupil as people age.

**Critical Observation**

*By analyzing the results obtained by NIST researchers on the CBSA Nexus iris scores, who claim that iris does not age, the counterarguments from the researchers of the University of Notre Dame, who claim the opposite, and our own results obtained on the same dataset, the conclusion is made that iris does age, however significantly less than face. Most importantly, iris aging, which is displayed in a weaker ability of pupils to dilate, can be efficiently rectified algorithmically by iris recognition software. This is in contrast to faces, for which no age-rectifying face recognition algorithm exists at the moment.*

At the same time, the question on the iris longevity and the variability in the degree of aging among travellers is still one of the most debated topics in the research community, since the data used in the NIST report [194] had certain limitations[3] and also because it is expected that some people may show aging affects more than others. The issue of the complexity of the multi-factor analysis that is used in analyzing iris performance has been also raised, since (as highlighted in our study [4]) there are also other factors that affect the performance of the system, such as, for example, the location of the kiosk and the time of the day of its operation.

#### Facial modality

The aging of faces is a process that is well defined. For example, in [184], facial age-related trends are introduced as follows: *. . . "age-related trends affecting the appearance and profile of the face include the increasing prominence of the chin, the decreasing convexity of the skeletal nose, and the lengthening of the upper and lower lips. These trends are particularly evident from birth until age eighteen, but their effects are seen, though less dramatically, into adulthood and beyond. With increasing age, the skeletal profile of the human face begins to lose its distinctive, protuberant*

[3] The data that was provided to NIST in 2012 for iris aging analysis is a subset of a larger dataset that has been collected by the CBSA from 2003 to 2014. The key limitation of these data is that they contain only the scores of those travellers who were successfully recognized by the system. The data from the travellers who were not recognized were not recorded. Additionally, the data did not contain the information on the location of the kiosks and other kiosks attributes that are internal to CBSA and were not provided to NIST for their analysis. The analysis conducted internally by CBSA, reported in [4], partially addresses these issues.

*appearance as changes in the shape and orientation of the nasal bones lead to a flattening of the facial features. "* Smoking and the use of drugs and alcohol are other well-known ways to speed up the process of aging.

Due to known degradation of face recognition due to face aging, re-enrollment of faces in passports every 10 years is required, some countries doing it every 5 years.

One of the promising research areas in automated face recognition relates to the development of algorithms that would be able to take into account possible affects of aging on faces. Similar to the algorithms already developed for rectifying facial images with respect to the angle of view, facial expression and lighting, such new age-rectifying algorithms would be used to match faces belonging to different age groups.

### 4.6.2 Degradation related to travellers health / physiology conditions

#### Iris in drug and alcohol intoxication cases

Various substances, such as alcohol intoxication, LSD, MDMA, cocaine, and marijuana consumption, affect iris properties. These substances temporarily dilate or constrict pupil to a large extent. Authors [203] show that alcohol influences iris recognition significantly. Iris recognition under influence of these substances can be viewed as a form of attack on the integrity of a biometric system.

#### Iris performance with contact lenses

Contact lenses are used to correct eyesight as a replacement for glasses. They also used for cosmetic reasons also where texture and colour of iris region is superimposed with a thin textured lenses. They have been also considered as a potential point of attack, if someone tries to spoof the system by overlaying patterned lenses over their eyes. It has been long been believed that clear prescription contact lenses do not affect the accuracy of iris recognition. However, experimental results show that wearing these lenses does have effect on recognition accuracy. The experiments show that both transparent (prescription) and colour cosmetic lens (textured) affect the verification accuracy, especially when the lenses of different types are used in enrollment and passage [189].

#### Facial recognition under plastic surgery

The statistics clearly indicate the popularity of plastic surgery among all age groups, ethnicity and gender. Similar analysis from different countries illustrates the popularity of plastic surgery. Matching post-surgery images with pre-surgery images becomes an arduous task for automatic face recognition algorithms.

### 4.6.3 Robustness to spoofing

#### Faces

Two techniques have been reported recently related to spoofing a face-based access/border control systems. One reported by the researchers from the University of Bologna [179], who showed that it is possible to generate a synthetic facial photo-image from two people (one being a "Criminal" in watch list, the other an "Accomplice") such that it can be validated by a human (at a Passport issuing institution) as being that of Accomplice, and then the same photo will be also matched by e-gate system to the Criminal, thus allowing the Criminal to cross the border under the name of the Accomplice.

In the other case, a person was able to use make-up to look like one of the enrolled subjects to spoof the face recognition system [180]. In both cases, the intruder is able to bypass the liveness detection implemented in the system.

**Iris**

Iris modality is less vulnerable to spoofing, compared to face and fingerprints. This is due to the dynamic nature of pupil which moves and dilates, as light changes, thus allowing one to develop efficient techniques for liveness detection.

The key risk in spoofing the iris system in seen in using specially designed lenses, which are printed with the iris pattern of another person. Albeit hypothesized, such spoofing attacks have not been yet reported successful. Additionally, techniques exist that allow one to detect lenses using the different pattern of light reflection.

## 4.7 Conclusions

The key observation stemming from analysis of the issues with existing ABC systems is best summarized in quote below from Dr. Mansfield, one of the most respected experts in the field of biometrics, which has been extracted from the UK Parliament archives.

**Critical Observation**

**Q553 Dr Turner:** *Can you give me your views, please, on the risks involved in this project [IRIS], and do you think that the Home Office has considered them seriously enough?*

**Dr Mansfield:** *...The risks I would say are probably because it is a very large project, a very large procurement, of which biometrics is just one small part. There seems to have been a focus on the biometric element as being the most technical and perhaps least understood element of the whole scheme, and to my mind assuming that is where all the risks lie is totally incorrect.*

UK Parliament, Examination of Witnesses (Question 540-559), May 3, 2006 http://www.parliament.the-stationery-office.co.uk/pa/cm200506/cmselect/cmsctech/1032/6050307.htm

By examining the issues with the deployed biometric-enabled automated border control systems, including those that led to closing of the UK IRIS program [77] and those that contribute to deviating performance of e-gates in Europe, the following conclusions can be made.

- **Conclusion 1:** A substantial percentage of failure observed in those systems is due to sources of risks other than those related to the biometric recognition performance. For example, EU e-gate systems send approximately one in eight (12%) travellers to manual control, with rejection rate varying drastically from one country to another. This indicates that there are many other factors in addition to biometric recognition quality that influence the performance of the system [109, 110, 112]. Some of these factors can be controlled, such as machine-human interfaces, ergonomic of man-traps, airport logistics and border officer training. Other factors, including traveller fatigue, or (non)familiarity with system, cannot be controlled.
- **Conclusion 2:** The ABC system is one of many components in a complex semi-automated border crossing process, which deals with granting travellers an entry to a country. Therefore, any failure or risk related to the deficiency of the biometric recognition can be mitigated by other non-biometric means. It is, therefore, important to understand what a general e-border crossing process is and what role a biometric-enabled technology/component plays there.

In the conclusion of this chapter, the key three discussion items are put forward:

1. The need to identify and taxonomize all factors that influence ABC performance, specifically by such categories as: machine-related vs. human-related, controlled vs. uncontrolled, quantitatively described vs. qualitatively described – to permit better description and comparison of the systems;

2. The discussion on the high value of iris modality for future ABC applications, as, following the termination of IRIS program in UK, there may appear an erroneous perception of the unsuitability or lesser value of this modality for ABC; and finally

3. The need for better ABC performance and reporting practices, because the existing practices leave room for ambiguity and false interpretations.

### 4.7.1 Factors affecting ABC performance

For developing ABC deployment strategies and performing cost-benefit analysis of ABC systems, which can be done using simulation tools, it is important to know all factors that influence ABC performance. The list of these factors is produced, taxonomized by two categories: human-related factors vs. machine-related factors, and controlled vs. uncontrolled. Some factors can be measured using quantitative metrics, whereas the others may only be described qualitatively.

*Machine-related factors* include: limitations of capture devices, matching algorithms, machine-human interfaces, ergonomics of the kiosk or e-gate, airport logistics and process flow, which can be controlled and potentially improved, as well as system component or supporting technology failure due to intentional or unintentional attack, which is not controlled.

*Human-related factors* include: those related to guidance and decision-making of border officers, which can be controlled, and those related to travellers such as traveller fatigue and other social, psychological, ethnic, cultural, religious, and geographical factors, which may not be controlled.

The factors that cannot be controlled can be predicted, and all of them should be taken into account when designing the system.

**Critical Observation**

*The key objective of ABC designers is to reduce the number of factors affecting ABC performance to the minimum possible, and then use simulation tools to develop ABC models that take into account all remaining factors. Only then can the performance of the ABC system be optimized with respect to all factors and various performance metrics.*

### 4.7.2 Future of the iris modality

Despite critical remarks about the IRIS program, it can still be treated as a success. The IRIS system demonstrated better rejection performance compared to any other deployed traveller authentication technology. The IRIS project has also provided indispensable experience and a set of lessons, which can be used for designing and evaluating other large-scale biometric border control systems [107]. Furthermore, compared to the face modality, the iris modality has shown a number of advantages, which are summarized in Table 4.9.

To contrast the negative comments from media on iris kiosks in UK quoted earlier, it should also be mentioned that there are many travellers who openly applaud in social sites [4] the convenience and efficiency of

[4] See, for example, Google:"on the awesomeness that is NEXUS", "If I didn't have NEXUS, I would have definitely missed my flight", Retrieved March 16, 2015.

Table 4.9: Advantages of the iris modality.

1. *Invariance to orientation and facial expression.* – Compared to faces, iris is much less affected by face orientation and expression. Dilation is practically the only factor that affects iris performance and can be algorithmically taken in account.
2. *Less affected by work/life conditions and aging* – Compared to faces and fingerprints, iris is much less affected by work and life conditions and thus can be used equally well with people from different social classes. Iris is age considerably less than faces and the effect of aging on iris can be rectified by algorithmically.
3. *Best suitable for national ID programs and medical applications.* – Because of its performance, resistance to aging, diseases, person's life or work conditions, and because it does not require physical contact with the sensor, iris has been preferred modality for use in hospitals for managing and tracking sick people. Recently, for the same reasons, it has also been chosen as preferable modlity for national ID programs [199]. This is in addition to its use for membership programs (the largest of which is the CBSA's NEXUS program).
4. *Affordable and easy to implement.* – Iris images can now also be captured using commodity cameras, including those on mobile devices, and following the expiration of the Dougman's original patent [186], the same algorithm that is used in commercial iris systems has now become affordable and can be reproduced by researchers and industry, becoming a commodity for public and research use. E.g. there is now iris login software for Android devices. Iris recognition algorithms are also easy to implement and run faster, compared to face or fingerprint recognition.
5. *Easier to predict and analyze.* – Iris is the only known modality, the impostor scores distribution of which is known in advance and the False Accept Rate of which can be computed as function of the threshold. This makes it easier to understand, predict and analyze iris system performance, compared to that of faces.
6. *Less vulnerable to spoofing.* – Due to the dynamic nature of pupil, which moves and dilates with light changes, it is possible to develop efficient techniques against spoofing attacks.
7. *Overall highest recognition performance and capacity for improvement.*.- Overall, iris has several orders of magnitude lower false accept/reject rates than faces (See Appendix F). This makes iris-based verification (one-to-one comparison) the most reliable of all touch-less biometric modalities. This also makes it possible to use iris in identification mode (one-to-many comparisons), especially if both iris images are used.
8. *Capacity for improvement.* – Iris has also the largest capacity for further improvement of recognition, by using ocular and periocular regions, for which a number of high-performing recognition algorithms have been already developed [205].
9. *Allows for additional stress analysis.* – Finally, the motion of iris and pupil is shown to be very valuable for stress and lie detection [98], which can be further explored for designing automated behavior screening and interviewing technologies, which is further discussed in the next chapter.

the iris kiosks in Canada.

At the 2014 International Biometric Performance Testing Conference (IBPC 2014), the following questions were discussed while addressing the issue of choosing the best biometric modality for a lifetime identification document [198]:

1. Does biometric aging hinder the integration of biometrics to breeder documents (e.g. birth certificates)?
2. Which biometric characteristics are most stable over a long (life-time) time-span?
3. Which biometric characteristics are most suitable to be captured at early ages from an ethical point of view?
4. Can potential aging effects be modeled and systems be parametrized to actively handle aging?

The answers to these questions led to the conclusion that iris modality is the best suited for being used in national ID programs. Similar conclusions were presented the IEEE International Joint Conference (IJCB 2014) by a representative from the Brazilian government who showed the results of a three year study that led to the decision to choose iris modality (over faces and fingerprints) for the national ID program in this country [199]. At the same conference, FBI has also shared their vision for extensive use of iris modality in their NGI program [202].

The key impeding factor in the development of iris-based border control worldwide is seen in its lower social use or the so called depth of social integration (defined in Section 2.2), compared to that of faces and fingerprints. Even though ICAO provides standards for including iris in e-passports, most countries do not use this additional biometric modality yet. This situation however may change, if more countries start using iris for national ID programs, following UAE [201], India [200], and recently Brazil [199].

To conclude, this study suggests that iris modality has a lot of potential to be used in future ABC systems, in particular, as part of a multi-modal biometric-enabled authentication system, where iris is captured at the same time with the face, and where it can also be used for behavioural screening (stress analysis) using the interview assisting technology further analyzed in the next chapter. Importantly, the capabilities of the cameras deployed in ABC kiosks and e-gates permit doing that, namely simultaneous capture of face and iris, and tracking of iris motion – for more reliable authentication and additional stress analysis.

### 4.7.3 Need for better ABC performance evaluation practices

At present, according to the existing industry standards, the performance of ABC systems is reported using transaction-metrics [172]. This results in rejection rates averaged over all transactions which may be very different and "overly optimistic" compared to the real rejection rates experienced by travellers.

For example in Table 4.5, 18.18% FFR (4 rejects in 22 passages) for travellers from Denmark (DNK) does not yet indicate that the system works poorly with close to one fifth of Danish citizens. It could have been possible that it was simply the same traveller who was rejected by the system four times. — Knowing that it was the same person who was rejected many times is very different from knowing that there were many people who used the system and that there is an almost 1 in 5 chance that they will be rejected.

To better understand system performance limitations and mitigate the factors that negatively influence the performance, *subject-based performance analysis* is highly recommended, which reports reject and accept rates statistics distributed over travellers, rather than distributed over transactions (passages). In brief, subject-based analysis allows one to estimate how many people were rejected by the system, as opposed to how many transactions resulted in rejections. The results of applying subject-based analysis to NEXUS iris recognition system are provided in [4, 143, 145]) and further described in Appendix E.

# Chapter 5

# Components of e-border

## 5.1 Five components (Pillars) of e-border

Through a survey of the border clearance technologies used in the last two decades, the study has established *five* key e-border traveller screening components, or Pillars, that make automated border control possible and efficient. They are described below, also summarized in Table 5.1.

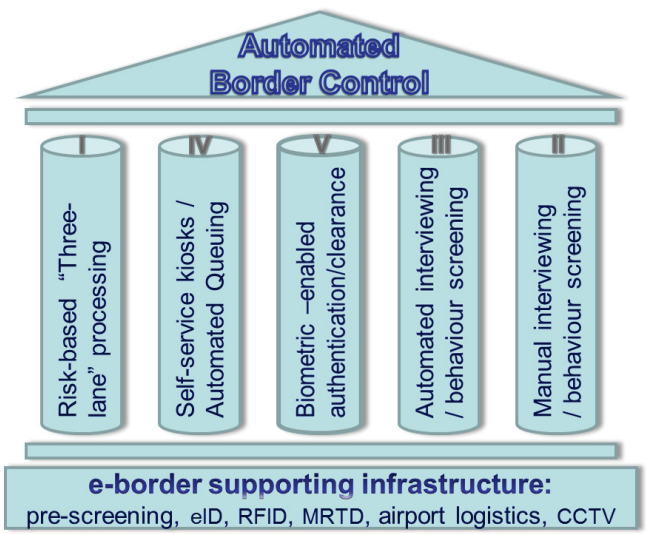



Figure 5.1: Five Pillars of e-border.

**I: "Three-lane" (Three-level) risk-based processing**: Divides travellers into three risk categories: high risk, low risk and unknown risk. Various physical topologies for implementing "Three-lane processing" are possible, including "two-lane" (lower-risk travellers use separate lane) and "single-lane" (lower-risk travellers use the same lane as everyone else, but are asked fewer questions) topology currently used with trusted / registered travellers programs in Canada and worldwide. It is defined as follows [27, 28, 48]:

$$\texttt{3-lane technology} \equiv \begin{cases} \texttt{High-risk traveller,} \\ \texttt{Unknown traveller,} \\ \texttt{Known (low-risk) traveller.} \end{cases}$$

This technology/concept aims at achieving the following effects:

1. Strengthened security by focusing resources where the risk is greatest,

Table 5.1: Five main technological components (Pillars) of traveller screening.

| # | Technology | Key Principle | Examples | Assumptions/Limitations |
|---|---|---|---|---|
| I. | "Three-lane" (Three-level) risk-based processing | Divides travellers into three risk categories so that to focus most attention on travellers of high or unknown risk. Division into categories ("lanes") can be topological or logistical, either accelerated by the traveller's involvement or not. | Processing of TTP/RTP members – using one or two topological lanes; TSA Black Diamond [117] (by travellerâĂŹs choice) – three topological lanes; APC/ABC kiosks (by travellerâĂŹs choice, according to citizenship) – two topological lanes. | There is a mechanism for distinguishing the travellers with respect to their risk-factor. Travellers cooperate when provided with an acceleration technology. / Has no limitations. |
| II. | Non-automated behaviour screening and interviewing | Involves trained border officers who conduct interviews and observe travellers to recognize their identity and risk. Based on human skills only. | Typical interviews conducted at Primary and Secondary inspection lines. Includes mass behavioural profiling programs such as SPOT), CAPPS, Secure Flight [84, 122]. | Humans can be trained to identify abnormalities. Trained personnel cannot be replaced by any behavioural profiling machine. Low use of technology. / Human abilities are limited, not persistent, not easily scaled. |
| III. | Automated behaviour screening and interviewing technology | Supports border officers in traveller interview in a number of ways (linguistic, with generation and processing of questions, detection of behavioural indicators) through the use of artificial intelligence and analysis of biometric measurements (such as facial expressions, voice, eye movement, pupil dilation). | The FAST project [65]. AVATAR systems [99]. | Machines can better handle high volume of travellers, be unbiased, multi-lingual, may better discern behavioural abnormalities. Interview questions can be intelligently generated by a machine. Person's biometric characteristics can reveal his/her emotion and level of stress, and can be measured remotely and conspicuously. / Requires a large combination of technologies. Least used and researched area. |
| IV. | Automated queuing and self-service technology | Collects and transfers advance data from travellers for their faster processing at primary inspection line. Delegates upstream border control (less intelligent tasks such as document scanning) to machines, and downstream control (more intelligent tasks) to border officers. | Self-service automated passport / border clearance (APC/ABC) kiosks deployed in Vancouver, Montreal, Toronto, and Chicago International Airports [105, 55]. Includes self-reporting and the *Pre-border Lane* concept [104]. | It is possible to separate border crossing operations with respect to the required level of intelligence (human vs. machines). / Does not perform authentication of document holders. |
| V. | Biometric-enabled authentication and clearance of travellers: ABC systems | Top component of the e-border functional hierarchy and may include other e-border components. —<br>Automates traveller clearance through 1) biometric-enabled traveller authentication (1-to-1 verification or 1-to-N identification, using his/her face/iris/fingerprint images), followed by 2) automated traveller risk assessment (via background checks and interviewing). and admissibility decision, which can be made final by default. | Gen-1 ABC: RTP-based (since 2002. UK: IRIS. Netherlands: PREVIUM. Canada: NEXUS [54]).<br><br>Gen-2 ABC: eID/ ePassport based (since 2006. EU, Australia/New Zealand [36, 38, 39]).<br><br>Gen-3 ABC: future e-border machines (2020) | Person's identity can be reliably authenticated using biometrics. Person's risk level can be established by the machine, based on local (provided by traveller and observed by the machine) and global (watch-lists and data-bases) information. / All biometric modalities have recognition limits, with faces having the largest one (with up to 10% of false rejects). Any single biometric modality can be circumvented through spoofing. Needs to be integrated into e-border infrastructure and supported by such technologies as pre-screening, e-ID, RFID, airport logistics, CCTV. |

2. Supporting this risk-based approach by integrating the traveller's information into the checkpoint process, and
3. Maximizing the throughput for the vast majority of travellers who are deemed to be low risk with no compromise on security levels.

Division into "lanes" can be:

- topological (i.e. separate lanes are for different risk categories) or logistical (when all travellers use the same physical lane, however are processed differently by the officer/machine depending on his/her risk category),
- either accelerated by the traveller involvement (when a traveller chooses whether to use the special lane or not) or not (when all travellers follow the same procedure).

Conceptually, risk-based processing is an assessment of *uncertainty about the traveller* [81]. Efficient implementations of the "three-lane" risk-based processing remains one of the highly demanded and unresolved problems, which many agencies are working on [83]. At the same time, a simplified "two-lane" risk-based processing is very commonly employed in RTP/TTP programs, where pre-registered "trusted" travellers are given special expedited passage at the border.

**II: Non-automated behaviour screening and interviewing**: Border officers attempt to recognize terrorists and persons with malicious intentions among travellers by observation and interviews. Scenario-based targeting techniques are used to guide specially trained behaviour detection officers towards a particular class of travellers of possible elevated risk, which is followed by interviewing techniques aimed at further exploring the hidden intents of flagged travellers.

Example programs are Screening Passengers by Observation Technique (SPOT), Computer-Assisted Passenger Pre-screening System (CAPPS), Secure Flight [84, 122]. The same technology is used in Tel Aviv's Ben Gurion Airport. The assumption used in these programs is that people convey emotions through unconscious gestures and facial expressions. Specifically, Facial Action Coding System (FACS) is used for measuring visually discernible facial motions in order to recognize person hidden intentions and emotions (see Figure 5.2).

The efficiency of non-automated behaviour screening is sometimes put in question, since it may lead to wrong critical decisions, especially with respect to individuals who have anxiety (5% of the household population, according to the Canadian Mental Heath Association [87] or other mental health conditions (almost 20% of the household population, from the same source) or who are coming from different cultural / religious backgrounds, possibly from long and stressful travel [1].

**III: Automated behaviour screening and interviewing technologies**: Automate the interview process and traveller risk factor analysis through a combination of 1) a computerized expert dialog system, which generates questions and processes responses from travellers, and 2) remote biometric multi-modal sensors capable of inconspicuously analyzing traveller's emotion and level of stress during the interview through his/her facial expression, voice, body / eye movement, pupil dilation, temperature, heart rate, etc.

The main idea is to separate the interview between the officer and the traveller into two parts:

$$\texttt{Interview} \equiv \begin{cases} \texttt{Traveller-machine}, \\ \texttt{Traveller-officer}, \end{cases}$$

and in this way to delegate the function of estimating the level of truthfulness in the traveller's response to the machine, using a special questioning technique.

A critical example of this component is the AVATAR technology,, developed by the University of Arizona under the funding from US BORDERS and CITeR consortiums, further assessed in Section 5.3.

[1] E.g. see Wikipedia: Robert Dziekanski Taser incident

**IV: Automated queuing and self-service technology**: Delegates the upstream border control to automated machines and the downstream control to border officers. This approach separates the operations with respect to the required level of intelligence (human vs. machines) :

$$\texttt{Queuing} = \begin{cases} \texttt{Upstream control by machine,} \\ \texttt{Downstream control by humans.} \end{cases}$$

Each machine plays the role of a data-collector and a filter: a traveller is directed to a particular lane based on the information he/she provided. Intelligent queuing technology is viewed as one of possible ways of deploying a semi-automated ABC machine.

The key examples of automated queuing technology are self-service **automated passport / border clearance (APC/ABC) kiosks** such as the ones deployed in major US airports and three Canadian airports (Vancouver, Toronto, Montreal), the further development of which is assessed in Section 5.4.

**V: Biometric-enabled authentication and clearance of travellers** or **Automated Border Control (ABC) systems**: Perform automated biometrically-enabled authentication of travellers followed by automated risk assessment and clearance (admissibility) decision. This is the top component of the e-border functional hierarchy, which potentially may include other e-border components.

The ABC machine action can be described in a simplified semantic form as follows:

$$\texttt{ABC machine} \equiv \begin{cases} \texttt{Traveller Risk Assessment,} \\ \texttt{Traveller Authentication,} \\ \texttt{Traveller Clearance.} \end{cases}$$

where, `Risk Assessment` are the activities required for the the assessment of traveller's risk via various forms of statistical surveillance such as pre-screening using government institutions and airport logistics. `Authentication` includes all operations related to the traveller's verification/identification. `Clearance` corresponds to the final act of consolidating all obtained information for generating the admissibility decision.

The categorization of ABC systems into three generations: RTP-based Gen-1 ABC system (such as NEXUS), eID/ePassport-based Gen-2 ABC system (such as SmartGates in Australia, EasyGates in EU, etc.), and next-generation Gen-3 ABC systems, which will rely on the entire Air Traveller Continuum e-border infrastructure, is done in Chapter 3. The analysis of issues with deployed ABC systems is presented in Chapter 4.

## 5.2 Supporting technologies

ABC technology will only be efficient if it is a part of the e-border infrastructure and integrates the following supporting technologies:

1. *MRTD and OCR technology*. Machine Readable Travel Documents and Optical Character Recognition technologies were the first widely adopted technologies for border control applications. They are part of old and new passports and can also be used for receipts/tokens that are printed by ABC kiosks and e-gates for communicating with each other.
2. *RFID technology*. The Radio Frequency IDentification technology should provide an efficient distribution of border crossing operations between the ABC machine, the border officer, and the traveller. It also includes tracking baggage, vehicles, tools, personnel (crew, service personnel, maintenance), and travellers. For example, the machine is not responsible for personal biometric data (they are stored in traveller's e-passport/ID), but the machine keeps the traveller's baggage trace file [124].

3. *Airport logistics*. It is assumed that the airport logistics should efficiently support the ABC machine, using the well-defined regulations, rules and signs, optimized streams of travellers, optimized surveillance, security, and responses to non-standard situations including possible attacks [82].
4. *Airport surveillance, including video surveillance and analytics*. This means that the traveller and his/her luggage must be tracked at any point of airport infrastructure; behavioural information about the traveller is monitored, and, if necessary, the behavioural risk factor is calculated. The technology readiness of video analytic technologies for automated recognition of travellers' identities and actions has been analyzed in precursor DRDC-funded studies [137, 138].
5. *Pre-screening (statistical surveillance)*. This means that the traveller's risk factor is estimated in advance of the travel, under the conditions of limited information sources. An overview of pre-screening technologies is provided below.

### 5.2.1 Pre-screening programs

**Pre-screening** (or also known as **statistical surveillance**) of travellers is assumed by default in all e-border and can be considered as a separate and critical component of e-border.

An example of a system that serves as a source of intelligence for border and transportation agencies is CAPPS [16, 119], mentioned earlier. It is a counter-terrorism system in place in US air travel industry. When a ticket is purchased, CAPPS can rate a passenger's risk using about 40 parameters such as address, credit history, destination, travel companions, type of payment, type of trip, etc., as well as the correlation between various parameters. This technology is called *electronic strip searches*, which is, however, too time-consuming to be used for screening every passenger. Therefore, it was proposed to be employed to screen those identified as high-risk passengers.

Another example of the program that is used for pre-screening travellers is that developed for the European Border Surveillance System (EUROSUR). Championed by Frontex [120], the EUROSUR system is one of the most ambitious surveillance systems ever envisaged by the EU. The main purpose of EUROSUR is to improve the "situational awareness" and to prevent irregular migration and cross-border crime. The cost of the EUROSUR is estimated at 2 billion euro.

A similar project is SEMAPHORE, which is the project coordinated by the Home Office in partnership with the key border control and law enforcement agencies in the UK. In this project, arriving passenger lists are checked against a variety of watchlists. The Joint Border Operational Centre manages all resources. The project initially targeted 6 million passenger movements a year travelling on a number of international air routes to and from the UK. The system processes advance passenger information provided by carriers on journeys to and from the UK. This information is screened against the watchlists in the Operations Centre. In addition to checking the passenger's information against watchlists, SEMAPHORE also receives reservation data for analysis against the profiles. This enables the identification of potentially high-risk individuals, using information contained in the carrier reservations data.

Finally, the FLUX (Fast Low Risk Universal Crossing) is a governmental partnership that uses biometric data from passengers of participating countries for identification [116]. This program offer a network of interconnected fast lane facilities to registered international travellers. Similar to the NEXUS agreement between the US and Canada which coordinates their Global Entry and CANPASS Air programs, FLUX coordinates between the US Global Entry and Netherlands Privium programs and is envisioned to include other countries such as Canada, Germany, the UK, and Japan.

## 5.3 Special interest: AVATAR-like systems

Recognition of travellers' hidden intentions and emotions is a complicated task. Even trained officers, as in SPOT program (Component II) may have difficulty correctly identifying "suspicious" behaviours. Furthermore,

humans will always be subject to the perception of "human bias" in making their decisions [86]. Computerized recognition of behaviour indicators, such as the emotional state of a traveller, may i) reduce the percentage of false alarms, ii) alleviate the "human bias", and iii) allow affordable scalability of the screening solutions.

One such technique is based on automated recognition of facial expressions from facial images captured by video, according to defined expressions /emotions groups (such as those shown in Figure 5.2).

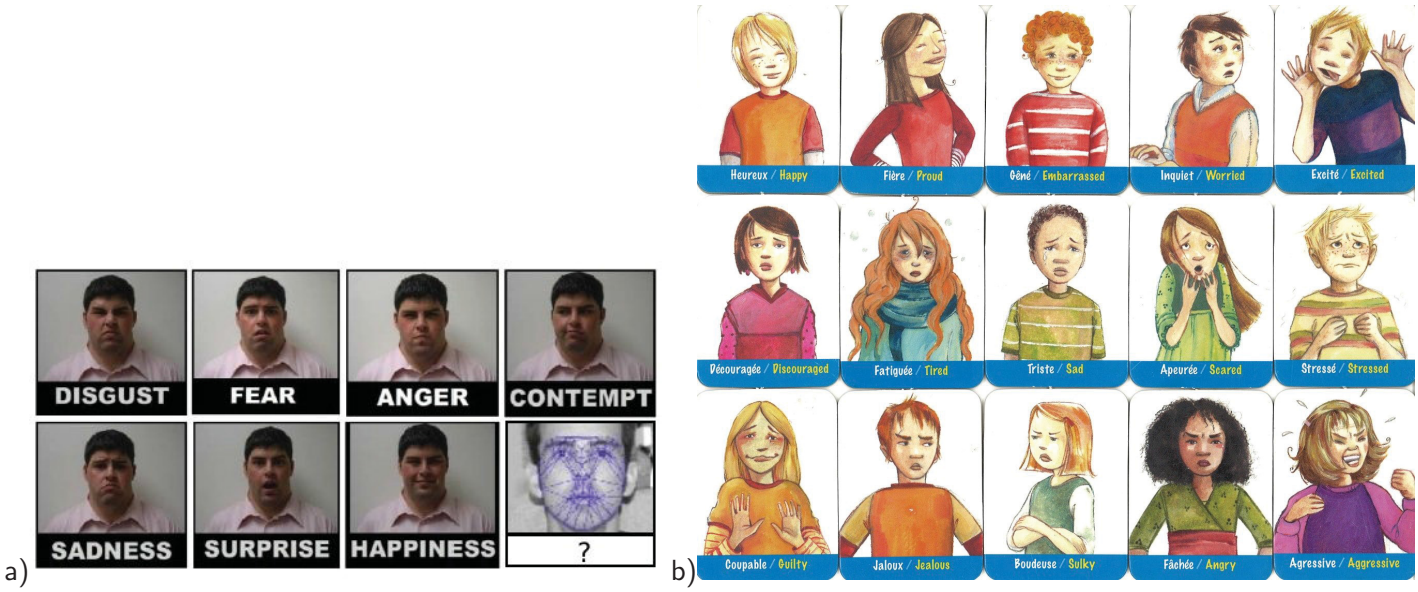



Figure 5.2: Emotions that can be recognized from facial images: a) Seven (7) emotions used in recognition by computers [101, 102], b) Fifteen (15) emotions recognized by psychologists [103].

Another approach is building a comprehensive system that uses a variety of biometric modalities combined with intelligently crafted dialog questions, as described below.

Following the introduction of the automated biometric-enabled behaviour screening interviewing system by University of Arizona under the name of AVATAR (short for Automated Virtual Agent for Truth Assessments in Real-Time) such automated traveller clearance systems are now referred to as AVATAR-like systems. Another key developer of AVATAR-like systems is University of Calgary, who refer to them under the name of the Interview Supporting Machines.

In the following, we overview the key features of the AVATAR-like systems, summarize the advantages they can bring for more efficient border management and suggest a practical roadmap for piloting and deployment such systems.

### 5.3.1 Background

The AVATAR system is introduced by University of Arizona, who has been investigating its validity and science for over two decades [93], and since 2008 with funding from BORDERS (US National Center for Border Security and Immigration) and CITeR (Center for Identification Technology Research, National Science Foundation (NSF) Industry/University Cooperative Research Center): `http://borders.arizona.edu` and `http://clarkson.edu/citer`. This is how they describe it:

> *"There are many circumstances, particularly in a border-crossing scenario, when credibility must be accurately assessed. At the same time, since people deceive for a variety of reasons, benign and nefarious, detecting deception and determining potential risk are extremely difficult. Using artificial intelligence and non-invasive sensor technologies, BORDERS has developed a screening system called the Automated Virtual Agent for Truth Assessments in Real-Time (AVATAR). The AVATAR is designed to flag suspicious or anomalous behaviour that warrants further investigation by a trained human agent in the field... The AVATAR has the potential to greatly*

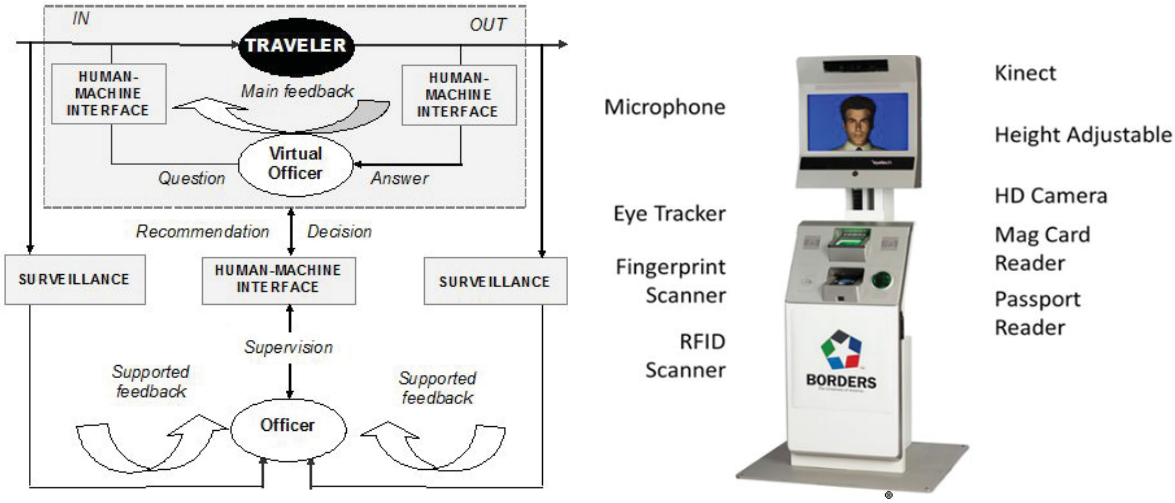



Figure 5.3: AVATAR-like system architecture: a) in terms of human-machine interfaces (from University of Calgary), b) design and sensors (from University of Arizona).

> *assist DHS by serving as a force multiplier that frees personnel to focus on other mission-critical tasks, and provides more accurate decision support and risk assessment. This can be accomplished by automating interviews and document/biometric collection, and delivering real-time multi-sensor credibility assessments in a screening environment. "*

The proof-of-concept of this system has been tested by the U.S. Customs and Border Protection with low-risk US citizens at a land border crossing at the Mexican border in Nogales, Arizona [94]. and by Frontex at the Henri Coanda International Airport in Bucharest, where it conducted brief interviews with non-EU travellers right after they disembarked from flights into Bucharest [95]. Speaking to travellers in their native languages, the AVATAR asks country-specific visa questions while monitoring respondents' body language and verbal replies to identify irregular behaviour that warrants further investigation.

A similar concept has been researched by the University of Calgary since 2006 and is presented in more detail in their publications [158, 159, 161].

Figure 5.3 outlines the architecture of the AVATAR system, in terms of the human-machine interfaces and the biometric sensors it uses (from work of the University of Calgary and University of Arizona). Two processes occur in the system simultaneously: collection of information (i.e., capturing and classifying the biometric measurements, according to the predefined emotion/stress classes), and expert decision making (i.e., generating the actions such as: interview questions for the system, and recommendations for the officer via mobile tablet).

An example of questions generated by the system is shown in Figure 5.4 (from [92]). As a traveller responds to the questions, his/her emotions (such as those shown in Figure 5.2) are analyzed from facial images captured by the camera and other sensors that can be installed in the kiosk.

Theoretical fundamentals of this approach are introduced in [89, 88, 90, 91]. It has been noted that in order to detect the deception , the fusion of 15 different cues out of 500 predictors can be done by the machine, whereas only two or three cues at one time can be controlled by human during the interview/interrogation (but not all 15). This can potentially make machines more efficient than humans in performing the task.

### 5.3.2 Potential Development

Based on the current technology readiness, potential development of AVATAR kiosks is seen as follows. It is suggested that deployment of AVATAR-like machines can be phased-in into operational border environment in

```
The Stress analyzer measures the human's responses to the following questions:
    - Have you ever lied to an authority?
    - Are you carrying weapon?
    - Do you intend to harm anyone on this airplane?
    - Do you have more than one passport?
The following blocks of questions are generated for the purpose:
Block #1:
 Q. 1: Please, describe in detail the content of your backpack or purse.
 Q. 2: I am detecting deception in your responses. Please, explain why that is.
 Q. 3: What will you do after you get through this checkpoint?
 Q. 4: Please, tell me how have you spent the last two hours.
Block #2:
 Q. 1: Has anyone given you a prohibited substance to transport through this checkpoint?
 Q. 2: Why should I believe you?
 Q. 3: What should happen to a person that unlawfully takes any prohibited substances
             through a checkpoint?
 Q. 4: Please, describe the last trip or vacation that you took.
Block #3:
 Q. 1: Do any of the items in the bag not belong to you? If so, please, describe
             which are those items.
 Q. 2: How do you feel about passing through this checkpoint?
 Q. 3: Please, elaborate on why do you feel that way.
 Q. 4: Based on your responses, the previous screeners have detected that you are nervous.
             Please, explain why that is.
Block #4:
 Q. 1: Are there any of your responses that you would like to change? If so, please describe what they are.
 Q. 2: Is there anything that you should have told us but have not?
 Q. 3: How do think that our assessment of your credibility will work out for you today?
 Q. 4: Why do you think that?
```

Figure 5.4: An example of questions generated by AVATAR border interview kiosk (from [92]).

.

**Critical Observation**

*The efficiency of behaviour screening by border officers is sometimes put in question, especially with respect to the individuals who have anxiety (5% of the household population, according to the Canadian Mental Heath Association[a]) or other mental health conditions (almost 20% of the household population, from the same source), or who are coming from different cultural / religious backgrounds, possibly from long and stressful travel [b].*

[a] http://www.cmha.ca/media/fast-facts-about-mental-illness
[b] Wikipedia: "Robert Dziekanski Taser incident"

a modular fashion. Specifically, the following phases of their deployment are envisaged.

- **Phase I** (no biometric sensing, no Artificial Intelligence, basic questionnaire analysis): The deployment of AVATAR systems can start with a "simple" application which does not use biometric-based intelligence and which works with pre-cleared or low-risk travellers, asking them basic declaration and border clearance

questions. This is the setup used in proof-of-concept tests[2] performed by University of Arizona with Frontex and DHS.

Even in these "simple" applications, one can observe a number of major contributions that this technology can bring to efficient cost-effective border control:

- There is no need to have bilingual officers. Other languages can also be easily adopted.
- They can also be combined with medical screening such as those used for controlling the spread of Ebola and other infections.
- They can be built using the existing APC kiosks infrastructure.

Once such AVATAR kiosks are deployed and integrated into e-border process, additional AVATAR sensors and functionalities can be added in a gradual manner, either by converting the existing APC kiosks or by adding new type of kiosk to the pool of kiosks used at the border.

- **Phase II** (no biometric sensing, adding Artificial Intelligence based support for the interview questions): Without modifying the work flow of the kiosk processing, more intelligence can be added to the system using expert systems that generate and process questions more like humans do it, similar to the Turing machine test [100], based on the traveller's answers and his/her current risk score. Some of the questions shown in Figure 5.4 can be intelligently crafted this way.

- **Phase III** (adding biometric analysis using standard kiosks sensors): Many kiosks are already equipped with audio recorders that can capture person's voice and high-resolution cameras capable of capturing person's facial expression and iris/eye motion. While this information is not currently used, it can greatly assist in screening a person for behavioural indicators. When such indicators are detected (or suspected), they will provide additional input to the expert system that generates the interview questions (such as those shown in Figure 5.4). It can also be noted, while biometric measurements are used to detect person's emotion and level of stress, they can also be used at the same time to further improve the authentication of a traveller.

- **Phase IV** (adding advanced biometric analysis using additional biometric sensors): additional remote sensors such as those used for lie detection by enforcement agencies, are added: for example, those that measure heart rate, temperature, perspiration. Since this type of sensors are not yet commonly used with general public, additional privacy impact assessment will need to be conducted prior to allowing their use in airports.

All of these phases can be implemented using the existing APC or ABC kiosks/e-gates infrastructure, or added as an additional infrastructure consisting of kiosks that perform only AVATAR functionalities. In either case, the travellers may not need to realize how many and which AVATAR functionalities are employed. At the present moment, in the proof-of-concept tests conducted by University of Arizona jointly with Frontex and DHS, the custom-designed system built by the University of Arizona team is used. However, one can foresee that these systems would be eventually built by ABC/APC integrators with AVATAR functionalities acquired separately from AVATAR developers.

Further consultation and research with researchers, industry and government partners is required to further elaborate and expand the AVATAR-like system deployment roadmap within a larger roadmap of e-border technology development.

[2] In tests conducted in the Budapest airport, the system was available to all arriving travellers who volunteered for the exercise. For tests conducted at the land border crossing with Mexico, the system was available to US citizens only.

a)  b) 

Figure 5.5: APC kiosks: a) first generation (in Detroit), b) second generation (in San Diego) . (Source: a) Google "APC", b) courtesy of Vision-Box)

## 5.4 Special interest: APC kiosks

Self-service Automated Passport Control (APC) kiosks, also known as clearance kiosks are a particular implementation of wider automated queuing technology (Component IV), where upstream control is implemented by using a passport reading machine, as well as the automated watchlist check performed on a database. travellers are prompted to answer a series of questions at the touch screen self-service kiosk. This process is finalized by assigning each passenger an encoded risk factor. The traveller then enters the downstream control, which is performed by a border officer.

### 5.4.1 Background

Two generations of APC are currently deployed in North America (see Figure 5.5). Gen-1 APC kiosks, such as those in Canada and the earlier installation in the USA, were not designed with biometric recognition in mind. Gen-2 APC kiosks represent the latest trend in APC deployment in the USA. They are designed to be biometric recognition capable and also easier to operate: they adjust automatically to eye level, have high-resolution cameras and active illumination to produce the ICAO-compliant face image of the traveller, which can be compared to the picture stored in the passport. At the present they do not perform biometric authentication but they will be able to do so if/when required.

The APC kiosk is a part of the e-border technology, which aims at self-service through some well specified border crossing operations, such as scanning/reading of traveller documents and answering the common questions. Verification of a traveller, and the final decision are the tasks of the border officer.

The APC kiosk aims at supporting a border officer in some border crossing tasks, which can be delegated to the traveller with an acceptable risk. Nevertheless, the border officer is responsible for traveller verification and making the final decision. The officer can operate with one or several kiosks, depending on the situation.

Key founctional components of the APC kiosk are:

- travel document scanner/reader,

**Critical Observation**

*Basic configuration of the APC kiosk can be considered as the platform for further extension of its functions such as*

- *Collecting early warning data about a traveller using biometric measurements,*
- *Verification of the traveller's documents using specific-purpose equipment,*
- *Improving interviewing assistant by using intelligent support technologies.*

- watchlist database,
- interviewing assistant by using touch-screen devices, and
- risk assessment assistant based on API, watchlist, and interviewing.

A watchlist in APC kiosk represents a minimal level of traveller risk assessment. It is designed as a special-purpose database, which is created using data from national and international databases.

### 5.4.2 Potential Development

A possible roadmap for the potential development and deployment in APC kiosks is seen as follows, adapted from [9]: (see also Table 5.2):

**Phase-I** (basic configration): the simplest component of a queuing technology which provides two main operations: (a) self-service scanning of a regular passport, and (b) basic risk assessment using watchlist. These are the kiosks of earlier installations in the US and the kiosks installed in Canadian Airports by the Vancouver Airport Authority;

**Phase-II** (with added interviewing/risk assessment support): a Phase-I extension by integration of the risk assessment and an additional source of personal data via the simplest interviewing assistant (without behaviour screening intelligent support, see AVATAR-like systems potential deployment roadmap in Section 5.3);

**Phase-III** (with biometric-enabled authentication and enhanced interviewing/risk assessment support): a Phase-II extension by providing biometric recognition for e-passport holders (functions of the Phase-III APC kiosks are equivalent to the functions of the Gen-2 ABC machines) and advanced AVATAR-like systems functionalities;

**Phase-IV** (Entry-Exit kiosks): a special design for immigration Entry-Exit systems, such as the US-VISIT system.

According to [9], this prediction of potential trends in the design of the APC kiosks is due to the following assumptions:

1. It is common in practice to use OCR (Optical Character Recognition) readers for converting various documents into electronic form. The simplest configuration of the APC kiosk is based on an OCR reader, a database for storing data, and a watchlist (database of "wanted" individuals).
2. It is technically possible to extend the Phase-I functions by integration of the risk assessment assistant and gathering information from available sources provided, for example, by the simplest interviewing assistant, a watchlist, and an API database.

3. It is feasible to extend the Phase-II functions for e-passport holders by integration of the MRID readers and biometric recognition assistants. The functions of the Phase-III will be equivalent to these of the Gen-2 ABC machine.
4. It is technically executable to satisfy the requirements of the Entry-Exit concept and to design an APC kiosk for immigration control based on the Entry-Exit systems, such as US-VISIT. In this design, a traveller can use the OCR and MRID readers of documents, including e-passport. Because fingerprints are a mandatory biometrics in the visa regulation process, a fingerprint station should be integrated in the Phase-IV kiosk.

Table 5.2: Potential development of APC kiosks.
(Adapted from the University of Calgary report [9])

| | Potential APC kiosk design | | | |
|---|---|---|---|---|
| **Component of the APC kiosk** | **Phase-I** | **Phase-II** | **Phase-III** | **Phase-IV** |
| OCR passport reader | ✓ | ✓ | ✓ | ✓ |
| Interviewing assistant | | ✓(*) | ✓ | ✓ |
| Watchlist | ✓ | ✓ | ✓ | ✓ |
| Risk assessment assistant | | ✓ | ✓ | ✓ |
| Biometric recognition assistant | | | ✓ | ✓ |
| MRTD e-passport reader | | | ✓ | ✓ |
| Fingerprint acquisition station | | | | ✓ |
| Entry-Exit system interface | | | | ✓ |

(*) *The simplest form of interviewing as a common question-answer machine with no intelligent support (see AVATAR-like systems potential deployment roadmap in Section 5.3).*

## 5.5 Conclusions

The five key e-border components (Pillars) described in this chapter (Table 5.1) support border officers in various ways such as:

- Delegation of some functions/operations to the traveller or/and the machines,
- Support of the officer's decision-making by the machine,
- Maximizing/simplifying the automation processing for all travellers or for registered travellers only.

With respect to these components, the following four important conclusions are made:

1. All e-border components are compatible; that is, each border crossing technology can be used as a part of another technology, or the results of application of one technology can be used in another technology.
2. All e-border components are biometric-enabled technologies (directly or by default), in the extended definition of biometrics (discussed in Section 2.5.1) as used for person authentication and person risk assessment.
3. All e-border components are user-centric technologies. That is, the ABC technologies are aimed at adapting to the traveller's needs, through an intelligent human/machine interface with feedback (learning), distance (non-contact) check, minimization of waiting time, minimum need of cooperation with the automatic devices, special accommodation for the travellers with disabilities, utilization of pre-screening and clearance techniques, mitigation of linguistic, cultural, and geographical differences.

4. The top of the e-border hierarchy is the ABC technology (Component V), the main feature of which is that this technology is open for further improvement and extension, for example, by using APC features (Component IV) and automated behaviour screening (Component III).

### 5.5.1 Roadmapping of future ABC solutions

Based on the evolutionary classification of ABC systems (Chapter 3) and the taxonomization of e-border components developed in this chapter, new ABC solutions can be defined though a composition of the technologies listed in Table 5.1. The examples of the envisaged ABC / e-border solutions are listed below:

- *Technology I+V:* an idealized 3-lane risk concept is implemented by using the 3-level risk ABC technology. This technological opportunity is widely used in EU and other countries.
- *Technology I+IV+V:* an idealized 3-lane risk concept is implemented in the upstream of the automated queuing technology further combined with biometric-enabled verification. This is an technological opportunity for APC kiosks deployed in USA.
- *Technology I+III+IV+V:* all automated technologies are combined in a single unit (either in a kiosk or e-gate design) based on the principles of 3-lane risk processing and performing document verification combined with biometric-enabled verification and automated interview supporting behaviour screening (AVATAR-like) functionality. This could be a technological long-term opportunity for Canada or any other country aimed at ultimate optimization of e-border efficiency and security.

**Critical Observation**

*It is envisaged that Automated Border Control (ABC) systems will eventually converge to a single all-in-one multi-component globally-connected user-centered system (in a form of a kiosk, e-gate or a combination of both) that will automate all traveller clearance tasks: lower intelligence tasks such as those performed by APC kiosks (Component IV) and higher intelligence tasks such as: traveller authentication via biometric authentication (Component V) and traveller risk assessment via AVATAR-like interview assistant and behaviour screening technology (Component IV).*

# Chapter 6

# Metrics and tools

As emphasized in Chapter 3 and illustrated in Figure 3.2, ABC systems are evolving drastically since their first deployment over a decade ago: from biometric-enabled access-control-like systems operated by a *set of known habituated users* towards complex e-border systems operated by a *flow of unknown non-habituated users*.

Whereas the performance of a biometric-enabled access control system can be evaluated using the biometric performance metrics defined by the ISO standards [172] (such as False/True Match Rates, False Acceptance/Rejection Rates, and ROC/DET curves), the use of such metrics for ABC systems is not sufficient. As a complex multi-component system working within a larger e-border infrastructure, ABC systems need to evaluated by means of the concepts used in evaluation and management of complex system, which take into account all system components and factors and their relationship with each other.

The factors that influence ABC performance are examined in Section 4.7.1. In the following, we establish the performance metrics that need to be considered when deploying ABC systems, provide an introduction to the two key approaches that can be used to evaluate ABC performance and risks: one – based on observation using the so-called degraded performance metric and the other – based on modeling and simulation, and present a tool for developing ABC deployment taxonomy based on on the criteria for evaluation of automated person authentication mechanisms.

## 6.1 Performance metrics

### 6.1.1 Top level metrics

There are three key top level metrics that are used for describing ABC systems:

$$\texttt{Performance metric} = \begin{cases} \texttt{Operational reject rate (ORR)} \\ \texttt{Throughput} \\ \texttt{Border wait time (BWT)} \end{cases}$$

These metrics characterize the performance of the ABC machine from a variety of perspectives.

The **ORR** is an integrated metric for evaluating the system effectiveness, since it represents the average number of travelers directed by the ABC machine to a manual control (regardless of the reason). For example, 10% of travelers, cannot be served by the ABC machine, and are directed to manual control. This metric is useful for analyzing service quality.

The **Throughput** measures the system efficiency, and is the average number of travelers served by the ABC machine per hour. This metric integrates both the number of travelers successfully served by the machine, and the number of those failed to be authorized and, therefore, directed to a manual control. This metric is useful to measure the system efficiency in case of large streams of travelers.

The **Border wait time (BWT)** characterizes the quality of services in terms of the amount of time each traveler spends waiting to be serviced. The ICAO and IATA recommend that BWT is no more than 10 minutes. The border waiting time addresses the ability of the system to serve travelers simultaneously, or in parallel, by several e-gates of the ABC machine.

### 6.1.2 Performance optimization areas

Using the above metrics the performance of the system needs to be defined and optimized along three performance dimensions:

$$\texttt{Performance optimization areas} = \begin{cases} \texttt{Facilitation} \\ \texttt{Security resources} \\ \texttt{Cost resources} \end{cases}$$

A trade-off among those areas is expected. For example, it is possible to achieve high performance of the ABC machine by easing the security requirements, or by utilization of all facilitation resources, in which case the solution will be extremely expensive.

### 6.1.3 Performance dependability areas

Following IEC 60300 standards [1] for complex system dependability management, the performance of the ABC system should be analyzed in terms of the ability of the system to perform its intended functions in *three* performance dependability categories:

$$\texttt{Dependability categories} = \begin{cases} \texttt{Reliability performance} \\ \texttt{Maintainability performance} \\ \texttt{Maintenance support performance} \end{cases}$$

An arbitrary deployment scenario for the ABC machine should begin with the dependability analysis over these three performance categories. It is impossible to reach the final desired top-level performance metric (ORR, throughput, BWT), if reliability, or maintainability, or maintenance support performance does not satisfy the requirements which are specifically defined for the intended ABC machine.

The foundation of the ABC machine performance lies in the area of dependability of complex systems, including risks and vulnerability [224]–[166]. This is the platform for specific-purpose framework.

Dependability deals with the performance issues at each of the life-cycle phases of an arbitrary complex system: planning, design, deployment, measurements, data collection, analysis, and improvement. The specific-purpose properties of the ABC machine are identified with respect to the three dependability areas as follows:

1. *ABC reliability performance,* which includes throughput, wait time, biometric modality efficiency (face, iris, fingerprints), authentication procedure (verification or identification), FAR, FRR, and security as their function, degraded performance, e-passport and its holder authentication, security level control (controlled and uncontrolled decision-making threshold), etc.
2. *ABC maintainability performance,* which includes performance parameters related to the discipline of service (1-stage or 2-stage e-gates), and mantrap topology (1-input 2-output or 1-input 1-output), ergonomic issues, discipline of human-machine interactions, as well as the mean time to restoration after failure or attack.

[1] This information is provided by the University of Calgary researchers. See Appendix C for more detail.

3. *ABC maintenance support performance,* which includes the location of e-gates with respect to security and service criteria, the parameters related to location of database (watchlist) and biometric reference templates, appliance configuration, remote control and diagnostic, skills of technical staff and their measures in terms of degradation, training of personnel such as short-term periodically intensive training, vulnerability to physical attacks such as explosions and bomb suicides, and other attacks (electrical, electromagnetic, etc.), and system developer/provider specifications.

### 6.1.4 Metrics for system specifications

The ultimate task for an agency interested in deploying an ABC system is to be able to develop technology specifications that would meet the agency's business requirements. To assist with this task and by the request from the CBSA, the University of Calgary researchers, have developed the list of operational requirements that should be consulted when developing the ABC specifications, based on the analysis of the ABC performance metrics presented above. This list is shown in Table 6.1. Units for the performance metrics are given in brackets, where "List" corresponds to a group of metrics. More detailed analysis of these metrics and the overall taxonomic hierarchy of ABC performance is given in [10].

## 6.2 Technology readiness assessment tools

Whether it is face or iris recognition on the move, AVATAR-like behaviour screening or border wait time estimation using video camera, any technological component, prior to being considered for inclusion into a production ABC solution needs to be assessed for its deployment readiness The concept of Technology Readiness Level (TRL) has been adopted by many agencies for this purpose [223]. Proper TRL assessment however may not be suitable for a wide community of users who may not have capacity or capability to conduct comprehensive TRL assessments. A light-weight alternative to the nine-point TRL assessment has been developed by the CBSA. Called PROVE-IT($x$), where $x$ is the name of the component, it uses a semaphore-like three-point scale to serve as a practical tool for preparing the recommendations related to the technology deployment and best investment opportunities [137]. Using the PROVE-IT($x$) technology readiness assessment framework, the readiness of face recognition in video and video analytic technologies has been done. Similar assessment for other technologies is recommended. More details are provided in Appendix G.

## 6.3 Analysis via observation: Degraded performance metric

In addition to the top-level performance metrics and the metrics that can be used for developing system specifications (Table 6.1), a combined life-cycle system performance metric is introduced in this study called *Degraded performance metric* specifically for the purpose of analyzing and comparing the biometric performance of ABC systems [2, 3].

It is motivated by the fact that the real operational performance of an ABC system is always and sometimes significantly less than its theoretical or expected performance. This phenomenon is attributed to the fact that, in such large-scale open-traffic applications as ABC, there are always factors (such those listed in Section 4.7.1) that are not accounted for and that will degrade the performance of the system below the expected level.

A combined performance metric is a way to evaluate performance using two or more techniques. For example, (a) evaluation of a system using notion of probability of the best and the worst scenario is useful in analysis of risks of deployment scenarios [160]; (b) evaluation of the matcher in a recognition algorithm, using the false match/non-match metric and cost curves addresses the early phases of the ABC machine design [218]. In this study, a combined metric is proposed for performance assessment at three phases of the ABC life-cycle.

Table 6.1: Performance metrics for defining specifications of ABC systems (from [10]).

| | **Performance of generic machine IEC 60300 Standards** | **Performance of the ABC machine and supportingdata IEC 60300 + ISO SC 37 Standards** |
|---|---|---|
| 1. | Availability performance | • Operational availability (dependability) (List)<br>• Efficiency of logistic support (List)<br>• Human factors (List)<br>• Depth of embedding in social infrastructure (List)<br>• Facilitation (List) |
| 2. | Reliability performance | • Predicted reliability performance (Probability)<br>• Reliability structure (Uniform data structure)<br>• Critical parts (Uniform data structure)<br>• Failures (Probability)<br>• Resources (List)<br>• False acceptance rate (FAR) (Probability)<br>• False rejection rate (FRR) (Probability)<br>• Operational reject rate (ORR)(Probability)<br>• Throughput (person/hour)<br>• Waiting time (Minutes)<br>• Degraded performance (available resources) (Probability)<br>• True rejections (Percentage)<br>• e-service including e-health and e-medicine (List)<br>• Intents (Percentage) |
| 3. | Maintainability performance | • Daily maintenance (List)<br>• Software update (List)<br>• Hardware upgrade (List)<br>• MTTR minimization (Minutes) |
| 4. | Maintenance support performance | • Logistic operations (List)<br>• Remote diagnostics (List)<br>• Administrative operations (List)<br>• System services (List)<br>• Stakeholder requirements (List)<br>• MTTR minimization (Minutes) |
| 5. | Multi-parameter performance optimization | • Social cost of the ABC errors (List)<br>• Passenger Queuing Time (minutes)<br>• Life-cycle cost ($)<br>• Cost/system effectiveness (List)<br>• Operational effectiveness (List)<br>• Personnel training (List)<br>• Operational availability/dependability (List) |

**Critical Observation**

*A particular feature of the ABC system is that its real observed performance can be significantly worse than the one specified by operational requirements (Table 6.1), because of the presence of the factors that are not accounted for (Section 4.7.1).*

**Definition 6.3.1** Degraded performance assessment *of the ABC system is defined by three measuring points of the ABC life cycle:*
$(a)$ *Design phase:* Theoretical *or algorithmic limit of performance; it is the performance of the biometric recognition algorithm tested on a database of biometric samples,*
$(b)$ *Prototyping phase:* Predicted *or lab-tested; this is a performance of the integrated biometric algorithm in the ABC machine, and*
$(c)$ *Deployment phase:* Operational *or real performance of the deployed ABC machine, which defines the ratio of travelers for whom the ABC machine cannot confirm the verification (they have to be sent to the manual control). It is expressed by the clause "one in $M$ travelers is directed to manual control".*

It follows from the above that (a) the real performance is always lower than the desired one, or its predicted limit; (b) there are certain factors that influence the performance degradation; and (c) it is difficult or impossible to estimate the contribution of these factors to the system operational performance.

Degraded performance assessment includes two metrics: (a) the False Reject Rate (FRR) [164] for measuring theoretical and predicted performance, and (b) Operational Reject Rate (ORR) for measuring operational performance [112].

### 6.3.1 Use of degraded performance metric

Compared with the ORR, Throughput, and Waiting time, which are more suitable for evaluation of service quality, the degraded performance does address not only the current scenarios, but also the strategic needs and planning. For example, using this metric, the ABC machines can be compared in terms of three criteria, including biometric modality performance. Note that the degraded performance (what the user of the deployed ABC machine gets) is equal to ORR.

The degraded performance assessment metric is useful due to the following reasons:

1. It carries the notion of a *potential, or available resource*, which can be achieved. This resource corresponds to the performance of the best recognition algorithms reported in literature, e.g. in NIST evaluations [176, 193].

2. It carries the notion of the *efficiency of utilization of a potentially available resource*, which represents the degree of the performance improvement.

3. It distinguishes the *system performance* and the *biometric recognition performance* expressed by the clause (a) "1 in $M$ customers is wrongly recognized" and (b) "1 in $N$ customers is wrongly directed to manual control".

In addition, the proposed degraded performance assessment metric provides the means to distinguish the controlled and uncontrolled factors. An example of such metric is given in Fig. 6.1, where the potential resource is estimated by ratio 10/25.

### 6.3.2 Performance comparison of the deployed ABC machines

The life-cycle combined performance assessment reported for some known ABC machines is summarized in Table 6.2. The first three columns contain the country of deployment, year of the reported results, and

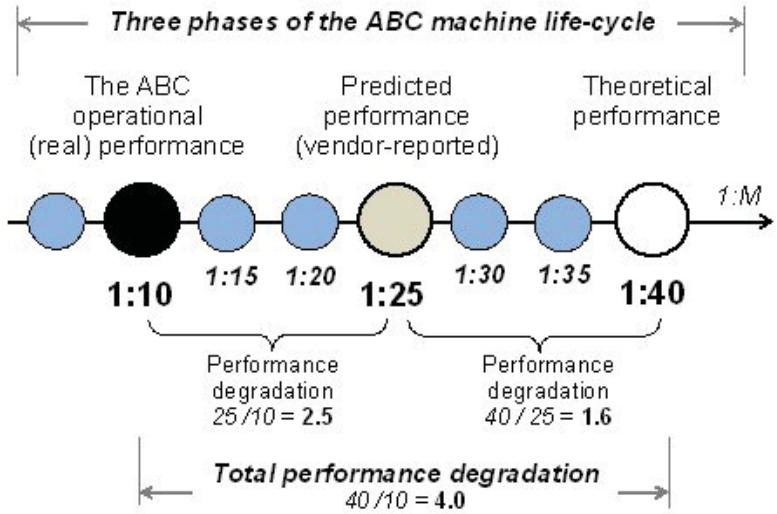



Figure 6.1: Example of the degraded performance assessment of an ABC machine: Theoretical performance (reported in literature) is 1:40. The predicted (obtained in lab test vendor-reported) is 1:25, and the ABC operational (real) performance of the deployed ABC machine is 1:10 (One of ten is rejected).

sources of information, respectively. Next four columns contain a type of biometric modality, operational (real) performance, predicted (claimed by vendor) performance, and theoretical (algorithmic) performance in terms of $1:M$ (1 person in $M$ is falsely unauthorized). For simplification, the data in the last column corresponds to the following algorithmic FRRs of the recognition algorithms: iris – $FFR = 0.1\%$, fingerprints – $FFR = 0.1\%$, face – $FRR = 1\%$, and fusion of face and fingerprint – $FFR = 0.1\%$ [176, 193]. Because of the limited available statistics, we assume that "the number of persons who are falsely directed to manual control" and "the number of persons who are directed to manual control" are the same. The table presents the "pessimistic" low-bound reported values for the FRR.

Table 6.2: Life-cycle combined degraded performance metric for the ABC machines deployed in the EU.

| ABC machine, | Operational | Predicted | Theoretical |
|---|---|---|---|
| UK[77] | 1:10 | 1:50 (2%) | 1:1,000 |
| Germany [111] | 1:8 | 1:20 (5%) | 1:100 |
| Germany [110] | 1:7 | 1:20 (5%) | 1:100 |
| Spain [108] | 1:8 | 1:20 (5%) | 1:100 |
| Spain [108] | 1:10 | 1:25 (4%) | 1:1,000 |

The following conclusions can be drawn upon the data from Table 6.2.

1. *Best practice:* Contemporary ABC machines operate at $\texttt{Performance}_{\texttt{ORR}} = 1 \texttt{ in } 10 \texttt{ travellers } (1:10)$. That is, 1 in 10 travellers is directed to the manual control.

2. *Potential:* All deployed ABC machines have a good capacity (or potential) for performance improvement. For example, the UK's ABC machine, based on iris recognition, utilized only $1/100$ of its resource (this machine was of the first generation, accordingly to our classification; the system was dismantled in 2012). Face-based ABC machines, deployed in Germany and Spain, utilize $1/10$ of their potential capacity. It is estimated that Spain's ABC machines, based on fusion of face and fingerprint modalities, have a hundred times more resource.

3. *Controllable factors:* A lot of effort was undertaken by various institutions such as NIST and ISO

to account for the factors that affect the performance of biometric recognition algorithms. A number of new designs and algorithms have been introduced that take many factors into account. However, one can observe that increasing the power of the recognition algorithms does not necessarily result in the performance improvement. For example, Spain's ABC machine that combines power of facial and fingerprint biometric modalities, performs just slightly better than the one with a single fingerprint modality.

4. *Uncontrollable factors:* International community, in particular, the IATA and ICAO [27], and FRONTEX (EU) [36] demonstrated the effort to reduce the dimensions of the uncontrollable factors. Additional study in various non-technical fields is needed in order to shift the weight of the non-technical factors contributing to the performance degradation into the technical factors that can be controlled much easier than the other ones.

## 6.4 Analysis via modeling: simulation tools

Modeling is the methodology for providing a *predictive estimated measurements* at any point/state of interest of e-border infrastructure, including the ABC machine and supporting technologies. Three levels of ABC modeling techniques are distinguished:

Figure 6.2: Level-1 simulators: Example of visualization and resource allocation analysis in airports using Simio simulation software [216].

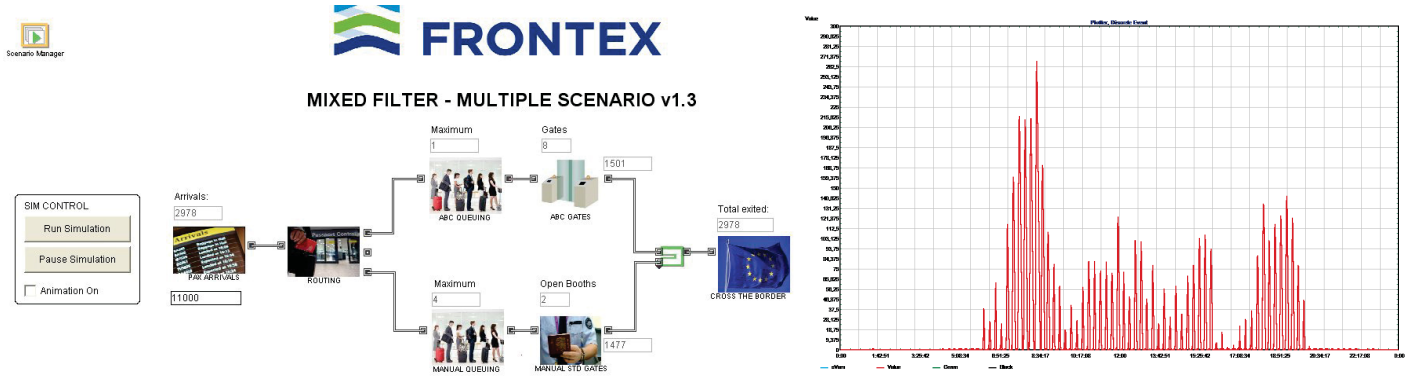



Figure 6.3: Level-2 simulators: Example of ABC simulation developed by Frontex for multiple scenario analysis using ExtendSim sofware: a model and border wait time forecast [40, 217].

### 6.4.1 1st level simulators

*1st level* of modeling includes simulators, which offer a general view of the border crossing process at a particular point, including simulation of illustrative examples/scenarios, and which allow one to conduct resource allocation or general bottleneck analysis at a particular point. Commercial software such as Arena [215] and Simio [216] are well suitable for this purpose and are used in a number of border control related applications such as passenger and baggage flow analysis, officers / shifts scheduling, airport master plan design, etc.

### 6.4.2 2nd level simulators

*2nd level* of modeling corresponds to the needs of a more complex ABC machine of the 2nd generation and supporting infrastructure. ExtendSim simulation software is used by Frontex for this purpose in order to conduct cost-benefit analysis of ABC solutions for EU members (Figure 6.3) [40]. According to case studies published by ExtendSim [217], it can be used to simulate probabilistic and Bayesian networks based models. This is an important feature for e-border solutions analysis through simulation.

### 6.4.3 3rd level simulators

*3rd level* of modeling involves powerful virtual simulators of global e-borders; this level is envisioned to be reached by year 2020+, according to the ICAO roadmap [27]. According to the University of Calgary researchers, there are no commercial solutions capable of this highest level of modeling. As a solution to the problem, they have developed a concept called the *e-Border Profiler*, which is a modeling technique and software aimed at simulating (or profiling) the risks of any e-border solution at any of its states using various scientific techniques such as Bayesian network, game-theory, Dempster-Shafer evidential, multi-agent simulation, etc.

An example of constructing and using an e-border profiler for ABC border wait time problem is shown in Figure 6.4, where a process of passing through a man-trap e-gate is modeled by using the Bayesian network defined by the a-priori probabilities describing the process. More details are provided in [8].

## 6.5 Criteria for deploying automated personal identification mechanisms

Another tool that has been identified by the University of Calgary researchers [10] relates to the description and taxonomization of ABC deployment scenarios, based on the state-of-the-art work on the evaluation of authentication machines in terms of various categories by Palmer [229].

In total of over 200 categories are defined by Palmer for developing automated personal identification mechanisms, of which a biometric-enabled ABC machine is example, grouped according to more general technical and non-technical notions into following key groups of categories, summarized below

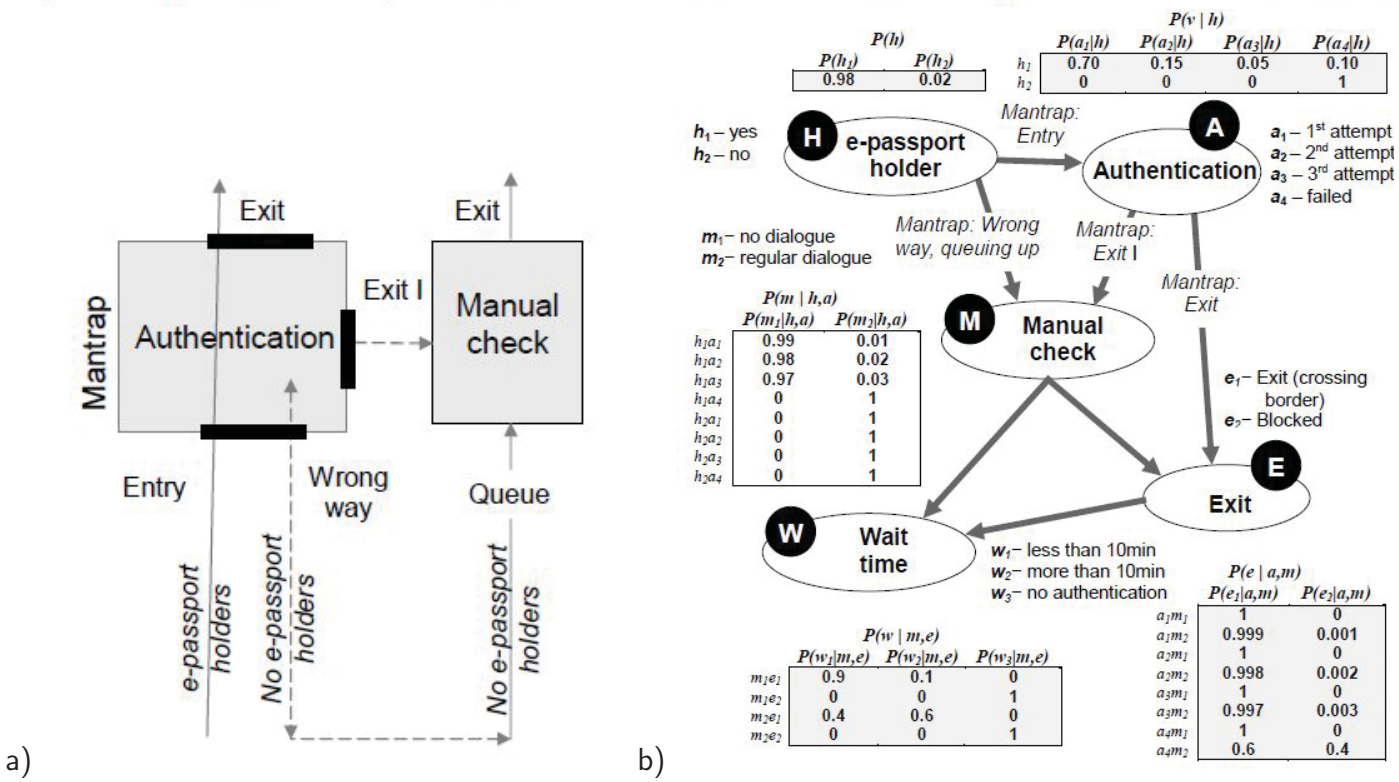
- risk assessment,
- social acceptability risk assessment,
- controls performance,
- assurance,
- technology, and
- security architecture.

This categorization can be used in a number of ways:

- It introduces a language to describe the ABC system as a general personal identification mechanism using the common language suitable for both the developers and stakeholders.

Table 1. Library of modelling modules for authentication task.

| | MODELING MODULE | STATE VARIABLES AND INITIAL DATA |
|---|---|---|
| 1. | e-passport | Security features, chip-optical data crosscheck, watchlist, verification, manual check. |
| 2. | Facial verification | Recognition, e-passport holder, number of attempts, watchlist, risk factor, manual check. |
| 3. | Pre-screenin | Risk-factor, airport surveillance, API (advanced passenger information), watchlists. |
| 4. | Pre-logistics | Signs, e-passport holder, surveillance, risk-factor, behavior (geography, ethnic) factor |
| 5. | Manual check | Machine assistance, risk-factor, behavior factor, interviewing, decision support/making. |
| 6. | Logistics attack | Topology, queuing, risk-factor, impostor/terrorist, behavior factor, surveillance. |
| 7. | Mantrap attack | Single traveller detector, baggage detector, risk-factor, behavior factor, topology. |
| 8. | Authentication attack | e-passport attack, plastic surgery, make-up detection, verification, manual check, risk-factor. |
| 9. | Watchlists | Searching time, combined database, risk-factor, updating, manual check, decision-making. |
| 10. | Training personnel | Personal skills degradation factor, decision-making/support, human-machine collaboration. |




| Authentication attempt | 1st | 2nd | 3rd | Failed |
|---|---|---|---|---|
| Risk (probability) of border crossing wait time > 10 minutes | 0.105 | 0.110 | 0.115 | 0.760 |

Figure 6.4: Level-3 simulators: Example of constructing an e-profiler (simulator) for estimating border wait time using the Bayesian network (from [8]).

The table shows a collection of modules required to model the authentication process at e-gate man-trap. The images show: a) a model of mantrap structure, b) simplified Bayesian network that models this mantrap, and final result, which shows the posterior probability that a traveller will be processed in more than 10 minutes as function of the number of interaction attempts with the authentication device (bottom). See [8] for more details.

- It suggests a novel taxonomy for conducting analysis and comparisons of ABC systems as personal identification mechanisms using the predefined general categories.
- It provides criteria for a perspective vision for ABC machine, acceptable for all phases of the life-cycle of currently deployed ABC machines, kiosks, and Entry-Exit systems, including strategic planning and attack countermeasures.
- It provides a novel training methodology

### 6.5.1 Applying Palmer's categories for developing ABC specifications

To show how Palmer-developed categories can be applied in the ABC context, the University of Calgary researchers [10] applied them to develop ABC specifications based on the recommendations for the ABC quality control developed by Frontex [36], as shown in Table 6.3.

### 6.5.2 Sensitivity of the ABC deployment categories in terms of terrorism risks

The University of Calgary researchers [10] shown that, using Palmer's categorization, each ABC category identifies capabilities that can be used by terrorists to impose damage to the ABC machines and supporting infrastructure, because each category contains information required for the development of specific set of attacks. They provide the following examples:

- Details of the deployed biometric recognition algorithm may give away information needed for development of attacks on the identification components. These attacks may be the threats such as false verification when impostor uses fake credentials (appearance, images, and templates); as a result the attackers may be granted border crossing.

- Available information on mechanisms of controlling the threshold may provide useful data for development of an attack on the decision-making components. The resulting threats of such attack can be observed as wrong decisions on travelers who are on the watch list (they may be granted border crossing). A summary of the ABC deployment categories that are vulnerable to various and hardware attacks is provided in Table 6.4.

## 6.6 Conclusions

The relationship between the needs and metrics constitutes the key part of the ABC machine performance analysis and becomes the foundations for developing ABC performance evaluations methodologies, two of which have been identified and refined by the University of Calgary researchers through the course of the study.

- **By observation:** To account for different factors and components affecting the ABC performance and to allow one to quantify the performance of an ABC system with respect to all factors and other ABC systems, the concept of the Life-cycle combined *Degraded Performance* is introduced. Examples of applying the concept to the evaluation of currently deployed ABC systems are presented. The key idea is that the performance of the complete deployed systems is worse than that of the prototype system, which in turn is worse than that of the reported in scientific literature.
- **By simulation:** Based on the developed formalization of an ABC system, the researchers introduce a probabilistic inference based methodology and tool, called *e-border Profiler*, which allows one to estimate (or profile), in probabilistic sense, all performance-related risks of an ABC system through modeling and simulations. The advantage of this methodology is that it can be implemented using a variety of scientific techniques, including Bayesian belief networks commonly used in forensics and security applications.

The PROVE-IT($x$) framework developed by CBSA for assessing the technology readiness of e-border components and supporting technology is presented. An application of the criteria for evaluation of automated person authentication mechanisms developed by Palmer to ABC is also presented and can be used to provide a common language between the ABC practitioners and developers.

More analysis of the techniques that can be used for modeling ABC performance including, ABC Profiler, and application of the Palmer's framework for the ABC deployment scenario development are presented in University of Calgary report [10].

Table 6.3: Recommendations for the ABC quality control developed by Frontex [36] described following the generalized categories defined by Palmer [229] (from [10]).

(a) Personal data SHALL NOT be stored for the purposes of quality control and statistics extraction unless properly anonymized.
(b) Anonymous operational data is stored in a centralized way at least at the ABC installation level (i.e. at the group of e-gates and monitoring and control stations at a given airport/port hall). Detailed maintenance and software debug traces MAY be stored at the local level (e.g. at a given e-gate computer).
(c) An entry in the operational register should be created for any transaction taking place in an ABC system. The following types of transactions SHOULD be logged:
- Access attempts with documents not accepted by the system (i.e. non- electronic passports, not a passport).
- Access attempts with non-eligible documents (i.e. underage Schengen citizens holding an e-passport, third country nationals holding an e- passport).
(d) Total verification time is defined as the time needed to fully verify an eligible traveller, regard- less of the outcome of each particular check (document authentication, biometric verification, background checks, etc.).
(e) Total access time: defined as the total time spent in the process by an eligible traveller since its first interaction with the system (presentation of the travel document in an integrated two-step process ABC system, entry in the mantrap space in one-step process ABC system, first inter- action with the verification modules in a single e-gate or segregated two-step process solution). The exact definition and estimate of this time will ultimately depend on the architecture of the system (e.g. when the full verification process takes place within a mantrap, this time measurement will always be greater than the verification time).
(f) It is RECOMMENDED that each ABC installation is uniquely identified within a national ABC deployment. It is RECOMMENDED that the identifier shows:
- A clear identification of the Border Crossing Point (e.g. airport moniker).
- Detailed information regarding the location within the Border Crossing Point (e.g. terminal number, arrival/departure hall number).
- Information regarding the type of Border Crossing Point: entries or exits.
(g) It is RECOMMENDED to include a subsystem for the logging of statistical and technical data regarding the biometric verification process, for the purpose of having a continuous quality control, the extraction of business statistics and the introduction of improvement to the ABC system. It is RECOMMENDED that the following details of the facial verification process are part of a data entry:
- Overall result of the face capture and verification process.
- Error messages from the face capture unit and the verification unit.
- Time effort for the biometric verification process.
- Delays resulting from the traveller behaviour (time effort from the start of the capture process until the first successfully captured image is provided to the verification unit).
- Amount of single verification events within the verification process.
- The threshold against which the verification scores were compared.
(h) For segregated two-step process systems in which access tokens are used, the following data SHOULD be part of an entry:
- If a physical token is issued, its serial number or any other identifier the token may carry.
- If a biometric token is used, the quality of the enrollment sample captured at the verification module (e.g. number of minutiae captured for a fingerprint).
- Total time invested in token generation or capture at the verification module.
- If a biometric token is used, the quality of the live sample captured at the access module (e.g. number of minutiae captured for a fingerprint).
- Total time invested in token reading/capture and authentication/verification at the access module
- Overall result of token reading/capture and authentication/verification at the access module.

Table 6.4: Samples of the ABC deployment categories and features, which, if publicly available, may support the development of cyber and terrorist attacks (from [10]).

| **ABC deployment sensitive data** | **Potential value for attack development** |
|---|---|
| 1. Details of iris, face, and fingerprint verification/identification algorithms | **Highly sensitive data**; its availability may lead to the template changes, or intervention at the decision- making level |
| 2. Authentication mode (1 to 1 or 1 to N) and details | Searching mechanism and databases |
| 3. Technical details of the e-passport/ID readers | **Highly sensitive data**; it can be compromised by using RFID-based attacks |
| 4. Machine decision making using fixed or variable thresholds for different people/location | **Highly sensitive data**; it may provoke a threshold- level changing attack |
| 5. Human intervention/interaction style | **Highly sensitive data**; may be a subject of an attacks on human-machine interfaces |
| 6. System procedure such as N e-gates per monitoring/supervision station | Logistics attack |
| 7. Supporting/additional technological components such as video cameras, sensors, etc. | **Highly sensitive data**; it provides critical information for developing an attack on sensors |
| 8. System developer/provider, biometric matching provider | Possibility of launching the integration software and hardware Trojans |
| 9. Security design model | Provide information on vulnerable points of the ABC machine which can be used for planning and implementation of attacks |
| 10. Mechanism processing location and infrastructure | Information on principles of storing information, types of databases and their location, distribution of processing platform in overall infrastructure is critical for attack planning |
| 11. Mechanism for maintenance | Trojan software and hardware components can be injected into the ABC machine and supporting infrastructure at any phase of maintenance |
| 12. User training requirements | Knowledge on qualification level of the ABC machine operator/staff is critical for attack planning and its realization |
| 13. Vendor assessment | Software and hardware Trojans can be integrated into a system by a vendor or contractors |
| 14. Performance tests | Any attack can be camouflaged as a performance test |

# Chapter 7

# Future outlook

This study is dedicated to the analysis of risk and trends in the development of Biometric-enabled Automated Border Control technology. This technology, referred throughout the study simply as ABC is established as the main and final top-level component (Component #V) of the e-border, which is the border crossing infrastructure to enable automated clearance of travellers at the border.

Other key e-border technology components include: AVATAR-like automated behavior screening technologies (Component #III), the proof-of-concept testing of which was done by DHS and Frontex, and APC/ABC self-service kiosks (Component #IV) , which have been deployed in three Canadian airports and are increasingly deployed in many US airports. The analysis of the potential developments of these technologies has been provided.

It has been noted that Automated Border Clearance (ABC) kiosks used in Canadian Airports should not be called ABC technology in the strict definition of ABC, because they do not perform authentication of travellers. They however play a critical role in the expansion of e-border infrastructure, as they provide the base for performing further automation at the border, including automation of traveller risk assessment via dialogs and behavior monitoring (Component #IV) and traveller authentication via biometrics, thus becoming a ABC machine (Component #V).

## 7.1 Impact areas

In the following, we define a number of areas, which we believe will impact significantly the future of the border crossing automation development.

### 7.1.1 Analysis of human factors and ergonomic issues

Efficiency of ABC technologies depends on the traveller's factors such as age, ethnicity, gender, skill level, and disabilities. There are many reasons why, for a given person, it may be very difficult to cooperate with an ABC machine. Such a person may repeatedly fail to identity the verification check points, or fail when using the human-machine interface. The resulting errors mean that this traveller will be directed to the manual control. Some of these reasons can be immediately identified, for example, physical disabilities. Other disabilities may be less obvious, such as memory or learning difficulties, degrees of autism, personality disorders, and other psychological effects. Designers of ABC systems should identify these human limitations, address possible scenarios of interface between the user and the system, and take into account human factors and ergonomic issues. Human-machine and machine-human interfaces in the ABC system must be user-friendly, that is, operate using simple and easy to remember commands, have simple error messages, direct and not cluttered with computer jargon. These interfaces must be supported by intelligent tools. The physical and cognitive constraints associated with visual perception must be well understood in the design of the automated border

crossing systems. Conducting subject-based analysis of ABC system will be important to ensure that systems work well with the entire population of travellers [4] and the percentage of ABC technology non-users is minimized.

### 7.1.2 Automated risk assessment of travellers

Automated clearance of travellers by the ABC system (i.e. the decision to allow or reject a traveller the entry to a country) requires not only automated authentication of travellers, but also automated risk assessment of the travellers, using all information gathered about the travellers from the entire Air Traveller Continuum (Figure 1.3). At the moment, most of the decisions related to assigning a traveller a risk factor are based on the information obtained at the pre-screening stage based on the historical data associated with the name or country of origin of the traveller. Improvement and automation of risk assessment of travellers at the pre-screening stage is reported to be of critical importance by Frontex [41], who has been actively working in this area. Making use of the new pieces of information, as they become available about the traveller during his/her travel, is seen as the next step in this direction.

### 7.1.3 Development of automated interview supporting and bevahiour screening systems

Key decisions related to the admissibility of a traveller to a country are made at the port of entry through the interviewing and behaviour/response observation process. As highlighted in Section 5.3, AVATAR-like automated interview supporting and bevahiour screening systems have high potential to significantly improve this process. They are also scalable and can be naturally integrated into existing travel process flow as part of the next-generation ABC kiosk. The development of the roadmap for integrating such system into the border context is recommended. Through a partnership with US BORDERS consortium and Frontex who provide support for the development of this technology, and based on the research foundation established by this study, the CBSA has high potential to further explore this technology and move it to the operational environment as part of its larger border modernization efforts.

### 7.1.4 Development of tools for training of ABC machine personnel

Training of the ABC machine personnel should be semi-automatic, periodic, intensive, as well as short-term and focusing on decision-making in cases of critical scenarios. Extension of the ABC machine function for training its personnel using the same platform, and not a special training simulator facility, will become a long-term high priority goal for developers of the new generation of ABC machines. International standards and guidelines, addressing the training of the ABC machine personnel, should be developed; currently, none exist. In the training methodology, the effect of automation bias or over-relying on the machine abilities should be the crucial point. This is because the underestimation of the importance of border officer/operator training may lead to inappropriate use of border crossing automation.

### 7.1.5 Development of tools for prediction and mitigation of system risks

The framework for developing risk prediction and mitigation strategies for ABC consists of tools and metrics for both quantitative and qualitative prediction of risks. This includes establishing tools for quantitative prediction (such as belief networks). This also includes establishing criteria/categories for qualitative prediction. The operational risks of deploying the ABC machine should be assessed by taking into account both controllable and uncontrollable factors. It includes unpredictable non-technical factors, such as the possibility of cyber-attacks, terrorism threats, and epidemics; as well as predictable technical factors, such as errors, failures, and faults.

Based on the IATA and ICAO roadmap, it is anticipated that the complexity of the ABC machines of the next generation will grow near exponentially. This means that the vulnerability will expand accordingly. Therefore, the strategic goal is to mitigate these threats by developing the corresponding countermeasures to various potential attacks. Because the ABC machines represent a new type of specific-purpose complex systems, innovative approaches to defend these systems from attacks are also required, such as those based on new modeling and simulation techniques. The work by Frontex [40] and University of Calgary [8] provide valuable insights on how modeling and simulation for ABC can be done. Additionally, the work of Palmer [230] is valuable for establishing ABC deployment scenario represented using a combination of various categories.

### 7.1.6 Development of new standards for ABC

Several standards exist to support various ABC components and its supporting border technologies, however there is no standard developed yet for the entire ABC process.In the absence of such a standard, the guidelines developed by Frontex provide the key source of information for stakeholders and decision-makers for this field at the moment. In 2009 the work on developing guidelines for ABC has also started by the ISO SC 37 "Biometrics" working group under the title 'Traveller Processes for Biometric Recognition in Automated Border Control Systems". At the time of conducting this study, this ISO work however has not been finished, showing inconsistency and incompleteness of the terminology and examples. To address the gap, substantial effort of this study has been put into helping the scientific community to establish such standards. Appendix C presents three packages of standards proposed for the purpose: first – related to generic complex system, second – related to specific-purpose systems based on biometric technologies, and third – related to the complete life-cycle of the biometrics-enabled ABC systems.

### 7.1.7 Development of privacy preserving biometrically secured electronic documents

Applications need to be developed to secure electronic travel authorizations documents, such as ePassports and eIDs. Rather than traditional biometrics, privacy enhancing techniques are used to derive references from the biometrics so that no biometric information must be stored by the application. Biometric-based privacy-preserving encryption techniques such as those developed by Bissessar [139, 140] open the way to developing a new set of technologies that provide maximum protection of travel authority documents used in automated border control. Further areas of work include development mobile passports (m-passports) and Smartphone security.

### 7.1.8 Development of tools for video-surveillance data mining and real-time alerting in airports

Video cameras installed in airport provide in many cases the most critical piece of evidence related to travellers passing though the airport. A number of video recognition technologies capable of extracting the information related to recognition of people and their activities in airport through video analytics and biometrics have been identified in [135, 137, 138], specifically those that can be deployed in PIL, corridors, and luggage area (Figure 1.2). The solutions such as those described in [134] will provide the basis for the development of a powerful suite of tools for border officers in airports to collect the evidence about travellers at all stages (zones) of the *air traveller continuum*, the schematics of which is developed in this study (Figure 1.3).

## 7.2 Final recommendations

To conclude the study, the University of Calgary researchers highlight two key types of risks in border crossing automation, both potentially leading to critical mistakes in management, planning, and vision of the ABC technologies.

- Type I risks: Risks of over-simplification of the e-border concept. Any simplification of the concept of e-border leads to misunderstanding, loss of horizon, and incorrect or wrong short-term and long-term decisions. For example,
  - The common mistake is to consider the ABC machine exclusively as a biometric system that has its specific properties and vulnerability. Social embedding of the ABC machines radically differs from social factors of biometric systems.
  - It is also incorrect to consider the border crossing automation exclusively only from a management point of view. The border crossing systems are being built on the frontiers of science and technology, and must be regarded accordingly.
- Type II risks: Risks of over-relying on the abilities of the automated border control (ABC) machines. Over-relying on the machine abilities (known as automation bias) leads to dangerous decisions regarding delegation of border officer duties to the machine. For example,
  - Implementation of a one-step automated clearance of travellers in the ABC machine, which does not allow border officers or other e-border components to rectify or improve the information about a traveller, is critically risky for border security policy.
  - Underestimation of the importance of border officer/operator training may lead to inappropriate use of border crossing automation. The latter shall only be used as an aid to the border personnel duties and functions.

In order to address these two types of risks regarding border crossing automation, further analysis and development of tools need to be done, in partnership with stakeholders, policy-makers, ABC technology developers, as well as ABC end-users (general public). The results presented in this report may serve as a foundation for this effort.

**Critical Observation**

*The final recommendation of the ART in ABC study is to base any border automation deployment decision on the expertise of a professional team that has the knowledge of art in all areas identified in this study to be able to provide the qualified research support for the increasingly growing field of ABC.*

# Appendix A

# References and additional resources

This part of the report presents an overview of main events, online resources and projects dedicated to ABC, including a list of key publications from related EU-funded projects, followed by the bibliography categorized by the subjects discussed in the report.

## A.1 Events dedicated to ABC

- European Association for Biometrics Research Projects Conference (EAB-RPC), Fraunhofer IGD, Darmstadt, Germany, 7-8 September, 2015. http://eab.org/events
- Global Conference on the Future of Border Checks, Warsaw, Poland, 17-18 June 2015. http://btn.frontex.europa.eu/events/global-conference-future-border-checks-2015.
- 2nd Global Conference and Exhibition on Future Developments of Automated Border Control (ABC), October 2013: http://frontex.europa.eu/assets/Images_News/ABC_Conference_Report.pdf
- Frontex ABC Workshops and Working Group meetings. http://btn.frontex.europa.eu/search/node/ABC
- Workshop on Border Security Standardisation - Automated Border Control: Shaping the European Standardisation Roadmap, 4 - 5 April 2013, Warsaw, Poland, http://www.nen.nl/Evenementen/M487-Border-security.htm.
- ICAO Ninth Symposium and Exhibition on MRTDs, Biometrics and Border Security, Montreal, 2013, http://www.icao.int/Meetings/mrtd-symposium-2013/Pages/(ppt).s.aspx.
- NIST International Biometric Performance Testing Conference, Special track on ABC, April 1-3 http://www.nist.gov/itl/iad/ig/ibpc2014.cfm.
- Global Identity Summit, formely Biometric Consortium Conference, Tampa, Florida, September 16 - 18, 2014, http://www.biometrics.org.
- Smart Borders 2014, 24 - 25 June, 2014, One Whitehall Place, London, UK, http://smartborders.wbresearch.com.

### A.1.1 Online resources for news

- http://www.biometricupdate.com/tag/kiosk, http://www.biometricupdate.com/tag/e-gate, http://www.biometricupdate.com/tag/border-control, http://www.biometricupdate.com/biometric-news/border-security
- http://www.futuretravelexperience.com/tag/automated-border-control/, http://www.futuretravelexperience.com/tag/kiosks/, http://www.futuretravelexperience.com/tag/e-gates/
- http://www.skyscrapercity.com/showthread.php?t=1654278

### A.1.2 Selected presentations

ICAO Ninth Symposium and Exhibition on Machine Readable Travel Documents (MRTDs), Biometrics and Border Security, 22-24 October 2013, Montreal. Online at http://www.icao.int/Meetings/mrtd-symposium-2013/Pages/Presentations.aspx:

- A Regional Perspective: the On-going Work of Frontex on ABCs in Europe, Maria Duro Mansilla, FRONTEX
- FastPass: A Harmonized, Modular Reference System for all Automated Border Crossing Points, Dr. Markus Clabian, AIT Austria and Claudia Schwendimann, FastPass Project, Austria
- Trusted Traveller Programmes: Experiences of Canada and the United States, Lily Ooi, Canada Border Services Agency and Kenneth Sava, U.S. Customs and Border Protection
- Integrated Border Management: Benefits and Challenges, Bert Wezenberg, Ministry of Security and Justice, the Netherlands
- Automated Border Control System - EasyGO, Petr Malovec, Directorate Alien Police Service, the Czech Republic
- Managing the Borders of Hong Kong: ABC Challenges, Solutions and Lessons Learnt, Corrado Chow, Hong Kong Immigration Department,
- Current Challenges and Opportunities in the Use of Technology at the Border Ian Niell, Border Force, United Kingdom,
- French ABC Model and Holistic Approach to Passenger Identification Hubert Gattet, French Directorate for Border Control and Jean-Francois La Manna, French Authority for Secure Documents, ANTS.

NIST International Biometric Performance Testing Conference (IPBC 2014). Online at http://www.nist.gov/itl/iad/ig/ibpc2014_presentations.cfm:

- John Campbell, New Zealand SmartGate – Using quantitative performance information to improve convenience + security,
- Arun Vemury, Biometric Technology Evaluations for Re-engineering Entry/Exit Operations in Airports,
- Markus Nuppeney, Automated Border Control - state of play and latest developments,
- Dan Bachenheimer Performance measurement in ABC and surveillance scenarios,
- Arun Vemury, DHS Biometric Technology Evaluations for Re-engineering Entry/Exit Operations in Airports.

## A.2 Research groups working in ABC

- European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union - Frontex, http://frontex.europa.eu/. Also, Border TechNet portal http://btn.frontex.europa.eu
- BORDERS: DHS Center of Excellence in Border Security and Immigration - http://www.borders.arizona.edu.
- CITeR: Center for Identification Technology Research - http://clarkson.edu/citer.
- STRaDe - Security Technologies and Development Lab, Department of Intelligent Systems, Faculty of IT, Brno University of Technology, Czech Republic, http://strade.fit.vutbr.cz/index.php?act=45&lang_id=2.
- NISlab, The Norwegian Biometrics Laboratory, http://www.nislab.no/biometrics_lab.
- Image and Information Engineering Group, School of Engineering and Digital Arts, The University of Kent, UK, http://www.eda.kent.ac.uk/research/res_image_processing.aspx.
- International Center for Biometric Research, West Lafayette, Indiana, https://tech.purdue.edu/international-center-for-biometric-research.
- International Centre for Migration Policy Development (ICMPD), Austria, http://research.icmpd.org/2398.html.

- Research groups working in information acquisition and fusion, intelligence-based risk assessment, threat classification and vulnerability assessment
  - Biometric Recognition Group at Universidad Autonoma de Madrid http://atvs.ii.uam.es
  - Swedish Defence Research Agency (FOI): http://www.foi.se/en
  - Intelligent Behaviour Understanding Group (iBUG), Department of Computing, Imperial College London: http://ibug.doc.ic.ac.uk/home
  - Austrian Institute of Technology: http://www.ait.ac.at/departments/safety-security

## A.3 Projects funded by the European Commission

This section lists the publications and key results from projects dedicated to border transformation and modernization that are funded by the European Commission under the Seventh Framework Programme. The papers that have been found particularly useful for the "ART in ABC" study are marked with (*).

Additionally, a portal page has been set to monitor the international research and development efforts related to Automated Border Control, Biometrics and Video Analytics: https://sites.google.com/site/vistercanada/international-projects, which provides additional details on each of the listed projects.

### A.3.1 ABC4EU: Automated Border Control Gates for Europe

News-letters and press released are available on-line from http://abc4eu.com/project-publications

### A.3.2 FastPass: a harmonized, modular reference system for all European automated border crossing points

**Selected publications** (available online from https://www.fastpass-project.eu/dissemination):

Testing the Document Readers to the limit, Franz Daubner, Frontex Workshop on vulnerabilities, 2014/11/21, Warsaw, Poland.

Towards Anomaly Detection for Increased Security in Multi-biometric Systems: Spoofing-resistant 1-Median Fusion Eliminating Outliers, Peter Wild, Petru Radu, Lulu Chen, James Ferryman, International Joint Conference on Biometrics (IJCB 2014), 2014/9/30, Clearwater, Florida, US.

* Understanding the factors affecting user experience (UX) and technology acceptance in ABC context, Mari Ylikauppila, Sirra Toivonen, Minna Kulju IEEE Joint Intelligence and Security Informatics Conference (JISIC), 2014 2014/9/24, The Hague, Netherlands.

Optical Security Document Simulator for Black-Box Testing of ABC Systems, Michael Gschwandtner, Svorad Stolc, Franz Daubner, IEEE Joint Intelligence and Security Informatics Conference (JISIC), 2014 2014/9/24, The Hague, Netherlands.

* Multi-Criteria Evaluation for Automated Border Control, Gunther Grasemann, Future Security Conference, 2014/9/16 Berlin, Germany.

* Non-use of Automated Border Control Systems: Identifying Reasons and Solutions, Anne-Marie Oostveen, The 28th British HCI Conference, 2014/9/09, Southport, UK.

* Automated Border Control: a comparative usability study at two European airports, A.M. Oostveen, E. Krempel, M. Kaufmann, G. Grasemann, IHCI, 2014/07/15.

Security Evaluation of ABC Systems, Gunter Schumacher, EAB - Research Projects Conference (EAB-RPC), 2014 2014/9/08 Darmstadt, Germany (ppt).

Stakeholders and Requirements of ABC, Sirra Toivonen, Erik Krempel, Gunther Grasemann, EAB- Research Projects Conference (EAB-RPC), 2014 2014/9/08, Darmstadt, Germany (ppt).

Monitoring as a service for ABC, Andreas Kriechbaum-Zabini, EAB- Research Projects Conference (EAB-RPC), 2014 2014/9/08 Darmstadt, Germany.

* Smart Borders: Comparing the Use of New Technology in Border Controls in the US and the EU, Maegan Hendow, American Geographers Annual Meeting, 2014/04/08, Tampa, Florida (ppt).

FastPass: European usage of eMRTDs for ABC, Markus Clabian, ICAO MRTD Report Vol.9 No 1 2014, pp 28-29 2014/04/30, Online article.

Key Technologies for Enhancing Security and User Statisfaction at Airports, M. Kommenda, A. Kriechbaum, B. Micusik, C. Beleznai, M. Rauter, R. Pflugfelder, 8th Future Security Conference, 2013 2013/09/17, Berlin.

* Towards User Requirements For Harmonised Automated Border Control Gates, L. Salmela, T. Ahonen, C. Beleznai, R. Knapik, C. Bier, W. Wojciechowicz and S. Toivonen, 8th Future Security Conference, 2013 2013/09/18, Berlin.

Document security in the age of fully automated border control system, A. Kriechbaum; Authors: S. Stolc; M. Gschwandtner, 2nd Global Conference and exhibition on future developments of ABC, 2013/10/10, Warsaw.

Visual surveillance technologies for enhancing ABC secure zones, S. Veigl et al. 2nd Global Conference and exhibition on future developments of ABC, 2013/10/10, Warsaw.

Dependability Management in Automated Border Control, Toni Ahonen, Laura Salmela, 2nd Global Conference and exhibition on future developments of ABC, 2013/10/10 Warsaw.

Biometrics in ABC: counter-spoofing research. H. Wei, L.Chen, J.Ferryman, 2nd Global Conference and exhibition on future developments of ABC, 2013/10/10, Warsaw.

A harmonized, modular reference system for all European automatic border crossing points Markus Clabian (AIT), Frontex Event, 2012/10/24, Warsaw (ppt).

Automated Border Control - What about standards? Chris Hurrey (Intrepid Minds) Frontex ABC working group 2013/02/27 Helsinki Power Point (ppt).

### A.3.3 BEAT: Biometrics Evaluation and Testing

**Selected publications** (available online from https://www.beat-eu.org/publications/index.php/publications):

Nils Tekampe, (ppt). Attack Detection: Towards a structured approach for tailored metrics, 2014.

Javier Galbally and Sebastien Marcel, Face Anti-Spoofing Based on General Image Quality Assessment, 2014.

Sebastien Marcel and Nesli Erdogmus, Spoofing Face Recognition with 3D Masks (2014), in: IEEE Transactions on Information Forensics and Security, 2014.

Norman Poh and Ajita Rattani, Biometric System Design Under Zero and Non-Zero-Effort Attacks, 2013.

* Jose Mario de Martino, Sebastien Marcel, AndrÃľ Anjos Rabello and Tiago de Freitas Pereira, Can face anti-spoofing countermeasures work in a real world scenario?, in: International Conference on Biometrics, Madrid, Spain, 2013.

* Sebastien Marcel, Matti Pietikainen, Abdenour Hadid, Jukka Komulainen and Andre Anjos Rabello, Complementary Countermeasures for Detecting Scenic Face Spoofing Attacks, in: International Conference on Biometrics, Madrid, Spain, 2013

Marta Gomez-Barrero, Javier Galbally and Julian Fierrez, Efficient software attack to multimodal biometric systems and its application to face and iris fusion (2013), in: Elsevier

Javier Galbally, Marta Gomez-Barrero, Arun Ross, Julian Fierrez and Javier Ortega-Garcia, Securing iris recognition systems against masquerade attacks, SPIE Defense, Security, and Sensing, 2013

Norman Poh, Josef Kittler and Fuad Alkoot, A discriminative parametric approach to video-based score-level fusion for biometric authentication, in: Pattern Recognition (ICPR), 2012 21st International Conference on, Tsukuba, pages 2335-2338, 2012

* Norman Poh and Josef Kittler, A Unified Framework for Biometric Expert Fusion Incorporating Quality Measures (2012), in: IEEE Trans. on Pattern Analysis and Machine Intelligence, 34:1(3-18)

* Norman Poh, Arun Ross and Ajita Rattani, Analysis of User-specific Score Characteristics for Spoof Biometric Attacks, in: CVPR Workshops'12, pages 124-129, 2012.

Javier Galbally, Arun Ross, Marta Gomez-Barrero, Julian Fierrez and Javier Ortega-Garcia, From the Iriscode to the Iris: A New Vulnerability of Iris Recognition Systems, Las Vegas, 2012.

Els Kindt, The Processing of Biometric Data. A comparative legal analysis with a focus on the proportionality principle and recommendations for a legal framework., KU Leuven, 2012.

### A.3.4 Tabula Rasa: Trusted Biometrics under Spoofing Attacks

**Selected publications** (available online from http://www.tabularasa-euproject.org/publications):

Can face anti-spoofing countermeasures work in a real world scenario?, T. de Freitas Pereira, A. Anjos, J. M. De Martino and S. Marcel, in: International Conference on Biometrics, 2013.

Complementary Countermeasures for Detecting Scenic Face Spoofing Attacks, J. Komulainen, A. Hadid, M. PietikAinen, A. Anjos and S. Marcel, in: International Conference on Biometrics, 2013.

**Demonstrations:** Various demonstration systems have been developed to show the vulnerability of biometric systems (face recognition, voice recognition, fingerprint recognition, iris recognition, vascular recognition) to spoofing attacks and to show the efficiency of developed counter-measures to these attacks. Some demonstrations that available at the TABULA RASA YouTube channel: http://www.youtube.com/channel/UCoHA9lGDrtEUim_mdtPwQ6w.

**Evaluations (TABULA RASA Spoofing Challenge 2013)**: In 2013, Tabula Rasa Spoofing Challenge invited researchers to develop ingenious attack plans and to deceive various biometric authentications systems of different modalities. With large participation of researchers, visitors and contestants, the challenge has successfully raised awareness about spoofing vulnerabilities of biometric systems and additionally, it has given way to many different and creative ways to attack the systems. In total, 9 attacks participated in the challenge - 6 in face verification (both Vis and NIR) and 3 in fingerprint verification. The Best Award attack was given a person who used make-up to look like one of the enrolled subjects to spoof the 2D face recognition system in visible spectra. She succeeded to be recognized as her victim, and additionally, due to the intrinsic nature of the attack, she could easily bypass the liveness detection that was implemented in the system.

### A.3.5 Literature categorization

In the following section, the bibliography is organized by the subjects discussed in the study according to the following categorization (Table A.1).

Table A.1: Categorization of the "ART in ABC" study bibliography.

1. Publications produced by the study
   (a) Internal memoranda
   (b) Conference/journal publications and division reports
   (c) Contractor reports
2. Operations-driven publications
   (a) Overviews / Reviews
   (b) Guidelines and normative references
   (c) Border agencies publications
   (d) Media coverage
3. Publications on e-border components and supporting technology
   (a) Traveller risk assessment
   (b) Behaviour screening and interviewing technology
   (c) Queuing technology and self-service kiosks
   (d) Biometric-enabled ABC
   (e) Pre-screening technology
   (f) Other supporting technology
4. Research-driven publications
   (a) By CBSA Science and Engineering Directorate
   (b) Other government funded
   (c) By the University of Calgary's a Biometrics Lab
   (d) Biometrics fundamentals
   (e) Standards
   (f) Face recognition related
   (g) Iris recognition related
   (h) Subject-based biometrics performance analysis
   (i) Research tools
      i. Modeling / Simulation tools
      ii. Statistical
      iii. Other

# Bibliography


## [1] Publications produced by the study: a) Memoranda

"Science and Engineering for AIR Modernization", CBSA-S&E Memorandum DG-2015-02-21. — Outlines the areas of Science and Engineering work that can be done for Air Travel Modernization projects.

"Facial Recognition performance for biometric-enabled kiosks", CBSA-S&E Memorandum DG-2015-01-27. — Provides overview and recommendations on the commercial face recognition algorithms that can be deployed for biometrics-enabled kiosks.

"Use of iris by 2020", CBSA-S&E Memorandum DG-2015-02-24. – Overviews advantages of iris over other biometric modalities to suggest its growing use as part of a multi-model ABC system of the future.

"The evolution of Biometrics: from authentication to risk assessment applications", CBSA-S&E Memorandum DG-2015-01-16 — Provides the overview and justification for the non-ISO compliant use of the terms "biometric", "biometric technology", "biometric-enabled border control".

"Feedback on Strategic Risk Brief: Biometrics", CBSA-S&E Memorandum DG-2015-03-17 — Lists considerations that need to be taken into account when deploying biometric solutions for automated border control, highlights the difference between the systems that are used for limited population of pre-cleared travellers and those that are used for every traveller carrying an e-Passport.

"Simulation tools for eBorder", CBSA-S&E Memorandum DG-2015-03-27 — Overviews three commercial software packages available on the market for performing the simulation of ABC / eBorder solutions: Arena, Simio and ExtendSim, and outlines the operational research tool based on the latter developed by Frontex for cost-benefit analysis of e-gates in EU.

"AVATAR-like traveller clearance systems at the border: backgrounder and prognosis", CBSA-S&E Memorandum DG-2015-03-30 — Provides the background and prognosis on the development and deployment of automated interview supporting risk assessment tools such as those developed by the University of Arizona.

## b) Conference/journal publications, division reports

[2] D. Gorodnichy, S. Eastwood, V. Shmerko, S. Yanushkevich, *"Automated Border Control systems as part of eBorder crossing process".* Proceedings of the NIST International Biometrics Performance Conference (IBPC 2014), Gaithersburg, MD, April 1-4, 2014 (CBSA Border Technology Divisio Report 2014-09). Online at www.nist.gov/itl/iad/ig/ibpc2014_presentations.cfm

*Abstract*: The analysis of the automated border control (ABC) technologies deployed and piloted over the last two decades is presented. This analysis becomes the basis for the development of the formalized description of an ABC system as a part of a larger eBorder traveller clearing process which deals with granting or denying an entry of a traveller to a country.

[3] D. Gorodnichy, V. Shmerko, S. Yanushkevich *"Automated Border Control: Problem Formalization"*. Proceedings of 2014 IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM 2014), December 9-12, 2014, Orlando, USA (Extended version with poster: CBSA Border Technology Division Report 2014-41)

*Abstract:* This paper introduces a formalization of the Automated Border Control (ABC) machines deployed worldwide as part of the eBorder infrastructure for automated traveller clearance. Proposed formalization includes classification of the eBorder technologies, definition of the basic components of the ABC machines, identification of their key properties, establishment of metrics for their evaluation and comparison, as well as development of a dedicated architecture based on the assistant-based concept. Specifically, three generations of the ABC machines are identified: Gen-1 ABC machines which are biometric enabled kiosks, such as Canada's NEXUS or UK IRIS, to process low-risk pre-enrolled travellers; Gen-2 ABC machines which are eGate systems to serve travellers with biometric eID / ePassports; and Gen-3 ABC machines that will be working to support the eBorder process of the future. These ABC machines are compared in this paper based on certain criteria, such as availability of the dedicated architectural components, and in terms of the life-cycle performance metrics. This paper addresses the related problems of deployment and evaluation of the ABC technologies and machines, including the vulnerability analysis and strategic planning of the eBorder infrastructure.

[4] D. Gorodnichy and M. Chumakov, *" Subject-based performance analysis of Nexus iris recognition system"*, CBSA S&E Division Report, in preparation.

*Abstract:* For agencies deploying biometric-enabled automated border control systems such as e-gates and biometric kiosks it is critical to know how well the systems performs over the entire population of travellers. – Travellers who are efficiently processed by the system will keep gladly using it, while travellers experiencing the problems will be trying to avoid using it next time and will have lower level of satisfaction with border services. This is why conducting subject-based system performance analysis, which examines the variation of system performance among the subjects (travellers), is highly recommended. This report presents the results of the subject-based performance analysis of the Nexus iris recognition system obtained using the historical data gathered by CBSA from 2004 till 2014. The percentage of travellers who consistently experienced the problem with the system (expressed in high dissimilarity score and high average number of attempts) is shown to be much higher for those travellers who used the system only a few times, compared to those who used it many times. Two hypothesis are examined: 1) the "biometric menagerie" phenomenon – that there exists a class of users who are intrinsically hard to recognize and who, as result, stop using the system, and 2) the "habituation phenomenon" – that the performance improves as users become more experienced with the system. Other factors influencing iris recognition performance are also investigated. Recommendations for future work to improve the performance of Nexus and future biometric kiosks, based on the results obtained, are presented.

[5] D. O. Gorodnichy, *" New age glossary of biometric terms: focus on automated border control and video surveillance applications. "*, CBSA S&E Border Technology Division Report, in preparation.

*Abstract:* New applications demand for the revision and extension of the existing terminology. This is becoming the case with biometrics – the technology for automated recognition of people from their biological characteristics. Originally applied to such applications as membership programs, physical security, forensics, where the number of processed subjects is known or limited, the use of biometrics is now increasingly extended towards applications, such as automated border control and video surveillance, where the flow of processed subjects is very high and subjects themselves are not known in advance to the system, thus resulting in a much higher chance of intentionally or unintentionally attacking system vulnerabilities. The outcome of the several years of work on DRDC-funded *PROVE-IT(FRiV)* and *"ART in ABC"* studies conducted by the CBSA in partnership with several academic, government and industry partners, this report presents the list of the new and revised biometric terms recommended for automated border control and video surveillance applications.

[6] D. O. Gorodnichy, V. P. Shmerko, S. N. Yanushkevich, *"Taxonomy of Deployment Scenarios of Automated Border Control Machines"*, CBSA S&E Border Technology Division Report 2015-14.

*Abstract:* In this paper, we consider deployment scenarios of the Automated Border Control (ABC) machines which aim at supporting the border crossing procedure. This support became possible due to the progress in biometrics, sensoring technologies, information gathering and classification, and other breakthrough achievements. Because of high complexity, the ABC machine deployment scenarios should be described in appropriate metric. In this paper, we propound a 3D projection of the ABC classification: in architectural, performance, and deployment categorization domains. The latter is the focus of this paper. We revisit a categorical description of the generalized authentication machines developed by A. J. Palmer (Criteria to evaluate automated personal identification mechanism, Computers and Security, vol. 27, 2008), and propose a four-step ABC design strategy based on it. We apply this approach to the analysis of the ABC machines deployed worldwide.

[7] S. C. Eastwood, V. P. Shmerko, S. N. Yanushkevich, M. Drahansky, and D. O. Gorodnichy, ''*Biometric-Enabled Authentication Machines: A Survey of Open-Set Real-World Applications"*, IEEE Transactions on Human-Machine Systems, 2015 (CBSA S&E Border Technology Division Report 2015-15).

*Abstract:* This paper revisits the concept of an Authentication machine (A-machine) that aims at identifying/verifying humans. Although A-machines in the closed-set application scenario are well understood and commonly used for access control utilizing human biometrics (face, iris, and fingerprints), open-set applications of A-machines have yet to be equally characterized. This paper presents an analysis and taxonomy of A-machines, trends, and challenges of open-set real-world applications. This paper makes the following contributions to the area of open-set A-machines: i) a survey of applications; ii) new novel life-cycle metrics for theoretical, predicted, and operational performance evaluation; iii) a new concept of evidence accumulation for risk assessment; iv) new criteria for the comparison of A-machines based on the notion of a supporting assistant; and v) a new approach to border personnel training based on the A-machine training mode. It offers a technique for modeling A-machines using belief (Bayesian) networks, and provides an example of this technique for biometric-based e-profiling.

[8] S. Eastwood, V. Shmerko, S. Yanushkevich, D.Gorodnichy *"Risk-based performance evaluation of Automated Border Control systems"*, CBSA S&E Border Technology Division Report 2015-16.

*Abstract:* Compared to access control systems, Automated Border Control (ABC) systems have many more technological components, operational tasks, and are used by a significantly larger population of people, many of whom are not habituated with the systems and have other travel-related stresses to deal with while operating these systems. The performance of ABC systems may no longer be evaluated simply by using biometric recognition metrics (such as false/true reject/accept rates, DET/ROC curves etc) as done for access control systems, but rather should be evaluated in a holistic manner, which takes into account its all components and associated risks.This paper introduces a probabilistic inference based methodology and tool, called ABC Profiler, which allows to do that. Based on a belief network designed with a library of predefined modeling modules, ABC Profiler performs assessment of the risks of any state of the ABC system. The application of the new methodology is demonstrated using a real operational scenario, in which a biometric-enabled document and its owner are authenticated with a certain degree of reliability. The obtained results are shown to provide valuable insights which can be used in designing and monitoring such systems.

## c) Contractor reports

[9] S. Yanushkevich, V. Shmerko, S. Eastwood, "Automated Border Control. Part I: Overview, Trends and Challenges", CBSA Contract report, University of Calgary, March 2015.

*Abstract:* The purpose of Technical Report (Part I TR) is to provide analysis of the state-of-the-art Automated Border Control (ABC) machines and supporting technologies deployed worldwide. This Report is a

continuation and extension of a previous work in border crossing automation, such as the ICAO, IATA, DHS, and Frontex reports. Our aims according to the Contract tasks of Defense R&D Canada and Canada Border Service Agency, (CBSA) are as follows: (a) to update and extend the terminology in the ABC area, (b) to represent a systematic view of ABC landscape, (c) to improve understanding of the contemporary ABC machines and supporting technologies, (d) to help in analysis and classification of eBorders components, and (e) to provide challenges and a horizon of the ABC technologies. This Report can be useful for practitioners of Border Service Agencies internationally and CBSA, in particular, as well as other Government Institutions responsible for national security strategic planning. The results of this Report are also pertinent to developers of biometric-enabled machines and the biometric industry.

[10] Yanushkevich, V. Shmerko, S. Eastwood, "Automated Border Control. Part II: Guide for Deployment", CBSA Contract report, University of Calgary, March 2015.

*Abstract:* This is the second part of the Technical Report (TR) on the results of the research conducted in the Biometric Technology Laboratory at the University of Calgary in 2013-2015 through the Contract Risk analysis of face and iris biometrics in automated border/access control applications (CSSP- 2013-CP-1020). This Part-II TR is a critical call that addresses the following problems of border crossing automation: 1. Risks of over-simplification of the eBorder concept, and 2. Risks of over-relying on the abilities of the automated border control (ABC) machines. Both types of risks can lead to critical mistakes in management, planning, and vision of the ABC technologies. Our call is motivated by the two reasons: (a) the growing complexity of the ABC technologies, and (b) their vulnerability. To achieve this goal, we suggest a categorical language that is common for all professionals involved in the ABC automation. Based on this, we introduce various classifications of the eBorder machines, their deployment, vulnerability, personnel training, and standardization. This Report is intended for practitioners of Border Service Agencies internationally and CBSA, in particular, as well as other Government Institutions responsible for national security strategic planning. The results of this Report are also pertinent to developers of biometric-enabled machines and the biometric industry.

# Operations-driven publications

## a) Overviews / Reviews

[11] Acuity Market Intelligence, The Global Automated Border Control Industry Report: Airport eGates and Kiosks, http://www.acuity-mi.com/ABCair_Report.php

[12] D. Anderson, , S. E. Thompson, C. E. Wilhelm, and N. A. Wogman, Integrating Intelligence for Border Security, *J. of Homeland Security,* Jan., 2004, http://www.homelandsecurity.org

[13] B. Elias, Airport passenger screening: Background and issues for Congress, Congressional research service, 7-570, www.crs.gov, R40543, April 23, 2009. http://www.fas.org/sgp/crs/homesec/R40543.pdf

[14] European Commission. 'Smart borders': enhancing mobility and security. IP/13/162 Feb. 28, 2013; http://europa.eu/rapid/press-release_IP-13-162_en.htm

[15] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm

[16] D. Harris, How to Really Improve Airport Security, *Ergonomics in Design*, Winter, 2002, pp. 1–6. https://www.hfes.org/web/Newsroom/Improve_Airport_Security.pdf

[17] J. Kephart, "Biometric Exit Tracking: A feasible and cost-effective solution for foreign visitors traveling by air and sea", *Center for Immigration Studies*, 2013. http://cis.org/biometric-exit-tracking-feasible-and-cost-effective

[18] J. Kephart, "Implementation on an entry-exit system: still waiting after all these years", Testimony before the House Judiciary Committee, November 13, 2013. http://judiciary.house.gov/_files/hearings/113th/11132013/Kephart%20Testimony.pdf.

## b) Guidelines and normative references


[19] Biometrics for Airport Access Control Guidance Package. Version release Sept. 30, 2005, https://www.acconline.org/documents/biometrics_guidance.pdf

[20] CEPS (Centre for European Policy Studie): "Justice and Home Affairs Databases and a Smart Borders System at EU External Borders An Evaluation of Current and Forthcoming Proposals," 18 Dec. 2012. http://www.ceps.eu/publications/justice-and-home-affairs-databases-and-smart-borders-system-eu-external-borders

[21] CRS (Congressional Research Service): A. Siskin, Visa Waiver Program, Congressional Research Service February 12, 2014. https://www.fas.org/sgp/crs/homesec/RL32221.pdf

[22] GAO (Government Accountability Office): Defense Biometrics. Additional Training for Leaders and More Timely Transmission of Data Could Enhance the Use of Biometrics in Afghanistan, *United States Government Accountability Office (GAO), Report to Congressional Requesters*, GAO-12-442, Washington, D.C., April 2012. http://www.gao.gov/assets/600/590311.pdf

[23] GAO: Defense Biometrics. DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies, *United States Government Accountability Office (GAO), Report to Congressional Requesters*, GAO-11-276, Washington, D.C., March 31, 2011 http://www.gao.gov/new.items/d11276.pdf

[24] IATA: Passenger Facilitation program. http://www.iata.org/whatwedo/passenger. Includes: ABC Recommended Practices RP 1701-I, ABC Implementation Guide - 1st Ed., ABC Case Studies (UK, Portugal, Canada, Indonesia). Viewed on: 14 July 2015.

[25] IATA: Simplifying the Business (StB) initiative. http://www.iata.org/whatwedo/stb

[26] IATA: Automated Border Control map. Online: http://www.iata.org/whatwedo/stb/maps/Pages/automated-border-control.aspx. Also: http://www.iata.org/whatwedo/stb/maps/Pages/passenger-facilitation.aspx. Last update: 9 September 2014

[27] IATA: Checkpoint of the future. Executive summary. 4th Proof. 2014." http://www.iata.org/whatwedo/security/Documents/cof-executive-summary.pdf (Authorization required). See also: "IATA Reveals checkpoint of the future,, Press release no. 35, June 7, 2011. Also: http://www.icao.int/MID/Documents/2011/dgca_mid1/docs/ip07_en.pdf

[28] IATA: Securing aviation's future – IATA calls for harmonization and vigilance, Press release no. 48, 2011.

[29] IATA: Security access and egress. Implementation Guide. Passenger Facilitation. First edition. 2010. http://www.iata.org/whatwedo/stb/Documents/pf-guide-security-2012.pdf

[30] IATA: Guidance on introducing Radio Frequency Identification (RFID) into airline maintenance operations International Air Transport Association safety, operations, and infrastructure, May 2013.

[31] IATA: Recommended Practice 1701 I, 2011, page 4. http://www.iata.org/whatwedo/stb/Documents/rp1701-traveler-scheme-2012.pdf

[32] ICAO 9303 "Part 1: Machine Readable Passports. Volume 2 - Specifications for Electronically Enabled Passports with Biometric Identification Capability" Section II.13. Online: http://www.icao.int/Security/mrtd/pages/Document9303.aspx.

[33] ICAO, 18th meeting of the Technical Advisory Group (TAG) on Machine Readable Travel Document (MRTD), "Update on the Application of Photo Standards in the e-MRTD Issuing Process". Online: http://www.icao.int/Meetings/TAG-MRTD/Documents/Tag-Mrtd-18/TAGMRTD.18.WP10.PhotoStandards.pdf

[34] Frontex: Futures of Borders. A Forward Study of European Border Checks, *Research and Development Unit*, Warsaw, December 2011. - http://frontex.europa.eu/assets/Publications/Research/Futures_of_Borders.pdf

[35] Frontex: Conference Report, the 2nd global conference on future developments of Automated Border Controls (ABC), Warsaw October, 2013. - http://frontex.europa.eu/assets/Images_News/ABC_Conference_Report.pdf

[36] Frontex: Best practice technical guidelines for automated border control (ABC) systems, *Research and Development Unit*, Warsaw, 2012. - http://frontex.europa.eu/assets/Publications/Research/Best_Practice_Technical_Guidelines_for_Automated_Border_Control_Systems.pdf

[37] Frontex: Operational and technical security of electronic passports, *Research and Development Unit*, Warsaw, 2011.

[38] Frontex: BIOPASS II Automated biometric border crossing systems based on electronic passports and facial recognition: RAPID and SmartGate, Warsaw, 2010.

[39] Frontex: Study on automated biometric border crossing systems for registered passenger at four European airports, Warsaw, 2007.

[40] Frontex Workshop "CBA for Automated Border Crossing Systems", ABC Operational Research Training, Sofia, April 2013.

[41] Frontex Research and Development Unit, "Risk Assessment of PAX", Internal Document, February 2015.

[42] Frontex Global Conference on the Future of Border Checks, Warsaw, Poland, on 17-18 June 2015, http://btn.frontex.europa.eu/events/global-conference-future-border-checks-2015.

[43] ICAO Document 9303, part 1, vol. 2, e-passports. Retrieved 8 Sept. 2010. http://hasbrouck.org/documents/ICAO9303-pt1-vol2.pdf

[44] ICAO (International Civil Aviation Organization): Driving technology developments and innovation: Next generation screening. High level component research roadmap. Working paper. Presented by Canada, Netherlands, UK, ACI, ICCAI, and IATA. *Proc. High-Level Conf. on Aviation Security (HLCAS-WP/26)*. Montreal, Sept, 2012. http://www.icao.int/Meetings/avsecconf/Documents/WP%2026/HLCAS.WP.26.Next%20Generation%20Screening.FINAL%20FINAL.pdf

[45] ICAO: High-level conference on aviation security (HLCAS). International Civil Aviation Organization (HLCAS-WP/26) *Working paper*, Montréal, Sept. 2012 http://www.icao.int/Meetings/avsecconf/Documents/WP%2026/HLCAS.WP.26.Next%20Generation%20Screening.FINAL%20FINAL.pdf

[46] Hawley, K. Testimony, July 24, 2008, before the United States House of representatives committee on transportation and infrastructure subcommittee on aviation. http://www.tsa.gov/press/speeches/072408_hawley_aviation_security.shtm.AccessedApril27,2009.

[47] SITA: END-to-end border management: An integrated approach to passenger data collection, identity verification and risk management. *Sociéte Internationale de Télécommunications Aéronautiques (SITA) positioning paper,* 2012, http://www.sita.aero/file/8505

[48] SITA: A unique promise: Biometrics & border management, *Air Transport IT Review,* issue 2, 2012. http://www.sita.aero/content/a-unique-promise

[49] A. M. Wolf, European ID Policy and Border Crossing, *Proc. Biometric Consortium Conf.*, 2013. http://www.biometrics.org/bc2013/presentations/int_wolf_wednesday_1400.pdf

## c) Border agencies publications

[50] ACBPS: Australian Customs and Border Protection Service 2012-2013 Annual Report. 2013:p.16. http://www.customs.gov.au/webdata/resources/files/ACBPSAnnualReport2012-13.pdf

[51] ACBPS: Australian Customs and Border Protection - Blueprint for Reform 2013-2018. 2013:1-44. http://www.customs.gov.au/webdata/resources/files/ACBPS-Blueprint-for-Reform-2013-2018.pdf.

[52] Australian Customs and Border Protection Service, SmartGate website http://www.customs.gov.au/smartgate/smartgate.asp. See also New Zealand's SmartGate: https://www.passports.govt.nz/Before-you-travel---SmartGate, http://www.customs.govt.nz/features/smartgate/Pages/default.aspx

[53] CBSA: CANPASS website. http://cbsa-asfc.gc.ca/publications/pub/bsf5017-eng.html

[54] CBSA: NEXUS website. http://www.cbsa-asfc.gc.ca/prog/nexus/menu-eng.html

[55] CBSA: Automated Border Clearance Program, http://www.cbsa-asfc.gc.ca/media/facts-faits/104-eng.html

[56] CBSA: Entry/Exit Information System Phase I Joint Canada-United States Report http://www.cbsa-asfc.gc.ca/btb-pdf/eeis-ponerep-sdes-rappun-eng.html

[57] CBSA-DHS: "Beyond the Border" Action Plan. Statement of Privacy Principles by the United States and Canada. http://www.dhs.gov/xlibrary/assets/policy/beyond-the-border-action-plan-statement-of-privacy-principles.pdf

[58] CBSA: Entry/Exit Fact Sheet Phase II. http://www.cbsa-asfc.gc.ca/btb-pdf/eefs-dies-eng.html

[59] CBSA: Border Wait Times. http://www.cbsa-asfc.gc.ca/bwt-taf/menu-eng.html, See also: http://bwt.cbp.gov/

[60] http://actionplan.gc.ca/en/content/beyond-border

[61] http://www.dhs.gov/beyond-border-shared-vision-perimeter-security-and-economic-competitiveness The CBSA is positioned to enhance the facilitation of people and goods and to enforce Canadian law at ports of entry (POEs) in the near future.

[62] http://www.cbsa-asfc.gc.ca/media/release-communique/2012/2012-04-25-eng.html

[63] CIC: International use of biometrics http://www.cic.gc.ca/english/department/biometrics-international.asp

[64] DHS (Department of Homeland Security): DHS S&T and CBP Announce the Opening of the Maryland Test Facility, 2014 http://www.dhs.gov/blog/2014/07/03, http://www.dhs.gov/st-snapshot-new-dhs-facility-tests-biometric-technology%-improves-air-entryexit-operations

[65] DHS (Department of Homeland Security): Future Attribute Screening Technology (FAST) Project, Science and Technology Directorate, 2008. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf

[66] Bureau of Transportation Statistics - United States Department of Transportation. Total Passengers on U.S Airlines and Foreign Airlines US Flights Increased 1.3% in 2012 from 2011. April 4, 2013; http://www.rita.dot.gov/bts/press_releases/bts016_13.

[67] Rodríguez A. Biometrics at the border? El Paso Inc. Sept. 29, 2013.http://www.elpasoinc.com/news/personal_finance/article_47376d98-291d-11e3-98ee-0019bb30f31a.html.

[68] German Federal Police (BundesPolizei), EasyPASS website: http://www.easypass.de/EasyPass/EN/What_is_EasyPASS/home_node.html, (See also: Germany's new ABC System EasyPASS, May 2014 Christoph Maggioni, Bundesdruckerei GmbH. http://www.easc-ev.org/files/pdf/20140522_Germanys_new_ABC_System_EasyPASS_Border_Control_Practice_final.pdf

[69] India: Unique Identification Authority (UIDAI). http://uidai.gov.in/auth.html. See also: https://en.wikipedia.org/wiki/Aadhaar

[70] UK Border Agency, Iris recognition immigration system (IRIS) Project website. http://www.ukba. homeoffice.gov.uk/managingborders/technology/iris/ (Last visited: in 14 November 2013), See also: https://en.wikipedia.org/wiki/Iris_Recognition_Immigration_System

[71] *Delivering statistical benefits from Semaphore (formally e-Borders)*, Office for National Statistics, Research Report, 2011. http://www.ons.gov.uk/ons/guide-method/method-quality/imps/latest-news/delivering-statistical-benefits-from-e-borders/index.html

[72] E-borders programme review of the code of practice on data sharing, version 1.1, 19 December 2008. http://www.ukba.homeoffice.gov.uk/sitecontent/documents/managingourborders/eborders/codeofpractice, Also: E-borders: Overview of Legislation. http://www.statewatch.org/news/2013/oct/uk-e-borders-overview-legislation.pdf

[73] Department for Transport. UK Aviation Forecasts. 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/223839/aviation-forecasts.pdf.

[74] UK Border Force. Registered Traveller Scheme. 2013; https://www.gov.uk/registered-traveller-scheme

[75] Rymer, T., E-Borders: Friends of presidency group meeting Brussels, Home Office, *Border & Immigration Agency*, 2008.

### d) Media coverage

[76] CBC NEWS: Ottawa recalls sensitive database in border project, February 16, 2009. http://www.cbc.ca/news/ottawa-recalls-sensitive-database-in-border-project-1.809365

[77] J. Best, $9 m cost of eye scanning "would have been better spent on immigration staff", *Government Computing*, April 11, 2012, http://www.theguardian.com/government-computing-network/2012/apr/11/iris-ukba-egates-eborders-report

[78] $9 million iris recognition scheme introduced to slash queues at airports is scrapped, *Mail Online*, Sept. 5, 2013, http://www.dailymail.co.uk/travel/article-2102489/Iris-recognition-scheme-airports-scrapped-years.html

[79] ICT fails entry requirements for Border Control, 2012. http://professionaloutsourcingmagazine.net/presszone/ict-fails-entry-requirements-for-border-control

[80] E. Doyle, US report casts doubt on reliable biometric systems, IT PRO, 29 Sep, 2010, http://www.itpro.co.uk/627298/us-report-casts-doubt-on-reliable-biometric-systems

## Publications on e-border components and technologies

### a) Traveller risk assessment

[81] P. Garvey, Analytical Methods for Risk Management: A System Engineering Perspectives, Chapter & Hall/CRC Taylor & Francis Group, Boca Raton, FL, 2009.

[82] L. McLay, A. J. Lee, and S. H. Jacobson. Risk-Based Policies for Airport Security Checkpoint Screening. Journal *Transportation Science*, Vol. 44 Issue 3, 2010, pp. 333–349.

[83] Frontex: Passenger Analysis Model Project: http://btn.frontex.europa.eu/projects/internal/advance-information-0

[84] J. Florence, and R. Friedman, Profiles in terror: A legal framework for the behavioral profiling paradigm, George Mason Law Review, vol. 17:2, 2010, pp. 423–481. http://www.georgemasonlawreview.org/doc/17-2_FlorenceandFriedman.pdf

[85] Future Attribute Screening Technology. http://en.wikipedia.org/wiki/Future_Attribute_Screening_Technology

[86] "ACLU sues TSA over behaviour screening program" (USA USA TODAY, March 19, 2015). http://www.usatoday.com/story/news/2015/03/19/aclu-tsa-behaviour-detection-spot/24974421

[87] Statistics Canada: http://www.statcan.gc.ca/daily-quotidien/130918/dq130918a-eng.htm. See also: http://www.cmha.ca/media/fast-facts-about-mental-illness.

[88] A. Santos, et. al., and J. Guerra, Secure access control by means of human stress detection, *Proc. IEEE Carnahan Conf. Security Technology (ICCST)*, 2011.

### b) Behaviour screening and interviewing technology

[89] P. Ekman, and E.L. Rosenberg, Eds. *What the Face Reveals: Basic and Applied Studies of Spontaneouse Expression Using the Facial Action Coding System (FACS)*, Oxford University Press, 1997.

[90] *The Polygraph and Lie Detection*, The National Academies Press, Washington, DC, 2003.

[91] R. F. Royal, and S. R. Schutt, *The Gentle Art of Interviewing and Interrogation: A Professional Manual and Guide*, Prentice-Hall, 1976.

[92] J. F Nunamaker, D. C. Derrick, A. C. Elkins, J. K. Burgoon, and M. W. Patton, Embodied conversational agent-based kiosk for automated interviewing, *J. Management Information Systems,* vol. 28, no. 1, 2011, pp. 17–48.

[93] Aaron Elkins, Elyse Golob, Jay Nunamaker, Judee Burgoon, and Douglas Derrick, Appraising the AVATAR for Automated Border Control. Results of a European Union Field Test of the AVATAR System for Interviewing and Passport Control. Report to FRONTEX. October 2014

[94] AVATAR project: http://www.scientificamerican.com/article/avatar-officer-installed-mexico-border.

[95] AVATAR project: http://btn.frontex.europa.eu/node/1603.

[96] R. Beale and C. Creed, Affective interaction: How emotional agents affect users. *Int. J. Human-Computer Studies,* vol. 67, no. 9, 2009, pp. 755–776.

[97] R. Cowie et al., Emotion Recognition in human-computer interaction, *IEEE Signal Processing Magazine,* 2001, pp. 33–80.

[98] P. Treigys, V. Marcinkevikius, A. Kaklauskas, Analysis of Iris and Pupil Parameters for Stress Recognition,?Journal of Applied Research and Technology 41(1):7-15ů April 2012.

[99] AVATAR: Border patrol kiosk detects liars trying to enter U.S. *Homeland Security News Wire*, August 21, 2012. http://www.homelandsecuritynewswire.com/dr20120821-border-patrol-kiosk-detects-liars-trying-to-enter-u-s

[100] The Turing Test: Alan Turing and the Imitation Game (from Artificial Intelligence Tutorial by Eyal Reingold) http://www.psych.utoronto.ca/users/reingold/courses/ai/turing.html

[101] Andrew Ryan, Jeffery F. Cohn, Simon Lucey, Jason Saragih, Patrick Lucey, Fernando de la Torre, and Adam Rossi Automated Facial Expression Recognition System, In IEEE International Carnahan Conference on Security Technology. October 2009. Zurich. http://www.humansensing.cs.cmu.edu/projects/autofacial.html

[102] Dmitry O. Gorodnichy and Oleg P. Gorodnichy, Using associative memory principles to enhance perceptual ability of vision systems, The First IEEE CVPR Workshop on Face Processing in Video (FPiV) 2004, Washington, D.C., USA. http://www.visioninterface.net/fpiv04

[103] Audrey Leblanc; Meťlanie Martel "Memory game : to learn about and recognize emotions!" http://www.groupeformationintervention.com/jeux-educatifs.php

## c) Queuing technology and self-service kiosks

[104] PreBorderLane. Project description. *Fraunhofer Institute for Computer Graphics Research IGD*. http://preborderlane.eu. Also http://www.igd.fraunhofer.de/en/Institut/Abteilungen/Identifikation-und-Biometrie/Projekte/PreBorderLane

[105] Automated Passport control technology to launch at Chicago Midway International. http://www.passengerterminaltoday.com/viewnews.php?NewsID=53566

## d) Biometric-enabled ABC

[106] IRIS Project, Pilot review report, V3.0, *Home Office*, UK, 2006. www.statewatch.org/news/2007/mar/bio-iris-project-review-pilot.pdf

[107] A. J. Palmer and C. Hurrey, Ten reasons why IRIS needed 20:20 foresight: Some lessons for introducing biometric border control systems. *Proc. European Intelligence and Security Information Conf.*, 2012, pp. 311–316.

[108] D. C. Cantarero, D. A. P. Herrero, and F. M. Mendez, A multi-modal biometric fusion implementation for ABC Systems, *Proc. IEEE European Intelligence and Security Informatics Conf.*, 2013, pp.277–280.

[109] M. Nuppeney, M. Breitenstein, and M. Niesing, EasyPASS ? Evaluation of face recognition performance in an operational automated border control system, Federal Office for Information Security, 2010,

[110] Marzahn, B., E-gate case study: The German EasyPASS Project, Federal Office for Information Security, www.bsi.de, Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD), International Civil Aviation Organization, 12th Meeting Montreal, Sept. 2011.

[111] Nuppeney, M., Federal Office for Information Security, (BSI), "Automated Border Control based on (ICAO compliant) eMRTDs", NIST IBPC 2012. Online: http://www.nist.gov/itl/iad/ig/ibpc2012_presentations.cfm

[112] Markus Nuppeney, BSI, "Automated Border Control - state of play and latest developments". NIST IBPC 2014. http://www.nist.gov/itl/iad/ig/ibpc2014_presentations.cfm

[113] L.J. Spreeuwers, A.J. Hendrikse, K.J. Gerritsen, Evaluation of automatic face recognition for automatic border control on actual data recorded of travellers at Schiphol Airport. BIOSIG 2012, http://cs.emis.de/LNI/Proceedings/Proceedings196/99.pdf

[114] A.M. Oostveen, E. Krempel, M. Kaufmann, G. Grasemann, Automated Border Control: a comparative usability study at two European airports IHCI 2014/07/15 Lisbon. https://www.fastpass-project.eu/sites/default/files/IHCI.pdf

[115] Anne-Marie Oostveen, Non-use of Automated Border Control Systems: Identifying Reasons and Solutions. The 28th British HCI Conference 2014/9/09 Southport, UK. https://www.fastpass-project.eu/sites/default/files/BHCI-O.pdf

## e) Pre-screening technology

[116] FLUX: https://www.flux-alliance.eu/home. See also: http://en.wikipedia.org/wiki/FLUX_Alliance.

[117] TSA Announces Expansion of Diamond Lane Self-Select Pilot to Orlando, Boston, and Spokane Airports. *Transportation Security Administration (TSA)*, Press Office, (571) 227-2829, March 18, 2008. http://www.tsa.gov/press/releases/2008/03/18/tsa-announces-expansion-diamond-lane-self-select-pilot-orlando-boston-and

[118] L. McLay, , Jacobson, S.H., and Kobza, J.E., Making Skies Safer: Applying Operations Research to Aviation Passenger Pre-screening Systems, *Operations Research and Management Science*, vol. 32, no. 5, pp. 24–31. Reprinted in *Analytics*, Spring 2008, pp. 13–17. http://viewer.zmags.com/publication/840980b8#/840980b8/2

[119] Wikipedia: Computer-Assisted Passenger Pre-screening System, http://en.wikipedia.org/wiki/Computer-Assisted_Passenger_Prescreening_System

[120] Gregorio Ameyugo, Michal Art, Ana Sofia Esteves, Jakub Piskorski, Creation of an EU-Level Information Exchange Network in the Domain of Border Security, EISIC, 2012, European Intelligence and Security Informatics Conference, European Intelligence and Security Informatics Conference 2012.

[121] J. Piskorski; Tanev, H.; Balahur, A., Exploiting Twitter for Border Security-Related Intelligence Gathering, Intelligence and Security Informatics Conference (EISIC), 2013 European , vol., no., pp.239,246, 12-14 Aug. 2013.

[122] R. Poole, and G. Passantino, A risk-based airport security policy, *Reason Foundation*, Policy study No. 308, 2003. http://reason.org/files/359408528b992e7d0804df1b590dd424.pdf

[123] N. Melnikov, J. Scheonwalder. "Cybermetrics: User Identification through Network Flow Analysis". In Mechanisms for Autonomous Management of Networks and Services, 6155, Springer, pp.167-170, 2010. https://hal.inria.fr/IFIP-LNCS-6155/hal-01056631v1

## f) Supporting technology

[124] IEEE: The State of RFID Implementation and its Policy Implications, *IEEE-USA White Paper*, 2009.

[125] T. Chothia, and V. Smirnov, A Traceability Attack Against e-Passports, Proc. *14th Int. Conf. Financial Cryptography and Data Security*, 2010.

[126] E. A. Bogari, P. Zavarsky, D. Lindskog, and R. Ruhl, An Analysis of Security Weaknesses in the Evolution of RFID Enabled Passport, *Proc. World Congress on Internet Security (WorldCIS-2012)*, 2012, pp. 158–166.

[127] Mobile Biometric Identification, WHITE PAPER, Motorola, 2008. http://www.motorolasolutions.com/web/Business/Products/Biometrics/Mobile

[128] CLEAR Verified Identity Pass website. http://www.flyclear.com

[129] L. Babu, R. Batta, and L. Lin. Passenger grouping under constant threat probability in an airport security system, *European J. Operational Research*, vol. 168, 2006, pp. 633–644.

[130] P. Chawdhry and R. P. Da Silva, Advanced Registered Traveler Paradigm using Dynamic Risk Profile and Multimodal Biometrics, *Proc. IEEE Int. Conf. Systems, Man, and Cybernetics*, San Antonio, TX, USA pp. 3946–3951, 2009.

[131] X. Nie, R. Batta, C. G. Drury, and L. Lin, The Impact of Joint Responses of Devices in an Airport Security System, *Risk Analysis*, Vol. 29, No. 2, 2009, pp. 298–311.

[132] C. Coronel and S. Morris, *Database Systems: Design, Implementation, and Management,* Cengage Learning, 2015.

[133] R. Murthy and I. Pavlidis, Noncontact measurement of breathing function, *IEEE Eng. in Medicine and Biology Magazine*, May/June, 2006, pp. 57–67.

## Research-driven publications

### a) By CBSA Science and Engineering Directorate

[134] Jean-Philippe Bergeron and David Bissessar, "Accelerated Evidence Search Report", CBSA Science and Engineering Directorate, Division Report 2014-06. Also DRDC Contract Report, DRDC-RDDC-2014- C166, July 2014. Online: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc159/p800470_A1b.pdf

[135] Dmitry Gorodnichy and Eric Granger, "Target-based evaluation of face recognition technology for video surveillance applications", Proc. of IEEE SSCI CIBIM 2014 workshop, Orlando, December 2014.

[136] D.O. Gorodnichy, E. Granger, P. Radtke, . Survey of commercial technologies for face recognition in Video, Technical Report DRDC-RDDC-2014-C245, Online: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc159/p800510_A1b.pdf

[137] D.O. Gorodnichy, E. Granger, J.-P. Bergeron, D. Bissessar, E. Choy, T. Mungham, R. Laganiere, S. Matwin, E. Neves, C. Pagano, M. De la Torre, P. Radtke. "PROVE-IT(FRiV): framework and outcomes", Online: http://www.nist.gov/itl/iad/ig/ibpc2014presentations.cfm

[138] Gorodnichy, D.O.; Bergeron, J.-P.; Bissessar, D.; Choy, E.; Sciandra, J. "Video Analytics technology: The foundations, market analysis and demonstrations", Technical Report DRDC-RDDC-2014-C251, Online: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc167/p801081_A1b.pdf.

[139] David Bissessar, Dong Liu, Sherine Nahmias, John Harvey, "Architecture and Assessment: Privacy Preserving Biometrically Secured Electronic Documents", Technical Report DRDC-RDDC-2015-C055. Online: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc173/p801301_A1b.pdf

[140] David Bissessar, Cryptographic Credentials with Privacy-preserving Biometric Bindings. M.Sc. Dissertation, University of Ottawa, 2013.

[141] Dmitry O. Gorodnichy. "Multi-order analysis framework for comprehensive biometric performance evaluation", SPIE Conference on Defense, Security, and Sensing. DS108: Biometric Technology for Human Identification track. Orlando, 5 - 9 April 2010.

[142] Dmitry O. Gorodnichy, Michael Thieme, Dave Bissessar, Jessica Chung, Elan Dubrofsky, Jonathon Lee, "C-BET evaluation of voice biometrics". Proceedings of SPIE Defence, Security & Sensing Conference, Special Track on Biometric Technology for Human Identification VIII (DS108), Orlando, April 25-29, 2011.

[143] Dmitry O. Gorodnichy. "Multi-order biometric score analysis framework and its application to designing and evaluating biometric systems for access and border control". Proceedings of IEEE SSCI Workshop on Computational Intelligence in Biometrics and Identity Management (CIBIM), April 2011, Paris.

[144] D.O. Gorodnichy, R. Hoshino. "Calibrated Confidence Scoring for Biometric Identification". In Proceedings of the NIST International Biometric Performance Conference (IBPC 2010), NIST Gaithersburg, March 2-4, 2010. Online: http://biometrics.nist.gov/cs_links/ibpc2010/pdfs/Gorodnichy2_Dmitry_Calibrated_Confidence_Scoring_for_Biometric_ID.pdf.

[145] Dmitry O. Gorodnichy, Elan Dubrofsky, Richard Hoshino, Wael Khreich, Eric Granger, Robert Sabourin. "Exploring the upper bound performance limit of iris biometrics using score calibration and fusion", Proceedings

of IEEE SSCI Workshop on Computational Intelligence in Biometrics and Identity Management (CIBIM), April 2011, Paris.

## b) Other government funded

[146] Data at your fingertips: Biometrics and the challenges to privacy. *Office of the Privacy Commissioner of Canada*, http://www.priv.gc.ca/information/pub/gd_bio_201102_e.pdf

[147] DRDC: M. Culhane, "Survey of Technologies for the Airport Border of the Future", Technical Report DRDC-RDDC-2014-C65, April, 2014. http://cradpdf.drdc-rddc.gc.ca/PDFS/unc152/p800008_A1b.pdf

[148] DRDC: P. Meunier, Xiao, Q., and Vo, T. "Biometrics for National Security: The Case for a Whole of Government Approach", Technical Report DRDC-CSS-TM-2013-005, June, 2013. http://cradpdf.drdc-rddc.gc.ca/PDFS/unc124/p537494_A1b.pdf

[149] DRDC: "Biometric Border Security Evaluation Framework" by IBG in partnership with CBSA, DRDC-CSS-CR-2011-16, Oct., 2011.

[150] DAPRA: Total Information Awareness DARPA's Research Program, *Information and Security*, **10**:105–109, 2003. https://en.wikipedia.org/wiki/Total_Information_Awareness

[151] EU project: "ABC gates for Europe (ABC4EU)" 2014–2017 http://cordis.europa.eu/projects/rcn/111518_en.

[152] EU project: "FASTPASS: A harmonized, modular reference system for all European automated border crossing points". 2013–2016. http://cordis.europa.eu/projects/rcn/106743_en.

## c) By the University of Calgary's Biometrics Technologies Lab

[153] Yanushkevich, S. N., A. Stoica, V. P. Shmerko, and D. V. Popel, *Biometric Inverse Problems*. CRC Press/Taylor & Francis Group, Boca Raton, FL, 2005.

[154] Yanushkevich, S.N., Stoica, A., and Shmerko, V.P., Experience of Design and Prototyping of a Multi-Biometric Early Warning Physical Access Control Security System (PASS) and a Training System (T-PASS), *Proc. 32nd Annual IEEE Industrial Electronics Society Conf.*, Paris, France, pp. 2347–2352, 2006.

[155] Yanushkevich, S. N., A concepts of intelligent biometric-based early detection and warning system *Proc. Conf. Privacy, Security, Trust - PST2006*, Ontario, Canada, 2006, pp. 429–432.

[156] Yanushkevich, S.N., Stoica, A., and Shmerko, V.P., Fundamentals of Biometric-Based Training System Design, In Yanushkevich, S. N., Wang, P., Srihari, S., Gavrilova, M. (Eds.), and Nixon, M.S. (Consulting Ed.), *Image Pattern Recognition: Synthesis and Analysis in Biometrics*, World Scientific, 2007.

[157] Chague S., Droit B., O. Boulanov, S. N. Yanushkevich, V. P. Shmerko, and A. Stoica, "Biometric-Based Decision Support Assistance in Physical Access Control Systems", *Proc. Conf. Bio-inspired, Learning and Intelligent Systems for Security*, pp.11–16, 2008.

[158] Yanushkevich, S. N., O. Boulanov, A. Stoica, and V. P. Shmerko, Support of interviewing techniques in physical access control system, S.N. Srihary and K. Franke, Eds, *Computational Forensics*, Springer, 2008, pp. 147–158.

[159] Yanushkevich, S. N., V. P. Shmerko, O. Boulanov, and A. Stoica, Decision-making support in biometric-based physical access control systems: Design concept, architecture, and applications. N. V. Boulgouris, K.N. Plataniotis, and E. Micheli-Tzanakou, Eds, *Biometrics: Theory, Methods, and Applications*, IEEE Press, Wiley, 2010, pp. 599–631.

[160] Yanushkevich, S. N., Fundamentals of Biometric System Design. *Lecture Notes*, University of Calgary, Canada. http://www.ucalgary.ca/btlab

[161] Poursaberi, A., Vana, J., Mracek, S., et al. Facial biometrics for situational awareness systems, *IET Biometrics*, Vol. 2, Issue 2, 2013, pp. 35Ű-47.

[162] Eastwood, S. C. and S. N. Yanushkevich, Risk Profiler in Automated Human Authentication, *Proc. IEEE Workshop on Comput. Intelligence in Biometrics and Identity Management – CIBIM*, Orlando, Florida, 2014.

## d) Biometrics fundamentals

[163] *Biometric Recognition: Challenges and Opportunities*, J. N. Pato and L. I. Millett, Eds., The National Research Council, The National Academies Press, Washington, 2010. http://www.nap.edu/catalog/12720/biometric-recognition-challenges-and-opportunities

[164] R. Bolle, Connell, J., Pankanti, S., Ratha, N. and Senior, A. *Guide to Biometrics*, Springer, 2004.

[165] J. R. Vacca, *Biometric Technologies and Verification Systems*, Elsevier, 2007.

## e) Standards

[166] Standard IEC 60300-1. Dependability Management. Part 1: Dependability management systems. International Electrotechnical Commission, 2003.

[167] C. Busch, Biometric data format and related standards –needs, status, and trends. *Proc. Biometric Consortium Conf.*, 2013.

[168] NIST: Special Publication 800-63, Electronic Authentication Guideline, National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

[169] NIST: Special Publication 500-280, Mobile ID Device Best Practices Recommendation Version 1.0,38, August 2009. http://www.nist.gov/itl/iad/ig/upload/MobileID-BPRS-20090825-V100.pdf

[170] Biometric Standards Requirements for US-VISIT, Department of Homeland Security, Version 1.0 March 15, 2010, http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_biometric_standards.pdf

[171] ISO: Biometric Profiles for Interoperability and Data Interchange, Part 2: Physical Access Control for Employees at Airports. ISO/IEC 24713-2 (2008).

[172] ISO: Information technology – Biometric performance, testing, and reporting, Section 6.4.6, ISO/IEC19795-1 (2006).

[173] J. L. Wayman, *National Biometric Test Center Collected Works*, National Biometric Test Center, San Jose, CA, 2000.

[174] A. Mansfield and J. Wayman, Best Practice Standards for Testing and Reporting on Biometric Device Performance, *National Physical Laboratory of UK*, 2002.

[175] The national biometrics challenge. National Science and Technology Council, Subcommittee on Biometrics and Identity Management, 2011. http://www.biometrics.gov/Documents/BiometricsChallenge2011_protected.pdf

## f) Face recognition

[176] NIST Face Recognition Vendor Test (FRVT) 2010, Interagency Report 7709 - Report on the Evaluation of 2D Still-Image Face Recognition Algorithms. http://www.nist.gov/itl/iad/ig/mbe.cfm

[177] NIST Face Recognition Vendor Test (FRVT) 2013, NIST Interagency Report 8009, http://www.nist.gov/itl/iad/ig/frvt-2013.cfm

[178] Facial Recognition and Airport Security, *Imagis Technologies Inc. White paper*, 2004, http://www.imagisttechnologies.com

[179] Matteo Ferrara, Annalisa Franco, Davide Maltoni, "The Magic Passport", IJCB 2014, Clearwater, October 2014.

[180] TABULA RASA (Tabula Rasa: Trusted Biometrics under Spoofing Attacks) Spoofing Challenge 2013. https://www.tabularasa-euproject.org/evaluations/tabula-rasa-spoofing-challenge-2013

[181] Welti, P., J.-M. Suchier and C. Busch, Improving border control with 3D face recognition, *Proc. Biometrics and Electronic Signatures (BOSIG'2008)*, 2008, pp. 123–134.

[182] American Society for Aesthetic Plastic Surgery, 2008 statistics, http://www.surgery.org/download/2008stats.pdf

[183] American Society for Aesthetic Plastic Surgery 2010 Statistics http://www.surgery.org/media/statistics

[184] M. Taister, S. D. Holliday, and H.I.M. Borman, Comments on facial aging in law enforcement investigation, *Forensic science communication*, vol 2 no 2, 2000 http://www.fbi.gov/about-us/lab/forensic-science-communications

[185] H. Bhatt, S. Bharadwaj, R. Singh, and M. Vatsa, Recognizing Surgically Altered Face Images Using Multiobjective Evolutionary Algorithm, *IEEE Trans. Information Forensics and Security*, vol. 8, no. 1, January, 2013, pp. 89–99.

## e) Iris recognition

[186] J. Daugman, Patent US5291560 - Biometric personal identification system based on iris analysis. Filed: July 15, 1991. Published: 1 March 1994. http://www.google.ca/patents/US5291560

[187] J. Daugman, Iris Recognition at Airports and Border-Crossings. http://www.cl.cam.ac.uk/~jgd1000/Iris_Recognition_at_Airports_and_Border-Crossings.pdf

[188] J. Daugman, "Evolving methods in iris recognition and implementations from 200 billion iris comparisons", Invited talk at the IEEE Conference on Biometrics: Theory, Applications and Systems (BTAS) , 2007. http://www.cse.nd.edu/BTAS_07/John_Daugman_BTAS.pdf.

[189] S. Baker, A. Hentz, K.W. Bowyer, and P. J. Flynn. Degradation of iris recognition performance due to non-cosmetic prescription contact lenses. *Computer Vision and Image Understanding,* 114(9), pp.1030–1044, 2010.

[190] Kevin Bowyer. " Effects of Contact Lenses on Iris Recognition" by http://www3.nd.edu/~kwb/BakerHentzBowyerFlynnCVIU_2010.pdf

[191] K. Bowyer and E. Ortiz, Making Sense of the IREX VI Report, Computer Vision Research Lab Technical Report, Dec 2013. http://www3.nd.edu/~kwb/Making_Sense_Dec_23_2013.pdf

[192] Kevin Bowyer. Iris Recognition, Tutorial at International Joint Coinference on Biometrics (IJCB), 2014. http://www3.nd.edu/~kwb/IJCB_2014_Tutorial.pdf

[193] P. Grother, G. W. Quinn, J. R. Matey, M. Ngan, W. Salamon, G. Fiumara, C. Watson. IREX III: evaluation of one-to-many iris identification algorithms, NIST Interagency Report 7836, 2012, http://www.nist.gov/itl/iad/ig/irexiii.cfm

[194] P. Grother, J. R. Matey, E. Tabassi, G. W. Quinn, M. Chumakov, IREX VI: Temporal Stability of Iris Recognition Accuracy, *NIST Interagency Report 7948*, 2013. http://www.nist.gov/itl/iad/ig/irex.cfm

[195] P. Grother, "Age, Ageing, Acclimation: Time Dependence" http://www.biometrics.org/bc2014/presentations/Wed_1314_Grother_1120.pdf.

[196] P. Grother, J. Matey, "Iris Permanence What We Know, What We Don't, and How to Find Out More". http://www.biometrics.org/bc2014/presentations/Tues_1819_Grother_1400.pdf

[197] C. Rathgeb, A. Uhl, and P. Wild, *Iris Biometric: From Segmentation to Template Security* Springer, 2013.

[198] Christian Rathgeb, A biometric for life potential for a lifetime breeder document, International Biometric Performance Testing Conference (IBPC), 2014. http://www.nist.gov/itl/iad/ig/ibpc2014_presentations.cfm

[199] Sara Lais Rahal Lenharo, Brazilian National Biometric Selection: New and Legacy Challenges. IJCB 2014 Keynote speaker presentation: http://www.ijcb2014.org/Keynote_Speakers.html

[200] Vijay S. Madan Digital ID for Benefit and Service Delivery to Billion Plus People. ibid.

[201] Shukri Ali Al Braiki The UAE Population Register and ID Card Program: Achievements and the Challenges. ibid.

[202] William G. McKinsey (FBI), The Challenges of NGI, ibid

[203] S. Arora, M. Vatsa, R. Singh, and A. Jain, Iris recognition under alcohol influence: A preliminary study, *Proc. 5th IAPR Int. Conf. Biometrics Compendium (ICB'12)*, 2012, pp. 336–341.

[204] J. Nichols, Annual report: Contact lenses. 2011. http://www.clspectrum.com/articleviewer.aspx?articleid=106550

[205] Unsang Park, R. Jillela, Arun Ross, Anil Jain, Periocular Biometrics in the Visible Spectrum, IEEE Transactions on Information Forensics and Security (Volume:6, Issue:1), Page(s): 96 - 106, 2011.

## h) Subject-based biometrics performance analysis

[206] G. Doddington, W. Liggett, A. Martin, M. Przybocki, and D. Reynolds. Sheep, goats, lambs and wolves a statistical analysis of speaker performance in the NIST 1998 speaker recognition evaluation. Proc. Int. Conf. Spoken Language Processing, 1998.

[207] A. Jain and A. Ross. Learning User-Specific Parameters in Multibiometric System. In Proc. Int 'l Con! of Image Processing (ICIP 2002), pages 57-70, New York, 2002.

[208] M. Wittman, P. Davis, and P.J. Flynn., Empirical studies of the existence of the biometric menagerie in the FRGC 2.0 color image corpus, Proc. Conf. on Computer Vision and Pattern Recognition Workshop, pp. 33-33, June 2006.

[209] N. Poh, T. Bourlai, and J. Kittler, Improving biometric device interoperability by likelihood ratio-based quality dependent score normalization, in Proc. IEEE Conf. Biometrics: Theory, Appl. Syst., Washington, DC, 2007, pp. 1-5

[210] N. Poh, Kittler, J.: A Methodology for Separating Sheep from Goats for Controlled Enrollment and Multimodal Fusion. In: 6th IEEE Biometric Symposium, Tampa, Florida, USA (2008) pp. 17-22.

[211] Paone, J., Flynn, P.: On the consistency of the biometric menagerie for irises and iris matchers. In: Proc. IEEE Int. Workshop on Information Forensics and Security (WIFS), pp. 1-6 (2011)

[212] B. DeCann and A. Ross, Relating ROC and CMC Curves via the Biometric Menagerie, Proc. 6th IEEE Int.Conf. Biometrics: Theory, Applications and Systems (BTAS), (Washington DC, USA), 2013.

[213] J. D. Bustard, J. N. Carter, and M. S. Nixon, Targeted Impersonation as a Tool for the Detection of Biometric System Vulnerabilities, *Proc. IEEE 6th Int. Conf. Biometrics: Theory, Applications and Systems,* Arlington, 2013.

[214] Norman Poh, IEEE IJCB Tutorial: "System Design and Performance Assessment: A Biometric Menagerie Perspective", available at IJCB 2014 conference website: http://ijcb2014.org/Tutorials.html and http://personal.ee.surrey.ac.uk/Personal/Norman.Poh/talks.php.

## i) Modeling and other tools for complex system performance analysis

[215] M. Rossetti, *Simulation Modeling with ARENA*, John Wiley, 2010. https://www.arenasimulation.com

[216] Simio Case studies. http://www.simio.com/case-studies/index.php. Mike Lazzaroni, Modeling passenger and baggage flow at Vancouver airport

[217] ExtendSim Case studies: http://www.extendsim.com/sols_papers.html

[218] M. Sacanamboy,m and B. Cukic, Combined performance and risk analysis for border management applications, *Proc. IEEE/IFIP Conf. Dependable Systems and Networks (DSN)*, 2010, pp. 403–412.

[219] Aven, T., *Foundations of Risk Analysis*, 2nd ed, Wiley, 2012.

[220] K. Korb and A. Nicholson, *Bayesian Artificial Intelligence*, Chapman and Hall/CRC Press 2004.

[221] G. Shafer, *A Mathematical Theory of Evidence*, Princeton, University Press, 1976.

[222] John C.Mankins (6 April 1995). "Technology Readiness Levels: A White Paper". NASA, Office of Space Access and Technology, Advanced Concepts Office. http://www.hq.nasa.gov/office/codeq/trl/trl.pdf

[223] "Technology Readiness Assessment (TRA) Guidance". United States Department of Defense. April 2011. http://www.acq.osd.mil/chieftechnologist/publications/docs/TRA2011.pdf

[224] A. Birolini, *Reliability Engineering. Theory and Practice*, 6th edition, Springer, Heidelberg, 2010.

[225] B. Dhilon *Reliability, Quality and Safety for Engineers*, Boca Raton, FL, CRC Press, 2005.

[226] M. Rausand and Hoyland A. *System Reliability Theory: Models, Statistical Methods, and Applications*, Hoboken, NJ, Wiley, 2004.

[227] P. Tobias and Trindade D. C. *Applied Reliability*, 2nd ed., New York, Chapman and Hall, 1995.

[228] S. Rigdon and Basu A. P. *Statistical Methods for the Reliability of Repairable Systems*, New York, Wiley, 2000.

[229] A. J. Palmer, Criteria to evaluate automated personal identification mechanism, *Computers and Security*, vol. 27, 2008, pp. 260–284.

[230] A. J. Palmer, Approach for selecting the most suitable Automated Personal Identification Mechanism (ASMSA), *Computers and Security*, vol. 10, 2010.

[231] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, Hardware Trojan attacks: Threat analysis and countermeasures, *Proceedings of the IEEE, Special Issue on Trustworthy Hardware*, vol. 102, no. 8, 2014, pp. 1229-1247.

# Appendix B

# Overview of border modernization initiatives

In the following the key border challenges and initiatives from different countries are presented, summarized from [147, 36, 11, 17].

## B.1 Scan of international programs

### B.1.1 EU: "Smart Border" program

In February 2013 the EU Commissioner for Home Affairs announced the Smart Border initiative, intended to speed-up and reinforce border check procedures for foreigners and help the EU cope with an increasing number of travellers (expected to reach 720 million by 2030).[14] The package is comprised of two parts:

1. Registered Traveller Program: the RTP will allow frequent travellers from third countries to enter the EU using simplified border checks, subject to pre-screening and vetting. It is estimated that 5 million legitimate non EU-travellers per year will enroll in the new program. The RTP will make use of automated border control systems at airports.

2. Entry/Exit System: an Entry/Exit System will record the time and place of entry and exit of third country nationals travelling to the EU. An alert will be sent to national authorities when there is no exit record by the expiry time.

Within the EU is a border-free zone called the Schengen Area which guarantees free movement to the more than 400 million citizens of the 26 member nations. It functions as a single country for international travel purposes, with a common visa policy. Ireland and the UK are the only EU countries that are not part of the Schengen Area, while four non-EU countries (Iceland, Liechtenstein, Norway, and Switzerland) are Area members.

The backbone of the Area is the Schengen Information System (SIS), which is the largest shared information system for public security in Europe. Used by border guards as well as by police, customs, visa and judicial authorities, SIS consists of three components: a Central System, EU States' national systems and a communication infrastructure between the Central and the national systems. Information is entered into the SIS by national authorities and forwarded via the Central System to all Schengen States.[15]

The EU does not issue passports; rather they are issued by individual EU countries. However, EU passports do have a common design and layout: burgundy in colour with the words "European Union" printed on the cover, accompanied by the name of the issuing EU State. Schengen countries were obliged by law to implement machine readable facial images in their passports by August 28, 2006 and fingerprints by June 29, 2009.

A number of registered traveller programs are established in individual EU nations. Germany's Automated and Biometrics-Supported Border Controls (ABG) program is linked to the US's Global Entry program as of

2010. The US has also joined with the Netherlands in a program called Flux [116]. The goal is to grow Flux into a global alliance of trusted traveller programs to ease bottlenecks and expedite passenger processing around the world.

Many EU countries have deployed ABC gates, based on facial biometrics stored in e-passport.

Table B.1: European border control systems based on e-passports (from [111]).

| Country | System | Start | Biometric |
|---|---|---|---|
| Portugal | RAPID | 2007 | Face |
| UK | E-gate | 2008 | Face |
| Finland | ABC | 2008 | Face |
| France | PARAFES | 2009 | Face, fingerprints |
| Germany | EasyPass | 2010 | Face |
| Spain | ABC | 2010 | Face |
| Czech republic | EasyGo | 2011 | Face |
| Netherlands | No-Q | 2012 | Face |

### Frontex activities

Frontex, European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, was established on the 26 October 2004. One of the key Research activities of Frontex is seen in developing recommendations related to the use and deployment for ABC systems in EU. The Frontex ABC Working Group started in 02/2010 by NL, UK, FI, ES, PT, FR and DE, expanded in 2013 by CZ, IE, BG and Hongkong. [1]

In the absence of international standards on ABC deployment (see Appendix C), Frontex is currently one of the key sources of information for stakeholders and decision-makers in the field of ABC and Border of the Future. The most recent recommendations on ABC systems developed by Frontex include:

- Best Practice Technical Guidelines for ABC Systems, v2.0, 08/2012
- Best Practice Operational Guidelines for ABC Systems, v2.0, 08/2012

All reports are available via http://Frontex.europa.eu/publications/. Updates of the existing guidelines are expected for summer 2014. A new guideline document is under preparation regarding ABC systems for Third Country Nationals (TCN).

In its reports, Frontex provides key statistics on the performance of ABC in Europe. According to Frontex, as of March 2014, 13 European countries have ABC in place since:

- 2007-2009: PT, UK, FI, FR
- 2010-2011: DE, ES, CZ, NL
- 2012-2013: BG, NO, AT, IE, EE

In 2013, several European countries began trials of automated border clearance systems. By the end of 2014 Germany and UK had over 100 new eGates installed in their busiest airports. Ireland started a trial in May,

[1] The following abbreviation are used in EU for naming the EU members: BE - Belgium, BG - Bulgaria, CZ - Czech Republic, DK - Denmark, DE - Germany, EE - Estonia, IE - Ireland, EL - Greece, ES - Spain, FR - France, IT - Italy, CY - Cyprus, LV - Latvia, LT - Lithuania, LU - Luxembourg, HU - Hungary, MT - Malta, NL - Netherlands, AT - Austria, PL - Poland, PT - Portugal, RO - Romania, SI - Slovenia, SK - Slovakia, FI - Finland, SE - Sweden.

2013. Norway deployed new eGates at Oslo airport in September, 2013 and Portugal installed 24 at Lisbon International on November 7, 2013.

Systems can be used by EU/EEA/CH citizens [2]. Finland (FI) can also process third country nationals from Japan and Korea . E-passport is used as token supported by all systems. Additionally, systems in Germany (DE) and Spain (ES) can process national e-ID cards containing biometric data. Almost every system supports facial biometrics. ES and EE are doing multi-modal biometrics (face and fingerprint; Spanish ID card supports fingerprint match-on-card) FR is doing fingerprint only. This is summarized in Table B.1.

Annually Frontex holds the ABC Workshop, organized in cooperation with the UK authorities, which aims at looking into the latest developments on the ABC systems currently in use, under testing, or planned by EU Member States and Third Countries. This workshop is intended to foster the exchange of Member StatesŠ experiences and lessons learned through peer discussions on benefits and challenges of deploying ABC systems at different types of borders, including land and sea, as well as to share experiences and to address the vulnerability issues pertinent to ABC and the ways to mitigate them, within the larger context of Smart Borders Package.

Additionally, Frontex conducts research in Risk Assessment and Cost Benefit Analysis (CBA) of ABC, for which it develops a number of research tools, including ABC modeling software.

### B.1.2 UK: "e-Borders" program

The e-Borders concept has been introduced by the UK Home Office program as a part of the design to improve border security by screening travel document information electronically on people travelling to, and from, the UK [71]. This data is submitted by airlines and other carriers prior to travel and is used by Border Force, the UK Border Agency and the police to carry out security checks and deploy resources to deal effectively and efficiently with illegal immigration, crime, and threats to UK security. Although e-Borders is designed for border security purposes, the data collected also has the potential to deliver improvements to migration and population statistics.

In e-border management, the quality and quantity of border crossing, the training of border control forces, the ratio of the number of control agents against the control forces, the technical and technological equipment, and the optimization of wait time is of primary importance.

The U.K Border Force processed 220 million passengers through its airports in 2012 and this number is expected to jump to 315 million by 2030 [73]. In an effort to ease the growing congestion, the UK's Minister for Immigration announced in September 2013 a new registered traveller scheme that will provide regular travellers to the UK from certain countries expedited clearance at border controls. The program is open to individuals from Australia, Canada, Japan, New Zealand and the US who have travelled to the UK four or more times within a preceding 52-week period. The pilot ran to March 2014 [74].

Concurrently, the UK and Ireland announced a plan in July 2013 to create a "mini-Schengen" area to enable business travellers and tourists from fast-growing Asian economies to travel on common visas between the two islands (currently visitors must apply for visas to both countries). This is an expansion of the already existing Common Travel Area, a zone with minimal border controls comprising Ireland, Great Britain, the Isle of Man and the Channel Islands.

The UK currently uses eGates that use facial recognition technology similar to the Australian system. They can be used by UK citizens with an e-passport or by e-passport holders from a country in the European Economic Area (EEA). E-passports have been in use in the UK since 2006 and there are now about 25 million in circulation.

### B.1.3 Australia: Blueprint for Reform 2013-2018

In 2012, thirty-two million international travellers were processed at Australia's eight international airports. By 2017 the number is expected to reach forty million, and by 2023 fifty million [50] In July 2013, the Australia

[2] Citizen from EU, European Economic Area (EEA) and Switzerland (CH).

Customs and Border Protection Service announced the Blueprint for Reform 2013-2018, with the goal of modernizing its border systems to meet the expected rise in passenger volume. Among the highlights:
- Establishment of the National Border Targeting Centre to target high-risk passengers through better coordination and sharing of intelligence between partner agencies and targeting centres in the United States, Canada, the United Kingdom and New Zealand.
- Installation of next-generation eGate technology to process travellers faster.
- Future goal of a seamless, low-touch process from pre-departure to arrival and clearance [51].

In addition, in February 2013 the Prime Minister announced the Traveller Processing of the Future project, a two-year initiative to evaluate the latest technology offerings to support the "extending the border" concept (i.e. assessing passengers before they land in the country), and investigation into future technologies such as "face on the move" and "face in the crowd".

All eight international airports in Australia currently employ an automated border control (ABC) kiosk system called SmartGate, which uses the data in the traveller's e-passport combined with face recognition technology to perform the customs and immigration checks usually conducted by a border official. With the investigation into next generation eGates and mobile eGates to allow more travellers to self-process, including in remote locations, by 2020 ninety percent of international travellers will be able to use SmartGate (from a current rate of twenty percent) [52].

As part of the Trans Tasman agreement, Australians and New Zealanders can cross each other's border using SmartGate (both nations use the identical system). Travellers from the United Kingdom can also use SmartGate as of November 2013, and it is currently being trialled with United States Global Entry program members holding e-passports. A trial with Chinese e-passport holders begins in 2015. The eligibility requirement to use SmartGate in Australin and New Zealand has been recently lowered from 16 to 12 years.

### B.1.4 United States

Just over 815 million passengers passed through US airports in 2012. The 2013 Federal Aviation Administration (FAA) forecast calls for US passenger growth over the next 20 years to average 2.2 percent per year [66]. Technology will play a key role as the US tries to deal with the influx of visitors and immigrants. Trusted traveller programs such as the joint US/Canada program NEXUS and its international program Global Entry will continue to grow and become increasingly integrated with other programs around the world. Similarly, collaboration and information sharing among both national and international security agencies will expand. For example, the availability of Advance Passenger Information (API) and Passenger Name Record (PNR) data from airlines (as required by law) allows US Customs and Border Protection (CBP) to screen passengers against watch lists before they even arrive on American soil.

The problem of overstays creates additional border security issues for the US There are records of at least one million foreign nationals who entered the country legally for whom the Department of Homeland Security (DHS) has no record of departures, or that they obtained permission to stay. At a Congress hearing on Sept 29, 2013, DHS said a biometric exit plan will be in place to address the issue by 2015, but that it needs $3 billion to implement the system at airports alone. CBP works with the science and technology branch of DHS, which opened the Maryland Test Facility in 2014 to test biometric technology for the system. By mid-2015 the agency planed to test a pilot biometric exit system at a mid-size airport yet to be named [67].

### B.1.5 Canada: Border Modernization

International air travel to Canada is increasing rapidly following a post 9/11 decline, particularly in large airports such as Toronto, Vancouver, Montreal and Calgary. In Vancouver airport alone, international arrivals grew by over 22% - from 4.5 million passengers in 2007 to 5.5 million passengers in 2010. This growth was propelled by major shifts in the aviation market that include, Open Skies, Pacific Gateway and the 2010 Olympics.

Due to increasing volumes of airline passengers entering the country, the CBSA has experienced increased costs and wait times at all major international airports in Canada, and Airport Authorities (AA) are facing ever increasing costs to restructure and expand their facilities to deal with increasing numbers of travellers. The increase in traveller volumes led to pressures on the CBSA and AAs to develop innovative ways to deal with ever-increasing line-ups. Automating parts of CBSAŠs primary inspection process was considered an option that could create efficiencies for both the CBSA and AAs.

In 2005, the CBSA and Vancouver AA entered into a partnership to focus on the design and development of infrastructure and technology to improve service delivery. The idea was that an Electronic Primary Inspection Line (EPIL) would fit in with the trend for self-service automation throughout the entire airport environment. From e-passports, e-reservations, e-tickets, e-payment to e-check-in, self-serve technologies have succeeded in increasing speed, security and customer convenience and satisfaction. This process, known as the Automated Border Clearance (ABC) Program, was designed to reduce Primary Inspection Line (PIL) congestion at major airports by providing eligible travellers (Canadian citizens and permanent residents of Canada) to enter Canada by processing their entry through the use of touch screen technology to partially automate the primary inspection rather than the traditional face-to-face examination.

The ABC pilot project launched in 2009 at Vancouver International Airport (YVR) has produced key operational benefits, including, increased client satisfaction, reduced wait times and queuing times, increased processing capacity of the CBSA and avoidance of facilities and infrastructure expansion costs for both the CBSA and AAs. The project was approved for Canada-wide expansion for interested international airports using a phased approach, starting with Montreal-Pierre Elliot Trudeau International Airport (YUL) – on June 5, 2012, and then Toronto Pearson International Airport (YYZ), Terminal 3 – on January 30, 2013. Following implementation at YUL and YYZ (Terminal 3), the CBSA is focusing its efforts on upgrading the ABC pilot project technology by performing essential information technology related work to ensure that systems are sufficiently robust to support full expansion of ABC to additional airports.

The IATA statistics show more outbound international destinations from Canada than domestic trips within Canadian territory. In fact, even as airlines use larger planes to increase passenger traffic to key nations such as the United States and those in the EU, there is ample evidence that Canadian air transportation will expand into new and emerging markets such as Brazil, Eastern Europe, India and China. This predicted expansion is the inevitable result of focused Government of Canada (GoC) air transportation policy decisions, such as those being made by Transport Canada (TC) and the Canadian Air Transportation Security Agency (CATSA) to introduce efficiencies and reduce costs, as well as the well-publicized development efforts from profit-based corporate interests involved in air passenger transportation.

From the perspective of economics, profitability and passenger traffic volumes, the 2011 Oxford Economics Report on the air transport industry in Canada states that improvements in air transport connectivity contribute to the economic performance of the wider economy through enhancing its overall level of productivity. This improvement in productivity comes and will continue to grow through better access to foreign markets and by increasing the flexibility of labour supply which serves to reduce the natural rate of unemployment in Canada.

The Standing Senate Committee on Transport and Communications issued a report in June 2012 on the future growth and global competitiveness of Canada‘s airports. The report made a range of recommendations including, for example, the need to develop “a single, cohesive National Air Travel Strategy, including an updated National Airports System, to chart a new course towards increased air travel in Canada” and goes on to suggest that the current architecture for airport management and passenger processing unnecessarily dampens Canadian economic interests

In the next years, through the Canada-United States Beyond the Border (BtB) Action Plan and a suite of other modernization initiatives, Canada will be building additional layers of pre-border risk controls to lay the foundation for a new era in border management [60, 61]. The CBSA is positioned to enhance the facilitation of people and goods and to enforce Canadian law at ports of entry (POEs) in the near future [62].

## B.2 Entry-exit systems

The general purpose of the entry-exit system is to identify overstayers, that is, travellers who enter the country legally with a valid travel document and/or visa, but who become illegal migrants when their legal entitlement to stay expires; that is, the traveller fails to leave country upon expiration of their permitted stay. Data generated by the entry/exit system would be used by the competent immigration authorities.

### B.2.1 European entry-exit system

The basic principle of the EU Smart Borders program is the automation of the processes involved in border controls and immigration checks. Smart Borders aim at supplementing the SIS and VIS systems by logging movements in and out of the Schengen area and facilitating fast-track entry for registered travellers.

In Smart Borders procedures, a vast amount of personal data should be collected and retained for a range of purposes, including the profiling of travellers (in attempts to identify suspicious persons) and cross-checks against national security and police watch-lists. The entry-exit system is at the heart of the Smart Borders plans.

According to the EU Commission's Communication of 2008, the general purpose of EU entry-exit system is identifying overstayers. While it is often claimed that such persons comprise the largest category of illegal migrants in the EU, no accurate statistics exist [20].

### B.2.2 USA entry-exit system

US Immigration and Customs Enforcement (ICE), which is responsible for enforcing immigration law against foreign nationals who overstay or violate the terms of their admission, is now responsible for identifying overstays and determining overstay rates [17, 21]. Since 2008, US-VISIT has matured and interoperability between various government agencies is better defined. There are two phases in the US-VISIT system:

- Entry phase with ten-fingerprint search against large-scale databases to identify whether a traveller is on a watch list, and
- Exit phase when the system checks whether the traveller leaving is the same traveller who entered the country; for this, fast search is implemented using two fingerprints to match against the fingerprints of the claimed identity already in the record in the database.

For example, the process on exit includes the following operations:

- Scanning the passport or other travel document. The document number will lead to the traveller's record in the US-VISIT database.
- Submitting two fingerprints.
- Searching in database. If there is a match with the fingerprints in the file, the traveller will be cleared to exit unless there are behavioral questions that would justify further screening.

### B.2.3 Canada entry-exit system

Canada is working with international partner countries through the Five Country Conference (FCC) forum on biometric information sharing. Canada signed arrangements with the US, the UK, Australia and New Zealand in 2009 (High Value Data Sharing Protocol), allowing for the exchange of a limited number of fingerprint records in an effort to counter fraud and reduce the abuse of respective immigration programs [63].

## B.3 IATA future checkpoint roadmap

**The following overview of the IATA concept of future checkpoint with 2017 and 2020+ horizon from [27] has been prepared by V. Shmerko and S. Yanushkevich (Univesity of Calgary).**

Expected progress is related to three main areas: risk assessment, technology, and operation.

### The goals and key components of the checkpoint

IATA formulates three key goals of the concept of future checkpoint:

1. Strengthened security
   - Focus resources based on risk,
   - Increase unpredictability,
   - Better use of existing technologies,
   - Introduce new technologies with advanced capabilities,
2. Increased operational efficiency
   - Increase throughput, optimize asset utilization,
   - Ultimately, reduce cost per passenger,
   - Maximize space constraints and staffing resources,
3. Improved passenger experience by reducing waiting times, and using technology for a less intrusive and disruptive search.

IATA specifies the areas that might be included in the scope of the checkpoint of the future:

- Passenger differentiation,
- Known traveler,
- Data integration,
- Checkpoint configuration,
- Technology and detection standards,
- Randomness,
- Passenger experience and throughput,
- Biometrics and identity management,
- Behavioral analysis.

A general trend of the IATA concept is the shift towards risk based security measures. The key statement is that risk based passenger screening approach, including mutual recognition of risk amongst Member States, should respect fundamental human rights and privacy, and not in any way profile a passenger based on gender, religion, or race.

In IATA view, the concept of regulating differentiated screening and the use of risk based measures are critical. However, those measures are implemented in the Member States differently, because of different legislative bases. For example, the collection and use of passenger information may raise data privacy concerns on some States, and behavior analysis may not be acceptable in another, etc.

## Typical operations

Passengers are screened today to a predetermined National standard by the trained security staff. A typical screening checkpoint technology may consists of the following procedures:

- Screening of a passenger through a walk-through metal detector (WTMD),
- Conducting a physical search by hand of persons who cause an alarm activation or resolving such an alarm using security (body) scanner technology,
- Selecting at random a percentage of persons who have not caused the WTMD to alarm for a search by hand according to National legislation,
- Selecting passengers for further screening with a security scanner or by hand,
- X-ray screening of all items carried, including coats and jackets,
- Separate x-ray screening of shoes.

Cabin baggage is typically screened according to National legislation (x-ray screening of laptops, physical search of all items rejected by the x-ray operator, use of explosives trace detection, etc.) Typically, the following screening equipment is used: cabin baggage x-ray detectors, trace detectors, WTMDs, Hand Held Metal Detectors (HHMD), and various security scanners.

## Risk assessment and differentiation

IATA distinguishes the following premises of the risk based screening:

- The majority of passengers present low risk to aviation,
- An assessment may be conducted using the travel data,
- Further assessment can be made through a known traveler program, in which passengers voluntarily provide additional information about themselves,
- Behavior detection and interviewing techniques,
- Security can be increased by focusing on the unknowns.

**Definition B.3.1 Differentiation** *is defined as screening of different passengers in different ways. It does not mean screening based on race, gender or religious beliefs [27].*

Various approaches to differentiation can be used. IATA's roadmap introduces the following differentiation examples: passengers may be selected for an elevated level of screening randomly, in order to incorporate unpredictability, as is in the case of secondary screening, or for example, because of an unusual ticket purchase or other travel related behaviors; differentiation may be applied to an entire flight or all passengers for a specific time period, not just to an individual traveler. There are many inputs to the process of determination of how passengers are categorized for screening.

IATA states that criteria for risk assessment will be defined at National level, as will the choice of data sources to be scrutinized, the use of passenger data, and what factors will contribute to the assessment.

It is assumed in today's risk assessment technology that the authority, responsible for screening at the point of departure, will have primary responsibility for determination of risk assessment. The country of transfer or arrival may also make an assessment for security purposes. If there is more than one assessment, the highest level of the determined risk should be used for screening. Where Government assessment of risk is undertaken, it will be a contributing factor to other criteria, with the final categorization being made at the checkpoint entrance.

In IATA's roadmap, passenger risk measures is a critical point. The actual level of screening that each category of passenger undergoes will depend on the measures, applied by the screening authority. IATA report

on future checkpoint stresses that differentiation between the known traveler risk, normal and enhanced risk may mean different levels of divestiture, varying sensitivity of equipment, or different levels of randomness.

It should be taken into account, – IATA report says, – that passengers will need to be screened, as a minimum, to an acceptable baseline level, regardless of risk categorization. Some countries are moving away from a one-size-fits-all screening and following strict principles and a strong framework, and, interestingly, the security outcomes are similar. This means that additional screening after the checkpoint should not be required for passengers departing to other countries.

## Risk assessment as continuous process

IATA introduces the following sources of information for risk assessment as a continuous process that starts at ticket reservation and ends at boarding:

- Flight âĂŞ route or type (business, tourism),
- Traveler type (such as crew, staff, military personnel),
- Passenger data (Watch-list check from match with travel document information, rule-based analysis of reservations and check-in data),
- Membership of a known traveler scheme subject to background checks and current and valid membership,
- Presence on Interpol Lost and Stolen Passports database,
- Checks against other Government databases,
- Associated passengers on the same flight,
- Behavior analysis,
- Alternative measures such as random selection for enhanced screening, trace detection, and explosive detection by dogs.

ICATA characterizes the current trends in the automated border crossing technologies as follows: (a) Integrating new procedures to facilitate risk based screening and decision making, (b) Optimizing resource and asset utilization, and (c) Integrating available technology and re-purposing existing equipment.

## Today technologies and operations

IATA introduces the following contemporary technologies and operations for border passenger crossing:

- Remote image processing (checkpoint and airport specific areas),
- Biometric verification,
- Risk assessment,
- Explosive detection as an alternate measure prior to screening line,
- X-ray technology,
- Real time data collection of checkpoint such as queue time and throughput,
- X-ray threat identification,
- Passenger security scanners.

These technologies are used in the border crossing operations, such as dynamic passenger guidance of screening process, queue management program to display queue time and customer service support, improved staff allocation and use of behavior analysis, and program for regular passenger feedback that incorporates modern technology.

## IATA vision of the 2017 checkpoint

Based on contemporary border crossing technologies, IATA predicts the 2017 horizon. IATA expects that 2017 checkpoint will implement updating technologies and processes to increase the security value of the checkpoint, while maintaining a strong focus on customer service to enable greater passenger satisfaction. In particular, 2017 checkpoint will includes some major advances in risk assessment, dynamically delivering a result to the checkpoint to enable greater automation and better passenger experience. It envisages the increased use of biometrics and remote image processing, coupled with advances in screening technologies and targeted algorithms to achieve less divesting and faster throughput.

### Risk assessment

Specifically, IATA expects the following progress in the risk assessment technologies:

- National Targeting Centers or Passenger Information Units to analyze passenger data and other inputs, implemented in some States, in order to provide input to overall risk assessment,
- Covert and overt behavior analysis techniques deployed at checkpoint with limited connectivity to checkpoint for real-time update to risk score,
- International cooperation and recognition of known traveler programs,
- Dynamic risk score adjustment based on identity is in operation at select checkpoints.

### Technology

IATA expects the following progress in technology in short-term horizon:

- Remote image processing from checkpoint at airport and country levels,
- Identity management system based on travel document (already common at checkpoints across the globe),
- Automated biometric gates to determine access to known traveler lane,
- Risk assessment and identity management systems connected via a secure information network,
- Alternative measures for explosive detection at checkpoint and front-of-house airline processes,
- X-ray technology advancement to enable LAGS screening without any need to divest and no volume restrictions,
- Real-time data collection at checkpoints, such as passenger queue time and throughput, with forecast ability to provide queue time to passenger on-demand via a checkpoint management system,
- Regular deployment of flexible algorithms for X-ray targeted threat detection,
- Passenger security scanners are the primary device for passenger screening.

IATA expects that the aforementioned progress in technology will assist operational improvements as described below.

### Operations

- Separate the known traveler queue and lane with biometric identity authentication at entry,
- Dynamic device monitoring to support operational management decision making,
- Dynamic passenger guidance of screening process and way-finding at the entry and the checkpoint,
- Queue management program to display queue time and customer service support,
- Improved staff allocation, and use of behavior analysis,

- Checkpoint lane design, taking into account IATA Recommended Practice 1701H and passenger experience elements,
- Program for regular passenger feedback that incorporates modern technology.

## IATA vision of the 2020+ checkpoint

IATA introduces its vision of the 2020+ checkpoint using notion of risk assessment, technology, and operations. It is envisaged that the passenger will be able to flow through the security checkpoint without interruption unless the advanced technology identifies a potential threat. A passenger will have a level of security screening based on information from states of departure and arrival through bilateral risk assessments in real-time. In terms of the passenger experience, little to no queues will be encountered as a result of the enhanced speed at which screening can occur; and there will no longer be the burden of divesting by default.

### Risk assessment

According to IATA forecast, the following horizon in risk assessment will be achieved by 2020+:

- Passenger and flight data risk assessment is a common practice, using international cooperation,
- Unpredictable alternative measures are in effect to deter and detect,
- Automated behavior analysis with real-time update of the risk score is provided at the checkpoint,
- The known traveler program and differentiated checkpoint screening program are in place across multiple countries.

### Technology

IATA expects the following progress in technology:

- Stand-off identity management system based on biometric capture and verification,
- Automated biometric gates to confirm eligibility for all passengers regardless of status,
- Real time risk score updates and level of screening decisions,
- Alternative measures for explosive detection, incorporated into checkpoint and front-of-house processes,
- Screening technology, complete with advanced threat detection and dynamic adjustment, based on the risk score of the passenger,
- Remote image processing with automatic decision algorithms,
- Passenger security scanners are the primary device for passenger screening.

### Operations

IATA expects tht the above progress in technology will assist the operational improvements, in particular:

- Dynamic passenger guidance of screening process and way-finding at entry and in checkpoint,
- Queue management program to display queue time and customer service support,
- Improved staff allocation and use of behavior analysis,
- Fully flexible checkpoint lanes able to screen all risk categories of passengers,
- Program for regular passenger feedback that incorporates modern technology,
- Passenger and flight data risk assessments are common practice with international cooperation,
- Unpredictable alternative measures are in effect to deter and detect,

- Automated behavior analysis with real-time update of the risk score to the checkpoint,
- Known traveler program and differentiated checkpoint screening program across multiple countries.

Table B.2 summarizes the roadmap of future border crossing technologies and operations, using both the IATA and ICAO visions [27, 44].

Table B.2: Roadmap of future checkpoint [27, 44].

| Component | 2014 | 2017 | 2020+ |
|---|---|---|---|
| Passenger data | Basic risk assessment | Risk assessment based on wider range of data, national targeting centres | Global, national, international agencies, multi-lateral agreements, data sharing, interoperability |
| Known traveler | Risk assessment through national and bilateral known traveler programs | Expanded bilateral agreement of known traveler programs with mutual recognition of risk assessment | International, interoperable known traveler program with mutual risk assessment |
| Identity management | Biometrics data capture, automated document authentication | Identity confirmation at checkpoint, link to screening decision | Use of e-passports for identity authentication |
| Behavior analysis | Direct questioning. Behavioral observation | Automatic behavior detection. Automated integration with risk assessment | Behavioral characteristic observation (whole of airport) |
| Alternative measures | Explosive detection. Random selection for high risk screening | Document trace detection | Stand-off screening using remote screening technologies |
| Enhanced detection capability | Screen liquids without divesting. Automated detection of weapons. Process improvement for belt and shoe screening | Increased automated detection of explosives. Dynamic adjustment of equipment sensitivity (flexible lanes). Dynamic and risk based deployment of detection algorithms. | Screening of all personal electronics without divesting. Enhanced automated detection of explosives. Leaving coats and jackets on without divesting metals |
| Passenger experience | Checkpoint measurement and management system. Interface standards and approaches for connection of security equipment | Non-invasive approaches to record, measure and assess checkpoint performance | |
| Access and egress | Optimized queue structures for efficient lane utilization and throughput. Improved understanding of security rules and procedures to minimize delays due to non-compliance | | Simplified rules through automation and improved process |
| Non-sequential processing | | Separating the link between the passenger and bag screening process, in order to reduce dependencies and optimize throughput | |
| Remote image processing | Maximizing asset and officer utilization | | |
| Lane design | Improved equipment and process automation to maximize throughput | Flexible lane design for optimum operational efficiency | |

Table B.3: IATA vision of the 2017 and 2020+ checkpoint (sample) [27, 44].

| Today | 2017 | 2020 |
|---|---|---|
| •Remote image processing<br>•Biometric verification<br>•Risk assessment<br>•Explosive detection<br>• X-ray technology<br>•Real time data collection<br>•X-ray threat identification<br>•Security scanners | **Risk assessment:**<br>•National Targeting Centers<br>• Covert and overt behavior analysis<br>•International cooperation and recognition of known traveler programs<br>•Dynamic risk score adjustment<br>**Technology:**<br>•Remote image processing airport and country levels<br>•Identity management system based on travel document (already common at checkpoints across the globe)<br>•Real-time data collection<br>•Automated biometric gates to determine access to known traveler lane[1]<br>**Operations:**<br>•Separate the known traveler queue and lane with biometric identity authentication at entry[1]<br>•Dynamic device monitoring to support operational management decision making<br>•Queue management program<br>•Improved staff allocation, and use of behavior analysis | **Risk assessment:**<br>•Passenger and flight data risk assessment is a common international practice<br>•Automated behavior analysis with real-time update of the risk score<br>•The known traveler program is in place across multiple countries<br>**Technology:**<br>•Stand-off identity management system based on biometric capture and verification<br>•Automated biometric gates to confirm eligibility for all passengers<br>•Real time risk score updates<br>•Alternative measures for explosive detection<br>•Remote image processing<br>•Security scanners<br>**Operations:**<br>•Dynamic passenger guidance of screening process<br>•Queue management<br>•Improved staff allocation and use of behavior analysis<br>•Automated behavior analysis with real-time update<br>•Known traveler program across multiple countries |

[1] This is a particular IATA's view. The ABC machine is able to serve all travelers including trusted travelers. However, if ABC machine is not deployed, biometric enabled kiosks can provide verification of trusted travelers (*Comment by V. Shmerko and S. Yanushkevich*).

# Appendix C

# Roadmap for ABC standards

One of the objectives of this study was to contribute to better standards, including vocabulary, related to the use of biometrics for automated border control. This section presents a highlight from the University of Calgary report [10], which is develops a roadmap on developing standards for ABC technologies and which proposes to introduce a new Package of standards (Package III) specifically to address the analysis of all phases of life-cycle of ABC systems.

Additionally, the recommendations on the extended and revised vocabulary of biometric terms suitable for automate border control application is developed in [5], the excerpts of which are presented in Appendix D.

## C.1 Hierarchy of standards

**Contributed by V. Shmerko and S. Yanushkevich (Adapted from the chapter "Analysis of related standards" from [10]).**

At the start of the study, two packages of existing international standards that address ABC machine development, prototyping, evaluation, and exploitation are identified, summarized below.

### C.1.1 Package I: IEC 60300 standards

The first package of standards that needs to be consulted in relationship to the operation and performance of ABC systems (hereafter refered to as Package I) is the IEC 60300 Package on dependability management of large-scale systems developed by International Electrotechnical Commission (IEC IEC 60300). These standards address all phases of lifecycle of generic complex system in the area of deployment, operational requirements, and performance, briefly described below.

The basic standard "Dependability management systems", IEC 60300-1 (2003-06), provides key operational requirements, performance metric, and deployment requirements to generic computing system. This standard is supported by other standards such as "Guidelines for dependability management" (IEC 60300-2), "Analysis techniques for dependability" (IEC 60300-3-1), "Collection of dependability data from the field" (IEC 60300-3-2), "Life cycle costing" (IEC 60300-3-3), "Guide to the specification of dependability requirements" (IEC 60300-3-4), "Hazard and operability studies" (IEC 61882), "Risk management" (ISO 31000), etc. A summary of these and related standards is presented in Table C.1.

### C.1.2 Package II: ISO SC 37 of standards

The second package of standards relates to the specific-purpose biometric enabled component of the ABC system and is established by the International Organization for Standardization (ISO) and the International

Table C.1: Common standards provided by International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO) in the area of deployment, operational requirements, and performance of computer systems.

| Standard | Functions |
|---|---|
| Dependability management systems IEC 60300-1 (2003-06) and Guidelines IEC 60300-2 (2004-03) | (a) Concepts and principles of dependability management systems.<br>(b) Identifies the generic processes in dependability for planning, resource allocation, and control.<br>(c) Guidelines for dependability management of product design, development, evaluation and process enhancements. |
| Analysis techniques for dependability IEC 60300-3-1 (2003-01), Collection of dependability data from the field IEC 60300-3-2 (2004-11) | (a) General overview of commonly used dependability analysis techniques.<br>(b) Guidelines for the collection of data relating to reliability, maintainability, availability and maintenance support performance of items operating in the field. |
| Life cycle costing IEC 60300-3-3 (2004-07) | (a) Highlights the costs associated with dependability of the product.<br>(b) Explains the purpose and value of life cycle costing.<br>(c) Identifies typical life cycle cost elements.<br>(d) Guidance for conducting a life cycle cost analysis, including life cycle cost model development. |
| Guide to the specification of dependability requirements IEC 60300-3-4 (2007-09) | The content on availability, maintainability and maintenance support has been updated |
| Design review IEC 61160 (2005-09) | (a) Recommendations for the implementation.<br>(b) Provides specific details in reliability, maintenance, maintenance support and availability. |
| Mathematical expressions for reliability, availability, and maintainability IEC 61703 (2001-09) | Mathematical expressions for reliability, availability, maintainability and maintenance support measures |
| Hazard and operability studies IEC 61882 (2001-05) | Provides a guide for Hazard and operability |
| Requirements for functionality and tests IEC 62309 (2004-07) | (a) The concept to check the reliability and functionality.<br>(b) Criteria about the tests/analysis. |
| Ergonomics of human-system interaction ISO 9241 | A multi-part standard covering various aspects of ergonomics of human- computer interaction using hardware and software platforms. |

Electrotechnical CommissionâĂŹs Joint Technical Committee 1 (ISO/IEC JTC1) which in 2002 established subcommittee 37 âĂŞ- Biometrics (SC37) to facilitate the development standards in the field of biometrics.

Table C.2 summarizes Package II of standards that are developed by ISO SC 37 subcommittee. These standards include data collection formats, technical interfaces, data exchange and storage formats, data transmission profiles, as well as the standards on attacks and countermeasures, which is further discussed below.

External organizations, such as the International Civil Aviation Organization (ICAO), have also adopted many of these standards.

A sample of released ISO standards that support the Package II of standards are listed below[1].

ISO/IEC 14443 Identification cards, ÂŰ Contactless integrated circuit cards, ÂŰ Proximity cards,

ISO/IEC 19784-1:2006, Biometric application programming interface, Part 1: BioAPI specification,

ISO/IEC 19794-2:2011, Biometric data interchange formats,

ISO/IEC 19794-5:2011, Information technology ÂŰ Biometric data interchange formats, Part 5: Face image data,

ISO/IEC 7816-11:2004, ISO/IEC TR 24722:2007, Biometrics, ÂŰ Multimodal and other multi-biometric fusion

Table C.2: Sample of ISO SC 37 Package II of standards [170].

| Standard | Function | Examples |
|---|---|---|
| Data Exchange and Storage Formats | Specify: (a) the content, meaning, and representation of formats for the interchange of biometric data, (b) notation and transfer formats that provide platform independence, and (c) transfer syntax from content definition. | • ISO/IEC 19794-6:2005 Biometric Data Interchange Formats, Part 6: Iris Image Data;<br>• ANSI/NIST-ITL 1-2007 Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information;<br>• ANSI/NIST-ITL 2-2008 Type-10, Capture and Storage of Face Images;<br>• ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information. |
| Technical Interfaces | Specify interfaces and interactions between biometric components and subsystems, add plug-and-play capability to integrate system components into functioning systems | • ANSI INCITS 358-2002 BioAPI Specification (Version 1.1);<br>• ANSI INCITS 398-2008 Common Biometric Exchange Formats Framework |
| Transmission Profiles | Facilitate interoperability, specify application-specific criteria onto a base standard or enumerating values for optional or conditional requirements such as full-frontal face vs. token face | • FBI and DOD Electronic Biometric Transmission Specification,<br>• Interpol Implementation of ANSI/NIST-ITL 1-2007,<br>• IDENT Exchange Messages (IXM) Specification |
| Testing and Reporting | Specify biometric performance metric definitions and calculations, approaches to test performance, and requirements for reporting the results of these tests. | ANSI INCITS 409-2005 Biometric Performance Testing and Reporting:<br>(Part 1: Principle Framework; Part 2: Technology Testing Methodology Part 3: Scenario Testing Methodologies) |
| Cross-Jurisdictional and Societal | Address study and standardization of technical solutions to societal aspects of biometric implementations | • ISO/IEC 24714, Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies;<br>• ISO/IEC 24779, Pictograms, Icons, and Symbols for Use with Biometric Systems |

[1] Published ISO/IEC Standards are available from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on

### C.1.3 The need for additional package of standards

The ABC technologies are rapidly developing, and this presents challenges in the area of standardization. In the next section, we present strategic directions of the ABC technology standardization. Our analysis of the area suggests that existing ISO Package I and Package II do not cover the complete life-cycle of the ABC systems, and additional ISO standards and recommendations need to be developed. We suggest a systematic approach for the development of such package of standards and recommendations, called in this technical report *ISO SC37 Package III*, in order to overcome the gap between the existing ABC technologies and requirements to international standards.

## C.2 Package III: "ABC technologies"

### C.2.1 Goals and objectives

The overall goal of the new ISO SC37 Package III is to provide recommendations that address all phases of life-cycle of ABC systems. The objectives of the ISO SC37 Package III include the development of recommendations on terminology, overall description of process, metrics, vulnerability, modeling, proving ground, mobile applications, issues of global network, privacy issues, training personnel, pandemic prevention and counter-terrorism.

Sub-goals of our study can be specified by national and international needs in the development of various regulations regarding ABC technologies including personnel training and the development strategic plans.

#### Motivations

The state-of-the-art contemporary ABC technologies, as well as current trends in the ABC technologies are introduced in the IATA and ICAO roadmaps [27]. The mentioned that new initiatives are required for standardization in this area. The ABC machines and technologies possess a number of properties that make them different from the known systems and technologies. Specifically, ABC system is defined as

- biometric-enabled,
- large-scale,
- semi-automated,
- distributed,
- social-embedded,
- authentication-based

system, which can operate only in a specific infrastructure. These properties reflect the fact that the ABC system is an integrated high-complexity system. In the well-known publications and ISO SC37 documents, the ABC machines and technologies are associated with biometric devices and systems. However, the contemporary real-world ABC machines, deployed worldwide, cannot be simply defined in terms of biometric systems and devices. Specifically, we assert the following:

1. The standards from ISO Package I are appropriate for all phases of the ABC machine life-cycle. However, because the ABC technologies are highly dynamic and essential part of international border infrastructure, minimal latency regarding standardization is expected. In addition, the generalized complex machine properties must be specified based on the specific-purpose functions of the ABC machines. For example, the essential metrics of an ABC machine is the depth of its embedding into social infrastructure, which plays an important role at traveler risk evaluation. These metrics are absent in the definition of the generalized complex machines (Package I).

2. The standards from ISO SC 37 Package II address all phases of life-cycle of the key components of ABC machine. However, the ISO SC 37 Package II recommendations are limited and cannot be taken into consideration at the highest levels of analysis and description of the ABC machine.
3. The ISO SC 37 Package III aims at meeting the practice demand. Based on the fundamental value of the standards from Package I and Package II, the ISO Package III should help to deal with the new reality of the ABC technologies which are different from generalized complex machines (Package I) and biometric systems (Package II). For example, risks of a deployed biometric system represent a subset of the risks pertaining to an ABC machine. However, the performance of the ABC machine is estimated using a subset of performance metrics of a biometric system.

It should be noted that several documents related to the ABC technologies are under development by ISO SC 37. It demonstrates that the SC 37 attempts to support the ABC technologies developers and users. In this technical report, we suggest a systematic way to do so in the form of a standardization portfolio called ISO SC 37 Package III.

### C.2.2 Strategic directions for standardization

We introduce 11 strategic directions for standardization of the ABC technologies. These directions constitute the ISO SC 37 Package III. This package includes standards and recommendations for supporting the ABC systems at all phases of the ABC system life-cycle, in particular:

**1. Terminology of the ABC technologies.** These recommendations are based on ICAO, IATA, and Frontex initiatives [36, 29, 43, 170, 27], as well as contribution of this technical report (Chapter 1). We suggest to distinguish the following classes of the ABC technologies:

- e-border technologies,
- biometric technologies,
- traveller risk assessment technologies, and
- complex system management.

**2. Passenger flow processing in the ABC technologies.** Simplification of border crossing via ABC technologies means the shift of human-human (that is, border officer-traveler) interactions to human-machine (that is, traveler-machine) and machine-machine interactions[2]. The IATA and ICAO provide taxonomy for passenger flow processing in the ABC technologies [27]. The ISO initiatives in this direction are in great demand[3].

**3. Vulnerability of the ABC technologies.** The ABC technology vulnerabilities must be considered in a broader context than that recommended by the existing ISO documents[4]. In particular, the ABC technologies requires specific consideration in the following directions of security:

[2] K. Noyes, For the Airline Industry, Big Data Is Cleared for Take-Off, Fortune (June 19, 2014), http://fortune.com/2014/06/19/big-data-airline-industry/

[3] In 2009, initiated by UK and New Zealand, ISO SC 37 has initiated a technical report document aimed at developing the recommended best practices and processes for ABC systems using biometrics, specifically, using biometrics to verify and identity a claim by a traveller who uses an ePassport or an equivalent identity card as the basis for the claim. By the time of writing the current report, this document is still in a draft state and is not available to public.

[4] The ISO/IEC 24745:2011 standard outlines countermeasures, such as: Analysis of threats and countermeasures inherent in a biometric-based application models, Security requirements for binding between a biometric reference and an identity reference, Biometric system application models with different scenarios for the storage and comparison of biometric references, and Guidance on the protection of an individual's privacy during the processing of biometric information. Standard ISO/IEC 30107 provides details on attacks classification and their detection.

- Security Risk,
- Security Controls,
- Security Mechanisms,
- Security Architecture,
- Security Policies.

Specifically, the vulnerabilities of the ABC technologies are defined in the context of possible interaction scenarios between human and machines, such as

1. *Human-Human* (border officer – traveler) interactions,
2. *Human-Machine* (traveler – ABC machine, border officer – ABC machine) interactions,
3. *Human-Machine-Human* (traveler – ABC machine – border officer) interactions,
4. *Machine-Human-Machine* (ABC machine – traveler (border officer) – ABC machine) interactions, and
5. *Machine-Machine* (ABC machine – ABC machine) interactions.

In these scenarios, a risk factor that is assigned to each traveler is a critical factor, because it can initiate an arbitrary chain of interactions between humans and machines.

**4. The e-Border management guide.** The e-Border concept combines various breakthrough achievements and innovation solutions from various areas, in particular, from local and global communication, intelligent processing and machine-human interactions, biometrics, decision-making under uncertainty, and user-centric design and operation of large-scale machines. It includes biomedical, social, cultural, psychological, and geographical aspects. The very first e-Border was embodied in the Home Office program developed in 2003 (UK) to improve border security [72]. To the best of our knowledge, no taxonomy or recommendation for standardization exists in the area of e-border. We define the e-border (see Chapter 2) as an infrastructure for border crossing that operates in the controlled environments such as

- e-gates,
- e-passports and e-IDs,
- e-visas,
- e-health and e-medicine, and
- personnel e-training.

Special consideration should be given to potential recipients from e-health care units because the future ABC technologies will support e-health and e-medicine for travelers. The e-border infrastructure also includes local or/and global communication, databases, risk assessment technologies, and logistics. The e-border infrastructure assessment is critical for ABC technologies. To the best of our knowledge, there are no initiatives that pursue development of a standardized e-Border management guide.

**5. Metrics for the ABC technologies.** Various metrics are needed for the assessment of the ABC technologies, in particular,

- Service *Availability* Metrics,
- Service *Reliability* Metrics,
- Service *Performance* Metrics,
- Service *Scalability* Metrics, and
- Service *Resiliency* Metrics.

The existing ISO recommendations only partially cover these needs. Technical reports of this study contribute to this area. In addition, we have introduced our vision on the relationship between these metrics and various phases of the ABC machine life-cycle, including personnel training.

**6. Modeling of the ABC technologies.** There are various valuable ISO documents related to the statistical evaluation of technologies. Developing recommendations on modeling technical systems is extremely complex. However, the ABC machine is a well-defined specific-purpose complex system. Modeling is a crucial procedure which addresses all phases of the ABC machine life-cycle. For example, it is impossible to make a decision about a technology deployment without modeling of the following typical tasks or properties:

- deployment scenarios,
- vulnerability,
- predicted cost and performance,
- reliability,
- requirements to supporting infrastructure,
- countermeasures, and
- personnel training.

As a rule, modeling is a multi-criterion task carried under many uncertainties. There are various approaches to modeling which are distinguished with respect to scale of the problem, its complexity, and goals.

Moreover, the framework of modeling includes different philosophies of uncertainty understanding, such as Bayesian probabilistic approach, Dempster-Shafer evidential theory, and fuzzy logic models. Application of these models to the same ABC task may provide different results. They should be correctly interpreted, and such interpretation can be facilitated by developing appropriate ISO recommendations.

**7. Proving ground of the ABC technologies.** Scenario-based testing area, or proving ground, is needed because of high complexity of the ABC technologies and supporting infrastructure. In contrast, testing of biometric devices and system does not require special conditions. Examples of proving ground are DHS testing areas [64, 65]. Traditional testing and modeling of biometric devices and systems must be extended, in particular, in the following directions:

- Compatibility of all components, including the work of electromagnetic bands,
- Vulnerability of RFID infrastructure,
- Real-time modeling of cyber-attacks, counter-terrorism modeling, and personnel training,
- Real-world logistics modeling.

The ISO SC 37 has started developing the recommendations on best practices and processes in the above directions.

**8. Mobile ABC technologies.** It is apparent that the role of mobile authentication systems, including the ABC machines, will eventually increase. There are no standards regarding mobile ABC machines. However, NIST publication SP 500-280 provides guidance and operational requirements for mobile ID devices; it can be used as a starting platform for developing the recommendations on mobile ABC machines. There are many aspects of the mobile ABC which should be harmonized with the basic requirements to mobile biometric devices and systems [127], in particular:

- Architectural issues, including area of secure architecture,
- Portable RFID-based passports/IDs scanners and their vulnerability,
- Operational reliability in complex electromagnetic infrastructure,
- Management in complex authentication infrastructure, including physical and cyber-attack countermeasures,
- Testing of mobile devices and supporting infrastructure, including proving ground facilities, and
- Personnel training.

**9. The ABC global network.** According to IATA and ICAO roadmap [27], future ABC machines will communicate using a Global ABC-machine Network (GAN).

The radical difference of the GAN from contemporary semi-automated ABC machines that operate under border officer supervision (*Human-Machine* interactions) is that GAN implements *Machine-Machine* interactions, and their ultimate targets are travelers worldwide. A GAN may try to answer the questions:

- Who is this traveler?
- How risky is this traveler to other humans?

To do so, the GAN should retrieve information about the traveler from social networks. Thus, GANs have to be embedded in social infrastructure. This means that the GAN should be allowed to use various government and financial databases with personal information, social networks, and surveillance data.

**10. The ABC technologies for pandemic prevention and counter-terrorism.** The ABC technologies are frontiers of national and international efforts of prevention and counter-terrorism. According to IATA and ICAO roadmap [27] as well as strategic DHS developments [64, 65], the ABC technologies will be able to obtain early warning information by monitoring traveler health conditions at distance (called soft biometrics) [161]. Interview supporting machines with a virtual security officer help to prevent contacts of suspected travelers with personnel and other people [133, 92]. After identifying pandemic features (geographical, as well as biological measurements such as temperature, blood pressure, etc.), traditional technologies for human authentication can be used. Applications of ABC technologies for counter-terrorism is the focus of many studies such as [22, 82].

Recommendations for standardization, in particular, for the following tasks are needed:

- List of non-contact health condition measurements, processing, and management,
- Interview supported machines for non-contact health condition monitoring,

**11. Training of the ABC personnel.** Requirements for the ABC personnel qualifications increase in unison with technology maturing. For example, in the area of cyber-terrorism, operators of the next generation of the ABC machine should make decisions in the presence of insufficient data, denial of service outbreaks, virtualization attack, changing attacker's type (anonymous or trust exploitations attacker), traffic eavesdropping, malicious intermediary, and other aspects of security risks and challenges. It is expected that ISO recommendations will help to manage personnel training, in particular, by addressing the following questions:

- How to evaluate the skills of the ABC machine personnel steadily and automatically, while making sure that their skills are not critically degraded?
- How to use the ABC machine in a training mode? What are the requirements for additional tools, such as virtual biometric simulators, imitator of operational scenarios, including attack simulators?
- How to manage the automated short-term intensive training of personnel?

These and related problems are considered, in particular, in [156].

# Appendix D

# New age glossary of biometrics terms for automated border control applications

One of the objectives of this study was to contribute to better standards related to the use of biometrics for automated border control. This included reviewing and revising the existing vocabulary of biometric terms, which had been found insufficient for the application.

In effort to set a frame of reference for the development of new biometric terms for automated border control applications a separate report [5] is being prepared, the excerpts of which are presented below for discussion with the community.

## D.1 Introduction

New applications demand for the revision and extension of the existing terminology. This is becoming the case with biometrics – the technology for automated recognition of people from their biological characteristics. Originally applied to closed-set applications such as membership programs, physical security and forensics, where the number of processed subjects is known and limited, it is now increasingly extended towards open-set applications, such as automated border control and video surveillance, where the flow of processed subjects is very high, possibly unlimited, and subjects are not known in advance to the system, exhibiting a large range of skills, motivations, appearances. Such a shift in the application of biometrics results in a much higher chance of the system failure, through either an intentional or unintentional attack on its vulnerabilities, and requires the development of new biometric design, evaluation and deployment practices, which calls for the revision and extension of the existing biometric concepts and vocabulary.

The outcome of the several years of work on the DRDC-funded *PROVE-IT(FRiV)* and *"ART in ABC"* studies conducted by the CBSA in partnership with several academic, government and industry partners, this report proposes new and revised biometric terms recommended for automated border control and video surveillance applications.

## D.2 Normative references

ISO standards on "Biometrics" are developed by Sub-committee on "Biometrics" (SC 37). The latest approved revisions of the following related documents are freely available at http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html: ISO/IEC 2382-37:2012, Information Technology "*Vocabulary. Part 37: Biometrics*". ISO/IEC TR 24741:2007 Information technology - "*Biometrics Tutorial*". ISO/IEC TR 24714-1:2008, Information technology – "*Biometrics – Jurisdictional and societal considerations for commercial applications – Part 1: General guidance*".

Other key references on Biometric vocabulary include DoD Common Biometric Vocabulary developed by the Defense Forensics and Biometrics Agency (DFBA) Architecture Branch found at http://www.biometrics.dod.mil/Files/Documents/References/common%20biometric%20vocabulary.pdf and International Biometrics Industry Association (IBIA) Glossary developed by National Science & Technology Council's (NSTC) Subcommittee on Biometrics found at https://www.ibia.org/biometrics/glossary.

## D.3 Terms categorization

The following categorization of the biometric terms is suggested:

1. **General terms** related to recognition of human identities and their attributes, including those related to non-biometric recognition of human identities and attributes;
2. **Core biometric recognition terms**, i.e. those related to measuring human biometric characteristics for the purpose of recognizing his/her identity or attribute;
3. **Terms related to machines and technology** that execute biometric recognition, including:

   (a) terms related to technology design;
   (b) terms related to technology operators;
   (c) terms related to technology performance and evaluation;

4. **Terms related to people** that are being subject to biometric recognition;
5. **Terms related to specific applications: Automated Border Control**;
6. **Terms related to specific applications: Video Surveillance**.

## D.4 General terms

**recognition**: identification of a thing or a person from previous encounters or knowledge (from http://www.oxforddictionaries.com); the act of knowing who or what someone or something is because of previous knowledge or experience (from http://www.merriam-webster.com/dictionary/recognition).

NOTE 1: In relationship to a person, two key types of recognition (See **person authentication** and **person classification** below): 1) recognition related to person's identity (e.g., "She is Joanne Doe"), and 2) recognition related to person's attribute such as class, race, age, medical condition, or his/her other visually distinguishable features (e.g., "She is a young, dark-eyed, African, muslim, tired, with speckles, with acne, with Ebola symptoms, woman").

**automated recognition**: recognition by means of a computer device or an algorithm.

NOTE 1: automated recognition may or may not involve assistance from a human. When automated recognition leads to the final recognition result, it is referred to as **fully-automated recognition**. When it requires a human involvement to obtain the final recognition result, it is referred to as **semi-automated recognition**.

NOTE 2: automated recognition may involve one stage (*recognition as act*) or many recognition stages, each yielding additional piece of knowledge (*recognition as process*).

**authentication = person authentication = person identity recognition**: recognition of person's identity

NOTE 1: authentication can be achieved with or without a claim about person's identity (See **identity verification** vs. **identification** below).

NOTE 2: authentication can be done by using biometric information, (e.g., by using facial images, which compared by either a human or a machine) or by using non-biometric information (e.g. by using documents or **cybermetric**).

**person classification = person attribute recognition**: recognition of person's attribute(s) such as his/her class, race, age, medical condition, or other visually distinguishable features.

NOTE 1: Two types of person's attributes exist: *short-term attributes* (such as person's emotion, level of stress or medical condition) and *long-term attributes* (such as age, gender, race). In some cases, short-term attributes may become long-term ones.

NOTE 2: Person attribute recognition may contribute or be part of the recognition process leading to person identity recognition.

**cybermetric**: authentication of a person from his/her interactions and circle of friends in social networks, such as Facebook or Google+ (adopted from [123]).

**identity verification**: authentication of a person by means of validating (proving or disproving) the claim related to the person's identity.

**identification**: authentication of a person in which a claim related to the person's identity is not made.

**verification**: recognition by means of validating (proving /disproving) the claim related to person's identity or type.

NOTE 1: Applicable to both person authentication and person classification.

**closed-set recognition**: recognition in which a thing or a person being recognized was previously memorized (seen/leant) by the system/person who is recognizing it/him/her.

**open-set recognition**: recognition in which a thing or a person being recognized may or may not be previously memorized (seen/leant/stored) by the system/person who is recognizing it/him/her.

NOTE 1: in automated recognition, closed-set recognition is equivalent to 1-to-N search, where N is the number of things/persons memorized by the system.

NOTE 2: Person classification is a close-set recognition by definition (recognition among fixed number of classes or attributes).

NOTE 3: In automated border control applications, processing of pre-enrolled registered travellers is part of close-set recognition. In contrast, processing of all travellers holding an e-pasport is part of open-set recognition.

NOTE 4: In video surveillance applications, any person identification (whether it white-list/member recognition or black-list/watchlist recognition) is open-set recognition.

**memorization**: committing to memory (from http://www.oxforddictionaries.com), i.e. storing the information about a person or a thing.

NOTE 1: Also known as enrollment, as in enrolling a person into a data-base.

## D.5 Core terms related to biometric recognition

**biometric recognition = biometrics**: automated recognition of person's identity or attribute based on his/her biometric characteristics

NOTE 1: This definition extends current ISO definition of biometrics to include the recognition of person's attribute.

Compare to current ISO definition – **biometrics**: automated recognition of individuals based on their biometric characteristics.

NOTE 2: Commonly, machine learning algorithms that are used to person's identity recognition may also be used to perform person's attribute recognition.

**biometric characteristic = biometric feature**: biological and behavioural characteristic of an individual from which *distinguishing*, *repeatable* biometric features can be extracted for the purpose of biometric recognition.

NOTE 1: This definition extends current ISO definition of biometrics features to include the features that are distinguishable and repeatable with respect to a human attribute or class, such as features of a female (young, stressed etc.) face.

NOTE 2: This definition also recommends using both terms (characteristic and feature) as synonyms, as opposed their current definitions by ISO as two different terms. The reason is that in other languages, both terms often mean the same thing (In French feature is translated as "characteristique"). This will also reduce confusion caused by multiplicity of definitions (biometric data vs. biometric characteristic vs. biometric feature vs. biometric sample vs. biometric template vs. biometric model)

Compare to current ISO definitions –

**biometric characteristic**: biological and behavioural characteristic of an individual from which distinguishing, repeatable **biometric features** can be extracted for the purpose of **biometric recognition**.
**biometric feature**: numbers or labels extracted from **biometric samples** and used for comparison.
**biometric sample:** analog or digital representation of **biometric characteristics** prior to **biometric feature** extraction.
**biometric data:** biometric sample(s) at any state of processing, e.g. biometric reference, biometric probe, biometric feature, biometric property
**biometric model:** stored function generated from biometric data
**biometric template:** reference biometric feature(s)

**biometric sample:** data captured from a biometric sensor that can be recorded as a biometric reference for person's identity or attribute or used for comparison with previously recorded biometric reference data to verify or identify person's identity or attribute

**biometric template:** a machine representation of a biometric sample.

## D.6 Related to technology design

**biometric-enabled system:** system that performs biometric recognition.

EXAMPLE 1: *Automated Border Control (ABC)* e-gates and kiosks that use iris-, fingerprint- or face-recognition for verifying or identifying travellers.

**biometric-capable system:** system that has sensors sufficient for biometric recognition but which does not perform biometric recognition.

NOTE 1: In many cases, systems are called biometric-capable if they, despite having adequate sensors, are not performing biometrics due to some other reasons such as poor lighting, camera placement or privacy/legal considerations.

EXAMPLE 1: *Automated Passport Control (APC)* kiosks equipped with high-resolution cameras do not perform biometric recognition but are biometric-capable.

EXAMPLE 2: High-resolution surveillance camera capable of capturing faces at the resolutions sufficient for person classification or identification (more than 20 or 60 pixels between the eyes) may potentially be used for biometric recognition under proper lighting and motion constraints if allowed by policy-makers.

**biometric modality:** type of biometric characteristic (biometric feature) used for recognition

EXAMPLE 1: Iris modality – a picture of eye or two eyes, showing iris. It normally also includes ocular and periocular regions.

EXAMPLE 2: Face modality – a picture of a face, showing eyes, nose and mouth. Some of facial features may be occluded or not visible.

NOTE 1: In certain cases, one modality may contain information about the other modality. E.g. high-resolution face images contain information related to iris modality. Iris modality, contains information on ocular regions, which may be used by itself.

**biometric mode**: type of system operation which uses a particular biomeric modality

**multi-modal biometrics:** biometrics that uses several modalities

NOTE 1: This corrects current ISO definition. According to the new definition, a system that uses several recognition algorithms or sensors on the same facial image is not called multi-modal.

Compare to current ISO definition – **biometric mode**: combination of biometrics characteristic types, sensor types or algorithms.

NOTE 2: This definition also corrects confusion between biometric modality and *biometric mode*, which are currently defined as synonyms.

**biometric ergonomics:** the layout of the biometric system and the biometric process.

**biometric life-cycle:** stages of biometric system design, prototyping, deploying, and dismantling.

EXAMPLE: Iris recognition kiosks for trusted travelers deployed in UK in 2003 were dismantled in 2013. The life-cycle of these systems including their development is about 10 years.

## D.7 Terms related to technology performance and evaluation

**False Match and False Non-Match**: two types of recognition errors that can be exhibited by a biometric-enabled system when comparing a probe biometric sample to a reference biometric sample.

**False Accept and False Reject**: similar to False Match and False Non-Match, however may also be used in reference to final outcome of the recognition decision, which could be the result of multiple comparisons.

NOTE 1: In matching to a watch-list and, in particular, in video surveillance applications, terms False Match / Non-Match are normally used.

NOTE 2: In border control applications, where a person is matched to the picture in his/her passport, terms False Accept / Reject are normally used.

**Transaction-based performance analysis**: analysis of the system performance that reports the number of system successes / failures with respect to the number of transactions performed by the system.

NOTE 1: This is a commonly used analysis, defined by current ISO standards, that reports False Match and Non-Match Rates (FNMR, FMR) and related error-trade off curves.

**Subject-based performance analysis**: analysis of the system performance that reports the number of system successes / failures with respect to the number of subjects processed by the system.

EXAMPLE 1 (from [108]): Statistics from an eGate pilot in a Spanish airport showed that over a period of one month, the gate was used by Danish citizens 22 times, of which 4 times it rejected a person. Reported in the paper (transaction-based) False Reject Rate is $4/22 = 18\%$. However if it was the same person who was rejected 4 times, then subject-based False Reject Rate will be lower than 18%. Similarly, if in 18 cases when the system accepted a person, it was the same "frequently-travellering" person who used the system, then subject-based False Reject Rate will be substantially higher than 18%.

EXAMPLE 2 (from [143], see also Table E.2): The evaluation of an iris-recognition algorithm for the Nexus trusted traveller program has shown that at the operational level of FMR=0.1%, subject-based FNMR (12%) of the system is three times higher than its transaction-based FNMR (4%). This is the indication that some travellers are harder to recognize than others.

**Operational reject rate (ORR):** number of false rejections due to system or process limitations as a proportion of the total number of biometric claims that ought to have been accepted.

NOTE 1 : As opposed to False reject rate (FRR) and False non-match rate (FNMR), which report the failure of the system with respect to limitation of a biometric algorithm, operational reject rate is used to report the failure of the system with respect to all factors that are present in the recognition process, including technology-related factors and human-related factors.

EXAMPLE (from [112]:) The operational reject rate of e-gates in Germany is 12%, of which 5% is due to face verification failure (FNMR = 5%) and 7% is due to other non-biometric-related factors.

**attack**: the information channel, mechanism, procedure or data path that results in system's error. **threat** is the possibility of an attack.

NOTE 1: Two key outcomes of an attack are: false reject and false accept

**zero-effort attack**: attack that was not intentional.

EXAMPLE 1: Traveller was falsely matched to a criminal in watchlist by an e-gate, resulting in his/her false rejection by the system.

EXAMPLE 2: Traveller was falsely non-matched to his/her own picture in a passport, resulting in his/her rejection by the system.

**non-zero-effort attack**: attack that was intentional.

**spoofing:** a type of non-zero-effort attack in which an artifact, false data or a false biometric claim to be legitimate is presented in an attempt to circumvent the biometric system controls.

EXAMPLE 1: A criminal used make-up, glasses, hairstyle etc. so that he/she is not matched to a watchlist image (resulting in false non-match)

EXAMPLE 2: A criminal used a face mask so that he/she will be matched to the picture on the illegally acquired passport (resulting in false match).

**modeling and simulation**: a technique for estimating system errors over its life-cycle by replacing real-life processes by their appropriate mathematical models.

NOTE 1: The information obtained though modeling and simulation can be interpreted in terms of predicted, or potential, events, threats, and risks.

EXAMPLE: Estimation of Operational reject rate of an ABC system by means of modeling its performance with a simulation software that takes into account all factors that affect the system performance.

**biometric template aging = biometric modality aging** degree to which a biometric template changes due to aging of a biometric feature, resulting in the increase in error rates.

NOTE 1: This definition changes the current ISO definition of aging , in order to resolve the confusion around aging that has been caused by claims about "aging" vs. "non-aging" of iris.

NOTE 2: If a person's feature (such as iris or face) changes with time, but a biometric system is able to detect and rectify this change, meaning that the performance of the system is not getting worse (i.e. system error rates do not increase), that it is said that this modality is not aging.

Compare to current ISO definition – **reference aging:** The changes in error rates with respect to a fixed reference caused by time-related changes in the biometric characteristic, its presentation, the sensor and other components of the biometric technology.

## D.8 Related to people:

**usability:** extent to which a product can be used by specified individuals to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.

**subject = data subject**: individual who provides biometric data or biographical data for storage, processing or comparison, or about whom such data is collected by others.

**target subject = target:** a person from a what-list whom a system attempts to detect/recognize in a flow of data.

**probe subject = probe**: individual whose biometric data is being processed by the system.

**cooperative subject**: individuals who participate in recognition process and are motivated to be recognized by the system.

**non-cooperative = unaware subject:** individuals who are not aware of the system operation and may or may not be motivated to be recognized by the system.

**un-cooperative subject = evasive subject**: individuals who are motivated to be not recognized by the system.

**member list** instead of *white-list.*

**watch-list = wanted list** instead of *black-list*.

NOTE 1: To avoid racial associations.

EXAMPLE: As in http://www.cbsa-asfc.gc.ca/wc-cg/wanted-recherchees-eng.html

# Appendix E

# Subject-based performance analysis of Nexus biometric kiosks

One of the key objectives of this study was to perform subject-based analysis of iris and face biometric recognition performance. The outcome of this work, combined with previous work conducted by the CBSA on comprehensive biometric evaluation [141, 142, 143] and iris performance limits analysis [144, 145], is published as a separate report [5], excerpts of which are presented below for discussion with the community.

## E.1 What is subject-based analysis ?

The fact that some people are intrinsically much harder to recognize than others by a biometric system is very well known to biometric system developers [214]. Adversely affecting some groups of biometric system users, this phenomenon is called "biometric menagerie" or "Doddington Zoo", according to the original work of NIST researchers who discovered and reported it on voice recognition systems. It is best described by the images from the comprehensive tutorial on this subject by Norman Poh "System Design and Performance Assessment: A Biometric Menagerie Perspective" [214] (Figure E.1), which define four types of people, with respect to how well they are recognized by a biometric system. In the context of ABC, these four types of people are rephrased as follows:

1. "sheep" (satisfied with system and causing no security risk): majority of travellers who rarely/never get False Match or Non-Match errors,

2. "lambs" (satisfied with system but causing security risk): travellers who rarely/never experience False Non-Match, but who may cause frequent False Non-Match errors thus creating higher security risk for the system,

3. "goats" (not satisfied with system but causing no security risk): travellers who frequently experience False Non-Match problem, but do not cause False Non-Match errors,

4. "wolf" (not satisfied and causing risk) travellers who frequently get both False Match or Non-Match errors.

The presence of different types of travellers means that even though the average performance of a system (measured in false reject/accept rates averaged over all transactions) may be good, the system may still perform very poor with certain "non-satisfied" subjects, who simply do not use the system as often as "satisfied" subjects.

The concept of subject-based analysis is therefore introduced to allow researchers and agencies to better quantify and understand the performance of their systems.

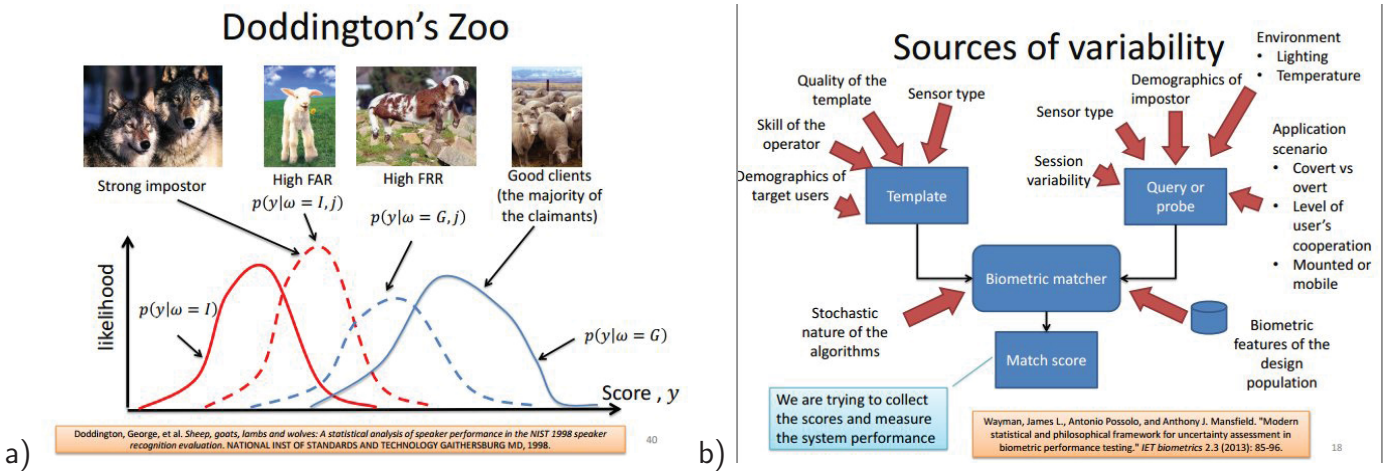



Figure E.1: Subject-based analysis: a) Four main types of recognition results - categorizing all users into four groups "sheep", "goats", "lamps" and"wolfs", b) Reasons for system performance variation (Reproduced with permission from Norman Poh, IJCB 2014 tutorial "System Design and Performance Assessment: A Biometric Menagerie Perspective")

---

**Definition E.1.1 Subject-based performance analysis** *of a biometric system is based on metrics that measure the number of subjects who are falsely matched/non-matched the system, as opposed to transaction-based analysis, currently used by industry [172] that is based on measuring the number of matched/non-matched transactions.*

## E.2 "Biometric menagerie" in iris systems

The "menagerie" phenomenon is well studied for voice and face modalities [214]. It has been much less documented and analyzed for the iris modality.

The first evidence of the effect of the "Biometric menagerie" phenomenon on the performance of iris systems has been reported by the CBSA in [145, 143], who conducted the experiments with anonymized iris images of Nexus members to show that performance of some travellers (images) was consistently worse than that of others.

Specifically, a set of balanced datasets was created (called "G-500", G-1000 etc.), where each traveller is observed at the passage exactly the same number of times (6 times) in order to remove any bias with respect to those who used the system often and those who used it only 6 times. These images were matched to each other using five different commercial iris recognition software, with both transaction-based and subject-based statistics computed. The results showed that subject-based results for all products where substantially worse than transaction-based results (see Table E.2 from [145]).

In the same papers [145, 143], the following observations and recommendation are made:

> *"The subject-based analysis has shown that the percentage of travellers who experience a false rejection problem (i.e. subject-based FNMR) is higher than the conventionally reported FNMR computed by averaging over all performed matches. This result does not come as a surprise though, because it is understood that the transaction-based FNMR equals subject-based FNMR only when the mismatched transactions are evenly distributed over all subjects, which is rarely the case even in a well balanced dataset such as the G-500 dataset. The situation however is even worse when FNMR numbers are measured in a live operational context. In real-life testing of a biometric system performance, the transaction-based results will show even more skewed results, because*

*normally the subjects who have more biometrics transactions are those who have less problem using it. The subjects who have higher false rejects rates may have much less transactions recorded, than those who do not experience false rejects. It is therefore strongly recommended, especially when the dataset is not large or when evaluation is done in a live pilot, to report subject-based performance measurements, instead of (or in addition to) transaction-based measurements."*

Table E.1: Iris recognition False Non-Match Rates (FNMR), reported using transaction-based and subject-based analysis (from [145]).

| FMR | G-500: 1 | 2 | 3 | 4 | +Calib: 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|---|---|
| 0.0001% | 0.09 (0.28) | 0.27 | 0.18 | 0.11 | 0.06 (0.16) | 0.24 | 0.99 | 0.05 |
| 0.001% | 0.06 (0.21) | 0.16 | 0.17 | 0.07 | 0.04 (0.10) | 0.09 | 0.99 | 0.06 |
| 0.01% | 0.05 (0.17) | 0.10 | 0.17 | 0.06 | 0.03 (0.06) | 0.07 | 0.17 | 0.05 |
| 0.1% | 0.04 (0.12) | 0.06 | 0.16 | 0.05 | 0.02 (0.03) | 0.04 | 0.16 | 0.05 |

The numbers in columns show FNMR for different values of False Match Rate obtained using four commercial iris recognition products on the so-called "G-500" dataset, which contains iris photo-images of 500 anonymized randomly selected NEXUS members, with one (1) image from enrollment and six (6) randomly chosen images from the passage taken for each person. Subject-based FNMR numbers are shown in brackets for the best performing product. They are significantly higher than transaction-based FNMR numbers. Although the result is shown for one product, the same phenomenon was observed with all other products too. The right part of the table (marked "+Calib") shows the result obtained after the calibration of scores for improved performance. See [145] for more detail.

## E.3 Additional results from NEXUS historical data scores

From 2007 till 2014, CBSA has recorded a substantial number of iris matching scores, which allowed us to conduct additional analysis of the variation in iris performance among travellers. The preliminary results of this analysis showed that, while the majority of travellers do not have problems being recognized by the system, there exists a proportion of about %2 of travellers who consistently experience difficulty being recognized by the kiosk, as shown in Table 4.7 of the main report.

This highlights the importance of conducting subject-based analysis of the system performance. It also provides a valuable piece of information that can be used in analyzing and optimizing border wait time of automated border control systems for all travellers.

The effect of travellers habituation on the system performance has been also examined. It is concluded that, if such phenomenon exists, it is likely of lesser scale, compared to other factors influencing the system performance. The most likely reason why the performance, measured in terms of the average number of attempts and average traveller dissimilarity HD score, looks better for people who used the system often, is that only those of travellers who do not have any issues with the system keep using it. Statistics suggests that those travellers who experience bad performance of the system just stop using it.

Other factors influencing iris recognition performance were examined and the following were found to affect negatively the performance of the system, order of their significance: quality of the camera used at enrollment, location of the kiosk, time of the day.

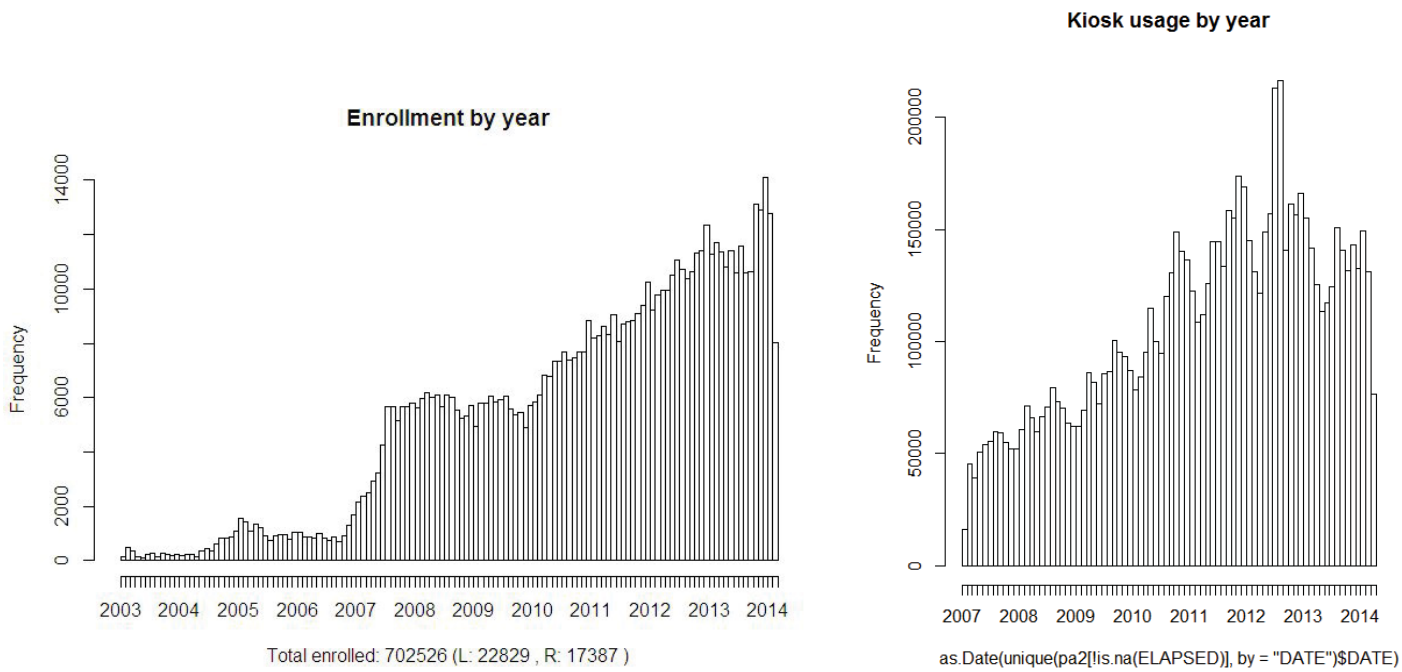



Figure E.2: Historical Nexus iris score data: distribution of enrollments (left) and recorded passages (right) by year.

---

### E.3.1 Dataset

The data consist of iris matching scores recorded by CBSA during the operation of the NEXUS iris kiosks between 2007 and 2014, with 702,526 enrolled NEXUS members, and 63 kiosks around Canada. The distributions of the enrollment and passage data per year are shown in Figure E.2 (Passage data is collected since 2007 only). Some people used the system many times (943 is the record), some used only a few times, some never used it.

### E.3.2 Metrics

The objective of the analysis is to estimate the fraction of travellers *(as opposed to the fraction of traveller-agnostic transactions)* who consistently experience issues with biometric recognition.

To conduct this analysis, the travellers who have used the system more than N times, N varying from 1 to 942 (which is the largest number of kiosk usages in the Nexus program) are extracted from the dataset. Two metrics are computed:

- Metric 1: The proportion of selected travellers (%) who in most cases used two or three attempts, i.e. for whom the average number of attempts is equal or greater than 1.5. Note that maximum of three (3) attempts is allowed to traveller within one session[1].

- Metric 2: The proportion of selected travellers (%) who had to minimum HD equal or higher than 0.2. Note that the HD threshold for accepting the person is 0.27.

Table 4.7 presented in the report summarizes the result. It shows the number of Nexus members who used the system more than 2,4,8,16,32,64,128 times, and percentage of those among them who consistently

[1]In reality, when three attempts are not enough, a traveller has an opportunity to launch a new interaction session with the same or other kiosks. This information however is not available in the logged data.

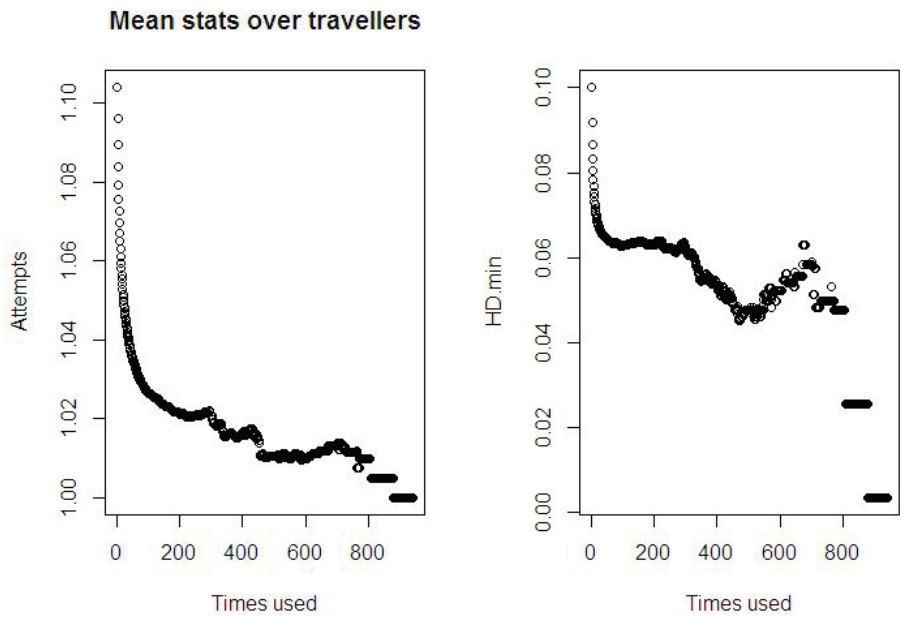



Figure E.3: The averaged number of *Attempts* (left) and the smallest dissimilarity score *HD.min* (right) for travellers who used the system different number of times.

The mean (averaged) statistics over all travellers of the group are shown. The usage frequency information is not included in this result (a person could have used the system many times spread over many years, thus not being a "frequent" traveller).

experienced difficulty in using the system, measured in terms of high average dissimilarity score ($HD$) and high average number of attempts ($Atmp$). It can be seen that of those travellers, who used Nexus kiosks more than 4 time, there are 2.4% of them who consistently had to apply more than one attempts (#Atmp $\geq$ 1.5) and who consistently had high dissimilarity score ($HD.min \geq 0.2$). However the percentage of such travellers of those who used the system more than 16 times and more than 64 times is significantly less: about 0.07% for the former, and less than 0.03% for the latter.

### E.3.3 Habituation vs. "Doddington zoo" phenomenon

As seen from the figures, the percentage of "poor performing" travellers (by both metrics: those who needed more attempts and those who had high HD) is especially high for those travellers who used the system only a few times (fewer than 10). At the first thought, this may appear as the evidence of the habituation phenomenon. That is, the more frequently a person uses the kiosk, the better he or she becomes in using it. However, at a closer look, especially by looking the distribution of HD scores among all travellers who used the system often and those who used it only a few times, one can suggest that the actual reason behind the observed phenomenon is simply that people who experienced problems with the kiosk decide not to use it next time, preferring manual border control for faster and more convenient processing.

To further validate this hypothesis, the statistics of both metrics (i.e. average number of traveller attempts and average HD of the traveller) is computed as a function of times the traveller used the kiosks. The results, averaged over all travellers for each group, are shown as graphs in Figure E.3.

One can observe that travellers who used the system only a few times (on the left side of the graphs) have increasingly worse results, compared to those who used it a lot (on the right side of the graphs). This is the indication that people who experience poor performance of the system likely stop using it.

## E.4 Conclusion

There is a percentage of travellers who consistently experience the problem with the system. Specifically (according to both metrics), around 2% of travellers need to try several times and have often very high HD, indicating that they have been also very likely rejected many times. Note that system does not keep the log of rejected transactions. According to the "Doddington Zoo" terminology, these travellers can be labeled "goats".

Compared to voice and face modalities, the number of observed "goats" is not very large, especially for those travellers who used the system often (more than 16 times) - less than 1%. However they still need to be taken into account. In some cases, they can also indicate a larger issue within the system, setup or the process, thus allowing to further improve the performance of the system. Additional multi-factor statistical analysis is also required to better understand and estimate the impact of all factors on the system performance.

Similar type of subject-based analysis is recommended for any border control system.

# Appendix F

# Recognition limitation of biometrics

The following analysis of the performance limitations of iris, face and fingerprint modalities has been prepared by the University of Calgary researchers, as part of their interim contract deliverable, supplemented with additional results from the CBSA's work on iris performance limitations [145, 143].

Table F.1, lists the best and worst-case error rates for face, iris, and fingerprint modalities, along with the progress in accuracy of recognition technologies (2003-2010). The numbers are taken from [164] (2003) and NIST reports [176, 177] [1]. For example, iris and fingerprints all operate around 10% FRR. Best-case FARs for iris and fingerprints are around $10^{-5}$ ($0.001\%$ or 1 in 100,000). Facial recognition is two-three orders of magnitude worse.

In 2010, the NIST reported the following progress: a 92% identification rate using a 1.6 million person criminal database, of fingerprints, and 95% accuracy using a 1.8 million person database consisting of visa applicants. The lowest FRR=4% is reported for the criminal database, and FRR=0.3% for the visa application database, at FAR=0.1%.

## F.1 Face

NEC face recognition technologies were ranked No. 1 in the MBE Still-Face Track in 2010 carried out by the National Institute of Standards and Technology (NIST) [176], commissioned by the Department of Homeland Security. MBE's Still-Face Track benchmark test employed accuracy evaluation tests with a dataset of over one million face images, which were collected from actual criminal databases and face images used for visa applications.

A more recent NIST evaluation [177] reported the improvement of face recognition technology, with miss rates reduced by about 28% for the best performing system (NEC), which is FRR = 6.4% (from FRR = 8.9%). This however was obtained for forensic applications, where no decision threshold is applied and rank-1 result is considered as the match[2].

## F.2 Iris

The key results of the IREX IV evaluation are described below (see Table F.2).

**Core Accuracy and Speed:** Iris recognition is known to be one of the more accurate and computationally efficient biometric technologies. Some matchers are capable of searching a single iris image against an enrolled population of 1.6 million people in less than a second (using just one processing core) while achieving false

[1] http://biometrics.nist.gov/cs_links/face/mbe/MBE_2D_face_report_NISTIR_7709.pdf

[2] I.e. an image that scored the best of all images in the gallery list is considered to be the match regardless of whether it actually resembles the probe image or not.

negative identification (i.e. "miss") rates below 1.5% at reasonably selective decision thresholds. Identification failures for the most accurate matchers were almost always the result of poor sample quality, where the eye is closed, off-axis, highly rotated, etc. Many of these errors can be corrected through the use of more advanced cameras or improved image collection and data handling practices.

**Contingent Use of Second Eye for Rapid Identification:** When applied to iris recognition, contingent fusion uses the second eye for identification only if the first does not return a decisive match. IREX IV found that contingent fusion achieves accuracy comparable to that of two-eye matching while only using the second eye between 1% and 2% of the time. There are several advantages to requiring the use of only one eye for the majority of transactions. First, it is less computationally expensive. Second, it consumes less bandwidth when the samples are transferred over a network for a back-end search. Finally, it obviates the need for operators of single-eye cameras to capture an image of the second eye when the first proves sufficient.

## F.3 Biometric performance in terms of convenience, security, and usability

The following three factors characterize face, iris, and fingerprint modalities [165]:

Factor 1: *Convenience*,
Factor 2: *Security*, and
Factor 3: *Usability*.

These factors include indirectly performance parameters.

*Convenience* includes the level of effort required to deploy and maintain the system, analyze its results, as well as convenience for untrained users such as travellers.

*Security* depends on the value of information obtained for verification/identification process. In particular, it depends on the number and quality of reference points (each point is a carrier of information). It also includes the potential (capacity) for further improvement of the recognition performance.

*Usability* is a degree the use of the modality in databases and social environment. It also includes user involvement with respect to the consideration whether a technology is privacy-intrusive or not.

In Table F.3 we estimate face, iris, and fingerprint biometric performance, in terms of convenience, security, and usability. We estimate that as a single modality application (without relations to environment conditions and other technologies which aim at supporting the verification/identification process), the fingerprint and iris modality are approximately equal and the most powerful biometric modalities with respect to convenience, security, and usability. Among all "touch-less" modalities, which do not require touching the sensor, iris modality is the distinct winner.

## F.4 Biometric performance in conjunction with other identification technologies of e-border

Important feature of the ABC technology is that it is the group of technologies that are used in conjunction with one another. In this group of technologies, the weak features of one technology can be mitigated by advantageous points of another technology. Performance and risks of facial, iris, and fingerprint devices in the ABC machine should be estimated in content of other eBorder supporting technologies such as the RFID (Radio Frequency IDentification) and OCR (Optical Character Recognition) used in e-passports, cybermetric, searching technologies in networks and databases, biomedical technologies and manual recognition by officers.

For example, e-passport combines at least the following technologies:

- OCR technology,
- RFID technology,
- biometric technology, and
- other eBorder processes and components.

That is, in e-passport biometric technology is supported by other technologies to improve verification/identification process. These technologies contribute in final (output) decision in various ways. There are a number of levels in decision making process before biometrics will contribute.

Based on the estimations given in Table F.3, we also evaluate the aforementioned biometric modalities in conjunction with OCR technology. In this group of technologies, for example, face image of a traveller is labeled using the personal data (name, place and date of birth, etc.) provided in his/her travel document. The results of such estimations are given in Table F.4. We estimate that security and usability of the signed face image should be increased from `Low` to `Moderate` rate. We argue that security is improved because the OCR technology provides additional information. We also argue that travellers are more perceptive to the combination of facial recognition (even with the rigorous rules, implied for the picture taking) and OCR technologies (utilizing the rigorous rules for the document scanning procedure). We assume that the rate of iris recognition should improve in conjunction with OCR technology. However, we believe that usability of fingerprint modality decreases from `High` to `Low`. We argue that this effect is due to the fact that the travellers are untrained users of the automated border control, and the fingerprints usable mainly for the applications such as national Automated Fingerprint Identification System, loose their most important assets.

Table F.1: Best and worst-case error rates for face, iris, and fingerprint modalities, and progress in accuracy of recognition technologies (2003-2010).

| **Modality** | **False Reject Rate (FRR)** or False negative identification | **False Accept Rate (FAR)** or False positive identification |
|---|---|---|
| Face* | $10-20\%$ | $0.1-1\%$ |
| Iris** | $2-10\%$ | $\geq 0.001\%$ |
| Finger | $3-7\%$ | $0.001-0.01\%$ |

* *In 2010, the NIST reported the lowest FRR=0.3% for the civil database at FAR=0.1%, and the lowest FRR=4% for the the criminal database at FAR=0.1%.*
** *In 2010, the NIST reported FRR=1% (see IREX I and IREX III).*

Table F.2: Iris performance results (compare to face recognition performance in Table 4.5) from 2009 NIST IREX-I evaluation on three different datasets. See also the result from the CBSA iris evaluation shown in Appendix E and [145].

| FMR | ICE: 1 | 2 | 3 | 4 | OPS: 1 | 2 | 3 | 4 | BATH: 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0.0001% | 0.023 | 0.023 | 0.025 | 0.050 | 0.002 | 0.005 | 0.006 | 0.008 | 0.010 | 0.018 | 0.030 | 0.031 |
| 0.01% | 0.009 | 0.010 | 0.014 | 0.015 | 0.0018 | 0.004 | 0.005 | 0.007 | 0.004 | 0.007 | 0.013 | 0.025 |

Table F.3: The present state of face, iris, and fingerprint modalities with respect to convenience, security, and usability factors [165].

| **Form factor** | **Rating** | | |
|---|---|---|---|
| | **Face** | **Iris** | **Fingerprints** |
| Convenience | High | High | Moderate |
| Security | Low | High | Moderate |
| Usability | Low | Moderate | High |

Table F.4: Performance of face, iris, and fingerprint biometrics in conjunction with other identification technologies of eBorder.

| **Form factor** | **Rating** | | |
|---|---|---|---|
| | **Face + OCR** | **Iris + OCR** | **Fingerprints + OCR** |
| Convenience | High | High | Moderate |
| Security | Moderate | High | Moderate |
| Usability | Moderate | Moderate | Low |

# Appendix G

# PROVE-IT($x$) assessment of e-border components and supporting technologies

The PROVE-IT(x) assessment framework is developed to provide a light-weight alternative to the conventional nine-point TRL assessment [222, 223] (Figure G.1). It uses a semaphore-like three-point scale ("green" or "+"- proved ready; "yellow" or "o" - possibly ready with additional R&D ; and "red" or "−" - proved not ready for deployment in the nearest future).

The relationship between the PROVE-IT($x$) assessment metrics and traditional TRL scale is shown in Figure G. Two sub-grades within the "ready" grade and "possibly ready" grade are introduced to permit additional level of assessment detail when such information is available.

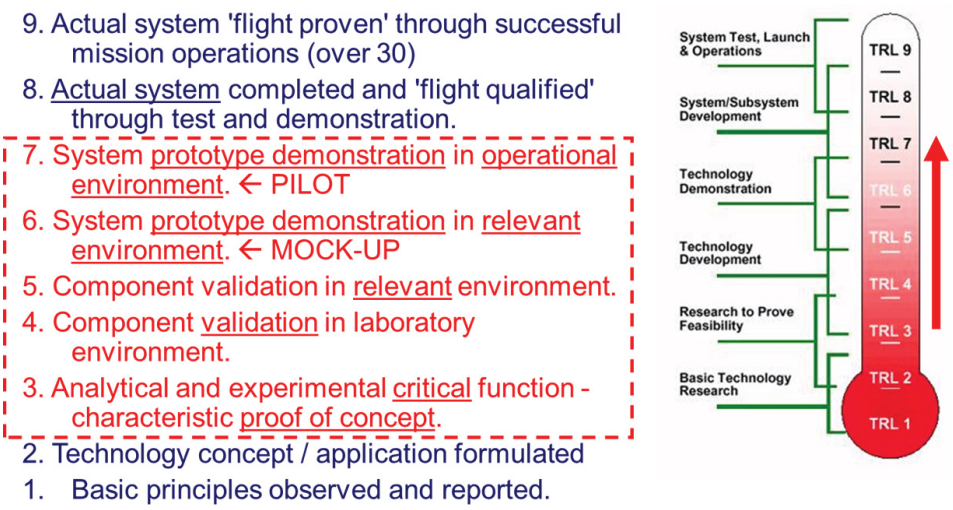


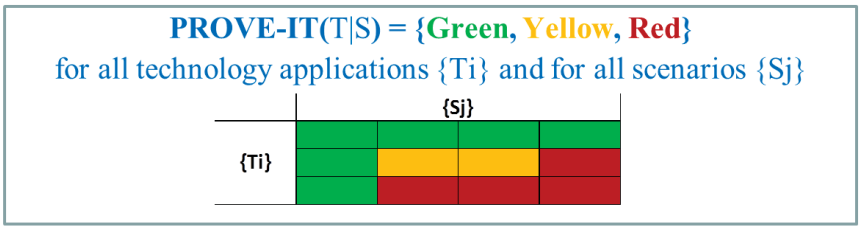

Figure G.1: Nine-grade TRL assessment scale.

## G.1 Development of the technology landscape map

Being an approximate (tentative) measure of readiness, PROVE-IT($x$) assessment can be used to estimate the technology readiness in the entire spectrum of possible deployment conditions and scenarios, using the following three steps.

**Step 1:** Define taxonomy of possible operational conditions (scenarios) {Sj}: ordered from simplest to most difficult;

**Step 2:** Define taxonomy of possible technology application variations {Ti}: ordered from simplest to most




| GRADE | TRL | DEFINITION |
|---|---|---|
| ++ | 8-9 | ***Operationally Ready***: Can be deployed immediately with no customization and predictable results. |
| + | 7 | ***Operationally with Configuration***: Deployed within 1 year with some customization; predictable results. |
| oo | 5-6 | ***Short-term Ready***: Possible within 1 to 3 years with a moderate investment in applied R&D |
| o | 4 | ***Medium-term Ready***: Possible within 3 to 5 years with a significant investment in applied R&D |
| - | 1-3 | ***Not Ready (Academic)***: Not possible within next 5 years; requires major academic R&D. |

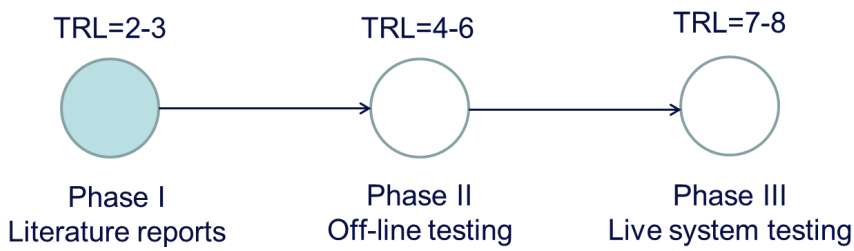



Figure G.2: The PROVE-IT($x$) framework: two-dimensional technology landscape map template (top), semaphore-like assessment scale (middle) and three-phase evaluation process (bottom).

difficult, thereby creating a two-dimensional technology landscape map table.
**Step 3:** Assign technology readiness colour (green, yellow, red) for each technology application variation at each PROVE-IT(Ti, Sj), using a three-phase performance assessment process described below, thereby filling out the technology landscape map table derived above.

## G.2 Three-phase technology readiness assessment process

Following the formal TRL definition described above, the following three key technology assessment phases are defined (see Figure G).
**Phase I:** Literature and market review (testing for up to TRL=3). This includes surveying of scientific and industry literature, including company offerings and patent analysis, for the purpose of identifying and harmonizing the lexicon and technology definitions as well as for obtaining the preliminary high-level overview of possible options and solutions; and selection of solutions and scenarios that are believed to be ready for off-line testing for further assessment
**Phase II:** Off-line testing (testing for up to TRL=6). This includes testing of the solutions on pre-recorded datasets corresponding to different CCTV scenarios, and measuring detection error tradeoff metrics.
**Phase III:** Live system testing (testing for up to TRL=8). This phase requires further customization and refinement of the technologies and scenarios tested in the previous phase for there further testing in a live environment with real operational surveillance cameras and CCTV users.

## G.3 Taxonomy of deployment scenarios

In the evaluation of technologies, it is proposed to categorize all possible deployment scenarios using "human-machine" factors space, from easiest to hardest, for human factors and machine complexity perspectives (see

Figure 3.2).

This space can be further taxonomized according to "who-what-where" factor triangle, in which "where" factors relate to the settings or components that traveller needs to use, "what" factors relate to the procedure imposed on the tarveller during the use of the system; and "who" factors relate to the traveller characteristics;

## G.4 PROVE-IT(FRiV) and PROVE-IT(VA) assessment

Using PROVE-IT($x$) TRL assessment framework the readiness of face recognition in video and video analytic technologies has been assessed as shown in Tables G.1 and G.2 (updated from [137]). Similar assessment for all e-border components and supporting technologies is recommended.

Table G.1: PROVE-IT(FRiV) results. The readiness of face recognition technology for video surveillance applications.

| FACE RECOGNITION IN VIDEO APPLICATION | TYPE 0[1] (EGATE) | TYPE 1 (KIOSK) | TYPE 2 (PORTAL) | TYPE 3 (HALLS) |
|---|---|---|---|---|
| **Detection (no Face Recognition)** | | | | |
| 1. Face Detection in Surveillance Video | ++ | ++ | + | oo |
| **Tracking (no Face Recognition)**[2] | | | | |
| 2. Face Tracking across a Single Video | + | + | + | - |
| 3. Face Tracking across Multiple Videos | + | + | o | - |
| **Semi-automated Recognition**[2]**: for post-event investigation (search and retrieval) applications** | | | | |
| *Video to Video (Re-Identification)* | | | | |
| 4. Face Grouping, Tagging, Tracking across multiple videos | + | oo | oo | o |
| *Still to Video* | | | | |
| 5. FR to aid manual forensic examination | + | oo | oo | - |
| **Fully-automated Recognition: for real-time border or access control applications** | | | | |
| *Video to Video (Re-Identification)* | | | | |
| 6. Instant FR in single camera | + | oo | o | - |
| 7. Instant FR from multiple cameras | + | o | o | - |
| *Still to Video* | | | | |
| 8. Instant FR for Watch List Screening – Triaging | + | oo | o | - |
| 9. Instant FR for Watch List Screening – Binary | + | o | - | - |
| **Micro-facial feature recognition** | | | | |
| 10. Facial Expression analysis: for emotion / intent recognition | + | oo | o | - |
| **Soft and multiple biometrics** | | | | |
| 11. Human attribute recognition (gender, age, race) | + | oo | o | - |
| 12. Personal metrics (height, weight, eye/hair colour) | + | o | o | - |
| 13. FR to improve voice or iris biometrics | + | o | - | - |

[1] The readiness of FR applications for cooperative scenario at eGate (Type 0) is provided as point of reference to contrast the performance of the same FR applications in non-cooperative scenarios (Types 1-3).

[2] See the results of person detection and tracking from PROVE-IT(VA) evaluation.

[3] Type 4 scenario (outdoors) is not included in the FRiV assessment since there is no evidence the technology works in easier setups.

Table G.2: PROVE-IT(VA) results. The readiness of video analytics technologies.

| Video Analytics Application | Type 1 (Kiosk) | Type 2a (Portal) | Type 2b (Portal) | Type 3 (Halls) | Type 4 outdoor |
|---|---|---|---|---|---|
| **Person Detection and Tracking (without Face Recognition)** | | | | | |
| a. Person counting | ++ | + | oo | o | o |
| b. Person tracking in single camera | ++ | + | oo | o | o |
| c. Person matching in single camera | oo | o | o | - | - |
| d. Person matching in multiple cameras | o | o | - | - | - |
| **Person Event Detection** | | | | | |
| a. Improper standing place | ++ | ++ | + | o | o |
| b. Opposite flow detection | ++ | ++ | oo | o | o |
| c. Running detection | ++ | ++ | oo | - | - |
| d. Tail-gating detection | ++ | ++ | oo | - | - |
| e. Loitering detection | ++ | + | - | - | - |
| f. Fall detection | ++ | oo | - | - | - |
| **Crowd Analysis** | | | | | |
| a. Density estimation | n/a | | oo | oo | oo |
| b. Rapid dispersion | | | oo | oo | oo |
| c. Crowd formation | | | oo | oo | oo |
| d. Crowd Splitting | | | o | - | - |
| e. Crowd Merging | | | o | - | - |
| **Baggage Detection and Tracking** | | | | | |
| a. Static Object (>n sec) | + | +[1] | o[1,2] | - | - |
| b. Object removal | o[2] | o[2] | - | - | - |
| c. Dropping Object | o[2] | o[2] | - | - | - |
| d. Abandoned Object | o[2] | o[2] | - | - | - |
| e. Unattended Object | o[2] | o[2] | - | - | - |
| f. Carried Object | - | - | - | - | - |
| **Person-Baggage Association Analysis** | | | | | |
| f. Person-Baggage Association | o | - | - | - | - |
| g. Owner change | - | - | - | - | - |
| **Camera Tampering Detection** | | | | | |
| Occlusion, Focus moved, Camera moved | ++ | ++ | ++ | ++ | + |
| **Physical Security** | | | | | |
| Virtual trip-wire, intrusion detection | ++ | ++ | ++ | ++ | + |

[1] For low traffic only.

[2] For large objects only.

# Appendix H

# Presentation at Frontex Global Conference on the Future of Border Checks

This appendix presents a slide presentation summarizing key outcomes of the "ART in ABC" project. A shorter version of this presentation was given at the *Global Conference on the Future of Border Checks* organized by Frontex in Warsaw, Poland, on 17-18 June 2015, and is available from their website: http://btn.frontex.europa.eu/events/global-conference-future-border-checks-2015. The webcast of the conference is available at http://streamonline.biz/pages/frontex.

Panel 6 of the conference entitled "*Staying Ahead of the Future Through Research – Focus on Identification*", where this presentation was made, starts on 11 hour 20 min of the webcast. The related discussions start on 12 hour 15 min and run until closing of the conference on 12 hour 55 min.

Title: "ART in ABC: from trusted traveller kiosks to e-border systems"

*Abstract:* Under the funding from Defence Research and Development Canada, the Science and Engineering Directorate of the Canada Border Services Agency has recently concluded a large-scale study dedicated to the Analysis of Risks and Trends in Automated Border Control (ART in ABC). One of the key outcomes of this study was the development of the ABC taxonomy within a larger e-border process that deals with automated clearance of travellers at the border, and the analysis of issues and potential developments in ABC and other e-border components, which is presented.

# ART in ABC: from trusted traveller kiosks to e-border systems

Dmitry O. Gorodnichy
Science and Engineering Directorate



Extended from presentation at:
*Global Conference on the Future of Border Checks (FoBC)*, Frontex, Warsaw, June 2015



## Disclaimer

- The presented opinions are only that of the author and do not represent the opinion of the Canada Border Services Agency (CBSA).
- In the presented study, the term ABC does not refer to and does not have any association with the CBSA's Automated Border Clearance program. It is used solely in reference to a general system that performs automated clearance of travellers at the border.

CSSP-2013-CD-1020

## Risk analysis of face and iris biometrics in border / access control applications

**Lead Organization:** CBSA-S&E

**Partnership:** University of Calgary

**Start-End:** June 2013 – March 2015

**Funded:** DRDC Center for Security Science
Canada Safety and Security Program

### Objectives:

**Generate critical knowledge for Gov't of Canada related to use of iris and face biometrics for ABC :**

1. Conduct benefit-risk analysis for existing ABC
2. Develop taxonomies and recommendations that that can be used for decision making
3. Develop recommendations and metrics for testing and deploying ABC systems;
4. Address programs/ policy /standard/ component related to use of biometrics for ABC

### Outputs:

**"Automated Border Control systems as part of eBorder crossing process".** NIST IBPC, April 2014.

**"Automated Border Control: Problem Formalization".** IEEE SSCI CIBIM, December 2014

**"ART in ABC: Analysis of Risks and Trends in Automated Border Control",** Final Study Report, June 2015



# Background

"**Risk analysis of face and iris biometrics in border / access control applications**" study (2013-2015)

- conducted by CBSA
- in partnership with University of Calgary
- under the funding of Department of National Defence.

**Objective: Generate critical knowledge for Gov't of Canada related to use of iris / face biometrics for ABC**

- Analysis of existing biometric-enabled ABC solutions
- Recommendations related to future ABC solutions

Ref: **"ART in ABC: Analysis of Risks and Trends in Automated Border Control",** Final Report, June 2015

# Outline

**Background: Canadian context**
**Part I. Establishing the foundation:**

- Key definitions: ABC, eBorder, Air Traveller Continuum
- Three generations of ABC:
  - Gen-1 ABC: Registered Traveller kiosks using iris
  - Gen-2 ABC: eGates using faces

**Part II. Roadmapping the future:**

- Gen-3 ABC: eBorder systems
- FIVE technological "pillars" eBorder
- Take-aways



# Canadian context

**Present:**

- Manual Primary Inspection Line (PIL)
- Nexus Trusted Traveller Programs (TTP) iris kiosks
  - for Canadians/Americans (>2003)
- ABC self-service declaration kiosks
  - for Canadians/Americans (>2010)
- Temporary Resident Biometric Program
  - fingerprints, temporary residents (> 2013)
- ePassports with ICAO-conformant faces (>2013)

**"Modernizing the Air Traveller Continuum. Strategy 2020"**

- Built on success of ABC kiosks, adding:
  - Eligibility verification
  - ePassport , TTP and TRBP
  - Automated declaration

# Key definitions

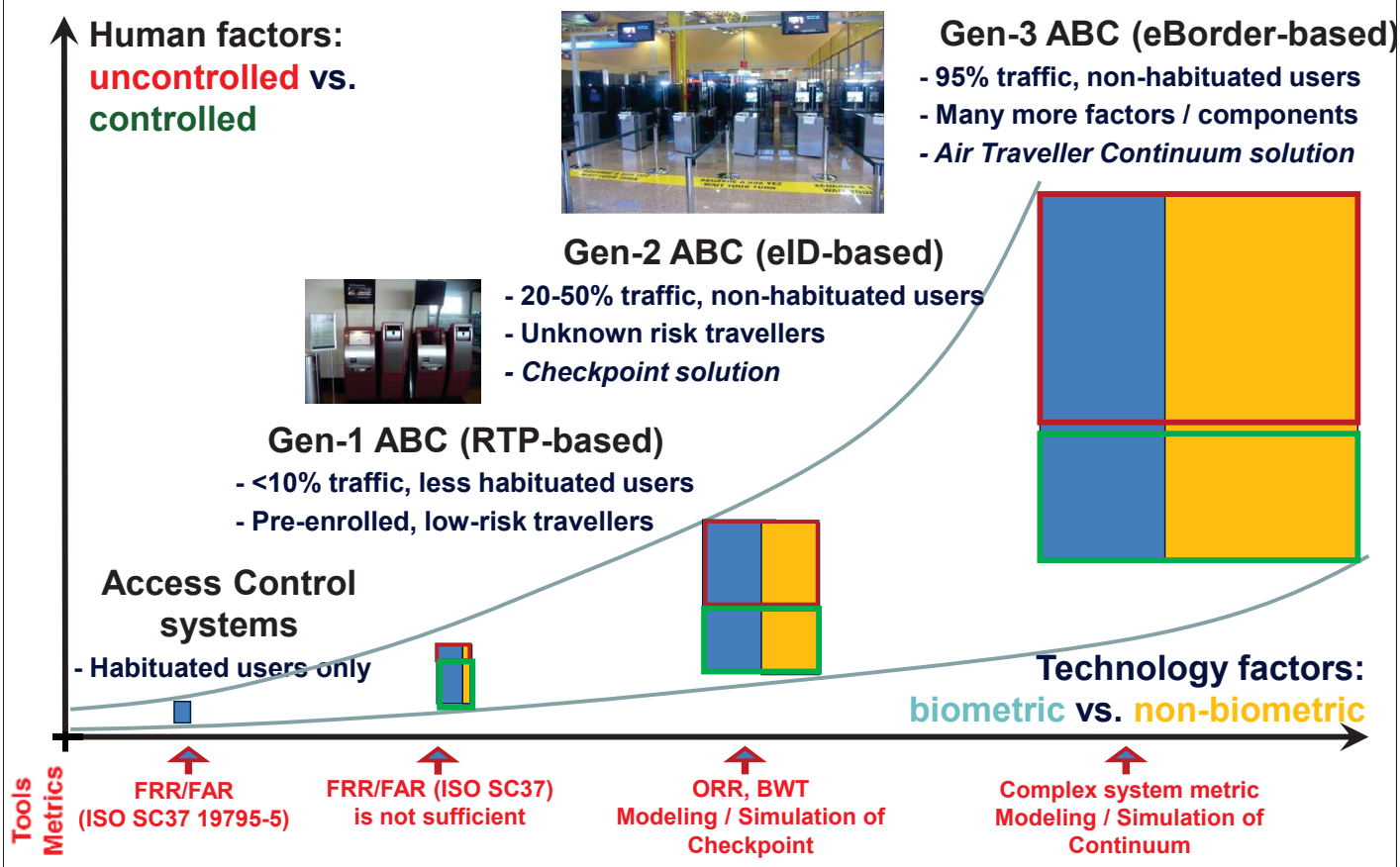
- **ABC: Automated Border** …
  - Clearance
  - Crossing
  - Checkpoint
  - Control: Key technological component of *eBorder*

- **eBorder:** infrastructure for border control and management aimed at automation of **traveller clearance***
  - specifically within *Air Traveller Continuum*

- Two ***traveller clearance*** functions :
  1. Traveller authentication – "Who are you?"
  2. Traveller risk assessment - "What is your risk factor?"

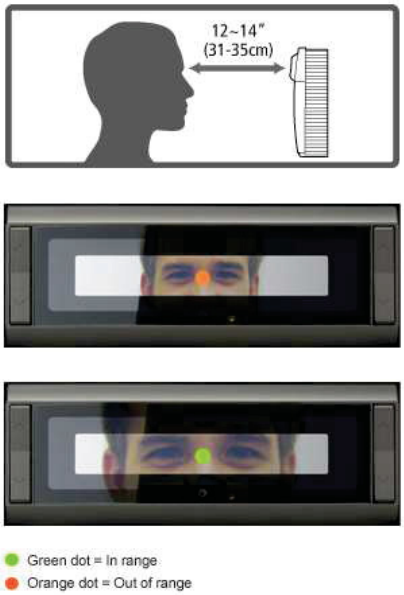


# Evolution of ABC



# Gen-1 ABC systems: take-aways

Example: Nexus kiosks deployments - 2003, 2007, 2014




- "marked" mirror to allow manual adjustment
- two iris captured at the same time
- ICAO-conformant face can also be captured !



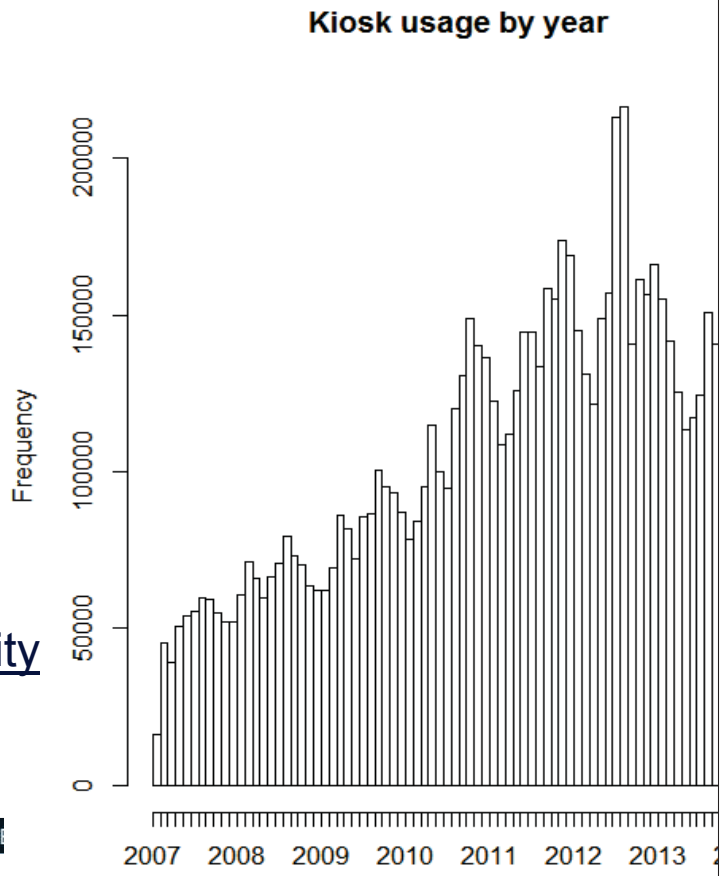
# Gen-1 ABC: performance (iris)

At FAR ~ 0.001%
FRR < 2 %

(Based on UK IRIS data)

- Much better than face.
- Can be improved by:
  - subject-based analysis
  - allowing different heights
  - better instructions (in operating the mirror)

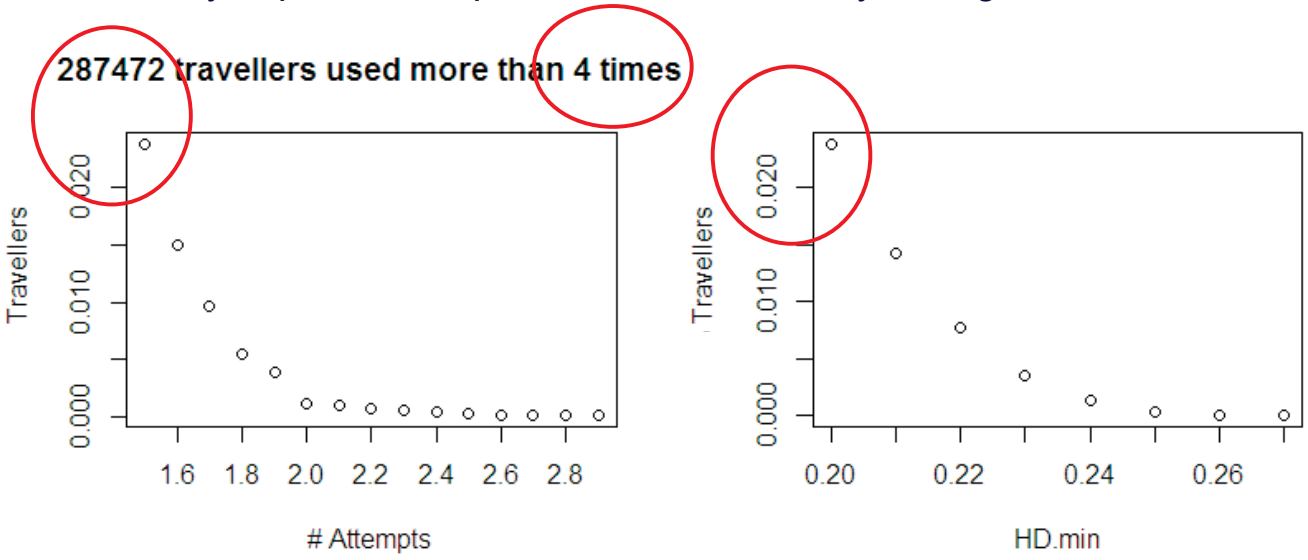
- Has higher long-term capacity for further improvement !
  - using second iris



# Subject-based analysis of Nexus kiosks

- Most travellers are recognized from single attempt & low dissimilarity score
- However there is a portion (~2%) which consistently experience the problem. <u>Key question:</u>

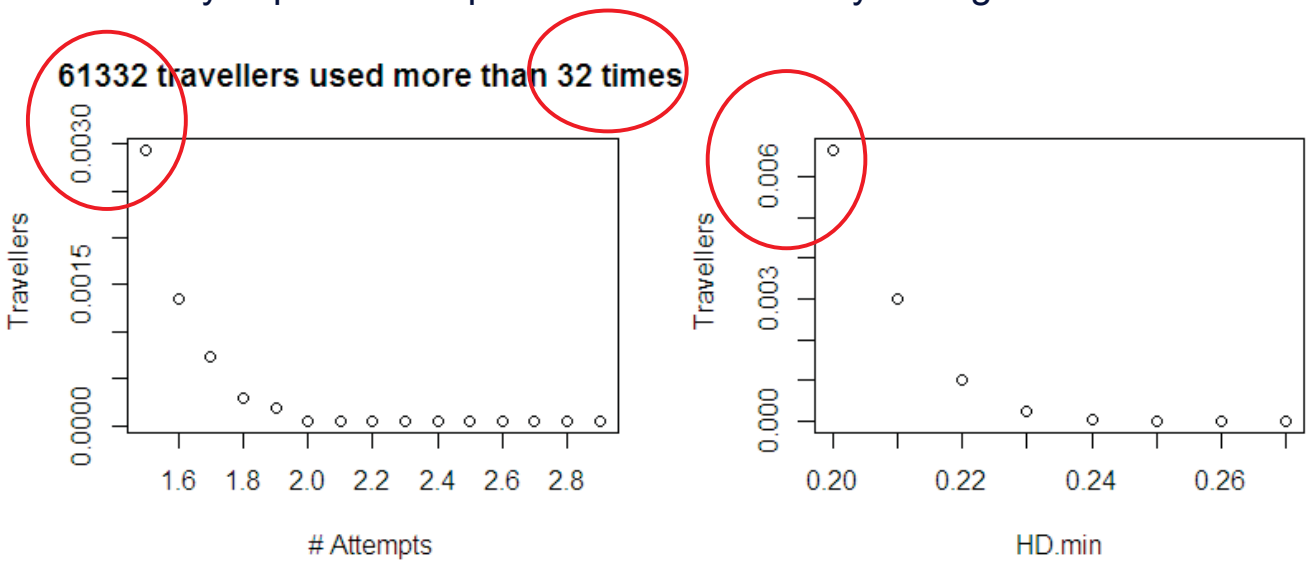
1. Do travellers stop using the system, or
2. Do they improve their performance drastically through habituation ?




# Subject-based analysis of Nexus kiosks

| Times used the system | >2 | >4 | >8 | >16 | >32 | >64 | >128 |
|---|---|---|---|---|---|---|---|
| Number of travellers | 383,463 | 287,472 | 196,573 | 119,538 | 61,332 | 24,383 | 6,530 |
| Percentage of them who experienced difficulty | 4.2% | 2.4% | 1.3% | 0.8% | 0.6% | 0.3% | 0.2% |

1. Do travellers stop using the system, or
2. Do they improve their performance drastically through habituation ?



# Gen-2 ABC systems: take-aways

- Example: EU eGate deployments. 2006 - 2014


- New deployments feature: mirror and self-adjusting camera
- Two-step vs. one-step topology
- All decisions validated by officer: <u>1 officer per 3-6 eGates</u>



# Gen-2 ABC (face)

At FAR ~ 0.1%
FRR ~ 5-15 %
(+a lot of variation)

- Worse than iris
- <u>However,</u> can be improved by using fusion with second modality.

Adding fingers, reduces FFR from 12 % to 4% ! (Spain example)

Data from: D.Cantarero et al. "A multi-modal biometric fusion implementation for ABC Systems" .2013

| | Country of origin | Passages 06-09/2012 | Rejected | FRR | Passages 02/2013 | Rejected | FRR |
|---|---|---|---|---|---|---|---|
| 1 | BEL | 531 | 115 | 21.59% | 108 | 11 | 10.10% |
| 2 | NOR | 97 | 16 | 16.49% | 25 | 4 | 16.00% |
| 4 | ITA | 2757 | 435 | 15.79% | 577 | 88 | 15.29% |
| 5 | DNK | 152 | 20 | 13.16% | 22 | 4 | 18.18% |
| 6 | NLD | 990 | 134 | 13.54% | 177 | 21 | 11.86% |
| 3 | ESP | 67508 | 9006 | 13.34% | 13478 | 1648 | 12.23% |
| 7 | FRA | 2687 | 341 | 12.69% | 647 | 57 | 8.85% |
| 8 | SVK | 49 | 7 | 14.29% | 11 | 0 | 0.00% |
| 9 | SVN | 40 | 4 | 10.00% | 7 | 1 | 14.29% |
| 10 | D | 1540 | 157 | 10.18% | 240 | 26 | 10.88% |
| 11 | POL | 214 | 22 | 10.33% | 30 | 3 | 10.00% |
| 12 | HUN | 70 | 6 | 8.57% | 28 | 3 | 11.54% |
| 13 | MLT | 10 | 1 | 10.00% | 1 | 0 | 0.00% |
| 14 | IRL | 749 | 64 | 8.58% | 173 | 17 | 9.64% |
| 15 | CZE | 97 | 10 | 10.53% | 19 | 0 | 0.00% |
| 16 | LTU | 56 | 5 | 8.93% | 14 | 1 | 7.14% |
| 17 | ROU | 367 | 27 | 7.42% | 94 | 10 | 10.99% |
| 18 | EST | 15 | 1 | 7.14% | 11 | 1 | 9.09% |
| 19 | GBR | 10914 | 823 | 7.54% | 2520 | 131 | 5.19% |
| 20 | SWE | 397 | 30 | 7.61% | 64 | 1 | 1.59% |
| 21 | CHE | 217 | 11 | 5.09% | 55 | 7 | 12.96% |
| 22 | AUT | 215 | 11 | 5.12% | 25 | 2 | 8.00% |
| 23 | PRT | 2172 | 118 | 5.45% | 443 | 6 | 1.36% |
| 24 | FIN | 155 | 7 | 4.52% | 28 | 1 | 3.57% |
| 25 | BGR | 135 | 5 | 3.73% | 26 | 1 | 4.00% |
| 26 | GRC | 187 | 5 | 2.67% | 37 | 3 | 8.11% |
| 27 | LVA | 56 | 1 | 1.79% | 16 | 1 | 6.25% |
| 28 | LUX | 13 | 0 | 0.00% | 4 | 0 | 0.00% |
| 29 | ISL | 10 | 0 | 0.00% | 3 | 0 | 0.00% |
| 30 | CYP | 5 | 0 | 0.00% | 1 | 0 | 0.00% |
| 31 | LIE | 1 | 0 | 0.00% | 0 | 0 | 0.00% |
| | Total | 92406 | 11382 | 12.32% | 18884 | 2048 | 10.85% |

# Gen-3 ABC systems

ABC is the system that:

1. Makes use of the entire eBorder infrastructure / related processes.

2. Performs authentication of travellers, based on all information accumulated through the air travel continuum

3. Performs risk assessment system, based on all information accumulated through the air travel continuum

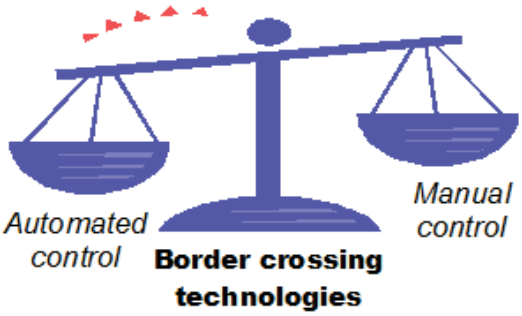
4. Communicates across the data network with other ABC systems

5. Requires trained operators, as a semi-automated system that operates under supervision of a border officer.

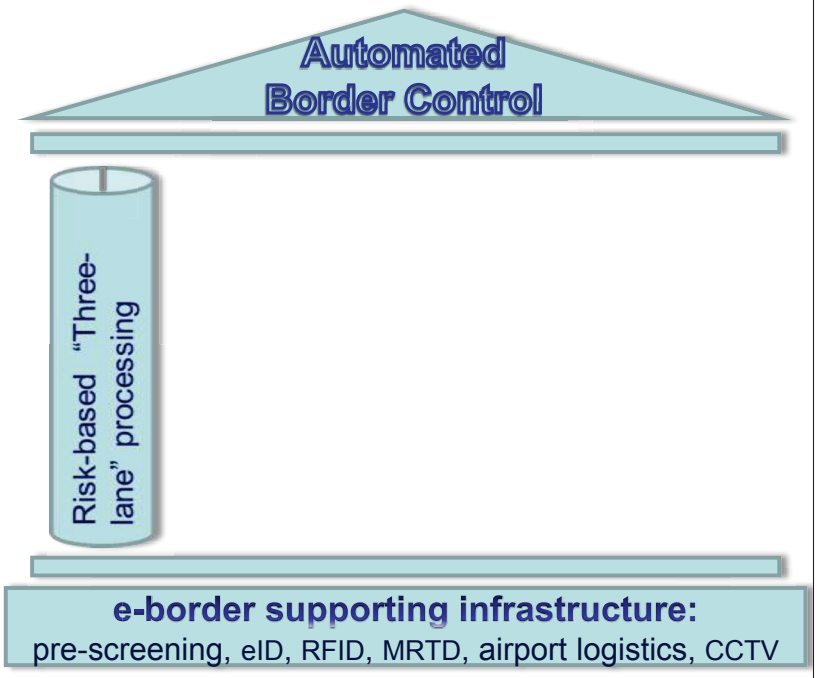
**Extends ABC from *Checkpoint* solution to *Air Continuum* solution.**



# Five pillars of e-border



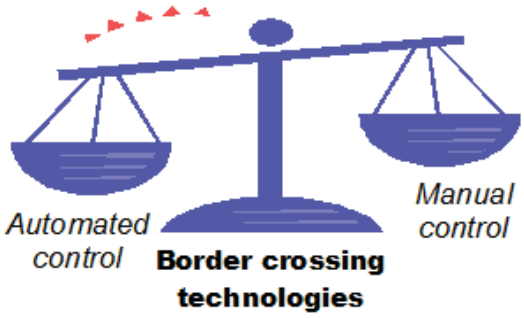


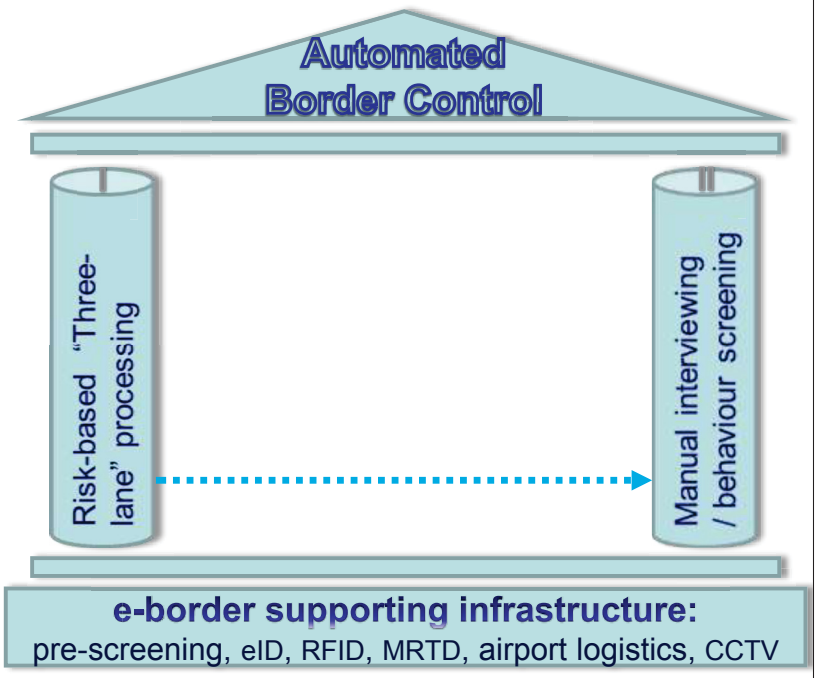



Three "lanes":

- Known low-risk, Known high-risk, Unknown risk.
- Topological vs. logistical, optional vs. mandatory
- Often used as two-lanes (with RTP/TTP)

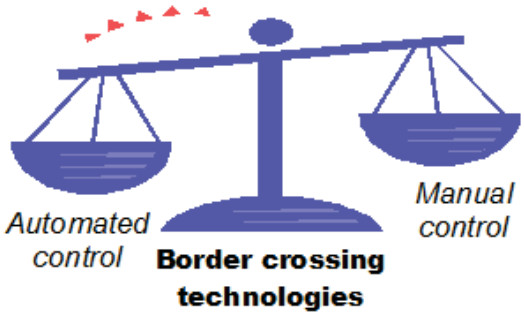
# Five pillars of e-border



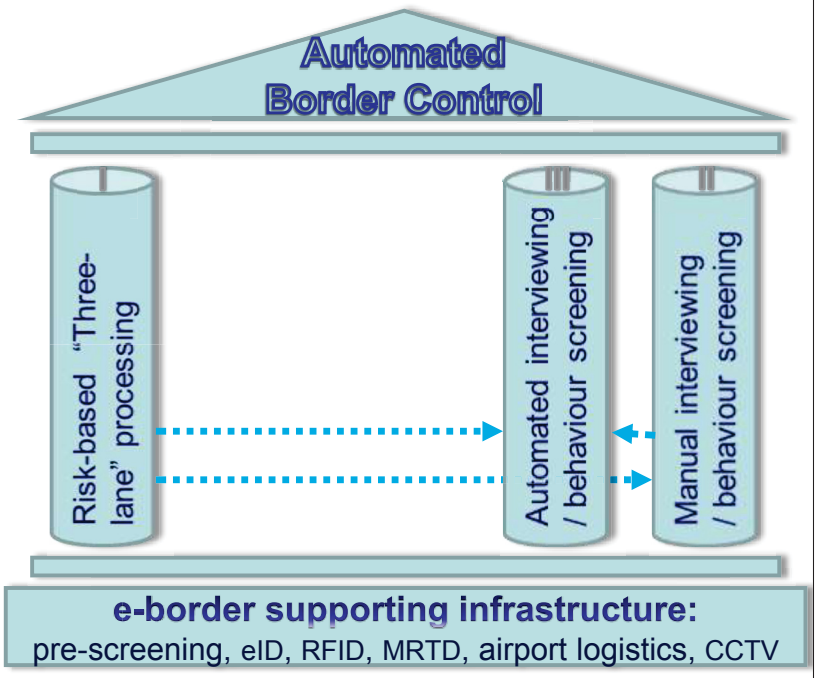




Officers try to detect mal-intentions
- Efficiency under question
- Issues with 5%-20% of population who have anxiety / mental health conditions

# Five pillars of e-border

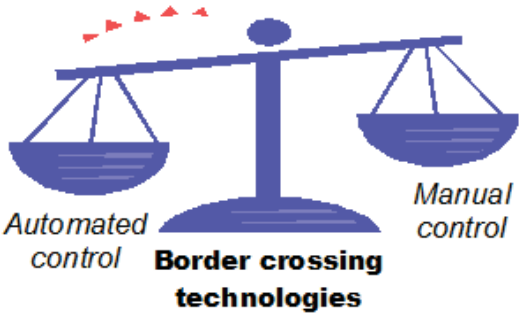


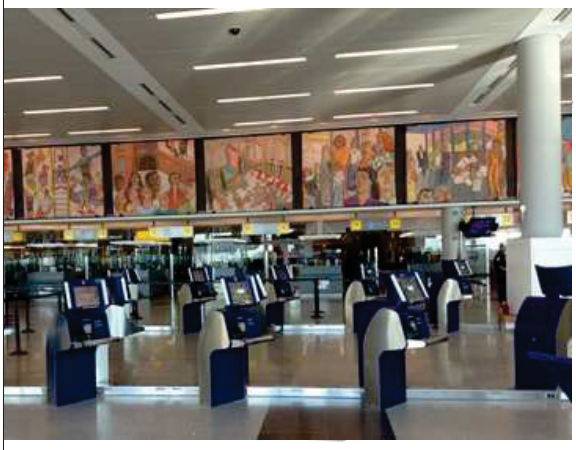


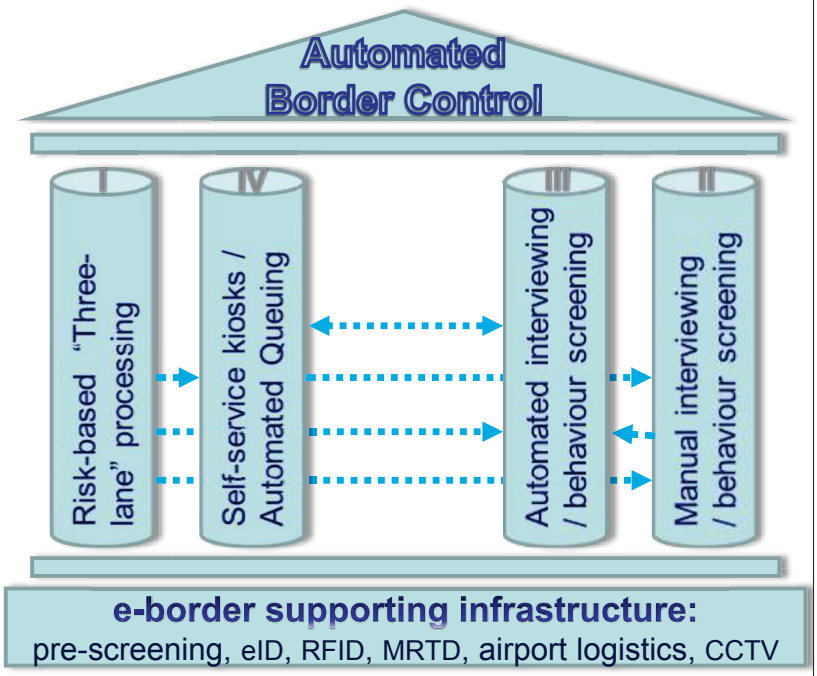



Turing-like machine to assist officers :
- Generates questions, monitors person response
- Scalable, can be integrated in existing kiosks
- Least explored area
- AVATAR project from Univ. of Arizona

# Five pillars of e-border

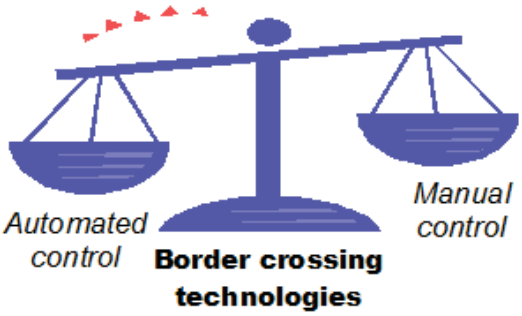


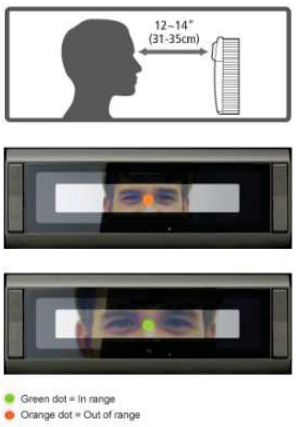



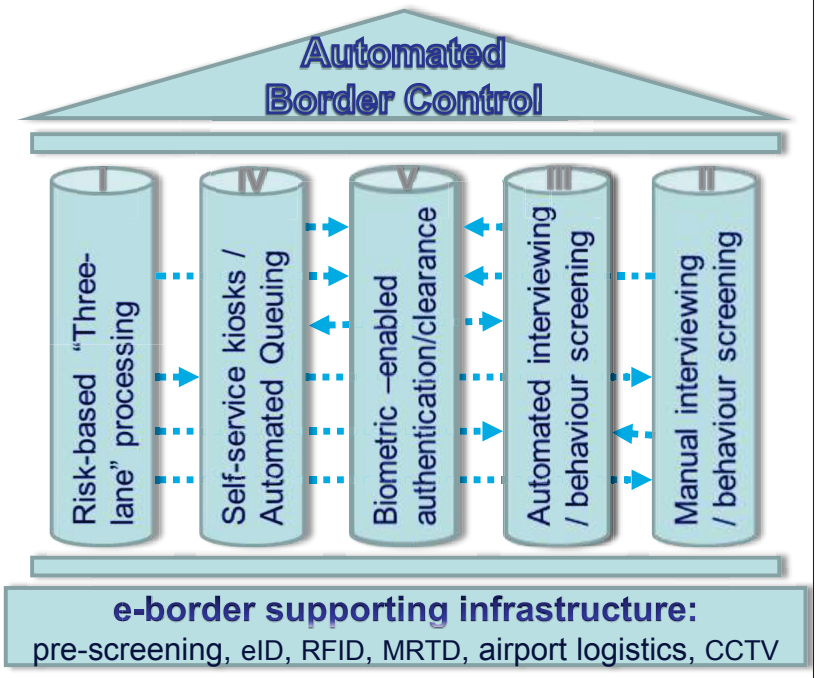



Automates all low-intelligence tasks
- Deployed in Canada / USA airports
- Used in EU as self-reporting for Land mode
- Provides platform for full automation (ABC)

# Five pillars of e-border

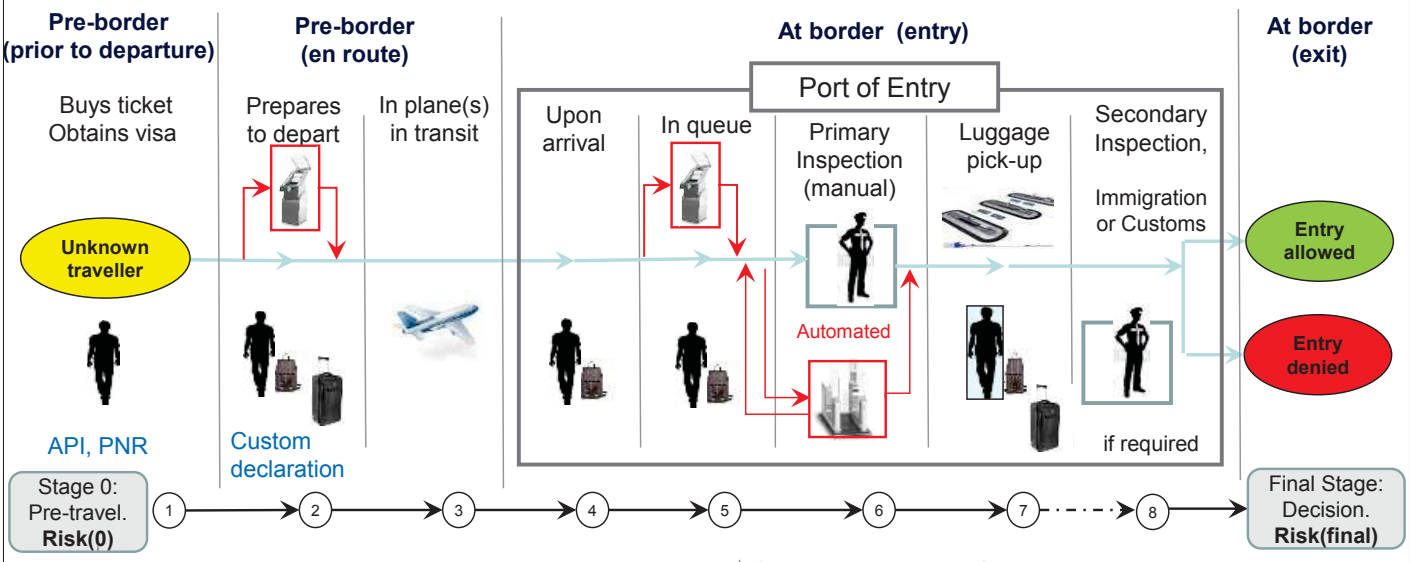



Authenticates travellers using biometrics
- RTP-based, eID-based, eBorder-based (as per Frontex, IATA, ICAO roadmap)
-- Top component, can integrate all other components

# Air Traveller Continuum (present)

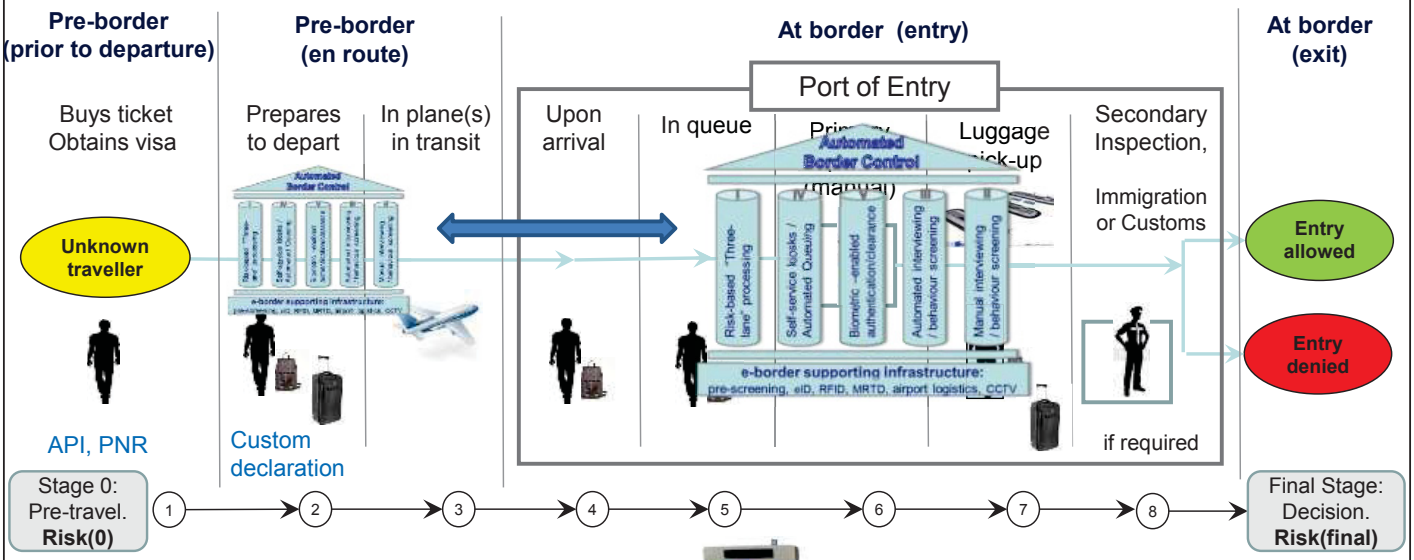



Data about the traveller is accumulated: for *Authentication* & *Risk assessment*
(biographic, biometric, cybermetric, behavioural, other)

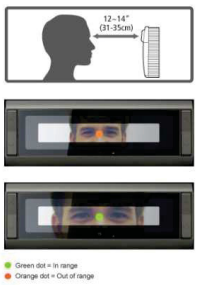
**e-border technologies**
(manual and automated, biometric and non-biometric)

- Entry-Exit kiosks or gates
- Self-service kiosks
- Biometric-enabled gates

# Air Traveller Continuum (future)




Several eBorder components can be combined in a single ABC unit:




# Implications

1. **Continuum-based identification:**
   - Use of the entire e-Border infrastructure
   - Coupled with **trust** / **risk assessment**
   - Person authentication as **evidence-accumulation** process
   - Growing use of ***cybermetric***
- Wider use of Biometrics – for stress/deceit detection

2. **Development of other eBorder components:**
- Automation of risk assessment
  - automation of statistical surveillance (data mining)
  - via interview supporting (AVATAR-like) technology
- Kiosk of the Future
  - face vs. (and) fingerprint and iris

3. **New tools required**
- For modeling ABC / eBorder. For training ABC operators



# Technical recommendations

***ABC Performance (Reliability, Facilitation, Cost) =***
***= Function (Technical factors, Non-technical factors)***

- Key objective of ABC design: Eliminate or minimize as many as possible sources of risks (number of factors)
  - User-centered designs – e.g. automated adjustment of camera
  - User in the loop designs – e.g. use of mirror to allow users to help
  - Auto-illumination, auto-detection

- Perform biometric Fusion, whenever possible

| Iris: FRR<2% @ FAR~0.001% | Face: FRR~5-15% @ FAR~0.1% |
|---|---|

- Iris and Face can be captured at the same time
  - Iris is becoming preferred modality for national ID programs

# Conclusions

- Several biometric-enabled technologies already used in airports
- There's a major difference between biometric-enabled access control and biometric-enabled border control
- ABC: the main technical component of eBorder for Air Traveller Continuum (ATC)
- Three types (generations) of ABC:
  - Gen-1 ABC: Registered Traveller kiosks using iris
  - Gen-2 ABC: eGates using faces
  - Gen-3 ABC: eBorder systems



# Conclusions (cntd)

- eBorder: built on 5 technological pillars:
  1. "Three-level" risk-based processing
  2. Manual screening
  3. Automated screening* (See: What's next)
  4. Self-service systems
  5. Biometric-enabled authentication
- ATC: has 8 zones for information gathering
- Iris: should not be excluded from discussion
- New tools:
  - for continuum-based identification
  - for performance assessment, for training
  - new designs

End of the report