Contribution to the evaluation and optimization of passengers' screening at airports

Carl Rizk

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par :

Institut National Polytechnique de Toulouse (Toulouse INP)

Discipline ou spécialité :

Mathématiques Appliquées

Présentée et soutenue par :

M. CARL RIZK

le vendredi 13 décembre 2019

Titre :

Contribution to the evaluation and optimization of passengers' screening at airports

---

Ecole doctorale :

Aéronautique-Astronautique (AA)

Unité de recherche :

Laboratoire d'Informatique Interactive (LII-ENAC)

Directeur(s) de Thèse :

M. FELIX MORA-CAMINO

M. HADJ BATATIA

Rapporteurs :

Mme PRISCILA MACHADO VIEIRA LIMA, UNIVERSITE FEDERALE DE RIO DE JANEIRO

M. WALID EL MOUDANI, UNIVERSITE LIBANAISE

Membre(s) du jury :

M. PHILIPPE MARTHON, TOULOUSE INP, Président

M. DANIEL DELAHAYE, ECOLE NATIONALE DE L'AVIATION CIVILE, Membre

M. FELIX MORA-CAMINO, ECOLE NATIONALE DE L'AVIATION CIVILE, Membre

M. HADJ BATATIA, TOULOUSE INP, Membre

M. LUIS CADARSO, UNIVERSIDAD REY JUAN CARLOS MADRID, Membre

Mme IOANA BILEGAN, UNIVERSITE DE VALENCIENNES, Membre

Acknowledgements

First, I would like to express my deepest gratitude to my thesis directors, Professor FELIX MORA-CAMINO and Professor HADJ BATATIA for their continuous guidance and support throughout the research. Their encouragement and advice led me to the right path and are greatly appreciated.

I would like also to thank all the members of my jury, especially Professor WALID EL MOUDANI from the Lebanese University and Professor PRISCILA MACHADO VIEIRA LIMA from the Federal University of Rio de Janeiro for their acceptance to review my thesis dissertation.

Also, I would like to thank Professor Philippe MARTHON from INP Toulouse for his acceptance to chair the jury of my PhD thesis. And many thanks also to the other members of the jury: Professor IOANA BILEGAN from "Université Polytechnique Hauts-de-France", Professor DANIEL DELAHAYE from ENAC and Professor LUIS CADARSO from "Rey Juan Carlos University".

I would also like to extend my deepest gratitude to my lovely wife HILDA KARAM for her unconditional love, support and assistance. I am also grateful to my son THOMAS RIZK, my parents FAYEZ RIZK and SAIDE EID, my sisters CHRISTINE and CARINE RIZK, my brother-in-law NAJIB MAALOUF, my nieces CLARA AND KATE MAALOUF, my father-in-law NAJIB KARAM, my mother-in-law HIND ABI NADER and the rest of my wife's family and everyone who, in one way or another, has helped me get through these years, such as Dr HAMDI CHAOUK (former DG of Civil Aviation in Lebanon), Mr MOHAMMAD CHEHABEDDINE (current DG of Civil Aviation), Dr ABBAS RAMMAL, DR ZAINAB AL SAGHIR, DR AMINE SAHILI, DR MAYDUN, DR SIBA HAIDAR and Mrs SALWA FAOUR (a Master's student).

Toulouse, December 13rd, 2019

Carl RIZK

"To May Daoud's soul…

To my wife Hilda, to my son Thomas…

To all my family, to all my friends…"

Abstract

Security threats have emerged in the past decades as a more and more critical issue for Air Transportation which has been one of the main ressource for globalization of economy. Reinforced control measures based on pluridisciplinary research and new technologies have been implemented at airports as a reaction to different terrorist attacks. From the scientific perspective, the efficient screening of passengers at airports remains a challenge and the main objective of this thesis is to open new lines of research in this field by developing advanced approaches using the resources of Computer Science.

First this thesis introduces the main concepts and definitions of airport security and gives an overview of the passenger terminal control systems and, more specifically, the screening inspection positions are identified and described. A logical model of the departure control system for passengers at an airport is proposed. This model is transcribed into a graphical view (Controlled Satisfiability Graph-CSG) which allows to test the screening system with different attack scenarios. Then, a probabilistic approach for the evaluation of the control system of passenger flows at departure is developped leading to the introduction of Bayesian Colored Petri nets (BCPN). Finally, an optimization approach is adopted to organize the flow of passengers at departure as best as possible given the probabilistic performance of the elements composing the control system. After the establishment of a global evaluation model based on an undifferentiated serial processing of passengers, a two-stage control structure is analysed which highlights the interest of pre-filtering and organizing the passengers into separate groups. The conclusion of this study points out for the continuation of this theme.

KEYWORDS: airport security, passenger control, graphs and networks, logical models, probabilistic models, optimization.

RÉSUMÉ

Les menaces à la sécurité sont apparues au cours des dernières décennies comme un problème de plus en plus critique pour le transport aérien, qui est l'un des principaux levier de la mondialisation de l'Économie. Des mesures de contrôle renforcées reposant sur des recherches pluridisciplinaires et sur de nouvelles technologies ont été mises en œuvre dans les aéroports en réaction à différentes attaques terroristes. Du point de vue scientifique, le filtrage efficace des passagers dans les aéroports reste un défi et l'objectif principal de cette thèse est d'ouvrir de nouvelles pistes de recherche dans ce domaine en développant des approches avancées utilisant les ressources de la science informatique.

Tout d'abord, cette thèse présente les principaux concepts et définitions de la sécurité dans les aéroports et donne un aperçu des systèmes de contrôle des terminaux de passagers, et plus précisément des postes d'inspection-filtrage qui sont identifiés et décrits. Un modèle logique du système de contrôle des départs des passagers d'un aéroport est proposé. Ce modèle est transcrit en graphiquement (Controlled Satisfiability Graph-CSG), ce qui permet de tester le système de filtrage sous différents scénarios d'attaque. Ensuite, une approche probabiliste pour l'évaluation du système de contrôle des flux de passagers au départ est développée, conduisant à l'introduction des réseaux de Petri colorés Bayésiens (BCPN). Enfin, une approche d'optimisation est adoptée pour organiser au mieux les flux de passagers au contrôle de départ compte tenu de la performance probabiliste des éléments composant le système de contrôle. Après la mise en place d'un modèle d'évaluation global basé sur un traitement en série indifférencié des passagers, une structure de contrôle en deux étapes est analysée, qui met en évidence l'intérêt du pré-filtrage et de l'organisation des passagers en groupes distincts. La conclusion de cette étude indique la poursuite de ce thème.

MOTS-CLÉS: sûreté des aéroports, contrôle des passagers, graphes et réseaux, modèles logiques, modèles probabilistes, optimisation.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

A-CDM	Airport Collaborative Decision Making
CDM	Collaborative Decision Making
CSG	Controlled Satisfiability Graph
BCPN	Bayesian Coloured Petri Nets
ICAO	International Civil Aviation Organization
DHS	Department of Homeland Security
TSA	Transportation Safety Administration
PKI	Public Key Infrastructure
XR	X-Ray
OPJ	Officier de Police Judiciaire
SPOT	Screening of Passengers by Observation Techniques
IED	Improvised Explosive Device
CNF	Conjunctive Normal Form
DNF	Disjunctive Normal Form
SAT	Satisfaction problem
DDL	Davis, Logemann and Loveland's procedure
WCSG	Weighted Controlled Satisfiability Graph
DAG	Directed Acyclic Graph
PN	Petri Net
TPN	Timed Petri net
STPN	Stochastic Timed Petri Net
CPN	Coloured Petri Net
RHS	Right Hand Side

CHAPTER I

GENERAL INTRODUCTION

Through the last decades, there has been a worldwide sustained growth of air transport industry, leading to saturation of airspace and airports, demanding for new investments in airports and technology.

Security threats have emerged in the past years as a more and more critical issue since air transport has characteristics propense to violation of security of people and estate, being used as well by the most affluent social classes as middle class people as a mass transportation system. Having also an international dimension that makes it a researched target by terrorists and unbalanced of any kind.

Airports face a whole range of security challenges, and large numbers of people are involved at every stage. Ensuring air transport security is a key issue for air transport activities, especially that, by 2030, the number of passengers is expected to reach 6 billion per year and the number of departures of aircraft, more than 50 million - about double that in 2011. Furthermore, the ICAO annual overview reports that there was a 5.8% growth of scheduled passenger air traffic observed in 2014, compared to the 5.5% growth in 2013. Such growth will gradually exert enormous pressure on all aviation systems, many of which are operating at full capacity.

Although passengers acknowledge the need for increased security, delayed boarding, cancelled flights, long waiting time have created an environment of passenger dissatisfaction. Passengers noticed the negative impact of increased security requirements and they are increasingly dissatisfied with some of the inconveniences associated with air travel, which led them to seek alternatives such as high-speed rail. It is of great importance for travellers to secure the minimum possible time spent on the way. The less time the passenger spends in the security system, the higher the satisfaction.

Thus, beyond the activities of verification of the tickets of the passengers, control measures aiming to improve the security of the air transport, each time reinforced after new attacks on it, have been implemented at the airports during the last decades. This has created a whole sector of activity within the airports using increasingly sophisticated control equipment and safety teams each time better trained.

However, the introduction of new technologies for the detection of liquids, gels, explosives and weapons, screening both baggage and passengers, leads to an increase of operational cost, delays and inconvenience to a large majority of harmless passengers.

The problem of the optimization of airport security measures and the improvement of its efficiency by introducing the concept of A-CDM (Airport Collaborative Decision Making) is present today.

From the scientific perspective, the efficient screening of passengers at airports remain a challenge and the main objective of this thesis is to open new lines of research in this field by developing advanced approaches using the resources of Computer Science.

This thesis consists of five main chapters:

- Chapter II first introduces the main concepts and definitions of airport security and the major challenges facing the world today, and then classifies the breaches of airport security before presenting various examples of breaches of this security.

- Chapter III gives a brief overview of airport information flows with a view to CDM (Collaborative Decision Making). The passenger terminal control systems and more specifically the screening inspection positions are identified and described.

- In Chapter IV, a logical model of the departure control system for passengers at an airport is proposed. This model is transcribed into a graphical view (Controlled Satisfiability Graph-CSG) which allows to test the screening system with different attack scenarios. This enables the analysis of its behaviour under these conditions and to assess its vulnerability with respect to different types of attacks, by researching special minimum costs paths in the associated CSG.

- The Chapter V focuses on the evaluation of the control system of passenger flows at departure through a probabilistic approach. After considering properties of Bayesian networks and Coloured Petri nets, Bayesian Coloured Petri nets (BCPN) are introduced to assess probability of success and failure of the passengers control system, allowing to take into account the sequence of events which characterize the control process.

- In Chapter VI, an optimization approach is adopted to organize the flow of passengers at departure as best as possible given the probabilistic performance of the elements composing the control system. After the establishment of a global evaluation model based on an undifferentiated serial processing of passengers, a two-stage control structure is analysed which highlights the interest of pre-filtering and organizing the passengers into separate groups.

- Chapter VII draws the conclusions of this study and presents different lines of study for the continuation of this theme.

CHAPTER II

ANALYSIS OF AIR TRANSPORTATION SECURITY THREATS

II.1 Introduction

Airport security refers to the techniques and methods used to protect large number of passengers passing through in addition to staff and planes from terrorism accidents, crimes and another threats. Airport security has heightened drastically after multiple severe crimes and terrorist attacks coupled with the increasing number of passengers traveling around the world. For several decades, the aviation sector has been monitoring the lowest gaps to secure flights, and in recent years it has become rare to link an accident to a technical failure, except for the latest B737 MAX jet accidents.

Currently, the aviation industry has become one of the main targets of terrorist acts and many people have lost their lives in recent years because of its vulnerability, its economic importance and the involvement of the integrity of people and property. Thus most travellers are dreading the once enjoyable airport experience: long lines, intrusive officers, and grumpy flyers make the Airport Security Checkpoint a less than desirable aspect of air travel. We present in the following the main concepts associated with this issue that will better define the framework of our study.

II.2 Security and Safety

In transport in general, security and safety have traditionally been opposed. Safety concerns the prevention against accidental events of mechanical, structural, meteorological or other origin, whereas security aims to take measures against "acts of unlawful interference".

The core business of civil aviation is historically the safety (ensure that aircraft fly safely). Unfortunately, the circumstances have led the civil aviation stakeholders to take more and more account of security. The evolution of threats has made aviation security a real priority for the ICAO (International Civil Aviation Organization) and the civil aviation authorities (ICAO 2002).

Aviation safety and aviation security tend to come closer to absolute reliability without ever reaching it.

Safety refers to legislation and to emergency prevention against mechanical, structural or meteorological failures. It is expressed through strict regulations, which impose standards for the manufacture, use and maintenance of aircraft, as well as strict criteria for the training and qualification of technical crews (pilots, flight engineers) and commercial. The regulations do not forget the air traffic control services, which are responsible for flight safety at the same time, guaranteeing take-offs and landings in the best possible conditions. Also the infrastructure of the airports does not escape this concern. Safety depends also on accidental unintentional events.

Security aims to prevention of any deliberate malicious act. The ICAO Annex 17 which is primarily concerned with administrative and co-ordination aspects, as well as with technical measures for the protection of the security of international air transport, defines the security as a "combination of measures and human, material resources to protect civil aviation against acts of unlawful interference". It refers to legislation and measures for the prevention and the protection from the intentional acts, somehow it represents the part of safety related to malicious acts.

Therefore, security measures include legal and/or regulatory arrangements for organizing, coordinating, implementing, assessing and controlling the human and material resources necessary to protect civil aviation against acts of unlawful interference. The acts of unlawful interference cover the capture or hijacking of an aircraft, sabotage or simply an attempt.

Aviation security must be inter-ministerial, international and partnership-based:

1. Inter-ministerial because civil aviation is not the only party to intervene in the security system. Major ministries, primarily the Ministry of Interior through the police and gendarmerie, are in charge of monitoring the implementation of security measures on the ground. We also see that we are in a field that sometimes imposes a number of acts that can affect privacy, such as the palpation of people or search of luggage. Screening operations are therefore carried out under the order and responsibility of the judicial police officers. In the ministries involved in the security process, there are other ones involved such as the Ministry of Foreign Affairs and Ministry of Defence.

2. International: The International Civil Aviation Organization (ICAO) brings together more than 180 countries and aims to ensure a minimum security standard for civil aviation, with the goal that no country lags behind in this area, the slogan being "no country left behind". It is therefore from ICAO that the major international impulses to be implemented come. The United Nations is also concerned about this matter: Security Council Resolution 2309, adopted in September 2016, underlines the importance of efforts in this area. This resolution has a very strong strategic and political significance.
3. Partnership-based, in the sense that security is the fruit of work and cooperation between all partners: aircraft operators, aerodrome operators, airport security companies, freighters. An airport could be considered as a group of multi-background actors, and whose security could not be achieved without permanent coordination. This coordination is done through institutional meetings, but also through regular contacts with all partners.

II.3 Major challenges facing air transport security today

The public areas such as airports where there are large quantities of unchecked luggage around lots of people have proven to be vulnerable targets of terrorism in the last years. In fact, airports were repeatedly submitted to a series of high profile security incidents such as terrorist attacks, aviation workers involved in criminal activity, sabotage, threat to life and property, hostage-taking on board aircrafts or on aerodromes and any other acts of unlawful interference.

The capabilities and systems in place to safeguard access to sensitive areas, the means by which passengers and airports' employees are screened and the security standards, policies and procedures applied, are creating pressure to concerned parties to maintain the safety at its highest level with the number of air travellers projected to nearly double in the next 20 years.

Terrorist attacks in major airports are becoming alarmingly common. Worse, the solutions proposed don't work. There needs to be more deterrents and policies related to security issues addressing the present flaws. Here below is a sample of terror attacks in international airports during the past years:

- 1961: Air France Flight 406, the aircraft was shattered into pieces when a bomb smuggled inside its cargo exploded on 10 May 1961, killing everyone on board.

- 1964: Pacific Air Lines Flight 773 crashed near San Ramon, California, on May 7, 1964, after a passenger shot the flight crew and killed himself, causing the plane to crash and killing all 44 on board.

- 1994: Air France Flight 8969 was hijacked after take-off from Algiers and flown to France on 24 December 1994.

- 2000: CityFlyer Express *Flight 8106*, operated by a BAe 146, was subjected to an attempted hijack on an international scheduled passenger flight from Zürich, Switzerland to London Gatwick Airport. The aircraft landed at Gatwick where the hijacker was arrested. There were no injuries amongst the 98 people on board.

- 2001: American Airlines Flight 11 was hijacked after take-off from Boston during the September 11, 2001, terrorist attacks. The aircraft was subsequently crashed into the North Tower of the World Trade Center in Manhattan, New York, City.

- 2001: United Airlines Flight 175 was hijacked after take-off from Boston during the September 11, 2001, terrorist attacks. The aircraft was subsequently crashed into the South Tower of the World Trade Center in Manhattan, New York, City.

- 2001: American Airlines Flight 77 was hijacked after take-off from Dulles on September 11, 2001. Terrorists crashed the aircraft into The Pentagon in Arlington County, Virginia.

- 2009: Northwest Airlines Flight 253 was the target of the attempted al-Qaida "Christmas Day bombing" on December 25, 2009. Nigerian-born Umar Farouk Abdulmutallab attempted to detonate plastic explosives concealed in his underwear, but was stopped by other passengers.

- 2014: Ethiopian Airlines Flight 702 was carrying 202 passengers and crews when it was hijacked by the co-pilot over Sudan and landed in Geneva International Airport. The co-pilot was arrested.

- 2014: A man carrying a backpack containing 16 firearms with ammunition flew aboard a Delta Air Lines passenger jet to Kennedy International Airport in New York from Hartsfield-Jackson Atlanta International Airport. The suspect was arrested in New York that day after a month's long investigation into gun smuggling to New York from Atlanta. After passing through the regular airport security checkpoints, the suspect received the guns from an accomplice, a Delta baggage handler who had easy access to secure areas of the airport and was able to carry firearms into the terminal.

- 2014: An American who died fighting with ISIS had security clearance at the Minneapolis Airport. Abdirahmaan Muhumed, a Somali man, had a job cleaning planes for the airport — a position that gave him security clearance as well as access to the tarmac and airplanes.

- 2015: The Transportation Safety Administration failed to identify 73 people on terrorism-related watch lists who were hired in the aviation industry, the inspector general of the Department of Homeland Security has revealed it. In a document published following an audit by the DHS, which oversees the TSA, the agency was found to have missed 73 people with terrorism-related category codes being employed by "major airlines, airport vendors, and other employers".

- 2016: Three suicide bombers opened fire on civilians before blowing themselves up at the entrance to one of the busiest airports in the world (i.e. Istanbul Ataturk Airport). At least 42 people were killed and hundreds wounded.

- 2016: Two jihadis blew themselves up at Brussels airport while a third man calmly walked out of terminal in 'planned exit'. Missing bomber's exit from airport was planned say officials, after footage showed him calmly walking out before explosions.

II.4 Mitigating the Threats

It goes without saying that the primary objective with regard to civil aviation security is to assure the protection and safety of passengers, crew, ground personnel, the general public, aircraft and facilities of an airport serving civil aviation, against acts of unlawful interference perpetrated on the ground or in flight.
This is carried out through a combination of measures and the effort of various human and material resources as developed below.

a- Passenger screening at aviation security checkpoints which is a critical component in protecting airports and aircraft from terrorist threats. Recent developments in screening device technology (i.e. Metal Detector, X-Ray, Biological Threat Detector, Chemical Threat Detector) have increased the ability to detect specific types of threats such as guns, knives, and explosives (Makkonen et al. 2015).

b- Optimizing the allocation of equipment and work teams to control the flows of passengers by minimizing the possibility of dangerous situations inside the passenger terminal including suspect passenger being admitted on board of an aircraft, while insuring a minimum quality of service to passenger.

c- Massively investing in new installations equipment and workforce to meet the new requirements of the security regulations.

d- Proper identification of passengers by introducing biometric passports and ID cards.
A biometric passport (also known as an e-passport, or a digital passport) is a passport that has an embedded electronic microprocessor chip which contains biometric information that can be used to authenticate the identity of passport holder. The passport's critical information is both printed on the data page of the passport and stored in the chip. Public Key Infrastructure (PKI) is used to authenticate the data stored electronically in the passport chip making it expensive and difficult to forge when all security mechanisms are fully and correctly implemented.

e- Encouraging Airport operators and air carriers to educate aviation workers on their role in mitigating insider threats and securing access to sensitive areas of airports.

II.5 Inconsistent Solutions

With the increasing demand for air transportation and new security policy, there are many operations that are influenced by limited resources and infrastructure. These constraints can create, among others, significant bottlenecks, long passenger queues, congestion and overall delays, customer dissatisfaction and rising financial costs (De Barros et al., 2007).

a- A large percentage of passengers could be screened using specialized, costly, and time-consuming devices. Yet, this resulting increase in security may carry the additional expense of longer processing times, increased screening device operational costs, and a larger taskforce of security personnel.

b- Passenger screening may lead to two types of errors in threat detection: false alarms and false clears.
   - False alarms refer to preventing a non-threatening passenger from going through the system. These can cause unnecessary delays for passengers and may result in missed flights.
   - False clears refer to letting a threat go through the system. These may have more significant effects such as considerable passenger injury or destruction in the airport.

c- The number of travellers per year is increasing along with their impatience and dissatisfaction with ever-changing airport security procedures and the useless time consumed.

d- The new security measures taken have influenced negatively air transportation demand levels to airlines due to the increasing airport taxes to cover the cost of security actions implemented and the huge investment in baggage-screening equipment used.

e- Screening and other airport security functions presumes that all air travelers are equally likely to be a threat, and mandates equal attention and spending on each, which is very wasteful of security resources.

f- Most of the times, the vast majority of passengers are screened solely for metallic objects. Yet a terrorist bent on either blowing up or taking over a plane could wear body-conformal plastique or carry a variety of non-metallic lethal weapons.

g- The fact that infrastructure capacity and the available number of resources at some airports is still limited such as the number of common check-in counters kept available and number of personnel available.

h- Security at airports is generally treated as an infrastructure issue (i.e. static picture of airport security). However, due to the complex operational airport activities that is evolving over time, the dynamics of airport security needs to be analyzed and studied.

i- The merging of cyber and physical creates new vulnerabilities and the potential points of cyber vulnerability in aviation are many and growing. Many systems in civilian aviation are potentially hackable: reservation systems, flight traffic management systems, access control management systems, departure control systems, passport control systems, cloud-based airline data storage, and hazardous materials transportation management, cargo handling and shipping.

II.6 Classification of breaches of aviation security

In this section are displayed the different types and modalities of breaches of aviation security (ICAO, 2013).

II.6.1 Typology of breaches of aviation security

The breaches of aviation security can be broken down into several major groups:

The unlawful capture or hijacking of aircraft in flight or on the ground of seizing an aircraft by violence or the threat of violence with a view to diverting it from its destination. Three main motives can be the basis of these acts, it is about flight, extortion and terrorism. The failing security of airports can encourage this type of violence.

More specifically, unlawful capture is defined by Article 1 of the Hague Convention "commits a criminal offense (hereinafter referred to as" offense ") any person who, on board an aircraft in flight:

- unlawfully and by violence or threat of violence, seizes or controls that aircraft or attempts to commit any such act or
- is an accomplice of a person who commits or attempts to commit any of these acts?

Diversion is the act of diverting an aircraft from its route for security reasons and with the concurrence of air traffic control. Diversion may occur in flight with or without the threat of violence.

Bombings that are carried out using explosive devices or using an aircraft as a flying bomb. They constitute 80% of terrorist acts;

Hostage-taking on an aircraft or at the aerodrome;

Force, intrusion on an aircraft, at an airport or within an aeronautical facility;

I**ntroduction of a weapon** on board an aircraft or an airport, a dangerous device or a dangerous substance for criminal purposes;

Communication of false information of a nature to compromise the safety of an aircraft in flight or on the ground, of passengers, navigators, ground personnel or the public, at an airport or in the enclosure of an installation of civil aviation.

II.6.2 Modalities of breaches for aviation security

Unlawful acts of intervention can be analyzed in different ways. For example, it can be discovered:

- individuals acting on their own behalf and those acting on behalf of a third party (limited partner).
- isolated authors of those belonging to a structured political organization (in the broad sense).
- acts committed according to the motivation of the authors and their seriousness.

What characterizes all the acts of unlawful interference directed against the security of the air transport of passengers, is this triangular relation: author-victim-target, common to the hostage/taking crimes and all the terrorist acts. It is indeed very rare in civil aviation, that the victim, itself is the target of the action. Isolated authors generally belong to the category described by psychiatrists as passionate idealists. These are subjects with strong paranoid

components, that is to say, proud, psychorigid, interpretants, maladjusted. In terms of groups, it was possible to observe that all conceivable combinations and alliances were possible, including outsourcing. This state of affairs has made for several years any logical analysis extremely difficult.

In the case of victims, they may be natural persons or goods: aircraft, airport facilities and aviation facilities. Targets, in turn, are often legal persons of public law and sometimes legal persons of private law.

Whether the perpetrators of the offenses act alone or in an organized group, there are two main categories of actions: those that target a legal person and those that are rarer, targeting a natural person.

Actions against a corporation may be classified as follows:

- Actions decided by certain States, executed directly by them or by terrorist groups in their service and intended to put pressure on another State;
- Actions taken as a framework of a State, in order to settle accounts which are perfectly foreign to it;
- Actions that seek to undermine the moral, political or economic credibility of a State or destabilize it;
- Actions to test the ability of a state to react;
- Actions targeting a legal person governed by private law and executed by common criminals (blackmail, extortion ...);
- Personal actions of irresponsible or mentally ill people (revenge, solidarity towards a cause ...).

Actions targeting a natural person may be of the following types:

- Actions directed against individuals occupying a specific function or exercising a specific occupation, without an institution or a state being targeted (journalist, artist, writer, teacher ...);
- Actions targeting an institution or a State and targeting individuals because of their ethnicity, religion political opinions or nationality and / or functions (embassy employee, activist ...);
- Actions executed by common criminals;
- Individual actions of irresponsible or mentally ill individuals.

Apart from one or two cases of no statistical value, it can be said that current safety measures are insufficient to discourage enthusiasts. Currently, the motivation of the authors follows, or sometimes precedes, with a slight shift, the curve of global political crises. The gravity of the acts follows, as for it, an increasing curve. In recent decades, unlawful acts of intervention have sought more to make a name for themselves, to raise awareness of their organization and determination, by numerous summary executions, than to obtain a real counterpart. Among the main reasons are the will to flee a country and its regime, the will to fight a country and its regime, the payment of a ransom or extortion.

II.7 Conclusion

In view of the diversity and complexity of threats that can be implemented at and through airports, the control of departing passengers at airports plays a central place in the security of air transportation.

In the next chapter, airport passenger control will be presented. Its composition, national and international regulations and practice will be analyzed.

CHAPTER III

AIRPORT PASSENGER INSPECTION

III.1 Introduction

The study of the safety of a terminal requires not only a thorough knowledge of the various functions assigned to it but also a perfect mastery of its composition in order to be able to impair efficiently the mischievous, planned or not, behaviour of the terrorists. In this chapter, after analysing the different flows involved with airport security, the inspection function of passengers, agents and luggage, is described and different inspection systems are considered. The main objective of this chapter is to introduce the necessary knowledge about airport inspection systems so that effective models can be built to assess their performance.

III.2 Flows in airports

The dangerous person or object necessarily infiltrate into the flows of people and goods implemented in the airport.

A flow is a movement of people or objects along a well-defined path to get from one point to another. There is a wide variety of flows in an airport: passenger flows, aircraft flows, baggage flows, personnel flows, service vehicle flows and others. They can interact with each other or not. The general safety rules impose constraints in terms of non-mixing of certain flows while maintaining some facilitation (processing capacity, system flexibility, passenger comfort).

The main rules generally accepted in airport passenger flow management are (GAO 2005, HMSO 2005):

- no mixing of flows at departure
- no mixing of flows on arrival (tolerance if flows have the same regime)
- no flow crossing
- existence of alternative routes in case of degraded situation
- minimizing distances to travel
- signage corresponding to these rules

III.2.1 Movement of airport staff, airlines and service companies

In order to avoid the intrusion of a dangerous person posing as an airport staff member, airline or Service Company, all personnel working at the airport must wear a security badge during the day when he/she is in a reserved area or in a security restricted area. The issuance of a security badge is subject to the applicant's attendance of a security awareness session and the approval of the application by the police services (criminal record check). The possession of a security badge does not mean the right to circulate throughout the reserved area of the airport which can be divided into several geographical areas. In France, for example, reserved area is divided into four geographical sectors (Russel et al., 2005):

A (plane): In zone A, near the plane, will circulate all those who take care of the device during his/her call (refuellers, baggage handlers ...).

B (luggage): This zone corresponds to the baggage galleries; baggage handlers and security operators can circulate there.

F (Freight): This area is dedicated to freight activities.

P (passengers): Zone P corresponds to the parts of the terminal where the passengers are travelling.

III.2.2 Circuits for passengers and hand luggage.

Different stages compose the circuit of a passenger within an airport. The necessary steps are based on the passenger (depending on whether he is departing, connecting or arriving, according to his nationality, according to his destination ...) and their effective order depends on the configuration of the terminal. Nevertheless, here it is considered a simplified circuit including the steps and controls common to all airports (Kaffa-Jackou, 2011). A simplified diagram of the departure and arrival circuits is displayed in Figure 3.1. It shows the main controls which passengers and baggage are submitted to in order to ensure security in the terminal and in the aircraft.

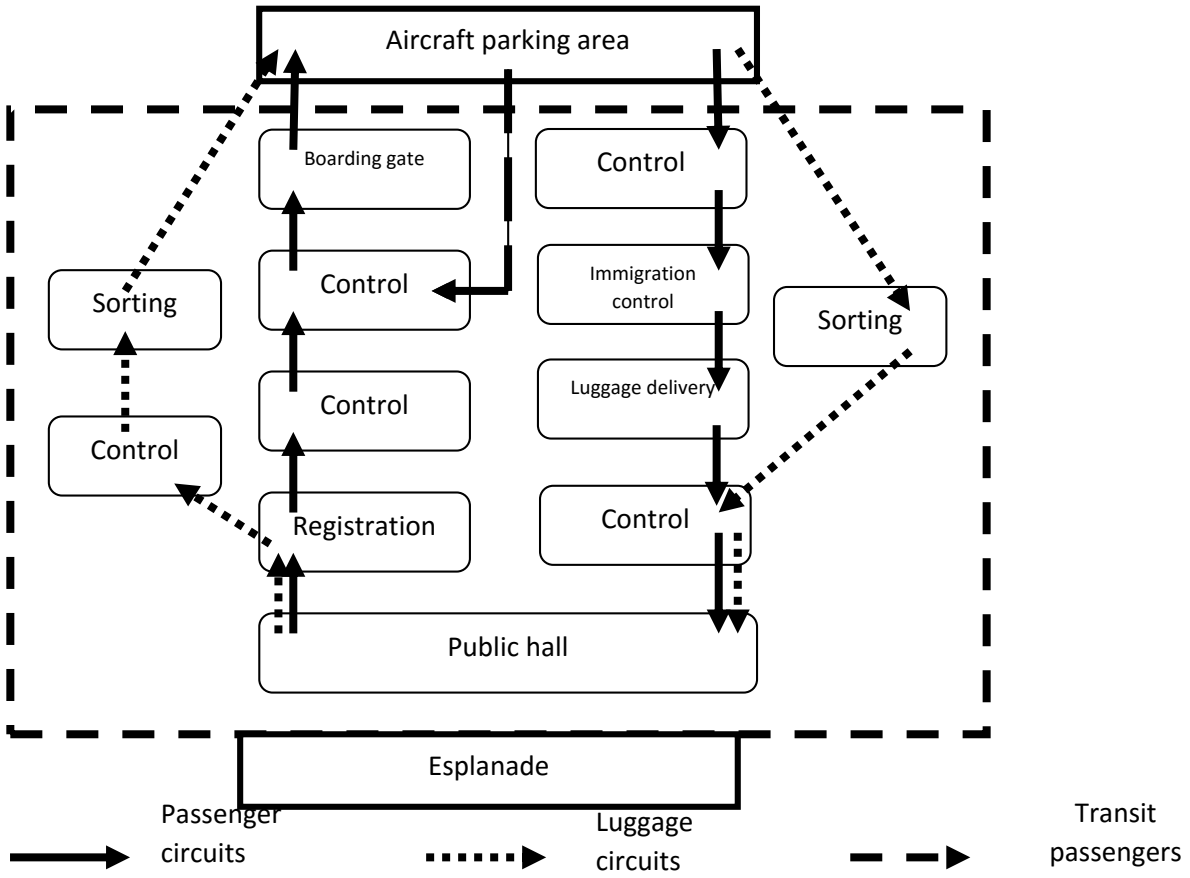


Figure 3.1 Passengers flows inside an airport

III.3 General Description of the Passenger Inspection Station

The inspection is a preventive operation carried out for the purpose of detecting prohibited articles (ICAO 2008). The means used may be a search, one or more detection equipment (radioscopic or explosives), safety patches or a combination of them. It usually takes place at the entrance of the security restricted area (see Figure 3.2).

III.3.1 Definitions

Prohibited articles are "any substance or object that may constitute a threat to the security of air transport". A distinction may be made between: (i) firearms, (ii) knives and sharp instruments, (iii) blunt instruments, (iv) explosives, (v) ammunition, (vi) flammable liquids prohibited in bolsters, (vii) corrosive products, (viii) neutralizing or incapacitating items prohibited in the hold, (ix) articles that may be used as a weapon, (x) items that may

be deemed to be a lethal weapon, (xi) chemical and biological items and substances that may be used in the attacks, (xii) restricted carriage of liquids since 6/11/06 in Europe, in the United States of America and in some African countries.

If not properly managed, security measures at airports may have adverse effects on the movement of departing passengers. To improve the management of security measures, the various stakeholders at the airport have well-defined missions. These different missions have their origins in the Standards and Recommended Practices of ICAO Annex 17, Doc 8973, National Security Plans or Airport Security Plans.

The people in charge of the screening inspection control can be state agents (police) or private security agents. They are required to:

- carry out the inspections in accordance with the regulations in force,
- follow initial and continuous training and periodic training,
- execute performance tests in operational situation,
- establish a safety program and a quality assurance program.

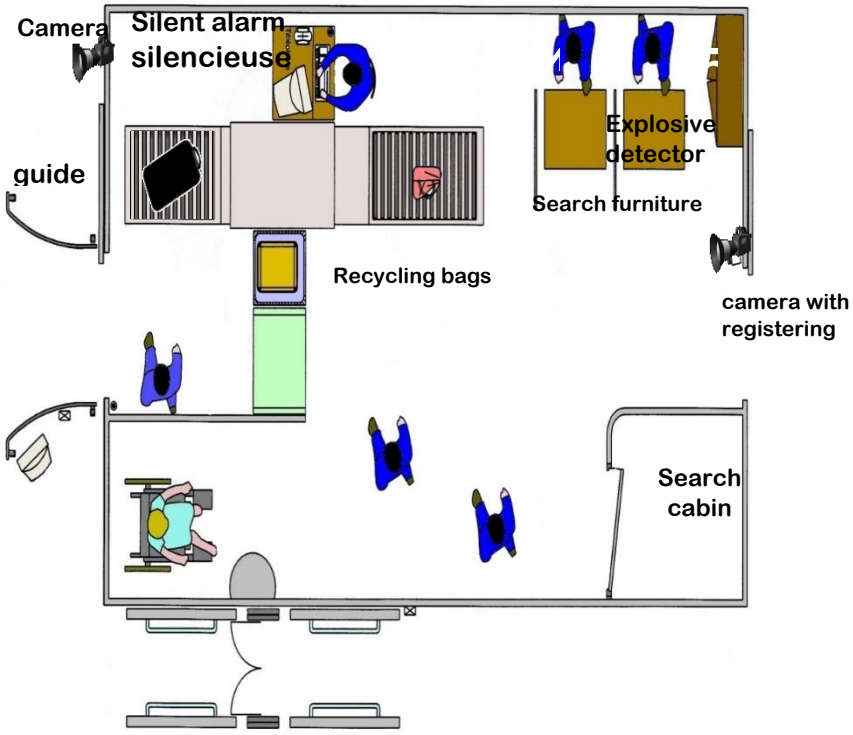


Figure 3.2 Layout of an inspection station

In the case of TSA (Transport Security Administration of USA), the inspection process is composed of four physical zones (see Figure 3.3):

- Zone A, where after their entrance in the departure hall, pre-checked passengers and regular passengers wait in their respective lines.
- Zone B, where, after check-in, pre-checked and regular passengers enter in lane and pass security scan.
- Zone C, where, if they pass successful security scan, they collect their belongings.
- Zone D, where passengers who fail security check, receive an additional inspection.

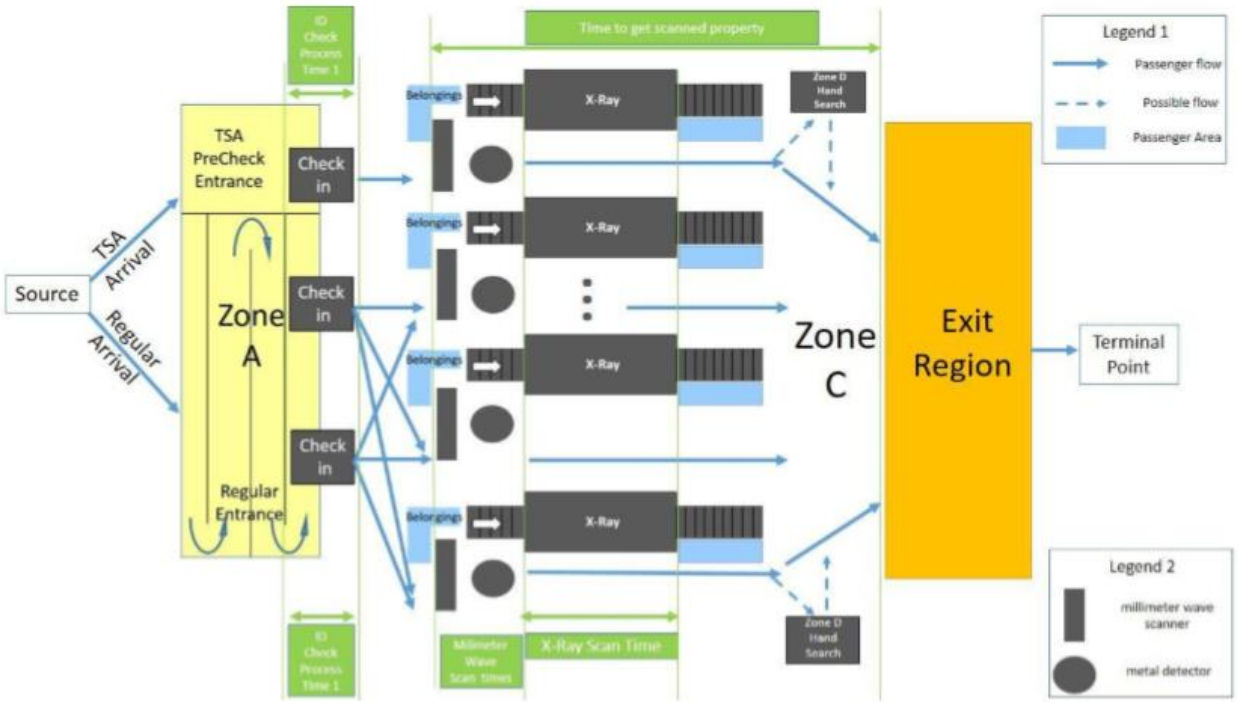


Figure 3.3 Example of physical organization of passengers inspection station (TSA)

The minimum equipment required today for the operation of a screening inspection station consists of:

- A device that closes and blocks the door when the station is not in use
- a magnetometer
- a cabin + table for the search
- a table to search the luggage
- a phone

- an XR and calibration means
- a silent alarm
- a poster to inform passengers
- a camera sometimes

Many airports now have a trace detector or use body scanners.

III.3.2 Human resources at inspection stations:

Screening procedures require well-trained staff, sufficient equipment and enough time to complete the controls.

The armament of the inspection station recommended by ICAO Doc 8973 is as follows:

- an upstream agent to check travel documents, boarding pass, handle baggage handling, electronic device management, electronic device management and small items;
- a downstream agent for the management of alarms, palpation (a woman / a man)
- a downstream agent to monitor images and interpret images
- an agent for the search of baggage downstream
- a trace detector
- a supervisor who must not perform duties other than risk assessment and dispute management

A rotation of security officers must be scheduled at least every twenty minutes. This will allow the officer that examines the X-ray images to rest his eyes. This activity should only be resumed after a period of 40 minutes.

The armament of the BIP depends on the flows processed and the type of flights. Inspection station staffing needs to be strengthened in the following cases:

- in special circumstances requiring increased security measures,
- a high level of passenger flow,
- Absence or unavailability of control equipment.

III.4 Control Procedures at the Screening Inspection Station

All passengers and their cabin baggage, all personnel and their equipment must undergo the screening. All personnel and equipment passing through the screening station must be screened.

III.4.1 Procedures for controlling persons

Passengers are greeted by a security officer or police officer. The agent verifies the access permissions:

- for the passenger, it is the travel document
- for aircrew, it is the navigator card or other valid document
- For the staff, it is an *ad hoc* title.

Then, the person wishing to enter the reserved area must pass through the portico.

There are the following steps:

- The passenger arrives at the inspection station, removes anything that contains metal and passes his cabin luggage under the XR.
- under the portico
- if the gantry crashes, the passenger passes under the gantry
- The portico does not ring. the passenger may experience random palpation or return to pick up his cabin baggage.
- If the alarms persist, the passenger must be palpated and scanned with a magnetometer
- If the security officer notices that the alarm has persisted, he/she calls on the OPJ or the person authorized to carry out a body search of the passenger. This search is done in cabin with the authorization of the passenger.
- If doubt cannot be removed, the passenger does not embark.
- If the passenger sounds the alarm, the passenger is palpated and can pick up his luggage
- If the passage under the gantry does not generate an alarm, the passenger may experience a random palpation
- The passengers wait to recover their cabin luggage. The cabin luggage is going under the XR. In case of doubt (opaque object or difficult to identify for example), the security agents may request the opening of the baggage which will be searched with the authorization of their owner. Objects prohibited in the cabin must be subject to

local instructions. Checks must continue even after discovery of prohibited articles or objects. Other items may be concealed. Cabin baggage may be randomly searched.

- Then, the passengers go to the departure lounge.

When a passenger refuses to submit to the check, it is planned to:

- report the person to the police
- warn the captain
- refuse boarding to the passenger
- Remove the passenger's hold baggage.

A passenger appearing nervous or arrogant should always be searched. In the case of the United States: the TSA, the US agency responsible for protecting air transport, has come to the conclusion that "the worst danger to commercial aviation comes less from objects that can be transported by the evil people than these people themselves". As a result, the TSA is setting up a new passenger screening system called SPOT (Screening of Passengers by Observation Techniques). As part of SPOT, TSA staff learn to recognize suspicious behaviour. "Awakening passengers with signs of anxiety will be reported to the local police, who will conduct face-to-face interviews with them to determine if they pose a threat."

III.4.2 Inspection procedures for cabin baggage and other goods and products

The security officers must apply the following rules to the handling of cabin baggage, when detection equipment is used:

- to proceed in case of alarm of the equipment of detection or absence of validation of the operator, with the search of the luggage or the object
- To carry out a random search of cabin baggage respecting the quantitative objectives by the authorities.

The alert or call to the police must be made when:

- the security agents discover a 1st or 4th category weapon, an improvised explosive device (IED),
- a security officer is attacked
- a passenger tries to pass in force at the inspection station

- When a passenger disturbs public order in the departure lounge.

Figure 3.4 Passengers inspection tasks and paths

III.5 The different filter inspection systems

The experiences of different states in screening passengers and their carry-on baggage have led to the development of three main systems commonly referred to as: (i) door-to-gate screening systems, (ii) a waiting room and (iii) at the entrance of a hall (Kaffa-Jackou, 2011).

III.5.1 General principles

Whichever system is used, it must include the necessary elements to prevent the introduction of firearms or knives and dangerous goods on board aircraft and to discover a potential aggressor before he ascends. on board. One of its basic elements is to be able to benefit from the assistance of law enforcement officers at each screening post. These officers should be armed to respond immediately and effectively to criminal activities involving weapons. They should be assigned to a location from which they can monitor each screening station. If such arrangements cannot be made, an officer should be able to intervene quickly at each screening post if assistance is required. Some states have established response times considered

sufficient for all circumstances; given the volume of screening operations, the level of the threat, and the configuration of the airport and passenger terminal.

It must be ensured that there is no possibility of mixing or contact at departure or arrival between passengers who have been subjected to a security check and persons not subject to such control, after the passage security screening points at airports; if there is mixing or contact, the passengers in question and their cabin baggage will be re-screened before boarding an aircraft.

In addition to the personnel mentioned above, the injection / filtering system should also include specialized devices. The manual search of passengers and their hand luggage is certainly effective but it is relatively slow and requires well-trained and qualified personnel. The use of metal detectors and X-ray machines will, however, greatly improve the efficiency of screening and, therefore, the routing of passengers. It is important to manually search for items that do not pass the electronic examination in a satisfactory manner.
The three main inspection systems and their respective advantages and disadvantages are described in sub-sections III.5.2, III.5.3 and III.5.4. Safety devices at a fixed location should always be between protected when not in use.

III.5.2 Inspection / screening at the boarding gate.

The screening is carried out immediately prior to boarding at a checkpoint located at the boarding gates that lead to the aircraft. The door can lead to a bridge that is directly connected to the aircraft or on an apron to access it. The screening takes place at the moment when the boarding of the passengers begins and when the door leading to the aircraft is opened. Staff and equipment are available on-site as quickly as possible (ie, so as not to unduly delay the flight). Security officers will only occupy the checkpoint when required, to perform the screening. However, the screening station and access by this post must be protected outside of hours of use.

III.5.3 Inspection / filtering at the entrance of a waiting room.

The screening is done at the entrance to an area designed specifically to keep passengers waiting before they board. The area is protected (i.e. rendered sterile) by appropriate walls or

barriers and all these access points are controlled. The waiting room may also be a vehicle specifically designed to transport passengers to a distant aircraft. The door leading to the traffic area remains locked until the actual embarkation (all or most of the passengers and their hand luggage will have been inspected / filtered). The waiting room should be kept secure when not in use. If it is not, it must be searched before being used to ensure that weapons or dangerous devices have not been introduced by a potential aggressor or an accomplice for later use. It will not be necessary to implement so many personnel and devices because in this case the inspection/filtering can be done more slowly. Security officers will only occupy the checkpoint at the time of screening.

III.5.4 Inspection / screening at the entrance of a hall.

Screening is done at the entrance to a hall or satellite that has multiple gates. All access points must be controlled to maintain sterility. After a full inspection at the beginning of the day confirms that the hall is sterile, the hall must be locked or patrolled when not in use. However, since sterile halls are usually employed continuously, or at least as long as the passenger terminal are open and accessible to the public, inspections do not need to be frequent. The screening is done simultaneously for several flights at a time. More personnel and equipment may be required than single-door or waiting-room checkpoints because of the higher number of passengers to be routed. Nevertheless, since only one checkpoint is use for several boarding gates, this method allows better use of resources in personnel and equipment, with a considerable economic benefit.

III.6 Evaluation

States do not agree on the advantages and disadvantages of each of the systems discussed above. Each state and airport authority will have to evaluate them and decide on the system or combination of systems that they deem most appropriate for the airport configuration, taking into account all the factors involved.

One of the benefits of the door-to-gate screening system is that it minimizes the possibility of firearms and other dangerous devices being surreptitiously handed over to passengers who have already been inspected / screened at the entrance. the waiting room would have the same

advantage, provided that it is checked carefully; before using this room, no weapons are hidden, and strictly maintain the sterility of this room each time it is used.

Other states consider that it is advantageous to separate the aircraft as much as possible from the point where a potential aggressor has to report to the security screening and that the screening/screening systems at the entrance to a security room waiting and hall allow such a separation. This is defined in time or distance. Screening at the entrance to the waiting room allows time separation primarily, since the checkpoint is usually only a few meters from the boarding gate. However, it happens very often that the aircraft is not parked there at the time of the inspection. On the other hand, the door that opens onto the gangway or the apron is locked until the passengers embark permanently. The security services may be confronted with a malicious person before the intended aircraft becomes accessible. The inspection system at the entrance of a hall is generally even more efficient because it allows separation both in time and space. Most of the time, passengers do not know at what station the aircraft must park, and if it is already there. The increased separation over time and space helps to improve the response time of the security services.

The two systems (waiting room and lobby) increase security by allowing screening officers to perform their duties at a slower pace, and therefore more carefully. They will more often decide not to control a suspicious or unidentifiable object if passenger inspections are to be accelerated due to the imminent departure of the aircraft. Moreover, it is likely that any difficulties will be more easily solved and that the agents of purity, less in a hurry, will kindly answer the questions of the passengers. They will be less likely to gather at the checkpoint to board an aircraft that is clearly ready to receive them as soon as possible. Flight disruption caused by delays can have a negative impact on the deployment of security personnel in this type of system.

They have little effect on the deployment of screening staff at the entrance of a lobby.
The police, gendarmerie and customs control the effective implementation of measures by all operators. They evaluate the performance of the security service or attend the tests in operational situation. They may also establish findings of breaches of the regulations.

Placed under the responsibility of the aerodrome operators, the screening of passengers at the entrances to boarding lounges has been considerably strengthened in recent years. All sharp or

blunt objects have been added to the list of prohibited items in the cabin. The sensitivity of the gates for detecting metal masses has been increased. Besides, a very large percentage of passengers are now subject to further examination.

Thoroughly, screening passengers and their baggage requires well-trained security personnel, adequate security equipment and enough time to complete the security process. If security controls are not carried out efficiently, compliance with air service schedules will be compromised. In addition, congestion at checkpoints can be exploited by people seeking to bypass the security system.

CHAPTER IV

ACCESSMENT OF VULNERABILITY OF INSPECTION STATIONS: A SATISFIABILITY APPROACH

IV.1 Introduction

This chapter develops a logical framework to access the vulnerability of passenger control process to different threats. The initial objective is to determine in which conditions a threat will be able to go undetected through a departure passengers control process. Chapter II has presented in detail the composition and operational procedures implemented in the screening inspection positions. Few models have been already proposed in the literature to represent and analyse the inspection process. Some early models are mere graphical representation of the different stages of the inspection process, others present a static logical framework where the involved resources and means are not formalized.

In this chapter are not considered or estimated probabilities of occurrence of passenger control failures, but only their possibility and the conditions for that.
Then, in this chapter, a pure logical framework is developed to establish the logical constraint each inspection station must satisfy to insure robustness to malicious behaviour. Considering the nature of the resulting logical satisfiability problem, an approach based on a graphical representation of the control process is adopted, leading to computing minimum length paths representative of optimal malicious behaviour.
The proposed approach turns it possible to detect the minimum number of elementary control defects that turn a control failure possible. It also allows to generate different attack scenarios to the control system by a threat, to analyse the behaviour of the system under these conditions and to evaluate their permeability with respect to different types of attacks.

IV.2 Theoretical background

Here the main idea is to formulate the inspection failure analysis as a constrained Boolean problem. Many studies and researches have been developed in the last fifty years, boosted by the continuous improvement on computers' performance.

IV.2.1 Boolean representation of constrained systems

Boolean algebra (Almos 1963, Givant et al., 2009) is an algebra defined on the truth values, true (T) or false (F), of the considered variables.

A *logical* or *Boolean formula* Σ is a string of symbols composed of Boolean variables, their literals organized in *clauses* and *binary operators*, such as ***negation*** ($\bar{x}$), ***and*** (∧), ***or*** (∨) and ***nor*** (⊗) leading to logical formulas. Π(Σ) denotes the set of variables occurring in Σ.

Example, for the formula Σ= (a∨$\bar{b}$∨c)∧(b∨c)∧($\bar{a}$∨$\bar{c}$), the set of occurring variables is Π(Σ) = {a, b, c}, appearing as literals: a, $\bar{a}$, b, $\bar{b}$, c, $\bar{c}$, with clauses : (a∨$\bar{b}$∨c), (b∨c) and ($\bar{a}$∨$\bar{c}$).

To each complete assignation *V* of truth values to Π(Σ), the truth value of the formula Σ can be computed by replacing the variables *x* by their values. If Σ is evaluated to be true, *V* is said to be a solution of Σ, or Σ(*V*)=T.

When a solution exists for formula Σ, Σ is said to be consistent or *satisfiable*. If no such solution exists, Σ is said to be inconsistent or unsatisfiable.

For example Σ= (a ∨ $\bar{b}$ ∨c) ∧(b ∨c) ∧($\bar{a}$∨$\bar{c}$) is satisfiable (take a=T, b=T and c=F).

A *logical constraint* can be formulated as a formula Σ being evaluated as T (or F) for a given assignation *V* to its variables.

Propositional calculus is a symbolic system of treating complex propositions and their logical relationships. In the case of Boolean logic, propositions are Boolean formulae and their relationships are defined by the different rules, such as the resolution rule.

In order to have a set of rules on Boolean formulae, it is useful to adopt a normal form that every formula must have. The most common normal forms are the *conjunctive normal form* (CNF) and the *disjunctive normal form* (DNF). Both forms use the concept of literal variable and its negation. For the disjunctive normal form, the main object is a disjunction of literals (x∧$\bar{y}$), or *cube*. A cube *K* is said unsatisfied when at least one literal is evaluated to be true. Disjunctive normal form formulæ are composed of a number *n* of conjunctions of cubes: $K_1 \vee ... \vee K_n$. A disjunctive normal form formula Σ is unsatisfied if there exists at least one assignation such that every cube in Σ is unsatisfied.

The main object in a conjunctive normal form is a *clause* which is a disjunction of literals (x∨$\bar{y}$). A clause *C* is said satisfied if there exists at least one assignation such that at least one of the literals

can be evaluated to be true. Conjunctive normal form formulæ are composed of a conjunction of clauses: $C_1 \wedge ... \wedge C_n$. A conjunctive normal form formula Σ is satisfied if there exist at least one assignation such that every clause in Σ is satisfied.

It is possible to convert any general Boolean formula to a conjunctive normal form formula Σ, however the computational time to get this result may increase exponentially with the size of the problem.

IV.2.2 The Satisfiability Problem

A problem of satisfaction of Boolean constraints (Bunning et al., 1995), also called *problem satisfiability*, consists, given a set of constraints defined with Boolean variables, to decide whether there exists an assignment of logical values to the variables which allows to satisfy all the constraints, and if possible to determine such feasible assignment. When this assignment does not exist and, it can be of interest to search for an assignment satisfying a maximum number of constraints, or to search for an assignment not satisfying a minimum number of constraints.

A Boolean constraint satisfaction problem is the problem known as SAT, of deciding whether a propositional formula (expressed as a conjunction of disjunctions) is satisfiable or not. The 2-SAT problem is the restriction of the SAT problem to conjunctive normal formulae with at most 2 literals per clause. The 3-SAT problem is the restriction of the SAT problem to conjunctive normal formulae with at most 3 literals per clause (Sais 2008). This problem as many other of the satisfiability family present computational problems when solving them effectively.

The *computational complexity theory* (Brookshear, 1989) distinguishes a limited number of large classes of complexity for discrete computational problems but with many slightly differentiated subdivisions. The complexity class *P* is seen as the class of computational problems which admits an efficient algorithm, i.e. an algorithm which provides a solution in an acceptable polynomial time or memory space. The complexity class *NP* is composed of problems that people would like to solve efficiently, but for which no efficient algorithm is known. Thus the class of the *NP*-complete problems contains the problems of *NP* which are the ones most likely not to be in *P*. While 2-SAT is of complexity class *P*, 3-SAT has been the first problem shown to be *NP*-complete by Cook in 1971 (Cook, 1971). Since it has remained a reference problem in the study of the *NP*-difficulty of computational problems. The *NP*-completeness of SAT ensures that no algorithm for this problem can be computationally effective *in its worst case* instance. However, for many

instances encountered in practical applications, this problem can be solved in an acceptable computing time. So, there are, in practice, many effective algorithms to solve instances of the SAT problem associated with real problems.

One of the first methods used to cope with the SAT problem has been the generation of truth tables. The algorithm to generate the truth tables creates every possible instantiation and whenever an instantiation provides a solution, the formula is proven satisfiable. If no instantiation provides any model, the formula is proven unsatisfiable.

A landmark is the algorithm developed has been the DDL (Davis et al., 1962) where the main idea is to remove variables until no variable can be removed or the empty clause is generated. This method needs a large memory to store all generated clauses. Its search scheme can be represented by a tree where each node of the tree represents the current state of the formula given at the root and simplified along the path between the node and the root.

Compared to those two first algorithms which can be qualified as *complete*, there exists a large number of *incomplete* algorithms, most of which use a local search schema. These algorithms, contrarily to the complete ones, may be unable to prove the unsatisfiability of a formula. This area has been and still is under active research with news algorithms integrating parallelization and propagation processes and others (Vizel et al., 2015).

IV.3 Logical modelling of nominal passenger control

The herein considered passengers logical control models make use of Boolean algebra and results from: (i) the arrangement of the various constituent elements of the airport control system and (ii) the nominal or non-nominal operating procedures of the latter. The model must be completed by scenarios concerning:

- The data available for a passenger posing a threat or not.
- The operational state of the system (equipment and control procedures operating or failing on an ad hoc basis or not).

The main purpose of the modelling specified in this sub-section is to evaluate the permeability of an airport terminal to boarding threats. It is considered that the passenger (staff members are not considered in this study, but should be in a complete threat study) are assigned with a data set whose components represent the real characteristics of the person:

- Does he/she hold one or more tickets?
- Does he/she have an identity card or passport in accordance with this or these tickets?
- Is he/she able to commit an act affecting the security of air transport?
- Does he/she possess material means constituting a threat?

All data can be represented by a set of Boolean variables and the transition from one area of the airport to another will correspond to the apparent satisfaction of certain logical constraints. As an example, consider the situation at the level of the constraints related to the registration bank, where the possession of a ticket and the possession of a piece of matching identity are validated. If the passenger has malicious intentions, they are modelled by logical conditions that check if they can be satisfied or not in a scenario. It is then a question of identifying the conditions of satisfaction of a breakthrough scenario. Then, taking into account its consequences for safety, possible adjustments of the control system and associated procedures should be proposed to turn it unfeasible.

IV.3.1 Passenger logical data

The information concerning a passenger is given by a data set whose Boolean components represent the information characterizing this person (either well or ill-intentioned).
Several stages take place in the evolution of the data set associated to a passenger:

- initial data;
- acquired data: for example, the transition to the registration banks with a ticket and a corresponding identity recognized true alters the initial resources by providing the data component "boarding pass".
- final data: they are obtained taking into account the possible contributions during the path of the target person (dangerous object obtained in the duty-free zone, accomplice handing an object, ...).

These components can be classified as:

- Identification:
  - X_1: possession of identity card,

- X_2: authenticity of identity card,
- X_3: possession of passport,
- X_4: authenticity of passport.

- Transport ticket:
  - X_5: possession of domestic title,
  - X_6: authenticity of domestic title,
  - X_7: possession of international title,
  - X_8: authenticity of international title,
- Boarding card:
  - X_9: Possession of a domestic boarding card,
  - X_{10}: authenticity of domestic boarding card,
  - X_{11}: possession of international boarding card,
  - X_{12}: authenticity of international boarding cards,
- Prohibited object:
  - X_{13}: no metal object located in the hand luggage,
  - X_{14}: no organic object located in the hand luggage,
  - X_{15}: no inorganic object in the hand luggage,
  - X_{16}: no metal object under the clothes,
  - X_{17}: no organic object located under clothing,
  - X_{18}: no inorganic object under the clothes.
- Dangerous object:
  - X_{19}: no dangerous metal objet in hand luggage,
  - X_{20}: no dangerous organic object in hand luggage,
  - X_{21}: no dangerous inorganic object in hand luggage,
  - X_{22}: no dangerous metal objet under clothes,
  - X_{23}: no dangerous organic object under clothes,
  - X_{24}: no dangerous inorganic object under clothes,
  - X_{25}: no prohibited or dangerous object in hold luggage.
- Concordance:
  - X_{26}: Air ticket and identity document coincide,
  - X_{27}: boarding card and identity document coincide.

IV.3.2 Control stages

To each control element of the passenger control station it can be associated the test on one or more components of the vector $\underline{X}$.
The lists below display the components tested by the different passenger control stages:

- Identity Document validation : X_1, X_2, X_3, X_4
- Ticket reservation: X_5, X_6, X_7, X_8
- Boarding card validation: X_9, X_{10}, X_{11}, X_{12}
- Cross beam detector: X_{16}, X_{22}
- Scanner: X_{13}, X_{14}, X_{15}, X_{19}, X_{20}, X_{21}
- Manual detection: X_{16}, X_{22}
- Passenger search: X_{16}, X_{17}, X_{18}, X_{22}, X_{23}, X_{24}
- Aleatory search: X_{13}, X_{14}, X_{15}, X_{16}, X_{17}, X_{18}, X_{19}, X_{20}, X_{21}, X_{22}, X_{23}, X_{24}
- Luggage search: X_{25}

Different clauses, or macro state variables in some cases, are introduced in order to define more clearly the constraints to satisfy. On one side they contribute to reduce the size of the logical expression describing the operations of the passenger control stations and on the other side they match the corresponding elementary control actions:

$$Z_1=(X_1 \wedge X_2) \quad (4.1\text{-a})$$

$$Z_2=(X_3 \wedge X_4) \quad (4.1\text{-b})$$

$$Z_3=(X_5 \wedge X_6) \quad (4.1\text{-c})$$

$$Z_4 = (X_7 \wedge X_8) \quad (4.1\text{-d})$$

$$Z_5=(X_9 \wedge X_{10}) \quad (4.1\text{-e})$$

$$Z_6=(X_{11} \wedge X_{12}) \quad (4.1\text{-f})$$

$$Z_7=(X_{16} \wedge X_{22}) \quad (4.1\text{-g})$$

$$Z_8 =X_{13} \wedge X_{14} \wedge X_{15} \wedge X_{19} \wedge X_{20} \wedge X_{21} \quad (4.1\text{-h})$$

$$Z_9 = (X_{16} \wedge X_{22}) \quad (4.1\text{-i})$$

$$Z_{10} = (X_{16} \wedge X_{17} \wedge X_{18} \wedge X_{22} \wedge X_{23} \wedge X_{24}) \quad (4.1\text{-j})$$

$$Z_{11} = X_{13} \wedge X_{14} \wedge X_{15} \wedge X_{16} \wedge X_{17} \wedge X_{18} \wedge X_{19} \wedge X_{20} \wedge X_{21} \wedge X_{22} \wedge X_{23} \wedge X_{24} \quad (4.1\text{-k})$$

$$Z_{12} = X_{26} \quad (4.1\text{-l})$$

$$Z_{13} = X_{27} \quad (4.1\text{-m})$$

$$Z_{14} = X_{25} \quad (4.1\text{-n})$$

An additional variable to be taken into account is Z_{15} which is T if international flight, and F if domestic flight. The checks carried out in the passenger control system may depend on each other, for example, the non-random manual search of hand luggage takes place only in the event of an "alarm" of the scanner.

IV.3.3 Passengers logical constraints

Here the set of constraints is represented by logical conditions so that the transition from one area of the airport to another will correspond to a test on a number of components of the resource vector. For example, at the boarding gate, the possession of an authentic boarding pass and a valid identity document / passport will be tested. If these conditions are verified, it is possible to go beyond the "boarding gate" control stage and access the aircraft. It should be noted that the satisfaction of these constraints is related to the instantaneous state of operation of the system.

In summary, at each step of the control system (passage of the control station, boarding, badge reader, ...) a sequence of values distribution to some logical variables must satisfy a set of constraints. The resource is then tested to validate access to the next zone.

The conditions to pass without detection through the different controls are given by:

Registration banks:

$$C_{rb} = (((X_1 \wedge X_2) \wedge (X_5 \wedge X_6) \wedge \overline{Z_{15}}) \vee ((X_3 \wedge X_4) \wedge (X_7 \wedge X_8) \wedge Z_{15})) \wedge X_{26} \quad (4.2)$$

or using the macro variables:

$$C_{rb} = ((Z_1 \wedge Z_3 \wedge \overline{Z_{15}}) \vee (Z_2 \wedge Z_4 \wedge Z_{15})) \wedge Z_{12} \quad (4.3)$$

Control and filtering station:

$$C_{cs} = ((X_9 \wedge X_{10} \wedge \overline{Z_{15}}) \vee (X_{11} \wedge X_{12} \wedge Z_{15})) \wedge (X_{13} \wedge X_{14} \wedge \cdots \wedge X_{24}) \quad (4.4)$$

or

$$C_{cs}=((Z_5\wedge\overline{Z_{15}})\vee(Z_6\wedge Z_{15}))\wedge(Z_7\wedge Z_8\wedge Z_9\wedge Z_{10}\wedge Z_{11}) \quad (4.5)$$

Immigration control:

Here the condition $C_{ic} = (X_5 \wedge X_6)\wedge (X_{11}\wedge X_{12}) = Z_2 \wedge Z_6$ must be satisfied if the associated flight is an international one. It can be written as:

$$C_{ic} = (Z_{15} \wedge (Z_2 \wedge Z_6\ )) \vee \bar{Z}_{15} \quad (4.6)$$

where Z_{18} is F if the flight is a domestic one and Z_{18} is T if it is an international one.

Boarding gate:

$$C_{bg} = (((X_1\wedge X_2)\wedge(X_9\wedge X_{10})\wedge\overline{Z_{15}})\vee((X_3\wedge X_4)\wedge(X_{11}\wedge X_{12})\wedge Z_{15}))\wedge X_{27} \quad (4.7)$$

then

$$C_{bg} = ((Z_1\wedge Z_5\wedge\overline{Z_{15}})\vee(Z_2\wedge Z_6\wedge Z_{15}))\wedge Z_{13} \quad (4.8)$$

Hold luggage control:

$$C_{hl} = X_{25} = Z_{14} \quad (4.9)$$

Once analysed the sequential operation of the passenger control station, one can establish the global constraint to be satisfied:

$$C = C_{rb} \wedge C_{cs} \wedge C_{ic} \wedge C_{bg} \wedge C_{hl} \quad (4.10)$$

or

$$\begin{aligned} C = (((Z_1\wedge Z_3\wedge\overline{Z_{15}})\vee(Z_2\wedge Z_4\wedge Z_{15}))\wedge Z_{12})\wedge(((Z_5\wedge\overline{Z_{15}})\vee(Z_6\wedge Z_{15}))\wedge(Z_7\wedge Z_8\wedge Z_9\wedge Z_{10}\wedge Z_{11})) \\ \wedge\ (\ (Z_{15} \wedge (Z_2 \wedge Z_6\ )) \vee \bar{Z}_{15}\ ) \\ \wedge \\ (((Z_1\wedge Z_5\wedge\overline{Z_{15}})\vee(Z_2\wedge Z_6\wedge Z_{15}))\wedge Z_{13})\wedge Z_{14} \end{aligned} \quad (4.11)$$

It should be noted that the test on the variable Z_{11} (random manual search) can be carried out legally on at least 10% of the passengers regardless of the value of the other variables. In the case where this search takes place, the variable Z_{11} must be set to T.

The sequential passengers control process can be represented as in Figure 4.1:

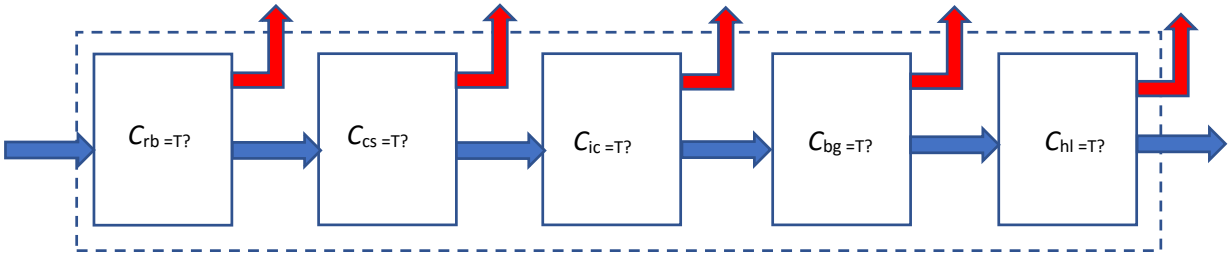


Figure 4.1 The different logical stages during passengers control

It is clear that:

- if variables X1 to X27, are all T Then C = T and the corresponding satisfiability problem is trivially satisfied.
- If some variables from X1 to X27 are F either for domestic or international passenger, then C = F.

However, in practice, passengers lacking some documentation or carrying forbidden objects may succeed in going through departure controls as the result of some control failure. So, it appears that this logical model must be enhanced to take into account the occurrence of control failures.

IV.4 Logical modelling of control failures

In this paragraph it is introduced the occurrence of failure at elementary controls, which can impair the detection of a threat associated with a passenger (inadequate documents, dangerous object, etc.). This can make such a passenger to go through the whole control process without being arrested. The preceding logical constraints must be complemented to include the instant effect of the failure of an elementary control caused either by equipment failure or staff mis-operation.

IV.4.1 Operational state of inspection station

The state of operation of the system at a given moment details which elements of the control system operate nominally and which ones are defective at this time. Each element *i* of the control system can be associated with a probability of good operation at the considered instant (or a probability of failure of the control element. Adverse events are expressed as logical conditions. Depending on the nature of the adverse event and the status of the controlled person, the list of these logical conditions may vary.

Each of the following control elements may behave correctly or not when the potentially dangerous passenger passes:

- check-in:
  Y_1: Identity control,
  Y_2: Ticket control,
  Y_3: coincidence air ticket and identity document.
- screening inspection station:
  Y_4: boarding card control,
  Y_5: cross-beam,
  $Y_{6:}$ scanner,
  Y_7: manual detector,
  $Y_{8:}$ manual search,
  Y_9: aleatory manual control
- to immigration:
  Y_{10}: passport and visa control.
- upon boarding:
  Y_{11}: boarding card,
  Y_{12}: identity control,
  Y_{13}: concordance boarding card and identity document.
- check of hold baggage: It is considered here a global operating condition for the screening inspection station, let Y_{14} be the corresponding logic variable. In fact, check of hold baggage and boarding are performed partially in parallel and there is no precedence constraint between them.

These checks can be seen as the minimum checks for a departing passenger, other means of control could be included: private passenger control units, face recognition, doors, anti-lift doors, badge readers, etc.

IV.4.2 Passenger control with malfunctions

The logical consequences of elementary failure of control equipment or staff are to change the logical values of some variables. Here false alarms are not considered since they are in general corrected and the result in that case remains unchanged. The matching between controls and macro state variables is made at this stage, such as:

At registration:

$$Y_1 \rightarrow Z_1 \vee Z_2, Y_2 \rightarrow Z_3 \vee Z_4, \; Y_3 \rightarrow Z_{12} \tag{4.12-a}$$

At the level of the inspection station:

$$Y_4 \rightarrow Z_5 \vee Z_6, Y_5 \rightarrow Z_7, \; Y_6 \rightarrow Z_8, Y_7 \rightarrow Z_9, Y_8 \rightarrow Z_{10}, Y_9 \rightarrow Z_{11} \tag{4.12-b}$$

At immigration control:

$$Y_{10} \rightarrow Z_2 \wedge Z_6 \tag{4.12-c}$$

At boarding:

$$Y_{11} \rightarrow Z_5 \vee Z_6 \, , Y_{12} \rightarrow Z_1 \vee Z_2, Y_{13} \rightarrow Z_{12} \tag{4.12-d}$$

At luggage inspection station:

$$Y_{14} \rightarrow Z_{14} \tag{4.12-e}$$

Here have been considered six different cases of causes and effects represented in Table 4.1.

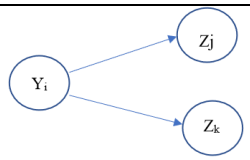
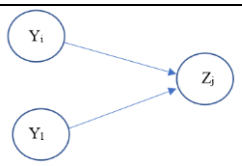
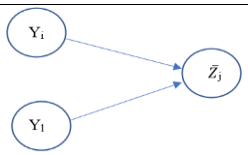
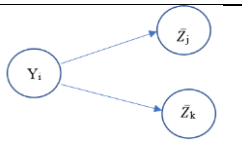
	Single effect	Multiple effect	Multiple causes
Z_j, Z_k =T nominal			
Z_j, Z_k=F nominal			

Table 4.1 Considered cause-effect cases

In the case of a single effect with T reference value, a failure of Y_i will declare Z_j to be T when it is F and T if it is T, Z_j should be replaced in any logical constraint by the logical expression $(Z_j \wedge Y_i) \vee \bar{Y}_i$ which has the logical table :

Z_j Y_i	T	F
T	T	T
F	F	T

Table 4.2 Truth table for $(Z_j \wedge Y_i) \vee \bar{Y}_i$

which is T when Z_j is F and Y_i is F.

In the case of a multiple effect with T reference value, a failure of Y_i will declare Z_j *and* Z_k to be T when both are F and T if both are T, Z_j should be replaced in any logical constraint by the logical expression $(Z_j \wedge Y_i) \vee \bar{Y}_i$, Z_k should be replaced in any logical constraint by the logical expression $(Z_k \wedge Y_i) \vee \bar{Y}_i$, and the logical expression $(Z_j \vee Z_k)$ will be replaced by $(Z_j \wedge Y_i) \vee (Z_k \wedge Y_i) \vee \bar{Y}_i$, while the logical expression $(Z_j \wedge Z_k)$ will be replaced by $(Z_j \wedge Y_i) \wedge (Z_k \wedge Y_i) \vee \bar{Y}_i$.

In the case of multiple causes with T reference value, when Y_i *and* Y_j imply the failure of Z_k, Z_k should be replaced by $(Z_k \vee (Y_i \wedge Y_j) \vee (\bar{Y}_i \vee \bar{Y}_j))$, when Y_i or Y_j imply the failure of Z_k, Z_k should be replaced by $(Z_k \vee (Y_i \vee Y_j) \vee (\bar{Y}_i \wedge \bar{Y}_j))$.

In the case of a single effect with F reference value, a failure of Y_i will declare $\overline{Z_J}$ to be T when it is F and T if it is T, $\overline{Z_J}$ should be replaced in any logical constraint by the logical expression $(\overline{Z_J} \wedge Y_i) \vee \overline{Y}_i$ which is T when $\overline{Z_J}$ is F and Y_i is F.

In the case of a multiple effect with F reference *value*, a failure of Y_i will declare $\overline{Z_J}$ and $\overline{Z_k}$ to be T when they are F and T if they are T, $\overline{Z_J}$ should be replaced in any logical constraint by the logical expression $(\overline{Z_J} \wedge Y_i) \vee \overline{Y}_i$, $\overline{Z_k}$ should be replaced in any logical constraint by the logical expression $(\overline{Z_k} \wedge Y_i) \vee \overline{Y}_i$. Here the logical expression $(\overline{Z_J} \vee \overline{Z_k})$ should be replaced by $(\overline{Z_J} \wedge Y_i) \vee (\overline{Z_k} \wedge Y_i) \vee \overline{Y}_i$, while the logical expression $(\overline{Z_J} \wedge \overline{Z_k})$ should be replaced by $(\overline{Z_J} \wedge Y_i) \wedge (\overline{Z_k} \wedge Y_i) \vee \overline{Y}_i$.
In the case of multiple causes with F reference value, when Y_i *and* Y_j imply the failure of $\overline{Z_k}$, $\overline{Z_k}$ should be replaced by $(\overline{Z_k} \vee (Y_i \wedge Y_j) \vee (\overline{Y}_i \vee \overline{Y}_j))$, when Y_i *or* Y_j imply the failure of $\overline{Z_k}$, $\overline{Z_k}$ should be replaced by $(\overline{Z_k} \vee (Y_i \vee Y_j) \vee (\overline{Y}_i \wedge \overline{Y}_j))$.

Following these conversion rules, the updated logical constraint to be satisfied to pass through the passengers' departure control and board an aircraft is given by:

$$\begin{gathered}
(((Z_1 \wedge Y_1) \vee \overline{Y_1}) \wedge ((Z_3 \wedge Y_2) \vee \overline{Y_2}) \wedge \overline{Z_{15}}) \vee (((Z_2 \wedge Y_1) \vee \overline{Y_1}) \wedge ((Z_4 \wedge Y_2) \vee \overline{Y_2}) \wedge Z_{15}) \wedge (Z_{12} \wedge Y_{13}) \vee \overline{Y_{13}}) \\
\wedge \\
(((Z_5 \wedge Y_4) \wedge \overline{Z_{15}}) \vee (Z_6 \wedge Y_4) \wedge Z_{15}) \vee \overline{Y_4}) \wedge ((Z_7 \wedge Y_5) \vee \overline{Y_5}) \wedge ((Z_8 \wedge Y_6) \vee \overline{Y_6}) \wedge ((Z_9 \wedge Y_7) \vee \overline{Y_7}) \wedge \\
((Z_{10} \wedge Y_8) \vee \overline{Y_8}) \wedge ((Z_{11} \wedge Y_9) \vee \overline{Y_9}) \\
\wedge \\
((Z_{15} \wedge ((Z_2 \wedge Z_6 \wedge Y_{11}) \vee \overline{Y_{11}})) \vee \bar{Z}_{15}) \\
\wedge \\
((((Z_1 \wedge Y_1) \vee \overline{Y_1}) \wedge ((Z_5 \wedge Y_4) \vee \overline{Y_4}) \wedge \overline{Z_{15}}) \vee ((Z_2 \wedge Y_1) \vee \overline{Y_1}) \wedge (((Z_6 \wedge Y_4) \vee \overline{Y_4}) \wedge Z_{15}) \wedge Z_{13}) \\
\wedge \\
((Z_{14} \wedge Y_{14}) \vee \overline{Y_{14}})
\end{gathered} \tag{4.13}$$

Figure 4.2 displays the influence of each control action on the different stages of the passenger control process.

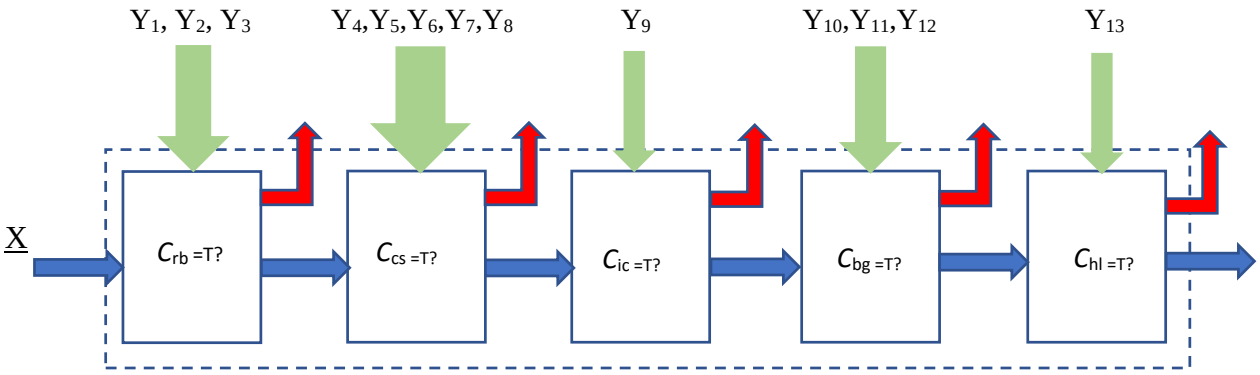


Figure 4.2 The different logical stages to be checked

Equation 4.12 involves 18 macro variables and equation 4.13 control failure variables, so a very large set of different scenarios could be analysed with this model, some leading to the possibility of a go through for unauthorized or dangerous passengers.

IV.5 Building a vulnerability analysis framework

Here the idea is to develop a tool, based on the logical constraint displayed in the previous paragraph, to check, once the personal data of a passenger has been provided, which minimum number of elementary controls should fail to allow this passenger to go undetected through the passenger control system. The proposed tool is a graph which is built to check the existence of a possible path for any passenger, from a no threat passenger to a multi threat passenger. In recent years and decades, many different graphical representations have been introduced to analyse logical constraints as pure mathematical objects. However, here, the structure of the considered logical constraint is based on a particular physical system, the passengers control system, and that makes a difference when searching for characteristically logical configurations.

IV.5.1 Controlled satisfiability graph

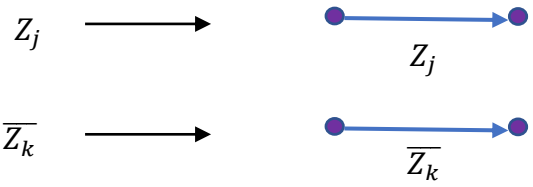
Here it is introduced a graphical representation of the global logical constraint given by expression 4.12, which is composed of a series of conjunctions of clauses (not necessarily in normal form).

Here the clauses are ordered according to the structure of the passengers control system. The rules of construction of the controlled satisfiability graph (**CSG**) are the following:

- a first node is created; it is node m = a.
- to each logical variable present in a clause is associated an orientated arc,
- to each control complex such as $(Z_j \wedge Yi) \vee \bar{Y}i$, $(\overline{Z_k} \wedge Yi) \vee \bar{Y}i$ or $(\overline{Z_k} \vee (Yi \wedge Yj) \vee (\bar{Y}i \vee \bar{Y}j))$ is attached a cycle,
- to each control complex such as $(Z_j \wedge Yi) \vee (Z_k \wedge Yi) \vee \bar{Y}i$ are attached two cycles.
- each $\wedge$ operator outside a control complex and linking two clauses, generates a new node, node m+1, and the arcs linking the previous node to this new one are according to the following clause.
- Clauses are treated according to their original ordering.

Figures 4.3 displays basic configurations for a CSG.

Variables without control:



Variables with control:

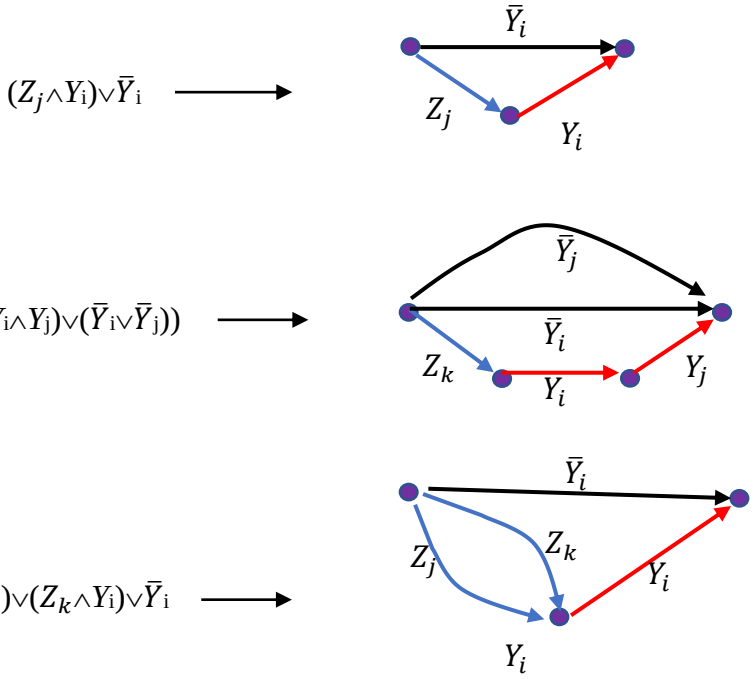


Figure 4.3 Basic configurations for a CSG

IV.5.2 The CSG associated to a passengers control system

The above rules are applied considering the following ordering: C_{rb} / C_{cs} / C_{ic} / C_{bg} / C_{hl} in expression 4.12. Then to each clause, it is associated the corresponding subgraph. Orange arrows represent possible entry points, blue arrows are resource logical variables, red arrows are control effective logical variables, black arrows are control uneffective logical variables, orange arrows are dummy arcs between the same nodes, green arrows are possible output points. Nodes are named with a letter in increasing lexicographical order according to their rank in the graph.

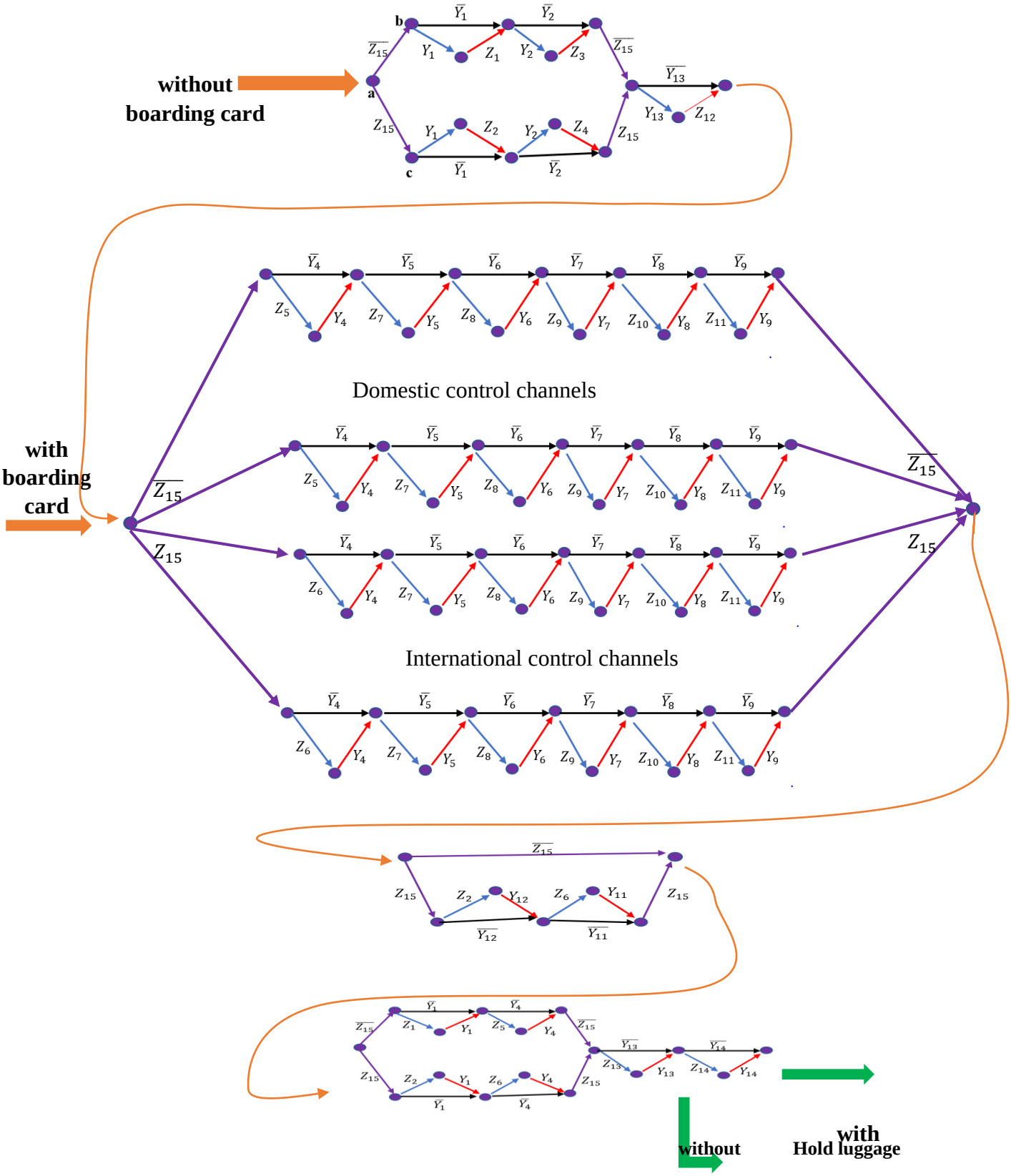


Figure 4.4 The CSG associated to a passengers control system

In the case considered, the structure of the control system and overall satisfiability constraint is mainly sequential with some parallelism when multiple differentiated control lines are available. More complex structures could be found when considering other types of control processes.

IV.5.3 Accessing vulnerability

To each arc of the CSG it is associated a weight:

- the weight of an arc associated to a control logical variable Yj, j ∈J , is :
  - ε if Y_j =T,
  - ∞ if Y_j = F, then $\overline{Y_J} = T$.
- the weight of an arc associated to a control logical variable $\overline{Y_J}$, j ∈J , is :
  - a strictly positive number αj< ∞, if $\overline{Y_J}$ =T,
  - ∞ if $\overline{Y_J} = F$.
- The weights of the arcs associated with controlled logical variables Zi, i ∈I , are such that :
  - if the variable is T, the weight is ε,
  - if the variable is F, the weight is ∞.
- The weights of the arcs associated with non-controlled logical variables Zi, i ∈I , are such that :
  - if the variable is T, the weight is 2 ε,
  - if the variable is F, the weight is 2 ∞.

Here ε and ∞ are real numbers such as : $0 < N \cdot \varepsilon \ll \alpha_j$ and $\alpha_j \cdot N \ll \infty \quad \forall j \in J$ where N is the number of literals in the global logical constraint. N is at the same time a size parameter for the global logical constraint and an upper bound of the number of arcs in the corresponding CSG.

For example for a logical constraint such as : (a ∨ $\bar{b}$ ∨c) ∧(b ∨c) ∧($\bar{a}$∨$\bar{c}$), N= 7. In the case of formula 4.12, N = 63.

Let WCSG be the Weighted Controlled Satisfiability Graph.

With this choice of the weigh, whatever the scenario adopted for the Zs and the Ys, the structure of the WCSG remains unchanged.

Once a passenger scenario has been built (Xs and then Zs), a new weighting is produced to the CSG. Then the vulnerability assessment is performed by searching the shortest path between the corresponding entry point and exit point in the CSG.

Entry points are either the entry node of the check-in subgraph or the entry node of the screening inspection station subgraph. The exit point for departure passengers is the exit node of the boarding subgraph (no hold luggage) or the exit node of the hold luggage check (passenger with hold luggage).

The length L^* of the shortest path π_{min} can be written as :

$$L^* = n + 2 \cdot K \cdot \varepsilon + 2 \cdot H \cdot \infty \tag{4.14}$$

Here *n* is related with the failed controls, *K* is the sum of the number of times controls are successful and of the number of times compliant no controlled variables are crossed. Finally, *H* is the number of times an uncontrolled variable is forced.

Different measures of vulnerability (and, contrarily, of robustness) can be considered:

- When $\alpha j = 1 \ \forall j \in J$, n is the number of times a control is failed along the chosen path. The pair (n, H) is a vulnerability measure of the control system with respect to the current passenger scenario. When H is different from 0, it means that H uncontrolled variables are in fact critical and should be controlled. Once this correction is implemented, the WCSG must be updated.
- The $\alpha_j \ \forall j$ could also be chosen to represent on a limited scale, say from 1 to 10, the difficulty to deceive control *j*. In that case $\sum_{j \in \pi_{min}} \alpha_j$ is an additive measure of the difficulty to coerce satisfaction of the downgraded logical expression.
- If the probabilities p_j of deceiving the *j* controls, $j \in J$, are available, choosing $\alpha_j = -\log p_j$:

$$1 - \prod_{j \in \pi_{min}} e^{\alpha_j} = = 1 - e^{n^*} \tag{4.14}$$

is the probability of not being able to go undetected through the whole control system when these probabilities are independent from one control to another?

- In the case of aleatory control, the probability of performing it must be taken into account in the weighting of the control variable.

IV.5.4 Solution algorithms

Here the WCSG is a directed acyclical graph (DAG) = [V,U] where V is the set of nodes {u ∈ V} and U is the set of arcs {(u,v)∈ U, u∈ V, $v \in V$}. Let $w(u,v)$ be the weight of arc (u,v) in the considered WCSG.

To solve this problem in the real domain, variations of shortest paths algorithms such as Moore-Dijkstra (Bondy et al., 2008), can be adapted by considering all the nodes of the acyclic graph ordered by increasing rank. A one sweep numerical algorithm is as follows:

1. Rank all the nodes in V;
2. Set the distance L (1) of the source node (node 1) to 0;
3. Set the distances to all other nodes to $+\infty$ and set all predecessors of $u \in V$, to node 1: P(u)=1;
4. For each node $u \in V$:
5. - Walk through all immediate successors v of u;
6. - If $L(v) > L(u) + w(u, v)$
7. - Set $L(v) \longleftarrow L(u) + w(u, v)$ and P(v)=u;

where $w(u,v)$ is the assigned weight to arc (u,v).

A symbolic version of this algorithm can be developed where the comparison of lengths at step 6 is done according to the following scheme:

Let $L = n + 2 \cdot K \cdot \varepsilon + H \cdot M$ and $L' = n' + K' \cdot \varepsilon + H' \cdot M$ be two path lengths, then:

- if $H > H' \geq 0$ then $L > L'$
- if $H = H'$ and $n > n' \geq 0$ then $L > L'$
- if $H = H'$, $n = n'$ and $K > K' \geq 0$ then $L > L'$

and of course, if $H = H'$, $n = n'$ and $K = K'$ then $L = L'$

Both versions of this algorithm present a polynomial time complexity as being special cases of know class P algorithm. So, this algorithm can be applied to very large CSGs.

IV.6 Generating scenarios

IV.6.1 Composition of scenarios

The scenarios consist of the initial resources of the target passenger and the assumed operational state of the system. The initial resources can be modified by the initialization conditions: for example, at the registration bank, the possession of a true {($X_5 = T$ and $X_6 = T$), or (X_7=T and X_8=T)} transport ticket and a true identity / passport document {($X_1 = T$and $X_2 = T$) or ($X_3 = T$ and $X_4 = T$)} concordant ($X_{25} = T$) are checked and, if these conditions are verified, at the exit of the registration bank, the target passenger obtains a valid boarding pass. The resources then obtained are the so-called acquired resources.

It should be noted that additional resources (not shown in the resource vector) can change the initial operating state. This would be the case, for example, with the existence of an accomplice, a member of the scanner detection staff: this complicity is then comparable to a failure of the "scanner control" component (Y_6= F in the vector $\underline{Y}$).

Note that, here, the registration is not a strictly mandatory crossing point, a person with a false boarding pass or a stolen embarkation card, can come directly to the inspection post, as shown in Figure 4.4.

From the 2^{27} possible scenarios for the elementary variable X_i s, 2^{17} scenarios can be constructed for the macro state variables while 2^{13} scenarios can be constructed for the sequence of controls for a target passenger. Among all these scenarios, only a few will be relevant for security analysis.

IV.6.2 Examples of application

First example: prohibited metal object under clothes

Here it is supposed that the target passenger performs an international flight (X_{15} = T), has a boarding card to collect and a hold luggage to deliver. It is supposed that he has everything in order except a prohibited metal object under his clothes (X_{16} =T) in that case, this implies that $Z_7 = Z_9 = Z_{10} = Z_{11}$ = F. Also, X_{25} = T since in this scenario no dangerous object is supposed to be in hold luggage.

The passenger control station is composed of two lines with unequal performance. The probability in both lines of performing aleatory control is taken equal to 0.10. The weights of the critical control variables are given in table 4.3 on a scale from 0 to 10.

Control variable	Y_5	$\overline{Y_5}$	Y_7	$\overline{Y_7}$	Y_8	$\overline{Y_8}$	Y_9	$\overline{Y_9}$
Line 1	∞	8	∞	7	∞	7	∞	1
Line 2	∞	9	∞	8	∞	6	∞	1

Table 4.3 Adopted difficulty levels for critical controls

The weight of $\overline{Y_9}$ in both control lines is 1 as the result of the product of the probability of aleatory manual control (0.10) by the highest level of difficulty (10).

In that case, the length of the shortest path is : 22+ 22 ε which means that 11 controls are passed with legitimate success while the difficulty of skirting the four critical controls is assessed to a scale of 22.

Second example: False passport with dangerous object in hold luggage.

Here it is supposed that the target passenger performs an international flight (X_{15} = T), has a boarding card to collect and a hold luggage to deliver. It is supposed that he has everything in order except a false passport (X_4 =F). In that case, this implies that Z_2 = = F. Also, X_{25} = F since in this scenario a dangerous object is supposed to be in his hold luggage, then Z_{14}=F.

The control of passport is performed different times during the control process: when getting the boarding card (Y_1), when passing immigration (Y_{12}) and again at boarding (Y_1). Passport control at boarding card desk and at boarding gate are not searching directly for authenticity of passport, but with existence and concordance with travel documents, while immigration control is directly concerned with passport authenticity. The weights of the critical control variables are given in table 4.4. In this case probabilities of control failure have been adopted.

Control variable	Y_1 at boarding desk	Y_{12} at immigration	Y_1 at boarding gate	Y_{14} hold luggage
-log(p)	-log(0.75)=0.125	-log(0.02)=0.699	-log(0.80)=0.097	-log(0.05)=1.301

Table 4.4 Adopted probabilities (-log(p)) for critical controls

In that case, the length of the shortest path is : 3.221+ 22 ε which means that 11 controls are passed with legitimate success while the probability of skirting the four critical controls is assessed to be exp(-3.221)=0.0006.

IV. 7 Conclusion

In this chapter, a pure logical framework has been developed to establish the logical constraint each inspection station must satisfy to ensure security in face of malicious behaviour. Considering the nature of the resulting logical satisfiability problem, an approach based on a graphical representation of the control process has been adopted where the Controlled Satisfiability Graph appears to be a powerful tool to analyse the vulnerability of a control scheme. This vulnerability is assessed here by considering minimum length paths pointing out the weakest sequences of control for each threat scenario. The proposed approach turns it possible to detect the minimum number of elementary control defects that may result in a control failure. It also allows to generate different scenarios of attack to the control system by a threat, to analyse the behaviour of the system under these conditions and to evaluate their permeability with respect to different types of attacks.

It appears that the proposed approach is of interest for a wide area of applications beyond theoretical satisfiability problems: diagnostics, reliability assessment and catastrophe scenarios generation, among many others.

CHAPTER V

ASSESSING INSPECTION OUTCOMES WITH BAYESIAN COLOURED PETRI NETS

V.1 Introduction

The objective of this chapter is to develop a tool to analyse in a systematic way the performance, in terms of probability of achievements, of an inspection station when faced to a departing passenger. The adopted approach is microscopic since it concentrates on the processing of a single passenger at a time.

An inspection station can be seen as a dynamic process where a succession of tasks is performed, successfully or not, according to some distributions of probability on each controlled passenger. The probability of success or failure at the output of this process depends in a complex way of the succession of probability of success or failure of the anterior elementary control tasks. Then, the probabilistic interactions between the considered set of random variables characterizing the inspection process may be represented by joint probability distributions.

In general, when analysing these probabilistic interactions, even considering only the case where random variables are binary, it has appeared that the size of the joint probability distributions grows exponentially with the number of variables. Indeed, the joint distributions must contain one probability for each configuration of the random variables. Then compact representations for reasoning about the state of large and complex systems involving a large number of variables, have been studied and the concept of Bayesian networks has been introduced by Judea Pearl in 1985. It uses a graphical representation to encode dependence and independence relations among the random variables. The dependence and independence relations lead to a compact representation of the joint probability distributions.

In practice, cause-effect relations between entities of a problem domain can be represented by a Bayesian network using a graph of nodes representing random variables and links representing cause-effect relations between the entities (Jensen, 1996). So, there is an interest to associate, for the performance assessment of the operation of an inspection station, a Bayesian network. However, the operations that an inspection station performs over a passenger depend on intermediate results and this process can be seen as a set of conditioned sequences, which are performed in a dynamical context. In order to account for that latter aspect of the model, another tool also appears of interest: Petri nets.

The doctoral dissertation of C. A. Petri in 1962 (Petri, 1962) discussed the basis for a theory of communication between synchronous processors of a computer, being mainly interested in describing the causal relationships between events. His work began the development of Petri nets which have become today a large body of research and development. Initially, many researchers studied Petri nets with respect to theories and applications. Along the decades, the use and study of Petri nets have spread and have expanded to depth in theory and width in application. Many authors who have entered the research of Petri nets have provided suitable platforms in the areas of:

- Modelling and design of concurrent systems, such as information systems and manufacturing systems.
- Performance analysis of complex parallel/sequential systems.

Already some authors have initiated the work of introducing Petri nets to develop analysis of efficiency, safety and security operations issues at airports.

In this chapter, an original approach is developed where Binary Bayesian Networks and a special class of Petri Nets, the Coloured Petri Nets, are merged to produce an efficient tool to assess the expected performance of a passenger inspection station: Bayesian Coloured Petri Nets (BCPNs).

V.2 Discrete Bayesian Networks

V.2.1 Definitions

A Discrete Bayesian network (Charniak, 1991), N = (X, G, P), over variables, X, consists of an acyclic, directed graph G = (V, E) and a set of conditional probability distributions P. Each node v of the set of nodes V in G corresponds to a single discrete random variable $X_v \in X$ with a finite set of mutually exclusive states (two for a binary random variable). The directed links of the set of links $E \subseteq V \times V$ of G specify assumptions of conditional dependence and independence between random variables. There is a conditional probability distribution, $P(X_v | \Gamma_{X_v}^{-1}) \in P$, for each variable $X_v \in X$. The set of variables represented by the parents, $\Gamma_{X_v}^{-1}$, of $v \in V$ in G = (V, E) are sometimes called the conditioning variables of X_v.

A Bayesian network is fully specified by the combination of its graph structure and the probability table P(X_v |$I_{X_v}^{-1}$) ∈ P, for each variable X_v ∈ X, i.e. a Bayesian network encodes a joint probability distribution over a set of random variables, X, of a problem domain.

V.2.2 Example of Bayesian network

A small example of medical diagnostic based on a Bayesian network structure is shown below. This structure is designed to allow to diagnose whether a patient is suffering from a common cold (CC) and/or a dangerous Flu (DF), based on the following patients' symptoms: runny nose (RN) yes or no, headache (HA), yes or no and bursts of dry cough (BC), as well as a relevant background information: has he visited recently a tropical country (TC), yes or no. Here the adopted graph structure is given by:

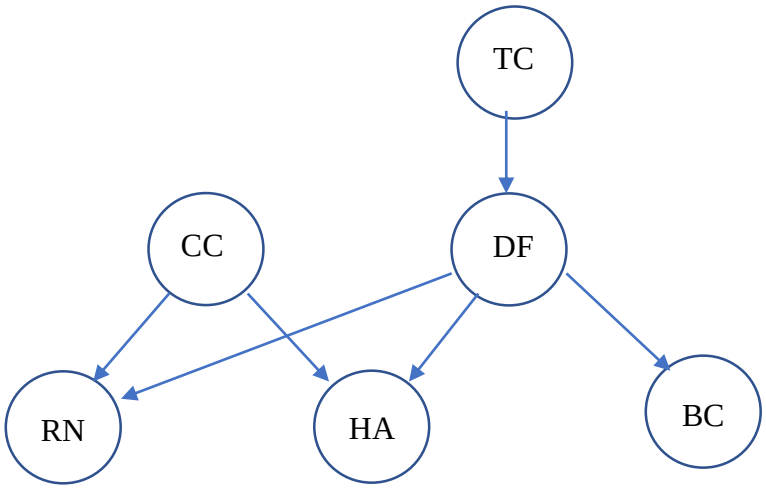


Figure 5.1 Diagnostic Graph

Assuming all six variables are binary, with T representing ``true" and F ``false", the probability tables for the network can be given as follows:

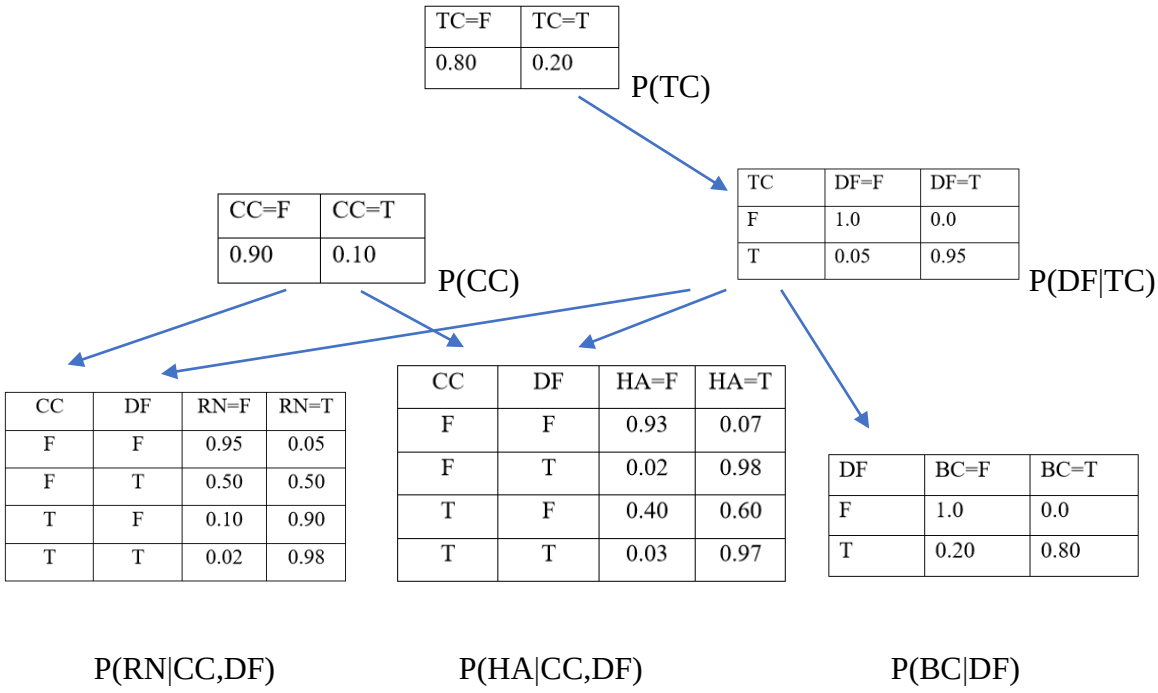


Figure 5.2 Available probability and conditional distributions

V.2.3 Building a Bayesian network

Once the Bayesian network has been defined, it can be used to compute any conditional probability one wishes to compute: For example, given that a person has recently visited a tropical country (TC=T) and has a runny nose (RN = T), the network above could be used to compute the probability that the person has the common cold (CC=T) but not the Dangerous Flu (DF=F): P(CC=T,DF=F|TC=T, RN=T).

The set of conditional probability distributions, P, specifies a multiplicative factorization of the joint probability distribution over X as represented by the chain rule of Bayesian networks:

$$P(X) = \prod_{v \in V} P(X_v | X_{I_{X_v}^{-1}}) \quad (5.1)$$

Even though the joint probability distribution specified by a Bayesian network is defined in terms of conditional independence, a Bayesian network is most often constructed using the notion of

cause-effect relations. Often, the construction of a Bayesian network proceeds according to an iterative procedure where the set of nodes and their states, and the set of links are updated iteratively as the model becomes more and more refined. Basic structures in Bayesian networks are represented in Figure 5.3:

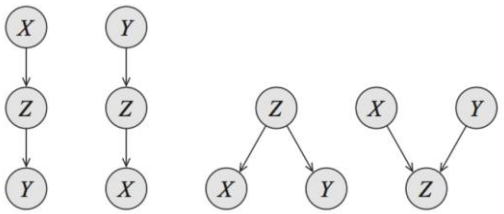


Figure 5.3 Basic structures in Bayesian networks

Here (1) and (2) are "cascade" structures, (3) is a "common parent" structure and (4) is a "common son" structure.

The set of all probabilistic independencies that hold for a joint distribution P is written I(P). That means that:

$$\text{if } P(X,Y)=P(X)\cdot P(Y), \text{ then it is written as: } X \perp Y \in I(P) \qquad (5.2)$$

In the case of a cascade structure $X \rightarrow Z \rightarrow Y$ where Z is observed, then, $X \perp Y|Z$. If Z is unobserved, then X and Y are not independent. Here Z holds all the information that determines the outcome of Y, whatever the value X takes.

In the case of the common parent structure *Common parent.* If the structure is of the form $X \leftarrow Z \rightarrow Y$, and Z is observed, then $X \perp Y|Z$. However, if Z is unobserved, then X and Y are not independent, Z contains all the information that determines the outcomes of X and Y. Once it is observed, there is nothing else that affects the outcome of X and Y.

In the case of the common son structure $X \rightarrow Z \leftarrow Y$, then knowing Z Couples X and Y. In other words, $X \perp Y$ if Z is unobserved, but X and Y are independent if Z is observed.

These structures describing the independencies of a three variable Bayesian network can be extended by applying them recursively over any larger graph.

V.2.4 Solving a Bayesian network

Solving a Bayesian network N = (X, G, P) consists in computing all posterior marginal probabilities given a set of evidence $\boldsymbol{e}$, i.e., P(X|ε) for all $X_v \in X$. If the evidence set is empty, i.e., $\boldsymbol{e} = \emptyset$, then the task is to compute all prior marginal, i.e., P(X_v) for all $X_v \in X$.

The quantitative representation of a Bayesian network is the set of conditional probability distributions, P, defined by the structure of G. Note that all distributions specify the probability of a variable being in a specific state depending on the configuration of its parent variables. The Bayesian network can be used to compute all prior marginal and the posterior distribution of each non-evidence variable given evidence in the form of observations on a subset of the variables in the model.

The specification of a conditional probability distribution P(X_v $|\Gamma_{X_v}^{-1}$) can be a very intensive knowledge acquisition task as the number of parameters grows exponentially with the size of dom($X_{fa}(v)$), where $fa(v) = \Gamma_{X_v}^{-1} \cup \{v\}$.

Different techniques can be used to simplify the knowledge acquisition task, assumptions can be made, or the parameters can be estimated from data. The complexity of a Bayesian network is defined in terms of the family $fa(v)$ with the largest state space size $\|fa(v)\| = |\text{dom}(X_{fa(v)})|$.

As the state space size of a family of variables grows exponentially with the size of the family, it is intended to reduce the size of the parent sets to a minimum. Another useful measure of the complexity of a Bayesian network is the number of cycles and the length of cycles in its graph.

In 1990, Cooper (Cooper, 1990) proved that exact inference in Bayesian networks is NP-hard. This result boosted research on approximation algorithms to probabilistic inference.

In 1993, Dagum and Luby (Dagum et al., 1993) proved that no tractable deterministic algorithm can approximate probabilistic inference to within an absolute error $\varepsilon < 1/2$. They also proved that no tractable randomized algorithm can approximate probabilistic inference within an absolute error $\varepsilon < 1/2$ with confidence probability greater than $1/2$.

In practical terms, these complexity results suggest that while Bayesian networks are interesting representations for Artificial Intelligence and machine learning applications, their use in large real-world applications must be tackled with caution. Their applicability can be eased by introducing structural constraints or by restrictions on the conditional probabilities.

The bounded variance algorithm of Dagum and Luby in 1997 (Dagum et al., 1997) was the first provable fast approximation algorithm to efficiently approximate probabilistic inference in Bayesian networks with guarantees on the error approximation. This powerful algorithm required the minor restriction on the conditional probabilities of the Bayesian network to be bounded away from zero and one by *1/p(n)* where *p(n)* was any polynomial on the number of nodes in the network *n*. However, in the application considered, the size of the resulting problems should remain rather small and then no dimensional difficulty is to be expected. So, in this case, complexity is not at stake.

V.3 Modelling with Petri Nets

V.3.1 Definition: Ordinary Petri Nets

A Petri net (PN) (Murata , 1989) can be defined as a four-tuple, PN = (*P, T, I, O*), where $P = \{ p_1, p_2, \ldots, p_n \}$ is a set of places, $T = \{ t_1, t_2, \ldots, t_m \}$ is a set of transitions, *I* is an input function, and *O* is an output function. The set of places *P* and the set of transitions *T* are disjoint sets : $P \cap T = \varnothing$

$I \subset \{P \times T\}$, and $O \subset \{ T \times P \}$ are sets of directed arcs.

A place p_i is an input place of a transition *tj* if $p_i \in I(tj)$ and p_i is an output place if $p_i \in O(tj)$. The structure of a Petri net is defined by its sets of places *P*, transitions *T*, input functions *I*, and output functions *O*.

Theoretical studies on Petri nets, viewed as mathematical entities, are based on the above formal definition of Petri net structures. However, a graphical representation of Petri net structures appears more useful for illustrating the concepts related with the operation of the Petri nets.

A Petri net graph uses in general circles to represent places (states) and bars to represent transitions (processes). Input-output relationships are represented by directed arcs between places and transitions. An arc directed from a place p_j to a transition *tj* defines the place to be an input of the transition. Multiple inputs to a transition are indicated by multiple arcs from the input places to the transition.

An output place is indicated by an arc from the transition to the place and multiple outputs are represented by multiple arcs. A Petri net is then a multigraph since it allows multiple arcs from one node of the graph to another. In addition, since the arcs are directed, the Petri net is a directed

multigraph. Since the nodes of the graph can be partitioned into two sets (places and transitions), such that each arc is directed from an element of one set (place or transition) to an element of the other set (transition or place), the Petri net is a bipartite directed multigraph. It is referred here simply as a Petri net graph. Figure 5.4 gives an example of Petri net graph.

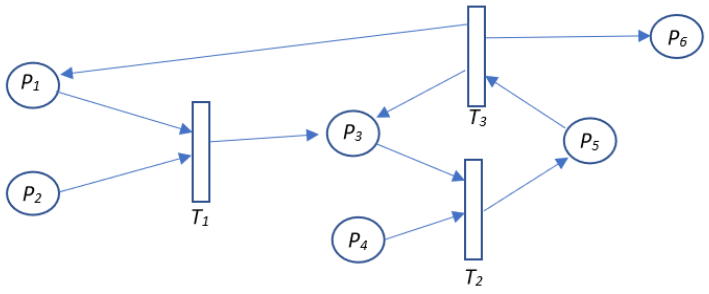


Figure 5.4 Example of Petri net graph

V.3.2 Marking of Petri nets

A Petri net M containing a marking is a marked Petri net (P,*T*,*I*,*O*,*M*). The marking of a Petri net is a function from the set *P* to the set of non-negative integers N:

$$M : P \rightarrow \mathrm{N} \quad \text{with } M(p_i)=M_i \in \mathrm{N} \tag{5.3}$$

M_i gives the number of tokens at place p_i. An initial marking is given to each place; tokens reside at a place when it is active. Tokens flow through the net depending on the present marking of the net. The marking of a Petri net can be represented by a vector $\underline{M}$ of dimension *n*, where *n* is the number of places and each value of the vector corresponds to the number of tokens in the corresponding place.

To each arc to or from a place is associated a weight *w* which is a positive integer, 1 being the default value.

In figure 5.5 the marked Petri net is such as $\underline{M'}$= (2,1,0,1,0,0)'.

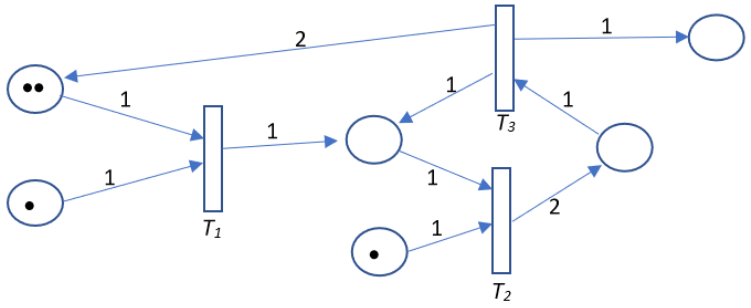


Figure 5.5 Example of marked Petri net

V.3 .3 Dynamic behaviour

When there is a token in each of the input places of a transition, that transition is enabled to fire. If the weights on each of the arcs between places and transitions are equal to one, then the transition fires by removing a token from each of its input places and by placing a token in each of its output places. When weights are different from unity, the corresponding number of tokens is retrieved from input places and added to output places. A transition will be only fireable when the number of tokens in its input places is superior to the weight in the corresponding input arc.

In Figure 5.5 only transition T_1 is fireable, the result of activating this transition is given in Figure 5.6 with a new marking $\underline{M} = (1, 0, 1, 1, 0, 0)$'.

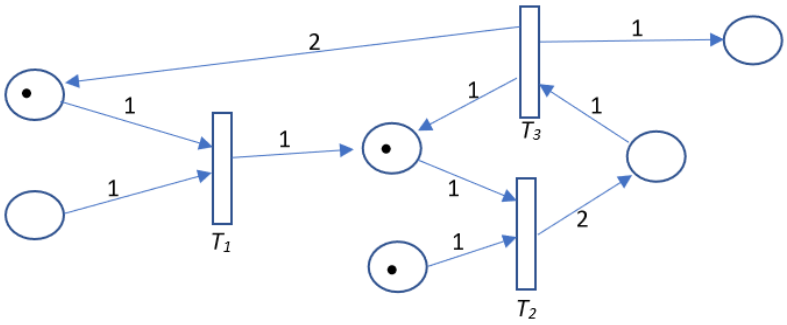


Figure 5.6 Firing transition T_1

A first representation of a passenger control unit at boarding could be as follows:

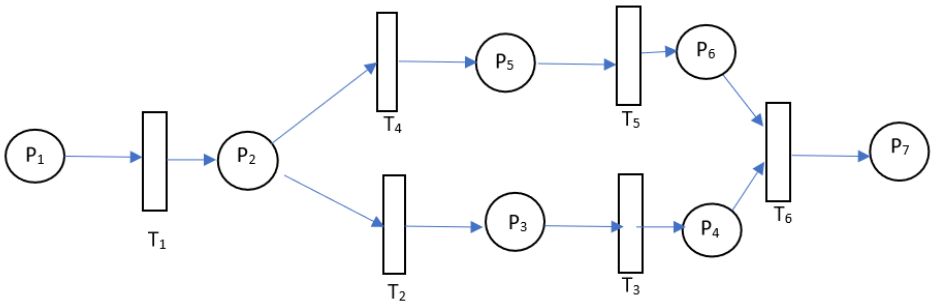


Figure 5.7 An initial Petri net representation of a passenger control unit

Here P_1 represents the presence of a passenger with his baggage, P_2 is the passenger and baggage at entrance of ray controls, P_3 is a passenger controlled by ray control, P_4 is a passenger manually controlled, P_5 is a baggage after ray control, P_6 is the baggage after manual control and p_7 is the passenger with his baggage inside the departure terminal. Here T_1 represents the boarding pass control, T_2 is the ray passenger control, T_3 is the passenger manual control, T_4 is a baggage ray control, T_5 is a baggage manual control, T_6 is the collection of the cleared baggage by the controlled passenger.

The execution of a Petri net is driven by the distribution of tokens in the Petri net. By changing the distribution of tokens in the places, this affect the sequences of firing transitions. This can be a way to study the dynamic behaviour of the modelled system.

- Enabling Rule: A transition T is said to be enabled if each input place P of Γ_T^{-1}contains at least a number of tokens M(P) equal to the weight I(T, P) of the directed arc connecting place P to transition T :

$$M(P) \geq I(T, P) \text{ for any } P \in \Gamma_T^{-1} \quad (5.4)$$

- Firing Rule: Only enabled transition can fire. The firing of an enabled transition T removes from each input place P of Γ_T^{-1}, the number of tokens equal to the weight of the directed arc connecting P to T and it also provide for each output place $P \in \Gamma_T$, the

number of tokens equal to the weight O(T, P) of the directed arc connecting T to P. After firing transition T, the new marking of place P ∈ Γ_T is given by :

$$M'(P) = M(P) - I(T, P) + O(T, P) \quad \forall P \in \Gamma_T^{-1} \tag{5.5}$$

Notice that since only enabled transitions can fire, the number of tokens in each place always remains non-negative when a transition is fired. Firing transition can never try to remove a token that is not there

Figure 5.8 displays the main elementary characteristic configurations modelled with PNs.

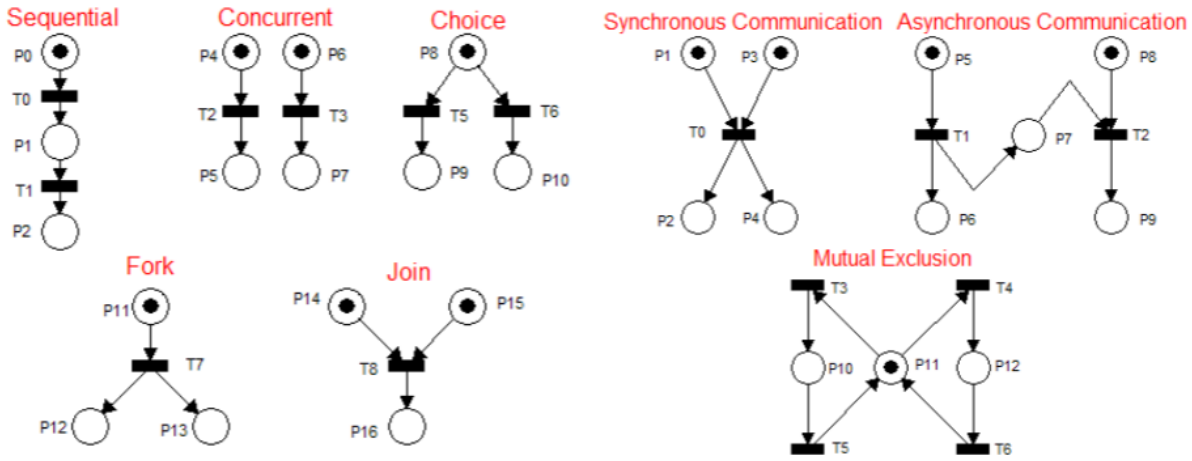


Figure 5.8 PN representation of elementary process structures

It happens that in many applications, basic Petri nets are unable to represent adequately the process under analysis and many extensions of Petri nets have been developed. In Section V.4 some of the main classes of extended Petri nets are briefly introduced.

V.4 Petri net extensions

Among the many extensions of Petri Nets to cope with specific classes of applications, Timed Petri Nets, Stochastic Timed Petri Nets and Coloured Petri Nets are briefly discussed here.

V.4.1 Timed Petri Nets (TPNs)

Petri net formalism provides a set of simple constructs that can allow to model a large variety of systems. However, a major weakness of ordinary Petri nets is that they provide no way to represent the passage of time. In general, information regarding the amount of time it takes to complete the different processes, is available. Tokens move from one place to another according to the transition firings, which have a given processing time.

Ramchandani (Ramchandani, 1974) and Sifakis (1977) introduced the main notions concerning timed Petri net (TPN). Ramchandani described a timed Petri net as a pair (PN, Θ), where PN is a Petri net and Θ is a vector of processing time functions that assigns a positive real number to each transition of the net. In a timed Petri net each transition T_i, once enabled, has a time delay θ_i before firing. When the firing times are chosen to be rational, the processing times can be discretized in units of time so that the state of the process can be determined at each instant of time. The rule of operation of a TPN is similar to an ordinary PN and, once a transition is enabled, the tokens are removed from the input places and are held for a time θ_i, after which the tokens are sent to all the output places. Transitions in TPN can be viewed as a list of events where multiple sets of tokens can be at different stages of the time delay. The firing and termination occur during the processing time and at the end of the execution, respectively.

The TPN studied by Ramchandani have deterministic processing times associated to the transitions. Sifakis considered associating delays to places and showed that the distinction between associating processing times with transitions or with places is not fundamental since TPN of one class can be converted into the other.

It appears that TPNs are of interest to perform throughput analysis of automated systems where the durations of the different successive or parallel elementary tasks are perfectly known. In the case of inspection stations, where the place of the human operator is essential, these durations evolve according to complex phenomena and have a stochastic character. Then STPNs have been considered.

V.4.2 Stochastic Timed Petri Nets (STPNs)

Some of the works discussed above can be extended to analyse TPN with random processing times by replacing these times by their expected values. However, the results obtained in this way provide

only very loose approximations to the average firing rate. Several researchers have tried to remedy this situation by converting the TPN into an equivalent Markov chain and then analysing the resulting Markov chain. Zuberek (Zuberek, 1980) was the first researcher to perform this transformation and was able to analyse a Stochastic Timed Petri Net (STPN), which only allowed very simple decision rules based on independent probabilities. Razouk and Phelps (1984) extended Zuberek's work to STPNs that can tackle time-out situations where the completion of one activity may disable others.

The decision rules are still based on independent probabilities. However, none of these articles show that the resulting Markov chain has a well-defined steady state probability distribution, and their procedures are applicable to only very small problems.

Molly (Molly 1983) solved somewhat larger problems by associating exponential processing times with transitions and by specifying a decision rule that stated that the transition whose processing time terminates first would fire first. Marson (Marson, 1985) extended Molly's results to manage also some transitions with zero processing times. The main weakness of all the works mentioned above is that they need to construct an equivalent Markov chain to model the evolution of the marking of the net to find the performance measures of interest.

In the case of an inspection station, adopting a simulation approach of the resulting STPN, the Markov assumption is not necessary. Then, the performance of the inspection station, seen as a network of processes linked by queues, can be assessed even in transient situations. This should allow to assess the dynamic workload of the different human operators and, eventually, tune their expected control performance.

V.4.3 Coloured Petri Nets

Coloured Petri net (CPN) is an extension to ordinary Petri nets in which « colours » are associated with tokens, and transitions fire according to a set of rules that match the appropriate colours. A coloured token is analogous to a subscripted variable. The advantage of coloured Petri nets is that they provide compact models of large systems, they maintain many useful properties of Petri nets and extend initial formalism to allow the distinction between tokens.

Jensen (Jensen, 1996) has introduced and defined the CPNs, whose main ideas are the relation between an occurrence colour and token colours (which were involved in the occurrence of the transition). The relation is defined by functions attached to the arcs. In addition, the CPN attaches

a set of possible token colours to each place and a set of possible occurrence colours to each transition.

Definition: A CPN can be defined as a tuple (P, T, A, Σ, C, N, E, G, I)
Where:

- P is a set of places,
- T is a set of transitions,
- A is a set of arcs with $P \cap T=P \cap A=T \cap A=\emptyset$,
- Σ is a set of colour sets,
- C is a colour function which maps places in P into colours in Σ,
- N is a node function which maps A into $(P \times T) \cup (T \times P)$,
- E is an arc expression function which maps each arc $a \in A$ into the expression e.

The input and output types of the arc expressions must correspond to the type of the nodes the arc is connected to. The use of node functions and arc expression functions allows multiple arcs to connect the same pair of nodes with different arc expressions.

- G is a guard function which maps each transition $t \in T$ to a guard expression g. The output of the guard expression is a Boolean value: true or false.
- I is an initialization function which maps each place p into an initialization expression i. The initialization expression must evaluate to multiset of tokens with a colour corresponding to the colour of the place $C(p)$.

Each place and each transition has attached a set of colours. A transition can fire with respect to each of its colours, then tokens are removed from the input places and added to the output places in the same way as that in a classical Petri nets. A functional dependency is specified between the

colour of the transition firing and the colours of the involved tokens and the colour attached to a token may be changed by firing a transition.

To illustrate briefly the above object, Figure 5.9 provides an example of firing a transition (here T_1) in a Coloured Petri Net with two colours (blue and red).

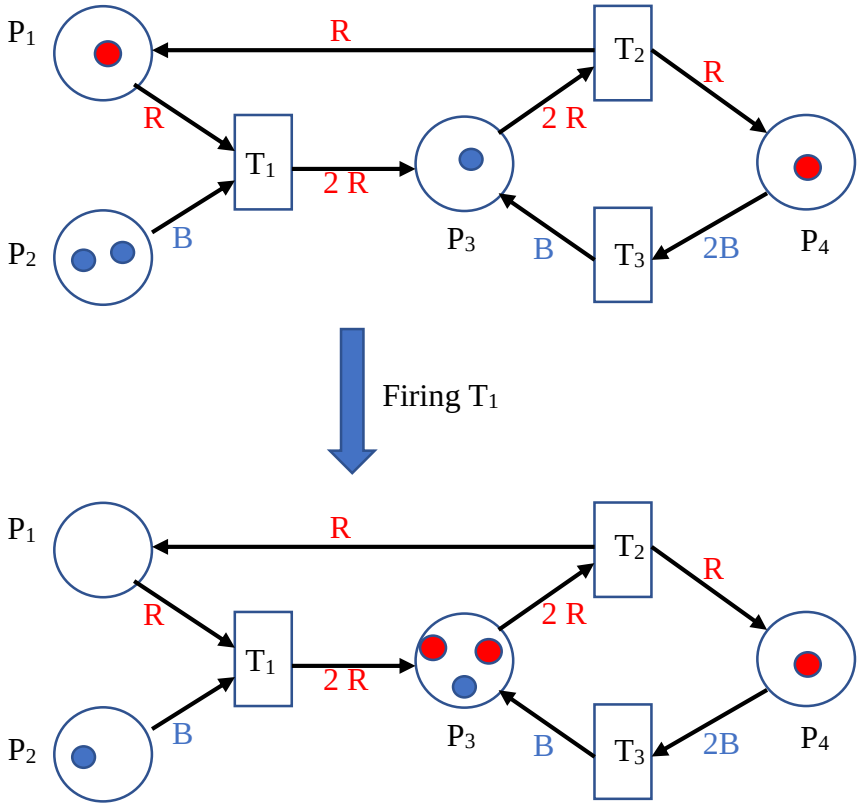


Figure 5.9 Example of firing a transition in a Coloured Petri Net

The CPN allows the modeller of systems with repetitive processes to view a smaller network in which tokens have changed colour to indicate process steps, assign attributes, or differentiate between tokens. It can be considered that the primary function of CPN is data management. CPNs lead to compact net models by using of the concept of colours.

For example, a simple manufacturing system with two machines M_1 and M_2, which process three different types of materials. Each type of material undergoes one stage of processing performed

either with M_1 or with M_2. Once processing is completed, the material is taken out and a new material is loaded. Figure 5.10 displays an uncoloured PN representation of the whole process involving 11 places and 12 transitions:

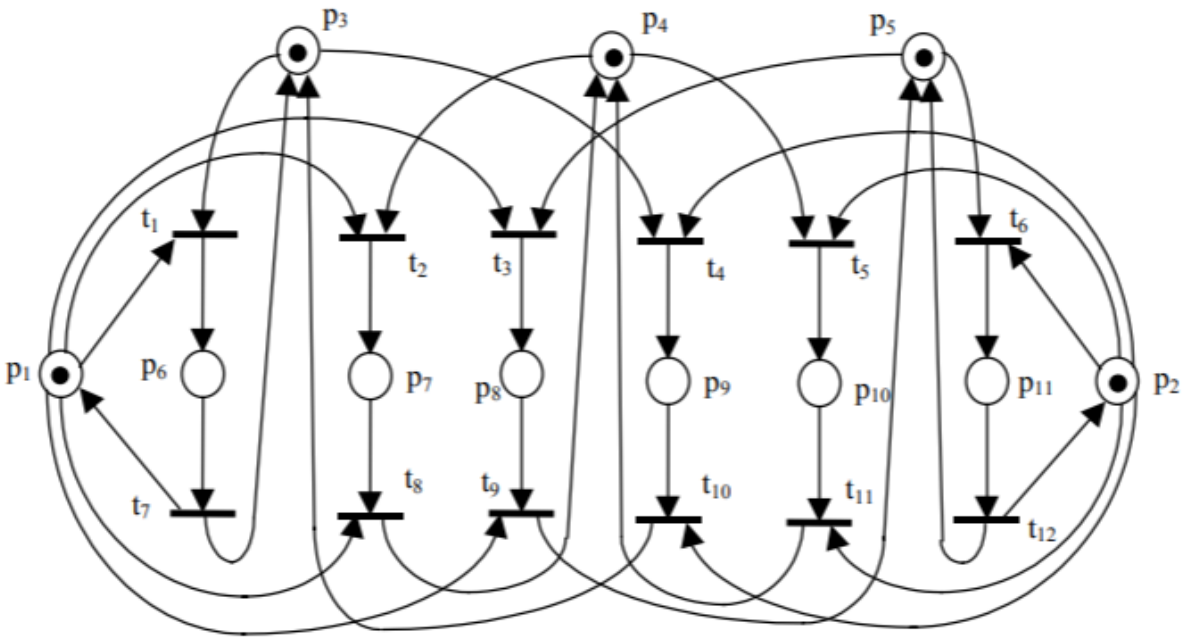


Figure 5.10 Uncoloured PN representation of a manufacturing process

The places and transitions in the model have the following meanings:

p_1 (p_2): machine M_1 (M_2) is available; p_3 (p_4, p_5): a raw material of type 1 (type 2, type 3) is available; p_6 (p_7, p_8): M_1 is processing a material of type 1 (type 2, type 3); p_9 (p_{10}, p_{11}): M_2 is processing a material of type 1 (type 2, type 3); t_1 (t_2, t_3): M_1 begins processing a material of type 1 (type 2, type 3); t_4 (t_5, t_6): M_2 begins processing a material of type 1 (type 2, type 3); t_7 (t_8, t_9):

M_1 ends processing a material of type 1 (type 2, type 3); t_{10} (t_{11}, t_{12}): M_2 ends processing a material of type 1 (type 2, type 3).

Now let us take a look at the CPN model of this manufacturing system, which is shown in Figure 5.11. As we can see, there are only 3 places and 2 transitions.

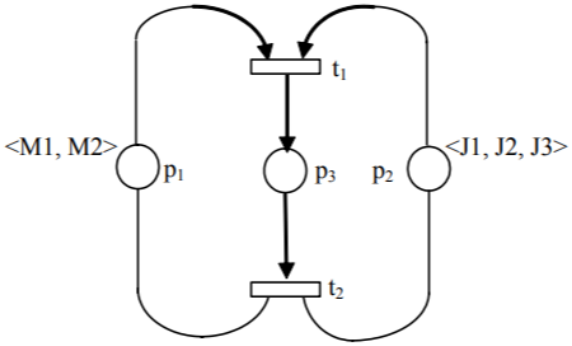


Figure 5.11 CPN reduced representation of the manufacturing process

Now, p_1 means that machines are available, p_2 means that material is available, p_3 means that processing is in progress, t_1 means that processing starts and t_2 means that processing ends. There are 3 colour sets: SM, SP and SM × SP, where SM = {M1, M_2}, SP = {J_1, J_2, J_3}. The colour of each node is as follows: C(p_1) = {M_1, M_2}, C(p_2) = {J_1, J_2, J_3}, C(p_3) = SM × SP, C(t_1) = C(t_2) = SM × SP.

CPN models can be analysed as for ordinary Petri nets, through reachability analysis by building a reachability graph. Even for small CPNs that graph can become very large, but tools exist to

construct it and analyse it automatically. Other techniques work on condensed occurrence graphs without losing analytic power.

CPN have been applied in many engineering fields and in particular to verify security protocols in communication systems.

V.5 Bayesian Coloured Petri Nets (BCPNs)

In this section it is proposed a new modelling tool which tries to take advantage of properties of both Discrete Bayesian Networks and Coloured Petri Nets in order to get a powerful modelling tool for multistep processes with uncertainty as is the process under investigation in this thesis.

V.5.1 Formal definition

A BCPN can be defined as a tuple $(P, T, PT, TP, \Sigma, C, NA, NT, E, \Pi, G, I)$

where:

- P is a set of places,
- T is a set of transitions,
- PT and TP are sets of arcs with $PT \cap T = PT \cap A = TP \cap T = TP \cap A = T \cap A = \emptyset$, $(P \cup T, PT \cup TP)$ is an acyclic directed graph with the set of nodes $P \cup T$ and the set of arcs $PT \cup TP$.
- Σ is a set of colour sets,
- C is a colour function which maps places in P into colours in Σ,
- NA is a node function which maps PT into $(P \times T)$ and NT is a node function which maps PT into $(T \times P)$,
- E is an arc expression function which maps each arc $a \in PT \cup TP$ into the expression e.

The input and output types of the arc expressions must correspond to the type of the nodes the arc is connected to. The use of node functions and arc expression functions allows multiple arcs to connect the same pair of nodes with different arc expressions.

- *Π is a probability function which assigns to the arcs leading to the places successor* $\{p_j \in \Gamma_{t_i}\}$ of each transition t_i a discrete distribution of probability $\{\pi_{ij}\}$, with :

$$\forall t_i \in T: \sum_{j,p_j \in \Gamma_{t_i}} \pi_{ij} = 1 \quad \forall j, p_j \in \Gamma_{t_i} : \pi_{ij} \geq 0 \qquad (5.6)$$

- *G* is a guard function which maps each transition *t*∈*T* to a guard expression *g*. The output of the guard expression is a Boolean value: true or false.
- *I* is an initialization function which maps each place *p* into an initialization expression *i*. and may provide initial distributions of tokens and colours.

Figure 5.12 displays an example of BCPN with 9 places and 4 transitions.

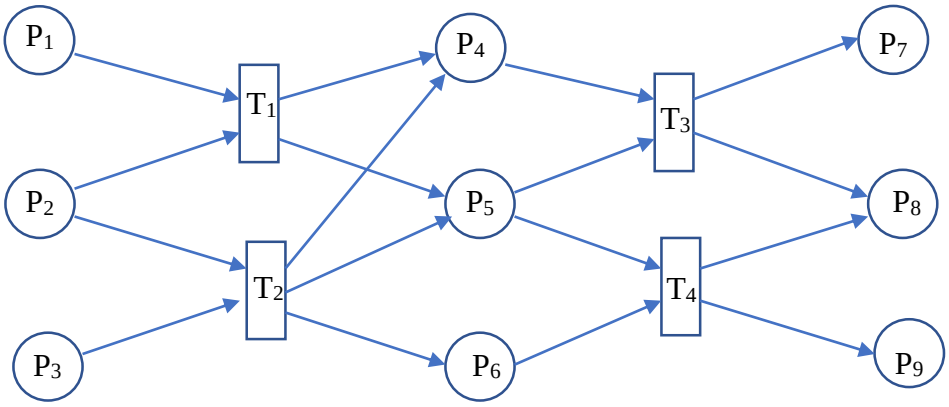


Figure 5.12 Example of BCPN

Here it is supposed that any place can have at most 2 tokens with three different colours (C(p)={R,B,V} $\forall p \in \{P_1, \cdots, P_9\}$), the weighting matrices are given by tables 5.1 and 5.2:

	T_1	T_2	T_3	T_4
P_1	R	-	-	-
P_2	B	V	-	-
P_3	-	B	-	-
P_4	-	-	R	-
P_5	-	-	B	V
P_6	-	-	-	V

Table 5.1 Incidence Places X Transitions

	P_4	P_5	P_6	P_7	P_8	P_9
T_1	0.5	0.5	-	-	-	-
T_2	0.2	0.4	0.4	-	-	-
T_3	-	-	-	0.2	0.8	-
T_4	-	-	-	-	0.4	0.6

Table 5.2 Incidence Transitions X Places

Place initialization can be given by the table 5.3:

P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9
R,V	B,V	B, R	-	R	-	-	-	-

Table 5.3 Initialization of tokens in the places of the BCPN

V.5.2 Firing transitions and computing probabilistic distributions

BCPNs have a dual nature, being at the same time a dynamic object and a stochastic model. Transitions of BCPNs are enabled in the same conditions of CPNs, however, contrarily to CPNs, the outcome of a transition is not deterministic and follows in the mean a probabilistic distribution. When a transition T is fired the places of Γ_T receive concurrently colored tokens according to the

probabilistic distribution of the outcome of the transition. In that case reachability trees acquire a probabilistic nature where probabilistic branching may be generated at the possibly enabled transitions.

In a BCPN, the tokens represent variables characterized by their colour. When a string of tokens arrives at a place, they form an ordered string of variables, ordered according to their order of arrival.

As for Discrete Bayesian networks, the BCPN is an acyclic, directed graph, so it presents initial nodes or source places and final nodes or sink places. It can be observed that among the 8 elementary configurations of PNs in Figure 5.7, only one presents cycles. Given the probability distribution of the colours of the flows of tokens arriving at the source places of a BCPN, it is possible to compute the distribution of probability of the flows of token arriving at the sink places of this BCPN.

Let $\Gamma_{T_j}^{-1}$ be the set of predecessor places of transition T_j in a BCPN, let c_{qj} be the enabling colour between place q and transition T_j, then the enabling probability μ_{qj} of place q for transition T_j is given by:

$$\mu_{qj} = P(X_{q1} = c_{qj}) \tag{5.7}$$

where q_1 is the first token in place q. If place q has no token, $\mu_{qj} = 0$. Then the enabling probability r_j of the uphill places of transition T_j is given by:

$$r_j = \prod_{q \in \Gamma_{T_j}^{-1}} \mu_{qj} \tag{5.8}$$

Consider:

- Ψ_j be the set of transitions which are in concurrence with transition j with respect to some uphill places (for example in Figure 5.8, $\Psi_1 = \{T_2\}$),
- Γ_{T_j} be the set of successor places of transition T_j in a BCPN,
- c_{jp} be the resulting colour between transition T_j and place p,

then the last token that arrives at place p has the probability of being of colour k given by:

$$P(X_p = C_k) = \sum_{\substack{j \in I_p^{-1} \\ C_{jp} = C_k}} r_j \cdot \pi_{jp} / (r_j + \sum_{k \in \Psi_j} r_k) \tag{5.9}$$

or

$$P(X_p = C_k) = \sum_{\substack{j \in I_p^{-1} \\ C_{jp} = C_k}} \left(r_j / (r_j + \sum_{k \in \Psi_j} r_k) \right) \cdot \left(\prod_{q \in I_{T_j}^{-1}} P(X_{q1} = C_{qj}) \right) \tag{5.10}$$

This formula is the equivalent to the propagation formula (5.1) of Bayesian networks. Then, starting from probabilities of colours at entry places, it will be possible to compute from a layer to the next of the BCPN the probabilities of the colours of any place in the network and particularly those of the exit places.

V.6 Application to the Modelling of Inspection Stations

Here it is considered that an inspection station is composed of a succession of elementary control processes, or cells, organized in sequence and that a complementary control will not be realized by the same equipment or operator.

V.6.1 Characteristics of a BCPN associated to an inspection station

The BCPN associated to an inspection station has the following characteristics, defining a sub-class of BCPNs:

- It is assumed that items to be controlled are either good (G) or wrong (W), G and W are then the considered colours.
- It is considered that the performances of controlling with success a good item or a bad item by any device/operator are different:

To an elementary control unit can be attached four probabilities: P_{GG}, P_{GW}, P_{WG} and P_{WW}, where P_{GG} and P_{WW} are probabilities attached to a successful control. In general $P_{GG} \neq P_{WW}$, where P_{GG} (declaring good a good item) and P_{WW} (declaring wrong a wrong item) are probabilities of successful control and $P_{WG} \neq P_{GW}$, where P_{WG} (declaring good a wrong item) and P_{GW} (declaring wrong a good item) are probabilities of unsuccessful control. Also in general:

$$P_{WG} \ll P_{WW} \quad \text{and} \quad P_{GW} \ll P_{GG} \tag{5.11}$$

Then it appears of interest, when considering the modelling of the process with BCPNs, to duplicate the transitions representing a single elementary control unit. Then these pairs of transitions are not allowed to fire simultaneously.

- Each transition has a unique predecessor place and two successor places.
- Coloration in arcs is limited to arcs leading to a transition.
- Colour of the tokens remain unchanged during progression inside the network.

V.6.2 BCPN Modelling an elementary control cell

An elementary control cell must declare a submitted item either Good or Wrong. As happens in many real inspection stations, a first check leading to a Wrong result is doubled checked before final decision. This lead to propose the following simple BCPN structure to represent it:

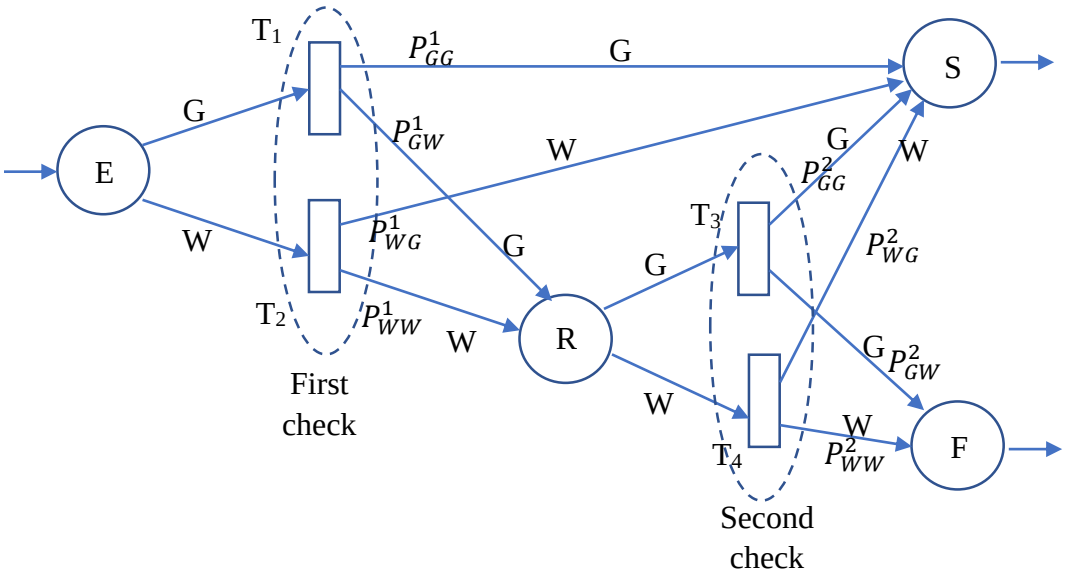


Figure 5.13 BCPN for an elementary control cell

Here E is the entry place, R is the recheck place, F is the fail declared place and S is the success declared place. A token with colour G or W is introduced at place E and the control process begins, it ends either by declaring the item represented by the token, good (place S) or wrong (place F).

The reachability tree of this BCPN will be the superposition of the following 6 paths to which are attached probabilities:

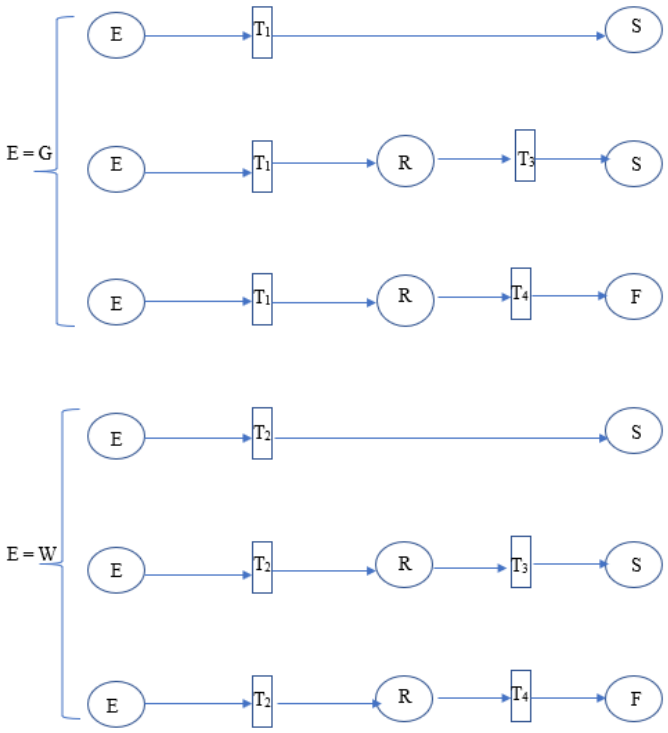


Figure 5.14 The different paths of the reachability tree of BCPN of Figure 5.13

V.6.3 Performance evaluation of an elementary control station

Probabilities of success

Here the success situations are:

In the case of a "good" entry: $P(S = G|E = G)$

This probability, as the others, is computed following backward the graph associated to the BCPN:

$$P(S = G) = P_{BB}^{1} \cdot P(E = G) + P(R = G) \cdot P_{GG}^{2} \quad (5.12)$$

with $$P(R = G) = P_{GW}^{1} \cdot P(E = G) \quad (5.13)$$

or

$$P(S = G) = (P_{GG}^{1} + P_{GG}^{2} \cdot P_{GW}^{1}) \cdot P(E = G) \quad (5.14)$$

Then:

$$P(S = G|E = G) = P^1_{GG} + P^2_{GG} \cdot P^1_{GW} \quad (5.15)$$

and in the case of a "wrong" entry: $P(F = W|E = W)$

$$P(F = W) = P^2_{WW} \cdot P(R = W) \quad \text{with} \quad P(R = W) = P^1_{WW} \cdot P(E = W) \quad (5.16)$$

or

$$P(F = W) = P^2_{WW} \cdot P^1_{WW} \cdot P(E = W) \quad (5.17)$$

Then:

$$P(F = W|E = W) = P^2_{WW} \cdot P^1_{WW} \quad (5.18)$$

The overall probability of success of the control process is then given by:

$$\text{P(success)} = (P^1_{GG} + P^2_{GG} \cdot P^1_{GW}) \cdot P(E = G) + P^2_{WW} \cdot P^1_{WW} \cdot P(E = W) \quad (5.19)$$

or also

$$\text{P(success)} = (P^1_{GG} + P^2_{GG} \cdot P^1_{GW} - P^2_{WW} \cdot P^1_{WW}) \cdot P(E = G) + P^2_{WW} \cdot P^1_{WW} \quad (5.20)$$

Probabilities of failure

The control process failure situations are:

$$P(S = W) = P^1_{WG} \cdot P(E = W) + P(R = W) \cdot P^2_{WG} \quad (5.21)$$

$$\text{with} \quad P(R = W) = P^1_{WW} \cdot P(E = W) \quad (5.22)$$

or

$$P(S = W) = (P^1_{WG} + P^1_{WW} \cdot P^2_{WG}) \cdot P(E = W) \quad (5.23)$$

Then:

$$P(S = W|E = W) = P^1_{WG} + P^1_{WW} \cdot P^2_{WG} \quad (5.24)$$

and

$$P(F = G) = P^2_{GW} \cdot P(R = G) \quad \text{with} \quad P(R = G) = P^1_{GW} \cdot P(E = G) \quad (5.25)$$

or

$$P(F = G) = (P^1_{GW} \cdot P^2_{GW}) \cdot P(E = G) \quad (5.26)$$

Then:

$$P(F = G|E = G) = P^1_{GW} \cdot P^2_{GW} \quad (5.27)$$

The overall probability of failure of the control process is then given by:

$$\text{P(failure)} = (P^1_{WG} + P^1_{WW} \cdot P^2_{WG}) \cdot P(E = W) + (P^1_{GW} \cdot P^2_{GW}) \cdot P(E = G) \quad (5.28)$$

or also

$$\text{P(failure)} = (P^1_{WG} + P^1_{WW} \cdot P^2_{WG} - P^1_{GW} \cdot P^2_{GW}) \cdot P(E = W) + (P^1_{GW} \cdot P^2_{GW}) \quad (5.29)$$

$P(S = G\|E = G)$	$P(S = G\|E = W)$
$P(F = W\|E = G)$	$P(F = W\|E = W)$

Figure 5.15 Successful (Blue) and unsuccessful (Red) outcomes

V.7 Modelling a Complex Inspection Station

Considering that a control process is composed of a set of elementary control stations organized along an acyclic directed graph as its nodes, it will be possible using the BCPN representation of an elementary control station (see figure 5.9) to link them according to that graph to get an overall BCPN representation of the control process.

Figure 5.16 provides an example of BCPN representation of a passenger control process (in this figure places connected by green arrows represent a single place of the BCPN).

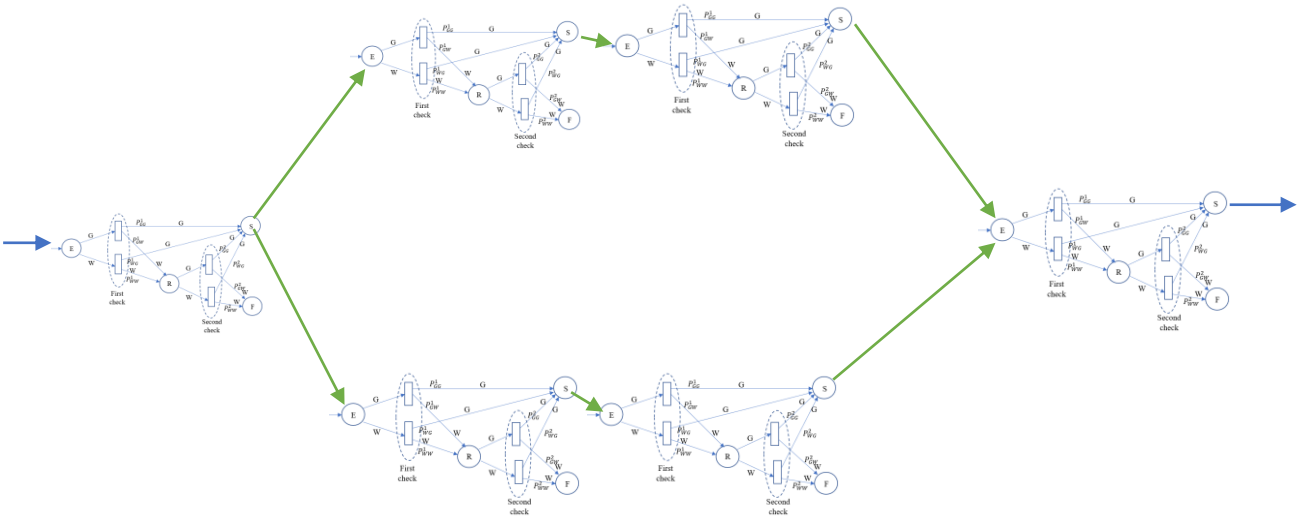


Figure 5.16 Example of a BCPN representation of a complex control process

V.8 Conclusion

In this chapter, a microscopic analysis of the performance of a departure passenger control process has been performed. The proposed process presenting simultaneously a dynamic behaviour, which can be represented by Petri nets, and a probabilistic behaviour, which can be modelled using distributions of probabilities and conditional probabilities as found in Bayesian networks, a modelling tool to catch these two dimensions has appeared of interest. Then, Binary Bayesian Networks and a special class of Petri Nets, the Coloured Petri Nets, have been merged to produce this new modelling tool, Bayesian Coloured Petri Nets (BCPNs).

It has not been the main objective here to analyse the mathematical properties of such modelling tool, this work remains to be done. However, its application to modelize elementary, or more complex, control structures has been displayed here providing a new tool to assess the expected performance of a passenger inspection station.

CHAPTER VI

OPTIMIZATION OF

MULTISTAGE PASSENGER SCREENING OPERATIONS

VI.1 Introduction

This chapter develops an optimization approach to improve, in the mean, the performance of the system of control of passenger flows at boarding, whatever their subsequent path, through a probabilistic approach.

Here contrarily to the previous chapter where passengers where considered individually, in this chapter passengers are considered as part of flows which are processed differently by a serial/parallel control structure. An analogy could be made with the filtering of a homeopathic solution which can be performed by successive filtering. This leads to address the problem as a multistage flow processing complex. This also opens the way to optimization of control operations at the flow level by providing mathematical formulations of control decision problems which impact the quality and the quantity of applied controls on departing passengers. The main objective of this chapter is to provide an approach to better master the control of the departing passenger flows by taking into account the mean performance of the control system as a whole as well as the mean performances of each of the elements that make it up, including staff. This should be a support for developing a strategy for improved control structure and security resource utilization.

The first part of this chapter is devoted to the development of the probabilistic modelling of multi-stage control structures. Once mandatory and complementary controls are introduced, three control structures are considered including pre-screening, post-screening and mixed screening. In the second part of this chapter, the post-screening case is developed with an a priori classification and distribution of threats types, introducing two levels of classification of controlled passengers:

- In the first situation, passengers are submitted to a common serial treatment at mandatory control stations and then they are distributed along complementary control processes, according to their detection performances and capacity, for post screening.
- In the second situation, mandatory control organizes passengers in separate groups for further screening and assignment to post screening control stations.

Different optimization problems rise in these two situations, where probability of threat detection must be maximized while probability of false alarm must be restrained. The final

question addressed is about uncertainty of the probability values with respect to the performances of the elementary components of the departing passenger control system.

VI.2 Probabilistic Modelling of Multi-Stage Control

From the security point of view, the multi-stage path of a passenger, presenting or not a threat, can be modelled by a directed graph (Figure 6.1).

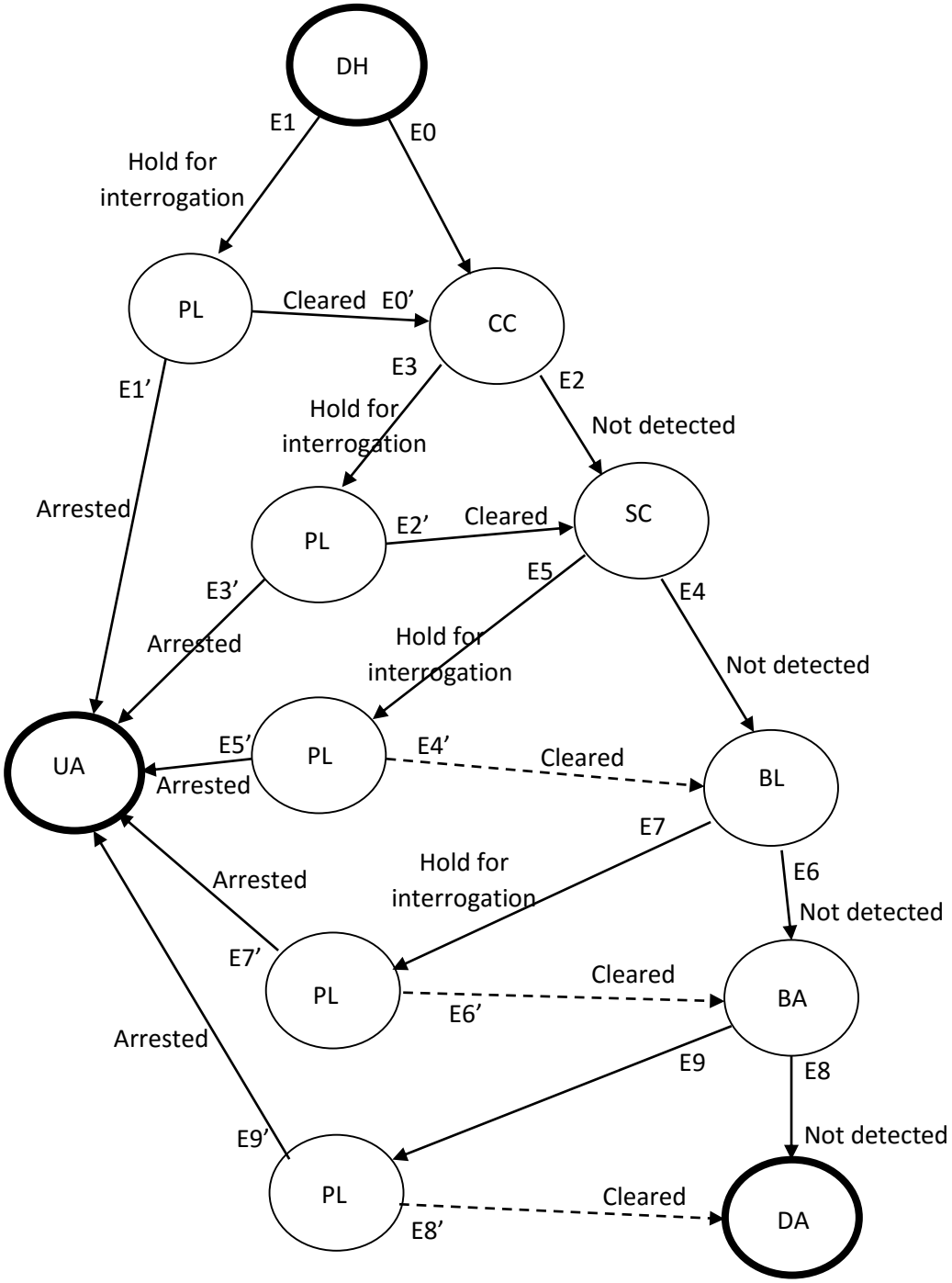


Figure 6.1 Multi-stage security screening

In the directed graph of figure 6.1, DH stands for “departure hall”, PL stands for “police”, UA stands for “under arrest”, “CC stands for “check-in counter”, SC stands for “passenger screening checkpoints”, BL stands for “boarding lounge”, BA stands for passenger “boarding aircraft” and DA stand respectively for “departed aircraft” with passenger on-board.
With regards to the threat situations, the events taken into account in this graph are:

- E0: “potential threat not detected at departure hall”,
- E0’: “potential threat cleared at departure hall”
- E1: “potential threat detected at departure hall”,
- E1’: “potential threat confirmed at departure hall”,
- E2: “potential threat not detected at check-in counter”,
- E2’: “potential threat cleared at check-in counter”,
- E3: “potential threat detected at check-in counter”,
- E3’: “potential threat confirmed at check-in counter”,
- E4: “potential threat not detected at security checkpoint”,
- E4’: “potential threat cleared at security checkpoint”,
- E5: “potential threat detected at security checkpoint”.
- E5’: “potential threat confirmed at security checkpoint”,
- E6: “potential threat not detected at boarding lounge”,
- E6’: “potential threat cleared at boarding lounge”,
- E7: “potential threat detected at boarding lounge”,
- E7’: “potential threat confirmed at boarding lounge”,
- E8: “potential threat not detected at boarding aircraft”,
- E8’: “potential threat cleared at boarding aircraft”,
- E9: “potential threat detected at boarding aircraft”,
- E9’: “potential threat confirmed at boarding aircraft”.

Here it is supposed that the following probabilities are available:

- P1: Probability of detecting a real threat at the departure hall.
- P3: Probability of detecting a real threat at the check-in counter.
- P5: Probability of detecting a real threat at security checkpoint.
- P7: Probability of detecting a real threat at the boarding lounge.
- P9: Probability of detecting a real threat at aircraft boarding.

These probabilities include primary detection of potential threat and confirmation by security service as shown in Figure 6.2. The estimation of these probabilities is difficult to be performed since not every undetected threat results in a visible terrorist attempt and remains unnoticed.

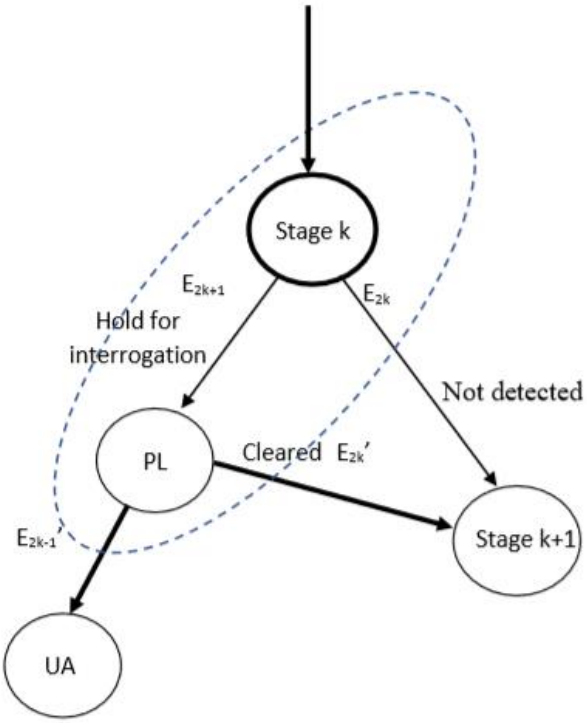


Figure 6.2 Graphical representation of a security stage

Other probabilities which contribute to characterizing the performance of the multi-stage security system are false alarm probabilities, which produce flow disruption, delays and discomfort for no threat passengers and unnecessary means and attention by security staff. Here these are at each stage:

- P0: Probability of false alarm at the departure hall,
- P2: Probability of false alarm at the check-in counter,
- P4: Probability of false alarm at security checkpoint,
- P6: Probability of false alarm at the boarding lounge,
- P8: Probability of false alarm on board aircraft.

Estimations of these probabilities can be obtained by statistical means by collecting data about controls resulting in a false alarm at each stage of the control process. Continuous progress has been performed over the years by improved staff training.

In the case of event E4', E6' and E8', depending of the imminence of flight departure, the no threat passenger may risk to lose his flight.

According to Figure 6.1, the global probability of successfully detecting a real threat (SDT) is given by:

$$P_{SDT} = P_1 + (1-P_1)\cdot P_3 + (1-P_1)\cdot(1-P_3)\cdot P_5 + (1-P_1)\cdot(1-P_3)\cdot(1-P_5)\cdot P_7 + (1-P_1)\cdot(1-P_3)\cdot(1-P_5)\cdot(1-P_7)\cdot P_9 \quad (6.1)$$

or

$$P_{SDT} = P_1 + \sum_{k=1}^{4}\left(\prod_{s=1}^{s=k-1}(1-P_{2s-1})\right)\cdot P_{2k+1} \quad (6.2)$$

The complementary probability of globally not detecting a real threat, P_{FDT}, is given by:

$$P_{FDT} = 1 - P_{SDT} \quad (6.3)$$

The global probability (success) of non-detection of a passenger (NDP) who is not a threat, P_{NDP} is:

$$P_{NDP} = \prod_{k=0}^{k=4}(1-P_{2k}) \quad (6.4)$$

and the complementary global probability of processing a false alarm, P_{FAP} is given by:

$$P_{FAP} = 1 - \prod_{k=0}^{k=4}(1-P_{2k}) \quad (6.5)$$

VI.3 Probabilistic Evaluation of a Control System with Pre-Filtering

To avoid all passengers to be submitted to every possible stage of control inside the airport, inducing unnecessary delays and discomfort for passengers, as well as increased security cost (more equipment and staff), passengers can be classified by security according to the potential danger they can represent. This can be done already, in part, today before the passenger reaches the airport for travelling, at the time of booking a flight according to his personal information.

VI.3.1 Multi-stage control structures

Here the a priori probability of having a threat associated to a passenger is written τ and it is supposed that there M different threats are considered, $T=\{T_1, T_2, \cdots, T_M\}$, with the following probability distribution : π_i, $i \in \{1, \cdots, M\}$.

Then it is supposed that arriving passengers are divided into N classes according to the a priori threat they may represent.

Here two types of controls are considered:

- Those that are mandatory, they belong to the set C1.
- Those that are not mandatory, but may reinforce the C1 controls in certain circumstances, they belong to the set C2.

So to each class n of passengers is assigned a subset C_2^n of controls of C_2. Each control subset is supposed to be able to detect with some success a subset of different types of threat T_n where $\bigcup_{n=1}^{N} T_n = T$ is the set of threats possibly detected by the complementary controls.

At this stage, three main different organizations of control can be considered:

- OB: C2 controls are realized before C1 controls so that a limited number of passengers pass through the mandatory controls C1;
- OA: C2 controls are realized after C1 controls so that C1 controls are reinforced by C2 controls;
- OM: C1 and C2 controls are mixed, for instance, some C2 controls are performed before C1 controls and others after.

Figures 6.3.a, 6.3.b and 6.3.c represent these different control organizations (Yellow for C_1, blue for C_2, red for positive detection).

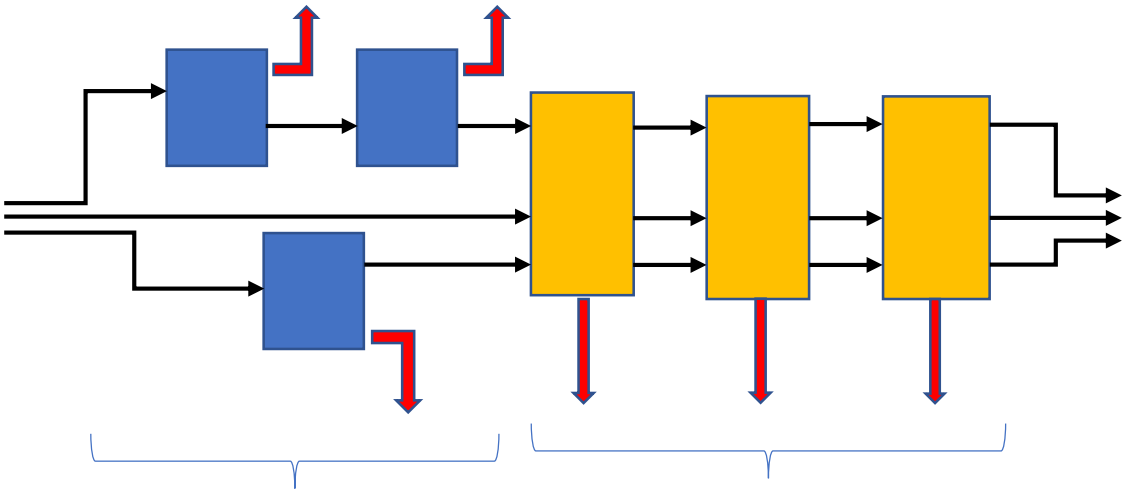


Figure 6.3.a Pre-screening configuration of controls

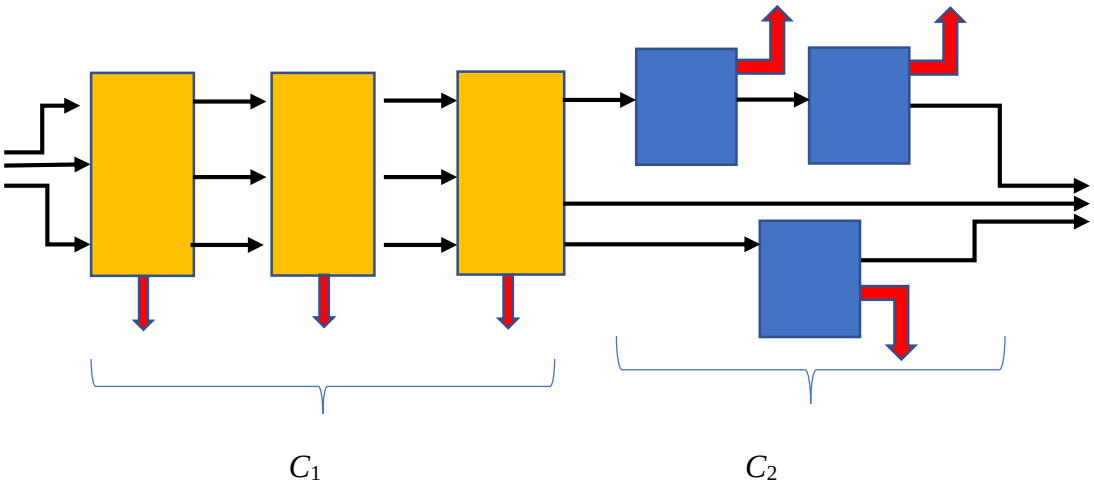


Figure 6.3.b post-screening configuration of controls

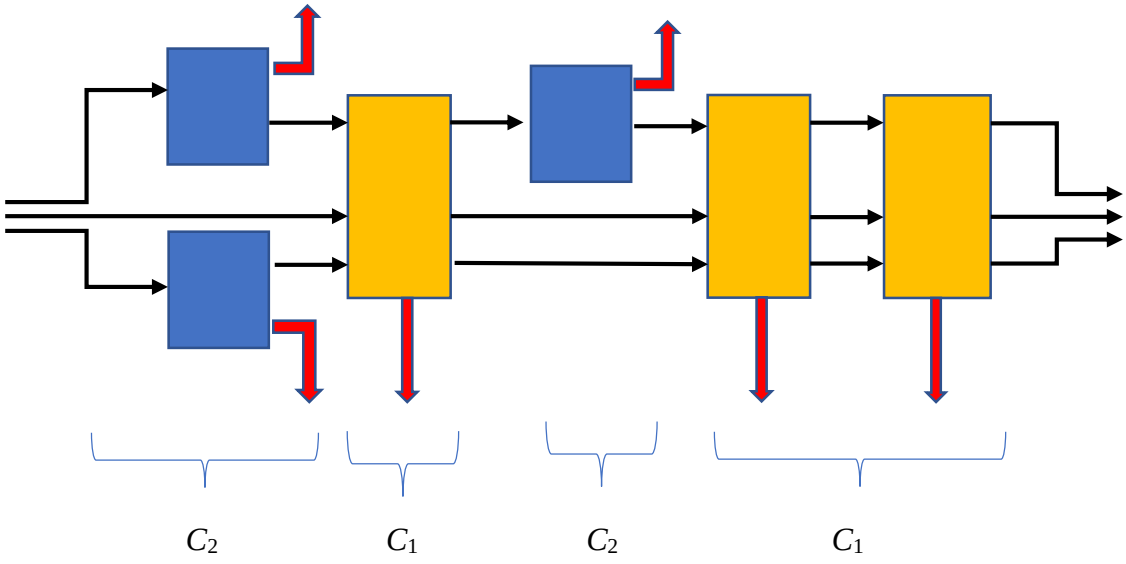


Figure 6.3.c mixed configuration of screening

To answer to the question of which organization is the best, many factors must be taken into account:

- The characteristics of the flow of passengers: degree of homogeneity and distribution of types of flights.
- Expected degree of danger: low, medium or high level of threat.
- The performances of the different control stations (differences in detection performances and complementarity).
- Availability of space, staff and equipment as well as overall layout of terminal.

VI.3.2 Mathematical representation of a multi-stage control structure

The proper functioning of a control *j* can be described by:

- the probability of detecting a real threat of type k at control j: $p_{kj}, j \in C_1 \cup C_2, k \in \{1, \cdots, M\}$;
- The probability of generating a false alarm at control j with respect to a no threat k: qkj.

Let during a given period of time x_i be the proportion of passengers assigned to threat class *I* and then to go through C_1 and C_2^n controls:

$$\sum_{i=1}^{N} x_i = 1 \qquad (6.6)$$

Consider that the proportion of passengers representing a threat is very small, so it can be considered that there is conservation of passenger flow from the first to the last control stages. The error, being extremely small, can be ignored here.

Then the proportion of passengers y_j passing through the control j, whatever its position in the control sequence is given by:

$$y_j = 1 \text{ if } j \in C_1 \quad \text{and} \quad y_j = \sum_{i=1, j \in C_2^i}^{N} x_i \quad \text{if } j \in C_2 \tag{6.7}$$

Figure 6.4 displays an example of post screening control structure:

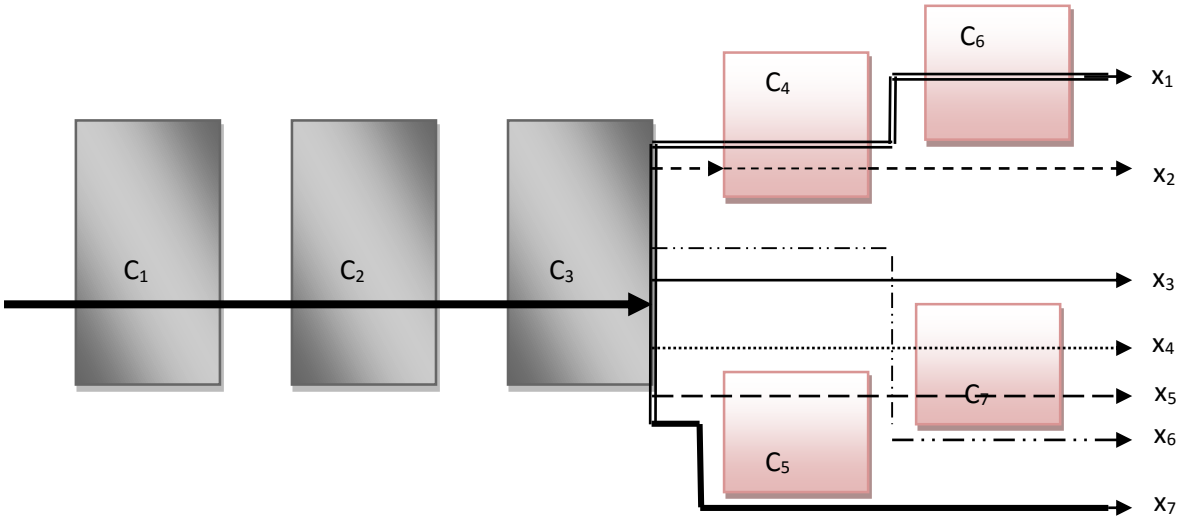


Figure 6.4 Example of post screening control structure with paths

In the example of Figure 6.4, the flow constraints are such as:

$$y_1 = y_2 = y_3 = 1, y_4 = x_1 + x_2, y_5 = x_5, y_6 = x_1 \text{ and } y_7 = x_4 + x_5 \tag{6.8}$$

Considering now that each control station j has a capacity of treatment K_j (given passengers/hour), and given the total flow of passengers per unit of time D ($\neq 0$) crossing the control structure, the proportion of passengers using it has a maximum value given by:

$$y_j^{max} = min\{\frac{K_j}{D} \ , \ 1\} \qquad \forall j \in C_2 \tag{6.9}$$

It is, of course, supposed that control stations of C_1 have a capacity sufficient to cope with total incident flow ϕ.

VI.3.3 Probabilistic performance evaluation

The probability of having an alarm at control "*j*" , P_j^a, is given by:

$$P_j^a = \left(\tau \cdot \left(\sum_{k=1}^{M} p_{kj} \cdot \pi_k\right) + (1-\tau) \cdot \left(\sum_{k=1}^{N} q_{kj} \cdot \pi_k\right)\right) \cdot y_j \qquad \forall\, j \in C_1 \cup C_2 \qquad (6.9)$$

where the first term of the RHS of equation (6.9) corresponds to the cases where there is a threat and an effective detection of the threat and the second term of the RHS corresponds to the case in which there is no threat but a false alarm is generated. Then the probability of having a false alarm when a passenger comes to controls is P_{fa} given by:

$$P_{fa} = (1-\tau) \cdot \sum_{j \in C_1 \cup C_2} \left(\sum_{k=1}^{N} q_{kj} \cdot \pi_k\right) \cdot y_j \qquad \forall\, j \in C_1 \cup C_2 \qquad (6.10)$$

and the mean number of false alarms per unit of time N_{FA} is given by:

$$N_{FA} = D \cdot P_{fa} \qquad (6.11)$$

This formula is also an approximation, since the occurrence of multiple or successive false alarms is not considered for having an extremely small probability (a sum of product of two or more probabilities of false alarm which are already very small).

The probability of non-detection of a threat when a passenger arrives to controls, P_{ndt}, is given here by:

$$P_{ndt} = \tau \cdot \sum_{i=1}^{N} \left(\sum_{k=1}^{M} \pi_k \cdot \left(\prod_{j \in C_1 \cup C_2^i} (1 - p_{kj})\right) \cdot x_i\right) \qquad (6.12)$$

and the mean number of detected threats per unit of time N_{DT} is given by:

$$N_{DT} = D \cdot (1 - P_{ndt}) \qquad (6.13)$$

VI.4 Optimizing the assignment of passengers to screening channels

The aim here is to minimize simultaneously the probabilities of non-detection of an existing threat and of generating a false alarm. While trying to guarantee a maximum level of false alarms and taking into account the average availability of the checkpoints.

VI.4.1 Problem formulation

The considered problem is a bi-criteria optimization problem where the two criterion may be antagonist: intensifying control along a path is expected to decrease the number of non-detected threats but also to increase the number of false alarms on the same flow. The initial formulation is as follows:

$$\min_{\boldsymbol{x}}\{P_{ndt}(\boldsymbol{x}),\ P_{fa}(\boldsymbol{y}(\boldsymbol{x}))\} \tag{6.12}$$

under the constraints:

$$\sum_{i=1,j\in C_2^i}^{N} x_i \ \leq y_j^{max} \quad \forall j \in C_2 \tag{6.13}$$

$$\sum_{i=1}^{N} x_i = 1 \qquad x_i \geq 0 \ \ \forall i \in \{1,\cdots,N\} \tag{6.14}$$

Two main techniques have been used to transform a multicriteria problem into a mono criteria one for which many solution algorithms have been developed to cope with many different classes of optimization problems:

- Construct a single criterion by predefining weights associated to each criterion:

$$\min_{\boldsymbol{x}}(w_1 \cdot P_{ndt}(\boldsymbol{x}) + \ w_2 \cdot P_{fa}(\boldsymbol{y}(\boldsymbol{x})))$$

with $w_1 \geq 0$, $w_2 \geq 0$ and $w_1 + w_2 = 1$ (6.15)

or

$$\min_{\boldsymbol{x}}\ ((P_{ndt}(\boldsymbol{x}))^{\alpha_1} \cdot \left(P_{fa}(\boldsymbol{y}(\boldsymbol{x}))\right)^{\alpha_2}) \tag{6.16}$$

with $\alpha_1 \geq 0$, $\alpha_2 \geq 0$ and $\alpha_1 + \alpha_2 = 1$

It appears that in both cases the original significance of the problem is lost in benefit of the mono criterion formalism.

- Choose a primary criterion which will be minimized with an additional constraint relative to a maximum admissible level for the secondary criterion. The difficulty here being to produce this maximum admissible level, different values can be tested. When the additional constraint is saturated at solution, this

produces a pair of non-inferior solutions. The set of generated non inferior solutions is called a Pareto frontier [ref].

The adopted formulations is as follows:

$$\min_{\boldsymbol{x}} P_{ndt}(\boldsymbol{x}) \tag{6.17}$$

under

$$P_{fa}\big(\boldsymbol{y}(\boldsymbol{x})\big) \leq P_{fa}^{max} \tag{6.18}$$

with constraints (6.13) and (6.14), where P_{fa}^{max} is the maximum admissible level of the probability of false alarms.

Considering the expressions of $P_{ndt}(\boldsymbol{x})$ (relation (6.12)) and of $P_{fa}\big(\boldsymbol{y}(\boldsymbol{x})\big)$ (relation (6.10)), this is a typical Linear Programming Problem (Dantzig et al., 1997 and 2003) for which many solvers, mainly based on the Simplex algorithm, exist.

VI.4.2 Numerical application

Here is considered the post-screening case, as depicted in Figure 6.4, where it has been considered that there are only four types of threats. The following table gives the probabilities of detection associated with the controls point by threat type, the probabilities by threat type and the probabilities of false alarms by control point.

Table 6.1 Adopted probability distributions

-	C_4	C_5	C_6	C_7	π
p_{1j}	0.990	0.980	0.850	0.750	0.40
p_{2j}	0.850	0.995	0.965	0.550	0.25
p_{3j}	0.980	0.950	0.580	0.990	0.25
p_{4j}	0.800	0.975	0.995	0.780	0.10
$q_{jk} = q_j$	0.001	0.001	0.002	0.002	-

In Figure 6.4 have been considered seven different control paths in the post screening phase.

Table 6.2 Considered post-screening paths

Proportion	Treatment
x_1	*Nil*
x_2	*C4*
x_3	*C4 – C6*
x_4	*C4 – C7*
x_5	*C5*
x_6	*C5 – C7*
x_7	*C7*

Mean processing times, without (t_i)and with alarms (θ_i) , are shown in the table below:

Table 6.3 Processing times at post-screening (in seconds)

-	C_4	C_5	C_6	C_7
t_i	10	15	10	15
θ_i	100	150	100	150

The unit of time adopted is T = 10 minutes and initially, a request of D=1600 passengers / hour to pass the control. It is assumed here that the controls consist of 6 stations operating simultaneously.

This leads to the formulation of the following linear optimization problem:

$$\min x_1 + 0.066500\, x_2 + 0.0\,06251\, x_3 + 0.022325\, x_4 \qquad (6.19)$$

$$+0.049250\, x_5 + 0.003237\, x_6 + 0.237000\, x_7$$

with the constraints:

$$x_2 + 3\, x_3 + 3\, x_4 + x_5 + 3\, x_6 + 2\, x_7 \leq 1002\ P_{fa}^{max} \qquad (6.20)$$

$$x_5 + x_6 \leq 0.9625 \qquad (6.21)$$

$$x_3 + x_6 \leq 0.9625 \qquad (6.22)$$

$$x_4 + x_6 + x_7 \leq 0.9625 \qquad (6.23)$$

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = 1 \qquad (6.24)$$

$$x_i \geq 0 \quad i = 1, 2, \cdots, 7 \qquad (6.25)$$

Taking P_{fa}^{max} = 0.003 (3 per 1000 checks), the following solution is obtained:

$$x_1 = 0,\ x_2 = 0,\ x_3 = 0.30729,\ x_4 = 0.03751,\ x_5 = 0,\ x_6 = 0.65520,\ \ x_7 = 0$$

It corresponds to a probability of not detecting a threat of 0.00488 for a false alarm probability of 0.00300.

By varying the total demand (the y_j^{max} $\forall j \in C_2$ change with *D*), the following table is obtained:

Table 6.4 Solutions for different levels of demand

D	x_1	x_2	x_3	x_4	x_5	x_6	x_7	P_{ndt}	P_{fa}
1400	0.0	0.0	0.33672	0.0	0.0	0.66328	0.0	0.00435	0.00300
1600	0.0	0.0	0.30729	0.03751	0.0	0.65520	0.0	0.00448	0.00300
2000	0.0	0.01254	0.29901	0.03232	0.02301	0.61194	0.02321	0.00476	0.00299
2400	0.12388	0.03452	0.25161	0.05223	0.03333	0.32712	0.17731	0.00628	0.00267
3200	0.42331	0.09612	0.08560	0.05726	0.09721	0.14281	0.09770	0.01329	0.00213

By varying $\boldsymbol{P_{fa}^{max}}$ (demand = 1600 pax / h), non-inferior solutions composed of the pairs (P_{ndt} , $\boldsymbol{P_{fa}^{max}}$) can be obtained. Table 6.5 displays these results:

Table 6.5 Solutions for different levels of $\boldsymbol{P_{fa}^{max}}$ (demand = 1600 pax / h)

$\boldsymbol{P_{fa}^{max}}$	x_1	x_2	x_3	x_4	x_5	x_6	x_7	P_{ndt}
0.00285	0.0	0.02105	0.23541	0.13908	0.13307	0.44116	0.01023	0.00482
0.00290	0.0	0.00015	0.24452	0.10043	0.06742	0.58320	0.00428	0.00475
0.00295	0.0	0.0	0.27745	0.06761	0.02381	0.63113	0.0	0.00461
0.00300	0.0	0.0	0.30729	0.03751	0.0	0.65520	0.0	0.00448

It appears from tables 6.4 and 6.5 that according to the level of demand for control and to the admitted level of false alarms, the optimal distribution of the flows of controlled passengers' changes significantly. This gives support to adaptive control procedures according to estimated level of threat and changing demand levels.

VI.5 Optimization of Passenger Assignment with Pre-Selection

It is assumed here that the sequence of mandatory checks C_1 makes it possible to make a first classification of the passengers with respect to the threats that they can represent (pre-selection).

It is assumed that the passengers have been divided at exit of C_1 in Z classes with a probability τ_m that a passenger of class $m \in \{1,\ldots,Z\}$ represents a real threat. Then these passengers' classes are supposed to be subdivided to go through a post-screening process (C_2).

VI.5.1 Problem formulation

Let z_m the given proportion of passengers in class m, m =1 to Z, then:

$$\sum_{m=1}^{Z} z_m = 1 \tag{6.26}$$

$$\text{with} \quad z_m \geq 0 \quad m = 1 \text{ to } Z \tag{6.27}$$

Variables x_{im} representing the proportion of passengers of the threat class m, m = 1 to Z, which are assigned to the control sequence i, i = 1 to N, are introduced. Here $N = \left|C_2\right|$. Then the following restrictions must be satisfied:

$$\sum_{i=1}^{N} x_{im} = z_m \qquad m = 1 \; to \; Z \tag{6.28}$$

$$0 \leq x_{im} \qquad i = 1 \; to \; N, \; m = 1 \; to \; Z \tag{6.29}$$

The assignment of the Z classes of passengers to the different possible control tracks will have consequences on the overall performances of the passenger screening system.

In this situation, the probability of non-detection of a threat is given by:

$$P_{ndt} = \sum_{m=1}^{Z} \sum_{i=1}^{N} \left(\tau_m \left(\sum_{u=1}^{M} \pi_u \prod_{j \in C_2^i} (1 - p_{uj}) \right) x_{im} \right) \tag{6.30}$$

while the probability of generating a false alarm is now given by:

$$P_{fa} = \sum_{m=1}^{Z} \sum_{i=1}^{N} \left((1 - \tau_m) \left(\sum_{k=1}^{M} \pi_k \sum_{j \in C_2^i} q_{kj} \right) x_{im} \right) \tag{6.31}$$

We can then formulate following the same approach than in the previous section, the problem of minimizing the probability of non-detection of a threat, under the constraints of a maximum level for the probability of false alarms and the availability of checkpoints.

$$\min_{\boldsymbol{x}} \sum_{m=1}^{Z} \sum_{i=1}^{N} \left(\tau_m \left(\sum_{k=1}^{M} \pi_k \prod_{j \in C_2^i} (1 - p_{kj}) \right) x_{im} \right) \tag{6.32}$$

under different constraints

- A false alarm constraint:

$$\sum_{m=1}^{Z}\sum_{i=1}^{N}\left((1-\tau_m)\left(\sum_{k=1}^{M}\pi_k\sum_{j\in C_2^i}q_{kj}\right)x_{im}\right)\leq P_{fa}^{max} \quad (6.33)$$

where P_{fa}^{max} is the retained maximum level of probability of false alarm.

- The capacity of the checkpoints of C2 during the period T:

$$\sum_{i=1,j\in C_2^i}^{N}\ \sum_{m=1}^{Z}x_{im}\ \leq\ y_j^{max}\quad j\in C_2 \quad (6.34)$$

- The constraints of proportion:

$$\sum_{i=1}^{N}\ x_{im}\ = z_m \qquad m=1\ to\ Z \quad (6.35)$$

- The domains of the variables:

$$0\ \leq\ x_{mi}\ \leq 1 \qquad i=1,\cdots,N \quad m=1,\cdots,Z \quad (6.36)$$

VI.5.2 Numerical application

The control structure of Figure 6.4 is again considered, but here it is supposed that the C_1 filtering leads to four classes (Z=4) of passengers with threat characteristics given in table 6.6:

Table 6.6 Passenger distribution after pre-filtering

m	1	2	3	4
z_m	0.70	0.15	0.10	0.05
τ_m	0.0001	0.001	0.001	0.002

For P_{fa}^{max} = 0.00300, the following solution is obtained (where $x_i=\sum_{m=1}^{Z}x_{im}$): x_1= 0, x_2 = 0, x_3 = 0.30634, x_4 = 0.02845, x_5=0, x_6=0.66531 and x_7= 0, which corresponds to a probability of not detecting a threat of 0.00439 for a false alarm probability of 0.00300.

By varying the total demand, the following table is obtained:

Table 6.7 Solutions with pre-filtering for different levels of demand

D	x_1	x_2	x_3	x_4	x_5	x_6	x_7	P_{ndt}	P_{fa}
1400	0.0	0.0	0.32655	0.0	0.0	0.67345	0.0	0.00428	0.00300
1600	0.0	0.0	0.30634	0.02845	0.0	0.66531	0.0	0.00439	0.00300
2000	0.0	0.01167	0.28784	0.03332	0.01983	0.64578	0.02139	0.00458	0.00300
2400	0.12388	0.03452	0.27023	0.04536	0.05452	0.55538	0.09351	0.00527	0.00287
3200	0.42331	0.09612	0.23945	0.04975	0.07843	0.42580	0.11045	0.09829	0.00254

Then by varying the level of P_{fa}^{max}, the following table is obtained:

Table 6.8 Solutions with pre-filtering for different levels of P_{fa}^{max}

P_{fa}^{max}	x_1	x_2	x_3	x_4	x_5	x_6	x_7	P_{ndt}
0.00285	0.0	0.01320	0.25231	0.18621	0.14320	0.39067	0.00841	0.00472
0.00290	0.0	0.0	0.24452	0.13429	0.07670	0.54449	0.0	0.00461
0.00295	0.0	0.0	0.28761	0.05462	0.04530	0.61277	0.0	0.00450
0.00300	0.0	0.0	0.30634	0.02845	0.0	0.66531	0.0	0.00439

Thus, in this numerical case appears the beneficial effect of selective pre-filtering which for the same level of false alarms leads to much lower levels of non-detection of threat.

VI.6 Coping with probability uncertainty

The optimization problems considered in this chapter, either (6.16)-(6.17) or (6.32)-(6.33)-(6.34)-(6.35)-(6.36), assume the availability of elementary probabilities $\{p_{kj}, k = 1 \text{ to } M, j \in C_1 \cup C_2^i \text{ or } j \in C_2^i, i = 1 \text{ to } N\}$ and $\{q_{kj}, k = 1 \text{ to } M, j \in C_1 \cup C_2^i \text{ or } j \in C_2^i, i = 1 \text{ to } N\}$. In general, these probabilities are not the result of statistics obtained in real operations conditions, they are the result of statistics obtained through costly and lengthy laboratory experiments, the result of expert knowledge or a mix of them. So, it can be expected that the level of accuracy of these estimations is not extremely high. Moreover, the operational conditions under which these phenomena appear (failure to detect nor failure to clear) are influenced by many factors of different origin whose impact is difficult to be quantized (equipment, operators, demand, period, weather, etc.). Then it appears of interest to represent the uncertainty attached to any set of probabilities proposed to formulate the above optimization problem so that some sensitivity

analysis with respect to the values of these probabilities can be conducted. Different approaches can be adopted:

- Classical sensitivity analysis of Linear Programming (Jansen, 1997) where variations of the values of the probabilities around reference values would be considered, does not apply easily to multiple uncertainty about constraint coefficients (constraints 6.18 and 6.33 are concerned).
- Random generation of numerical instances of the Linear Programming problems with resolution where an a priori distribution is assumed for each probability value. This intensive computational exercise should lead to a distribution of solutions and performance.
- Fuzzy representation of probabilities or fuzzy dual probabilities (Mora-Camino, 2018), could be considered, however, the solution of fuzzy linear programming problems leads in general to cumbersome calculations.

The more likely situation is that, Expert opinion, as a result of qualitative-quantitative analysis, will at most provide a sound interval for independent probabilities (the p_{kj} and the q_{kj}):

$$\{p_{kj}^{-} \leq p_{kj} \leq p_{kj}^{+}\text{ , } k = 1 \text{ to } M, j \in C_1 \cup C_2^i \text{ or } j \in C_2^i, i = 1 \text{ to } N\} \tag{6.37}$$

and

$$\{q_{kj}^{-} \leq q_{kj} \leq q_{kj}^{+}\text{ , } k = 1 \text{ to } M, j \in C_1 \cup C_2^i \text{ or } j \in C_2^i, i = 1 \text{ to } N\} \tag{6.38}$$

Then considering that P_{ndt} is a decreasing function of the parameters p_{kj} while P_{fa} is an increasing function of the parameters q_{kj}, two extreme scenarios can be constructed:

$$\left.\begin{matrix}\{p_{kj} = p_{kj}^{-}\, pkj, k = 1 \text{ to } M, j \in C_1 \cup C_2^i \text{ or } j \in C_2^i, i = 1 \text{ to } N\} \\ \{q_{kj} = q_{kj}^{-}, k = 1 \text{ to } M, j \in C_1 \cup C_2^i \text{ or } j \in C_2^i, i = 1 \text{ to } N\}\end{matrix}\right\} \tag{6.37}$$

and

$$\left.\begin{matrix}\{p_{kj} = p_{kj}^{+}, k = 1 \text{ to } M, j \in C_1 \cup C_2^i \text{ or } j \in C_2^i, i = 1 \text{ to } N\} \\ \{q_{kj} = q_{kj}^{+}, k = 1 \text{ to } M, j \in C_1 \cup C_2^i \text{ or } j \in C_2^i, i = 1 \text{ to } N\}\end{matrix}\right\} \tag{6.37}$$

The first instance of the linear programming problems, either (6.16)-(6.17) or (6.32)-(6.33)-(6.34)-(6.35)-(6.36), will provide a maximum value for P_{ndt} and the second one a minimum value for P_{ndt} while P_{fa} will remain at it maximum value P_{fa}^{max}. So this first result will be

obtained by solving twice each linear programming problem considered above. Then, for each flow solution, either in x_i or x_{im}, an efficiency interval will be defined:

$$x_i^{min} \leq x_i \leq x_i^{max} \quad i = 1, \cdots, N \tag{6.38}$$

or

$$x_{im}^{min} \leq x_{im} \leq x_{im}^{max} \quad i = 1, \cdots, N, m = 1, \cdots, M \tag{6.39}$$

VI.7 Conclusion

The probabilistic approach used in this study to manage passenger flows at security system, seen as a multistage processing complex, has led to the formulation of two linear programming problems of limited complexity.

This approach has several advantages:

- It allows putting in equation the dilemma (probability of non-detection versus probability of false alarm).
- It shows the interest of the differentiated control treatment of departing passengers.
- It shows the interest of establishing a first filtering before implementing a differentiated treatment that becomes then more efficient.
- The degree of complexity of the probabilistic models developed remains small and leads to problems of linear programming in small continuous variables.

Nevertheless, this approach also has important limitations:

- It is completely static and cannot provide online decision support.
- It does not take into account the stochastic natures of demand and service times which lead to the generation of external and internal queues in the control system. Then the modelling approach adopted cannot take into account the spatial organization of the control system inside the passenger terminal.
- Another difficulty is relative to the quantification of the optimization problems considered and the accuracy of the necessary probabilistic data.

The quantitative part of this study has only considered the post screening case, beyond numerical uncertainty of elementary probabilities, the probability of non-detection of a threat has remained very small. The approach developed could have been used to optimize the distribution of the passenger flows with the other two structures considered (pre-screen and mixed-screen) and to compare their respective performances.

It appears that the decision of which control units should be mandatory and which should be assigned to pre or post screening cannot be based only in distributions of probability: if repetitiveness can be admitted for false alarms, threat occurrences must be treated as unique events.

CHAPTER VII

GENERAL CONCLUSION

The operation of the passenger control system at an airport has special characteristics that lead to the formulation of original problems of analysis, modelling and optimization.

Beyond the activities of verification of the transport title of passengers, control measures aiming at the security of the air transport, each time reinforced after new attacks, have been implemented or reinforced at airports during the last decades. The competition between the technology of security at airports and the malicious ingenuity of terrorists has led to the strengthening of the airport security sector, which uses ever more sophisticated control equipment and more and better trained security teams. This represents a considerable extra cost for the air transport sector, ultimately higher costs for passengers, hence the interest in guaranteeing its efficiency while limiting costs.

The main objective of this thesis has been to provide a methodological contribution to the assessment of the expected performances of the resources implemented at airports to ensure the security of passengers.

After having introduced the main concepts and definitions of airport security, an analysis of the passenger control system in airport terminals has been carried out. Then a logical model of the departure control system of the passengers in an airport has been constructed with the aim of allowing to test different scenarios of attack of the system, to analyse the behaviour of the system under different conditions and to evaluate the permeability with respect to different types of attacks. The proposed solution, through the graphical representation of the logical model, seems to be relevant for the analysis of other complex systems in future research and development works.

A probabilistic approach has then been developed to allow the evaluation of the departure passenger flow control systems by considering the possibility of the occurrence of wrong diagnostics at its elementary control stations with eventually a double check. This has led to considering Coloured Petri Nets to represent the dynamics of a control unit. However, since CPN have a deterministic behaviour, probabilities have been introduced at the outcome of their transitions. Then, considering the succession of control tasks induced a dependence, the structure in question has been related to Bayesian Networks, leading to the concept of Bayesian

Coloured Petri Nets (BCPNs). This concept has been illustrated in the case of a single passenger control unit and then extended to general control structures.
Here also, the proposed modelling tool, BCPN, seems to have a potential for application in other areas where a succession of controls takes place with possibility of local failure.

After the establishment of a global evaluation model based on an undifferentiated serial processing of passengers, a typification of threats and passengers has been introduced so that differentiated control along different control channels, perhaps at reduced cost, can be established. The cases without and with pre-filtering, this one allowing a premier classification of passengers, have been considered. This has led to the formulation of linear programming optimization problems for the distribution of the flows of passengers in the different control channels where the objective is to minimize the global probability of non-detection of a threat while limiting false alarm level. The numerical results obtained highlighted the interest of pre-filtering and organizing passengers in separate groups.

Thus, in this thesis, the approach that was initially purely descriptive and normative, has become analytical both in the logical analysis of the operation of control units, as in the modelling of expected performance for the system. The modelling of these performances has been carried out according to two points of view: first a possibilistic point of view through vulnerability analysis and then a probabilistic point of view with some involved dynamics. Finally, assuming the availability of elementary performance probabilities for the control units, an optimization approach has been developed to organize the control flows for a given level of demand.

Much remains to be done in this area, and the development of modelling, analysis, assessment and decision support tools such as those outlined in this thesis seems to need to be complemented by the development of big data analysis techniques in this field, allowing it to get free of the probability paradigm when facing unique events such as unprecedented terrorist attacks. This will ensure on one side the efficiency of the security system and on the other side the optimization of the allocated security resources.

REFERENCES

ICAO, *Safety management manual* (SMM), Doc 9859 AN/474, Third Edition, International Civil Aviation Organization. 2013.

ICAO, *Simplifying passenger travel's ideal process flow* (IPF). International Civil Aviation Organization Working Paper FALP/5-WP/6. Available via http://www.icao.int/icao/en/atb/sgm/fal/falp/Docs/wp06_en.pdf, 2008.

GAO-Government Accountability Office, Aviation security: *systematic planning needed to optimize the deployment of checked baggage screening systems*, GAO-05-365, Washington, D.C., March 2005.

Andreatta, G., Brunetta, L., and Righi, L. (2007) *Evaluating terminal management performances using SLAM: The case of Athens International Airport*, Computers & Operations Research, 34, 1532–1550.

Anderegg, A. 2007. *Risk model for dynamic aviation security*. Technical Presentation Mitre Corporation. Available <http://www.mitre.org/news/events/tech07/3088.pdf>

ARC 2009. *CAST Passenger Terminal Simulation* v. 1.8. Airport Research Centre GMBH. <http://www.airport.Consultants.com/index.php?option=com_content&view=article&id=26&Itemid=51>

Assa, O. and Thomet, M. (2004) *The Virtual Airport*, Bechtel Corporation, Working Paper, ACI Europe Communiqué Airport Business.

Boidin R., *Sûreté aéroportuaire à Nantes-Atlantique*, ENAC, novembre 2003.

Correia, A.R., Wirasinghe, S.C., and de Barros, A.G. (2007) *A global index for level of service evaluation at airport passenger terminals*, Transportation Research Part E: Logistics and Transportation Review, doi: 10.1016/j.tre.2007.05.009.

Frontex 2008. *BIOPASS, study on automated biometric crossing systems for registered passenger at four European airports*. Frontex Technical Report, ISBN 978-92-95033-00-9.

Gupta, A. and R. Davidson. 2007. *Simplifying passenger travel (SPT) program*. In Third symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards, Montreal, October2007.http://www.icao.int/mrtdsymposium/2007/Docs/W4_GuptaArun_DavidsonRobertt.pdf

HMSO 2005. BS7799-3:2005. *Information security management systems - guidelines for information security risk management*, Her Majesty's Stationary Office, UK. Available via <http://17799.standardsdirect.org/bs7799.htm>

ICAO 2008. *Simplifying passenger travel's ideal process flow* (IPF). International Civil Aviation Organization Working Paper FALP/5-WP/6 (28/02/08). Available via <http://www.icao.int/icao/en/atb/sgm/fal/falp/Docs/wp06_en.pdf>

OACI, *Annexe 17 à l'aviation civile internationale* , 7ème édition , Avril 2002.

Parlement Européen , Règlement 2320/2002, *Instauration de règles communes dans le domaine de la sûreté de l'aviation civile*, 16 décembre 2002.

Ray, C. and Claramunt, C. (2003) *A distributed system for the simulation of people flows in an airport terminal*, Knowledge-Based Systems, 16, 191–203.

Roanes-Lozano, E. Laita, L.M., and Roanes-Macías, E. (2004) *An accelerated-time simulation of departing passengers 'flow in airport terminals*, Mathematics and Computers in Simulation, 67, 163–172.

Roca G., *Sûreté aéroportuaire: Application à l'Aéroport Bordeaux-Merignac*, ENAC, 1998.

Russel, A.; Tritsch, C.; Deburghghaeve, M.; Duluc, T.; Bedis, G.; Hupays, M.; Guignier, F.; Vega, N.; Boutillier, P.; Cassat, P.; Le Meillour, S.; La *sûreté Aéroportuaire*; Mastère Management Aéroportuaire, ENAC, Toulouse, mars 2004.

Van Dijk, N.M. and van der Sluis, R. (2006), Check-*in computation and optimization by simulation and IP in combination*, European Journal of Operational Research, 171, 1152–1168.

Van Landeghem, H. and Beuselinck, A. (2002) *Reducing passenger boarding time in airplanes: A simulation based approach*, European Journal of Operational Research, 142(2), 294-308.

Yeh, C.-H. and Kuo, Y.-L. (2003) *Evaluating passenger services of Asia-Pacific international airports*, Transportation Research Part E: Logistics and Transportation Review, 39(1), 35-48.

Zografos, K.G. and Madas, M.A. (2006) *Development and demonstration of an integrated decision support system for airport performance analysis*, Transportation Research Part C: Emerging Technologies, 14(1), 1-17.

Stewart, J. M., *Responsible policy analysis in aviation security with an evaluation of precheck*, Journal of Air Transport Management 48 (2015) 13−22.

Appelt S., Batta R., Lin L., Drury C., *Simulation of passenger check-in at a medium sized airport*. Proceedings of the 2007 Winter Simulation Conference, pp.1252-1260.2007.

Leone, K. and Liu, R., *The key design parameters of checked baggage security screening systems in airports*, Journal of Air Transport Management, 11, 69–78.2005.

De Barros A. and D.D. Tomber, *Quantitative Analysis of Passenger and Baggage Security Screening at Airports*, Journal of Advanced Transportation, Vol. 41, No. 2, pp. 171-193, 2007.

Chawddhry P.K., *Risk modelling and simulation of airport Passenger departures process*. In: M. D. Rossetti, R. R. Hill, et al. (eds.) Conference Proceedings of Proceedings of the Winter Simulation Conference, 2009.

Makkonen J., L. A. Marsh J. Vihonen, A. Järvi, D. W. Armitage, A. Visa, A. J. Peyton, *improving reliability for classification of metallic objects using a WTMD portal*, Measurement Science and Technology Vol. 26, N°10, pp. 1−11, 2015.

Darryl J., A *primer on airport security*.

< http://www.maxwell.syr.edu/campbell/Governance_Symposium/jenkins.pdf >.

Jim, H.K. and Chang, Z.Y. (1998) *An airport passenger terminal simulator: A planning and design tool*, Simulation Practice and Theory, 6, 387-396.

Offerman, H. (2001) *Simulation to Support the Airport Stakeholder Decision-Making Process*, Air & Space Europe, 3(1/2), 60-67.

Kaffa-Jackou R.C., *Contribution à la gestion des operations de la sûreté aéroportuaire: modélisation et optimisation*, Thèse INPT-ENAC, Toulouse, 2011.

Kaltenhäuser, S. (2003) *Tower and airport simulation: flexibility as a premise for successful research*, Simulation Modelling Practice and Theory, 11, 187-196.

Ledru, Y., M. Lemoine, D. Bert, V. Donzeau-Gouge, C. Dubois, R. Laleau, F. Peureux, and S. Vignes. 2005. *Modeling Airport Security: the EDEMOI approach*. Available via <http://vasco.imag.fr/EDEMOI/PresentationsPubliques/ModelingAirportSecurity.pdf>

Lesieur, Jonathan, Nouvelles *contraintes de sûreté dans le transport aérien* , ENAC, 2003.

Madas, M.A. and Zografos, K.G. (2008) *Airport capacity vs. demand: Mismatch or mismanagement?* Transportation Research Part A: Policy and Practice, 42(1), 203-226.

Banks, J. (ed.). (1998), *The Handbook of Simulation*, J. Wiley & Sons, Canada.

Barber, Federico; Salido, Miguel A.; Introducción *a la Programación de Restricciones* ; Revista Iberoamericana de Inteligencia Artificial.< http://www.aepia.org./revista; 2003 >.

BiomCons 2009. *Introduction to biometrics.* The Biometrics Consortium. Available via <http://www.biometrics.org/ introduction.php>

Dash Associates. *XPRESS 12 Reference Manual: XPRESS-MP Optimizer Subroutine Library XOSL*, 2000.

Halmos, P. *Lectures on Boolean Algebras*. van Nostrand, 1963.

R. Givant S. R. ; P. R. Halmos , *Introduction to Boolean algebras.* Springer. pp. 21–22. ISBN 978-0-387-40293-2, 2009.

Escrig, M.T., Pacheco, J., Toledo, F., *El Lenguaje de Programación PROLOG*; 15 octobre 2000.

Larrosa, J. and P. Meseguer, Algoritmos *para la Satisfacción de Restricciones*; Revista Iberoamericana de Inteligencia Artificial. < http://www.aepia.org./revista; 2003 >.

Moore R. E., *Global optimization to prescribed accuracy*. Computers and Mathematics with Applications, vol.21(6/7), pp.25–39, 1991.

Brookshear, J. G., *Theory of computation: formal languages, automata, and complexity*. Redwood City, Calif.: Benjamin/Cummings Pub. Co. 1989.

Sais L., *Problème SAT : Progrès et Défis*, ISBN 2746218860, 2008.

Cook S. A., The Complexity of Theorem-proving Procedures , *Computing Surveys (CSUR)*, ACM, série STOC '71, p. 151–158, 1971.

Cook S., 2006, *The **P** versus **NP** problem*, in J. Carlson, A. Jaffe, & A. Wiles (eds.), *The Millennium Prize Problem*, pp. 88–104, Providence: American Mathematical Society.

Fagin, R., and Halpern, J., 1988, *Belief, Awareness, and Limited Reasoning*, *Artificial Intelligence*, 34(1): 39–76.

Fortnow, L., and Homer, S., 2003, *A short history of computational complexity*, *Bulletin of the EATCS*, 80: 95–133.

Petri, C. A. (1962).Kommunication mit Automaten. Ph.D. thesis. TechnischenHoschule Darmstadt.

Davis, M.; Logemann, G.; Loveland, D. , *A machine program for theorem-proving*, Communications of the ACM. **5** (7): 394–397, 1962.

Buning, H.K.; Karpinski, M., Flogel A., *Resolution for Quantified Boolean Formulas*. Information and Computation. Elsevier. **117** (1): 12–18.1995.

Clarke, E., Biere, A., Raimi, R., Zhu, Y., *Bounded model checking using satisfiability solving*, Formal methods in system design. **19**: 7, 2001.

Vizel, Y.; Weissenbacher, G.; Malik, S., *Boolean Satisfiability Solvers and Their Applications in Model Checking*, Proceedings of the IEEE. **103** (11), 2015.

Lima P.M.V., Morveli-Espinoza M.M., Pereira G.C. and França, *SATyrus: a SAT-based neuro-symbolic architecture for constraint processing*, Proc. of HIS'05: 5th International Conference on Hybrid Intelligent Systems. Los Alamitos, CA, USA: IEEE Computer Society Press, 2005. v. 1. p. 137-142.

Rushdi A. M. A. and W. Ahmad, *finding all solutions of the Boolean satisfiability problem, if any via Boolean equation solving*, JKAU, Eng.Sci., Vol.27, N°.1, pp:19-34, 2016.

Hooker J., *Logic-based methods for optimization: combining optimization and constraint satisfaction*, John Wiley & sons, New York, 2000.

Koller D. and N. Friedman, *Probabilistic Graphical Models: Principles and Techniques*. Cambridge, Massachusetts: The MIT Press, 2009.

Charniak, E., 1991. *Bayesian Networks without Tears*, AI magazine.

Roweis S. and Z. Ghahramani, 1999. *A Unifying Review of Linear Gaussian Models*, Neural Computation 11(2) (1999) pp.305-345

Koller D. and N. Friedman, *Probabilistic graphical models: principles and techniques*, MIT Press 2009

Adnan Darwiche A., *Modeling and reasoning with Bayesian networks*, Cambridge 2009

Jensen F.V., *Bayesian Networks and Decision Graphs*. Springer. 2001.

Edwards D., *Introduction to Graphical Modelling*, 2nd ed. Springer-Verlag. 2000.

Jensen F., *An introduction to Bayesian Networks*. UCL Press. 1996.

Cooper F. G., 1990, *The computational complexity of probabilistic inference using bayesian belief networks*, Artificial Intelligence, Volume 42, Issues 2–3, March 1990, Pages 393-405.

Dagum, P. and Luby, M. (1993) *Approximating Probabilistic Inference in Bayesian Belief Networks Is NP-Hard*. Artificial Intelligence, 60, 141-153.

Dagum, P. and Luby, M. (1997), An optimal approximation algorithm for Bayesian inference, Artificial Intelligence, Volume 93, Issues 1–2, June 1997, Pages 1-27.

Lauritzen S., *Graphical Models*, Oxford. 1996.

Russell S. and P. Norvig. *Artificial Intelligence: A Modern Approach*. Prentice Hall. 1995.

Spirtes P., Glymour C.N., Scheines R. (1993). *Causation, Prediction, and Search* (1st ed.). Springer-Verlag. ISBN 978-0-387-97979-3.

Garey M. R. and D. S. Johnson, *Computers and Intractibility, a Guide to the Theory of NP-Completeness*. W.H. Freeman and Co., San Francisco, 1979.

Bondy J. A. and U.S. R. Murty, *Graph Theory*. Springer.2008.

Murata T., Petri Nets: Properties, Analysis and Applications, Proc.IEEE, vol. 77, no. 4, pp. 541-580, 1989.

Ramchandani, C., 1974, *Analysis of Asynchronous Concurrent Systems by Timed Petri Nets*. PhD thesis.MIT, Cambridge, February 1974.

Sifakis, J., 1977.*Use of petri nets for performance evaluation. Modelling and Performance Evaluation of Computer Systems*. pp 75–93.

Natkin S., *Les Reseaux de Petri Stochastiques et leur Application a 1'Evaluation des Systkmes Informatiques*, Thèse de Docteur Ingenieur, CNAM, Paris, France, 1980.

Zuberek, W. M., Time Petri nets and preliminary performance evaluation, Proc. 7th Annual Symp. Computer Architecture, pp. 88-96, 1980.

Razouk, R.R. and C.V. Phelps, Performance analysis using timed Petri nets, Proc. Int. Conf. Parallel Processing, Aug. 1984.

Molloy M. K., *Discrete time stochastic Petri nets*, IEEE Trans. On Software Engineering, Vol SE-11, pp.417-423, 1985.

Marsan A., G.Balbo, G.Chiola, G.Conte, S.Donatelli, G.Franceschinis , An introduction to generalized stochastic Petri nets, Microelectronics Reliability, Volume 31, Issue 4, Pages 699-725, 1991.

Jensen, K., Coloured *Petri Nets* (2 ed.). Berlin: Heidelberg, 1996.

Pozna A.I., A. Fodor, M. Gerzson and K.M. Hangos, *Colored Petri net model of electrical networks for diagnostic purposes*, IFAC Papers Online 51-2 (2018), pp.260-265.

Yang I.T., C., Huang,S. and Yang, Q. (2005), *Improved petri net models based fault diagnosis approach for power networks*.PowerSystemTechnology,29(21),52–56.

Bird J. (2010), *Electrical circuit theory and technology*, Elsevier,fourth edition.

Calderaro V., Hadjicostis C.N., Piccolo A. and Siano P. (2011), *Failure identification in smart grids based on petri net modeling*. IEEE Transactions on Industrial Electronics,58(10),4613–4623.

Hangos K.and Cameron I. (2001), *Process modelling and model analysis*. Academic Press,London.

Jensen, K. (1996). *Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use*., volumeVolume1.Springer.

Lo, K., Ng,H.,and J. Trecat,(1997).*Power systems fault diagnosis using petri nets*. IEE Proceedings-Generation,Transmission and Distribution,144(3),231–236.

Ning, L. (2002). *Power system modeling using Petri nets*. Ph.D. thesis, Doctoral dissertation. Rensselaer Polytechnic Institute, NewYork.

K. Jensen. *Coloured Petri Nets -- Basic Concepts, Analysis Methods and Practical Use*. Vol. 1: Basic Concepts, 1992, Vol. 2: Analysis Methods, 1994, Vol. 3: Practical Use, 1997. Monographs in Theoretical Computer Science. Springer-Verlag.

K. Jensen. *Colored Petri Nets: A High-level Language for System Design and Analysis*. In G. Rozenberg, editor, Advances in Petri Nets 1990, volume 483 of Lecture Notes in Computer Science. Springer-Verlag, 1991. 3.

K. Jensen. *An Introduction to the Theoretical Aspects of Coloured Petri Nets*. In J.W. de Bakker and W.-P. de Roever, editors, A Decade of Concurrency, Reflections and Perspectives, volume 803 of Lecture Notes in Computer Science. SpringerVerlag, 1994.

Yu Q., L. Cai and X. Tan, *Airport Emergency Rescue Model Establishment and Performance Analysis Using Colored Petri Nets and CPN Tools*, International Journal of Aerospace Engineering, Volume 2018, Article ID 2858375, 8 pages, https://doi.org/10.1155/2018/2858375

Wang J., *Petri nets for dynamic event-driven system modeling*, in Handbook of Dynamic System Modeling, Ed: Paul Fishwick, CRC Press, 2007.

Cook, S., and Nguyen, P., 2010, *Logical foundations of proof complexity*, Cambridge, England: Cambridge University Press.

Artemov, S., and Kuznets, R., 2014, *Logical Omniscience as infeasibility*, *Annals of Pure and Applied Logic*, 165: 6–25.

George B. Dantzig (April 1982), *Reminiscences about the origins of linear programming*. Operations Research Letters. **1** (2): 43–48.

Dantzig G. B. and M. N. Thapa. 1997. *Linear programming 1: Introduction*. Springer-Verlag.

Dantzig G. B. and M. N. Thapa. 2003. *Linear Programming 2: Theory and Extensions*. Springer-Verlag.

Koltai T. And V. Tatay, *A practical approach to sensitivity analysis in linear programming under degeneracy for management decision making*, International Journal of Production Economics, Volume 131, Issue 1, May 2011, Pages 392-398

Jansen B., J.J.de Jong, C.Roos and T.Terlaky, *Sensitivity analysis in linear programming: just be careful*!, European Journal of Operational Research, Volume 101, Issue 1, 16 August 1997, Pages 15-28

Yang, Y., Jia, Y. And Zhong, Y.H., , *Parametric sensitivity analysis of linear programming with fuzzy variables*, Journal of Intelligent & Fuzzy Systems, vol. 33, no. 1, pp. 145-158, 2017

Xu G. and S. Burer, *Robust sensitivity analysis of the optimal value of linear programming*, Journal Optimization Methods and Software, Volume 32, 2017 - Issue 6, Pages 1187-1205

Mora-Camino F. And C.A.N. Cosenza, Fuzzy Dual Numbers, Theory and Applications, Springer, 2018.

ANNEX

Passenger Name Record (PNR)

Regulating the use of passenger name record (PNR) data (Source: European Council)

Passenger name record (PNR) data is personal information provided by passengers and collected and held by air carriers. It includes information such as the name of the passenger, travel dates, itineraries, seats, baggage, contact details and means of payment. The proposal for a directive presented by the Commission aims to regulate the transfer of such PNR data to member states' law enforcement authorities and their processing for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

The European Parliament and the Council agreed on a compromise text in December 2015. On 14 April 2016, the European Parliament adopted its position. The Council then adopted the directive on 21 April 2016. Member states will have two years to bring into force the laws, regulations and administrative provisions necessary to comply with this directive.

Organised crime and terrorist activities often involve international travel. As a response to the abolition of internal border controls under the Schengen Convention, the EU provides for the exchange of personal data between law enforcement authorities. The PNR system aims to complement the already existing tools to cope with cross-border crime. Processing PNR data would allow law enforcement authorities to discover persons unsuspected of crime or terrorism before a specific data analysis would show they might be.

In addition, most member states already use PNR data granted under national law to the police or other authorities. An EU PNR system would also harmonise member states' legal provisions, avoiding legal uncertainty and security gaps, whilst at the same time safeguarding data protection.

The draft directive aims to regulate the transfer of PNR data from the airlines to national authorities, as well as their processing of this data. Under the new directive, airlines will have to provide PNR data for flights entering or departing from the EU. It will also allow, but not oblige, member states to collect PRN data concerning selected intra-EU flights.

The directive establishes that PNR data collected may only be processed for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

In the context of these activities, PNR data can be used in several ways:

- for a pre-arrival or pre-departure assessment of passengers against defined risk criteria, or in order to identify specific persons
- as input in the development of these risk criteria
- for specific investigations or prosecutions

To protect the fundamental rights to protection of personal data, to privacy and to non - discrimination, the directive includes a series of limitations for the transfer, processing and retention of PNR data:

- the directive prohibits the collection and use of sensitive data
- PNR data can only be kept for a period of 5 years, and must be depersonalised after a period of 6 months so the data subject is no longer immediately identifiable

- member states are required to establish a passenger information unit to handle and protect the data; this unit must include a data protection officer
- member states must ensure that passengers are clearly informed about the collection of PNR data and of their rights.
- automated processing of PNR data cannot be the only basis for decisions producing adverse legal effects or seriously affecting a person.
- transfer of PNR data to third countries can only take place in very limited circumstances and on a case-by-case basis.

Passenger Name Record data as far as collected by air carriers:

(1) PNR record locator

(2) Date of reservation/issue of ticket

(3) Date(s) of intended travel

(4) Name(s)

(5) Address and contact information (telephone number, e-mail address)

(6) All forms of payment information, including billing address

(7) Complete travel itinerary for specific PNR

(8) Frequent flyer information

(9) Travel agency/travel agent

(10) Travel status of passenger, including confirmations, check-in status, no show or go show information

(11) Split/divided PNR information

(12) General remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)

(13) Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, Automated Ticket Fare Quote fields

(14) Seat number and other seat information

(15) Code share information

(16) All baggage information

(17) Number and other names of travellers on PNR

(18) Any Advance Passenger Information (API) data collected

(19) All historical changes to the PNR listed in numbers 1 to 18