Lappeenranta University of Technology
School of Industrial Engineering and Management
Degree Program in Computer Science

Kurosh Farsimadan

HUMAN-CENTERED DESIGN APPLIED TO SECURITY SERVICES IN AIRPORTS

Examiners: Prof. Ahmed Seffah
Prof. Ossi Taipale

Supervisors: Prof. Ahmed Seffah

ABSTRACT

Lappeenranta University of Technology
School of Industrial Engineering and Management
Degree Program in Computer Science

Kurosh Farsimadan

Human-Centered Design Applied to Security Services in Airports

Master's Thesis

92 pages, 13 figures, 14 tables, 7 appendix sections

Examiners: Prof. Ahmed Seffah, Prof. Ossi Tapale

Keywords: user experience, design methods, design, design thinking, HCI, HCISec, airport security, design process, IDEO, human-centered design

In airports, security technology and services are designed to guard persons, infrastructures and businesses against a broad range of hazards including crime, fire, accidents, espionage, sabotage, subversion, and malicious terrorist attacks. Security in airport is a big issue nowadays. In the proposed approach, the theory is that security concerns are problems that need to be solved through the usage of human-centered design methods and tools if we want to design and build security technologies that serve the people and their actual needs. These human-centered design concepts, methods, and tools were used in our research to brainstorm and collectively develop solutions and technology to mentioned problems. Design thinking brings to the product and service developers the opportunity to be innovatively active and consequently become more competitive. This paper discusses a five-stage process for innovation by design, called 5on5. It uses various design methods to identifying and solving security problems. We illustrate the applicability and add-values of this process using a case study of creating security services for airports by travelers, with travelers and for travelers.

ACKNOWLEDGEMENTS

I would like to first and foremost, thank my wife (Zahra Rezaeisavadkohi) for being the highest motivation in finishing this report. Her daily support and understanding attitude in writing and finalizing this report were priceless.

I would also like to thank my mentor and Professor Ahmed Seffah first and most importantly for his friendship and for investing time. Also, I want to thank Professor Seffah for having high amount of patience and giving me resources and guidance during my graduate studies, thus helping me to finish this report in Lappeenranta University of Technology. His guidance helped me in understanding my field of study in a very detailed manner, which lead to long lasting realizations and commitments to my future career goals not to mention that his open and innovative way of thinking, experimental attitude and instructions lead me to belief that all science and research will eventually lead to the wanted results despite failures at the first phases and thus aided me in becoming a more self-sufficient researcher and student.

Also, I want to thank every other Professor, which I had taken courses especially Dr. Uolevi Nikula for his clear, sincere, and career oriented advices, general deep care for student wellbeing, motivating speeches, and high input in my studies in terms of allocated resources and time. His courses throughout my studies aided me in becoming more detailed and firm in my work objectives and scopes, which I will never forget and hope to be able to repay somewhere in the future.

Last, but not least, I would like to thank the students of the fall 2015 course CT30A8920 or in other words “Sustainable Innovation by Design: A User Experience Perspective” for participating in the workshops and developing some of the case reports that were mentioned in this report.

Kurosh Farsimadan
Lappeenranta, Finland 30.11.2016

TABLE OF CONTENTS

APPENDICES

LIST OF SYMBOLS AND ABBREVIATIONS

ACS	Access Control System
ADA	American Disabilities Act, for equal access
AIT	Advanced Imaging Technology
AOA	Air Operations Area
AT X-Ray	Advanced Technology X-Ray
AVI	Automatic Vehicle Identification System
AWS	Automated Wait Time
BLS	Bottle Liquid Scanner
BPSS	Boarding Pass Scanning System
CAD	Computer Aided Dispatch
CAT	Credential Authentication Technology
CCTV	Closed-Circuit Television
CMSS	Computerized Maintenance Management Systems
CUPPS	Common Use Passenger Processing System
CUSS	Common Use Self-Service
ETD	Explosives Trace Detection
EU	European Union
FAA	Federal Aviation Administration
ICAO	International Civil Aviation Organization
ICS	Industrial Control System
ID	Identification Document
IT	Information Technology
MUBIDS	Multi-User Baggage Information Display System
MUFIDS	Multi-User Flight Display System
SCADA	Airport Supervisory Control and Data Acquisition
SIDA	Security Identification Display Area
SMGCS	Surface Movement Guidance and Control Systems
TDC	Travel Document Checker
TRB	Transportation Research Board
TSA	Transportation Security Administration

1 INTRODUCTION

1.1 Background

Airports are complex and dynamic transportation hubs and act as gateways by providing and serving air transportation for multinational aircrafts, cargo, land vehicles and most importantly the passengers to and from various domestic and international locations (OTA, 1984). The key elements and factors in designing airports are efficient passenger processing and flow, with maximum security precautions and control mechanism in place to reduce and/or prevent security risks and threats (TSA, 2004; 2006; 2011; 2012). As a consequence, security checkpoints are positioned as the primary separators of the airport boundaries into secured (sterile) and public areas i.e., their purpose is to minimize the malevolent attacks and human-induced threats and dangerous risk situations in high value targets/locations (TSA, 2006; 2011).

In airports, the principal security concerns are the transportation of illegal products and equipment or potential terrorist attacks i.e., security technologies and services are designed and deployed to safeguard high value targets like humans and infrastructures. The security concerns related to high value targets like humans and infrastructure that need to be protected includes employees, travelers, or security officers, tangible objects such aircrafts; and intangible property, such as highly classified national-security data or “proprietary” information (TSA, 2004; 2006; 2011; 2012).

The high value targets such as humans, airport tangible and intangible systems and data, and general infrastructure are protected against a broad range of hazards including smuggled and illegal items like drugs, explosives, dangerous weapons, hijackings, crime, natural disasters like fires and floods, malicious terrorist attacks, espionage, internal attacks or sabotage, malfunctions and unintentional human errors or accidents (TSA, 2011; 2012). The mainstream airport security assessment process has focused in reconfiguration of the airport security mechanisms as a countermeasure to a known and occurred threat situation based on historical analysis of past events, intelligence assessments, physical surveys, and expert evaluations (TSA, 2011; 2012).

Security systems are a critical issue in airports. Advances in security equipment technology have been numerous. Some of the more noteworthy examples include sensor devices that report unauthorized removal of items; personal-identification and access-control systems that directly “read” unique personal characteristics such as voice quality and hand geometry; surveillance devices that can scan premises at night; and devices that permit surveillance at considerable distances, making entry to the premises unnecessary (Purnell et. al., 2012; Murphy et. al., 2015).

Most security services emphasize certain hazards more than others, but the general rule is that the safety of people in the airports including employees, travelers, or security officers; tangible objects such as aircrafts; and intangible property such as highly classified national-security data or “proprietary” information, must be ensured (TSA, 2004; 2006; 2012). Most often security concerns have a negative impact on the usability and is seen as an obstacle of the usability and accessibility of airports. For example, the long waiting line in airport checkpoints is a source of unsatisfied travelers (TSA, 2006). Similarly, access control systems in airports require long, regularly changeable, complex, and unique passwords (not repeatable) that are not supposed to be written down (Murphy et. al., 2015).

Furthermore, even with a strong security mechanism in place, the system can become insecure since the users could find the system too difficult to be used in a correct way and as a consequence leads to security loopholes in the used system and associated systems through inadequate security system configuration in terms of functionality like firewalls, encryption and access controls due to reasons like poor usability design in security aspects for example hard to use interfaces (small input devices/interfaces, combinatory user ID and password authentication) and understandability of the given interface information (asterisk display format for login information) (Whitten, 1999; Stephano et. al., 2011; Theofanos et. al., 2011; Murphy et. al., 2015).

Knowledge-based decision making in designing airport security and services faced with uncertain, changing, and complex problem space is challenging. Various factors in the airport decision making, whether it occurs from the top-down (management) or bottom-up (airport staff, federal authorities) is affected by constraints like time, budget, and understanding of all the interdependencies in airport and airport systems and ambiguous, incomplete, and inconsistent information. To attain knowledge, a more detailed and thorough formal understanding is needed to address the complex interactions and the needed adaptability in airport security systems, by assessing and analyzing the airport systems and subsystems like security technologies, where various uncertainties caused by humans create uncertainties in airport systems. By pursuing a complete understanding of the present state and knowledge in the airport security systems, use cases, and dependencies combined with a precautionary study of the possible future states through design is crucial in demonstrating and detecting negative human experience factors and flaws in the used airport security technologies and thus taking a more proactive approach in tackling security problems without compromising the customer and employee experience.

It is a well-known problem that security and usability are into conflicts when deploying a new security technology in airports. Maintaining an acceptable compromise between these factors is not an easy task. As a consequence, a system that is secure but difficult to use and learn will not be used. A system that supports a high level of usability but is not secure will not be used either. Day-to-day observations show that usability and user experiences have been neglected somehow in the design and engineering loop as a consequence of budgetary or time constraints and organizational politics. The theory given in this paper is that knowing about the travelers, empathizing, defining, and engaging them in the design loop is what will make security technology more secure, yet usable in providing an efficient and enjoyable travel experience for the passengers cost-effectively. If security technology and services are to be successful, they must be carried out in a context of considerable understanding and cooperation of virtually the entire security technology developers, stakeholders and most importantly users.

Therefore, usability and security should be designed in harmony and a tradeoff between these two factors should be explicitly considered such a way that there exists a balance between usability and security for highly efficient workflow. Such approach needs first to avoid the current industry practices suggesting that usability and security can be treated by two different distinct teams that might not work as one multi-disciplinary team. The first team is the Human Factors designers responsible of the user interface (the front side of services) design and engineering. Their role is to ensure that the system supports an acceptable level of usability and a user experiences. The second team is the software and the security engineering developers. Their role is to ensure that the system is secure while engineering the integrity and confidentially of service or technology.

Cross-disciplinary expertise in various areas are necessary so that designing a new service or security technology takes wide range of possible human, technical, and environmental factors into consideration faced with uncertainties and complex-problems. After all, the security program is apt to be only as good as the overall human relations and experiences are part of the design and innovation process of the entire security systems and services.

1.2 Scope and delimitations

In understanding human-computer interaction from the security perspective in the context of airport system and subsystems, the boundary for the research was set on finding technological factors, aspects, and elements in airports, where the human-computer interaction occurs from passenger's point-of-view from arrival until their departure in the case of departing non-domestic flight without any extended flight connections.

The objective of this paper is to investigate design methods as an innovative, creative, and out of the box way of solving security problems and issues, while building new services for security in airports and hence, every other safety-critical environment. Additionally, this paper will cover on how design methods can be used to engage travelers and stakeholders, not only as possible users of services, but also as a source of innovations. Hobday et al. (2011), claims that design and innovation can benefit from each other. Design process seeing as a problem-solving activity, its methods and tools are drivers of innovation and productivity, and new approach to product development based on design thinking. Various researches agree that in order to incorporate design thinking to processes and complex systems, there is a need for cross-disciplinary cooperation in order to design feasible user-experiences that take both the technologies and humans into consideration (Cohen, 2014; Brown, 2009).

1.3 Research methodology and case study

For the purposes of this report, a qualitative and quantitative case study was conducted to examine how novice teams adopt various design methods in solving complex problems and ecosystems in the context of airports and airport security.

Furthermore, in the compilation of this report, the following goals were set such as (a) what airport infrastructure and layout consists of, (b) what technologies are used in airports, (c) summarize the findings related to design thinking and innovative design methods, (d) how design thinking can be used in the context of airport security process and technology improvement, and (e) conduct a workshop case study in analyzing and evaluating the concept. Various databases and sources were used in identifying and gathering the design thinking concepts and airport security related research articles, books, magazines, standards, and good practices. The major databases and sources are shown in the Table. 1.

Table 1. Used databases

Database	Description
IEEE Xplore	Scientific and technical journals, conference proceedings, technical standards, and books
Scopus	Largest abstract and citation database of scientific journals, books, and conference proceedings
ScienceDirect	Authoritative, full-text scientific, technical and health publications
ACM Digital Library	Full-text collection of ACM publications including journals/transactions, magazines, proceedings, newspapers, and books
Government Accountability Office	Independent and nonpartisan agency working for the U.S. congress
Société Internationale de Télécommunications Aéronautiques (SITA)	Multinational IT and telecommunications company for airport transportation industries
Federal Aviation Administration (FAA)	Provides various standards and good practice guidelines for aviation industry
Transportation Security Administration (TSA)	Mission and core of TSA is to ensure freedom, security, and effective transportation systems

Table 1. Used databases - continued

Database	Description
Transportation Research Board	Provides independent, objective analysis and advice to the nation (U.S.) and conducts other activities to solve complex problems and inform public policy decisions

1.4 Structure of the thesis

The thesis paper is segmented into 6 chapters. In chapter 2, the general airport security technologies and infrastructural factors will be researched and discussed in relation to the human concerns, based on the existing knowledge base to acquire insightful information for understanding on how design methods could be utilized in the context case. Reasons for going through the technical and infrastructural factors are, because we need to have secondary research sources in the demonstration of the proposed approach for designing new security and general services for airports and thus several of other similar safety-critical environments. Also, chapter 2 will showcase the several considerable dimensions for the proof of concept in designing security or general services for airports and thus several of similar kind of safety-critical environments, which require cross-disciplinary cooperation.

Also, chapter 2 will showcase the cross-disciplinary nature of airport design concerns and aids in understanding the case-study and the context. In chapter 3, the design related concepts will be researched so that the theoretical applicability of design in the context of airports will be understood. In chapter 4, a proposal for human-centric design will be explained so that there is a clear understanding on how design can help in managing and creating new and old airport security systems and services. Also, various design methods and tools will be showcased in how design can be applied to design a new airport security service.

In chapter 5, a case study will be conducted for a course workshop on how well design was applied in prototyping new airport security services. Finally, in chapter 6, a conclusion and future work will be covered.

2 AIRPORT SYSTEMS AND SECURITY SERVICES

The interaction between people and technology plays an important role in the field of airport security, for example, neither the screening and security officers nor the machines are able to detect prohibited items reliably and efficiently without the other. One weak point in the airport security service could have a wide impact on the whole airport ecosystem. As emphasized by Thomas Reid (1785), *"In every chain of reasoning, the evidence of the last conclusion can be no greater than that of the weakest link of the chain, whatever may be the strength of the rest."*

Various researches agree that in order to incorporate design thinking to processes and complex systems, there is a need for cross-disciplinary cooperation in order to design feasible user-experiences that take both the technologies and humans into consideration (Cohen, 2014; Brown, 2009).

In this chapter, the goal is to investigate what technologies are used in airports in order to achieve the highest performance and security so that relevant factors and elements could be used in the design steps. To do so, an understanding is needed of the airport layout and infrastructure, and general procedures in relation to the used technologies, which means a layered top-down zooming approach.

2.1 Airport infrastructural layout

Airports are large and dynamic transportation hubs, which serve multinational aircrafts, cargo, land vehicles and most importantly the passengers. They can contain public and civil administrative and organizational departments ranging from border control, police, fire department, concessionaire, and factories. The ownership and management of the airports varies according to the national regulations, but they can be mix of private and city, municipality, or government ownership and operated based on organizational and jurisdictional contracts (OTA, 1984).

There are various generally classifiable areas and implemented technologies in every airport despite the fact that every airport is unique in design and architecture based on provincial, national, and international standards. Additionally, each airport differs from one airport to another in their design layout, procedures, and systems (OTA, 1984).

In managing airport complexity and safety, the generally accepted procedure and standard has been to segment the airport infrastructure and layout into different recognizable areas, with their corresponding technologies, based on the international, national or airport vulnerability assessments (OTA, 1984).

The classifiable categories of airport layout according to the current standards (OTA, 1984; TSA, 2011; TRB, 2010) are airside facilities/zone, landside facilities/zone, and the terminal buildings, which interconnect the airside with the landside. Although, there are no clear boundaries or standards, which specifically segment the airport into landside, airside, or terminal building, there are some commonly accepted elements based on principles and standards, which are required for each zone (or passing through them). For example, from the International Civil Aviation Organizations (ICAO) perspective (TSA, 2011), the line of demarcation between landside and airside is drawn at the security checkpoint.

From Transportation Security Administrations (TSA), Federal Aviation Administration's (FAA) and Transportation Research Board's (TRB) point of view and definition, the different airport areas namely airside, landside and terminal mean the following, with their corresponding security requirements (TSA, 2011; TRB, 2010; Lazarick et. al., 2001):

1. Airside (Airside Terminal Facilities): By definition the nonpublic portion where aircraft operations occur separated from other areas of the airport by fencing or other boundaries and includes runways, taxiways, aprons, aircraft parking and staging areas and most facilities which service and maintain aircraft.
2. Landside (Landside Terminal Facilities): Defined as the remainder of the airport property not considered airside outside of the airside fence or other boundaries and includes all public areas.
3. Terminal building complex (Terminal Building Facilities): Defined as the building where the processing of commercial passengers and boarding of the aircraft occurs and is fully accessible to the general public, with no screening or regulatory security

constraints beyond general Closed-Circuit Television (CCTV) or law enforcement surveillance.

Furthermore, the different airport areas have been further categorized according the security requirements as Air Operations Area (AOA), Security Identification Display Area (SIDA), Secured Area, Sterile Area, Exclusive Use Area, and Tenant Security Program (TSP) area (FAA, 2001). Each of the airport zones and areas have their own set of procedures, security technologies, and processes.

2.2 Airport security

Airport systems are rapidly evolving in response to changes based on industry technological advancements, regulations, passenger trends in terms of preferences, services, and airport process changes. Embedded and real-time security systems and technologies mentioned in this report might not be the same technologies that will be used in a coming decade or so (Bellioti, 2008; Elizer et. al., 2012; TRB, 2010; Stocking et. al., 2009).

Reasons for understanding the technologies are related to increasing number of passengers, threats/risks in baggage and passenger screening, common-use and self-service check-in safety and user experience, aging population and people with disabilities or unmet needs, and unknown general threats where there is a need for a complete picture of the technologies, their functions (security measures, weaknesses) related to the services, passenger departure and arrival processes (TSA, 2004; 2006; 2011; 2012).

Security systems in airports are dynamic, complex, interconnected and have dependencies with each other. One security technology in the whole security screening checkpoint could consist of related activities, procedures, regulations, security technologies, operators, airport and national security personnel's. One security technology in the whole security process chain is used in conjunction with other technologies to minimize the security risks/threats layer by layer (Murphy et. al., 2015; TRB, 2008; TRB, 2010, TRB, 2012, TRB, 2015; Purnell et. al., 2012).

To understand the security systems in airports, various standards, guidelines, and articles were used in finding all the security technologies. In compiling the technology listing, there was some level of synthesis required as some terminology and information used to describe technologies in one source might be ambiguous and outdated, but they have detailed information regarding the used procedures and technologies in relation to the airport layout, while another report or source might have incomplete information in general, but up-to-date and detailed information regarding the generally used technologies. These reasons for inconsistencies vary as the sources might be targeted for some specific stakeholder group, technologies are being phased out, or some airports have moved their functions and IT system from their older locations to newer ones as the procedures and regulations have changed over the years (Stocking et. al., 2009). These changes in the airport technologies are result of various ways that the airports are trying to improve the flexibility and adaptability of security mechanisms to meet increasing amounts of threats, passenger flow, experience, revenue, and costs instead of reallocating or constructing newer facilities (TSA, 2011; Bellioti, 2008; TRB, 2008).

Such changes have varied impacts on passenger’s experiences in airports and the threat/risk levels in possible unknown dependency changes in the security mechanisms. Research is needed on the dependencies between various airport terminal landside and airside elements (e.g., roads, curbs, terminals, self-service kiosks, baggage drop) to identify improved ways of understanding new airport and passenger related threats and designing the proper services. For example, the concentration of unscreened check bags in the departures hall, at curbside check-in, or at a remote check-in location as a consequence of a new self-service kiosk may be perceived as a safety threat.

2.3 Security technologies

At the core of every airport which enables it to operate are its IT and embedded industrial control systems (Purnell et. al., 2012; Murphy et. al., 2015), which are not only dependent and connected to each other, but the people also. These complex socio-technical systems have their own design challenges like unpredictable context of use as they are bounded by various factors ranging from procedures and people to technical constraints (Murphy et. al., 2015). As the IT systems can be very complex, used terminology to describe the airport systems differ slightly or completely from one standard and guideline to another, but in general they can be grouped into four abstract layers and depicted in as layered architecture, which could be used to explain the system components and dependencies like the Table 2 (Purnell, 2012).

Table 2. Airport system architecture

Layer	Description
Physical Layer	Cable and Fiber Infrastructure
Networking Layer	LAN, WAN, and Wireless Communications
Application Layer	Airside Systems
	Landside Systems
	Passenger Processing Systems
	Business and Finance Systems
	Safety and Finance Systems
	Facility and Maintenance Systems

Although, the abstracted system architecture in Table 2, does not show all of the dependencies or layers; it will be used as a general frame for further description of the airport systems by decomposing the system layers in a general level. The descriptions for the Table 2 can be explained in the following way (Purnell, 2012).

1. Airside systems: Used to support an airport's aviation needs directly. Concerned with the physical movement and placement of aircraft on the ground and in the air and are usually located on the airfield. Some examples include resource management systems, airfield lighting, noise monitoring systems, surface movement guidance and control systems (SMGCS), and fuel monitoring systems.
2. Landside systems: Located in publicly accessible spaces, usually outside the terminal, and are not directly related to aviation operations but instead assist in passenger drop-off and pick-up at the airport. Some examples of landside systems are audio paging systems, automatic vehicle identification (AVI) systems, and roadway dynamic signage systems.
3. Passenger processing systems: Systems that provide the means for airports to operate a flexible environment in which multiple airlines can share resources for airport ticketing, gates, or baggage. Some examples of passenger processing systems are

common use passenger processing systems (CUPPS), common use self-service (CUSS) systems, and multi-user flight information display systems (MUFIDS).

4. Business/finance systems: Airport IT business/finance systems are used to meet the airport organization's administrative needs and are tailored to fit the airport’s unique business environment. Some examples of business and finance systems are financial management, human resource management, and asset management systems.
5. Safety/security systems: Systems that provide video surveillance, controlled and monitored access to secure areas, and the ability to detect, announce, and control disaster situations at an airport. Some examples of safety and security systems are CCTV, access control systems (ACS), badging systems, police systems, and computer aided dispatch (CAD).
6. Facility/maintenance system: Facility/maintenance systems ensure that mechanical systems work properly so that building environments are pleasant and functional in all conditions. Some examples of facility and maintenance systems are building management systems and computerized maintenance management systems (CMMS).

In finding the detailed information related to the general layered description of the airport systems, various state of the art best and design practices, guidelines and standards were used from sources like FAA (Lazarick et. al., 2001; Leng, 2009), GAO (Kutz et. al., 2007; Berrick, 2003; Berrick, 2004), TSA (TSA, 2004; TSA, 2006; TSA, 2011; TSA, 2012) and TRB (Bellioti, 2008; TRB, 2008; TRB, 2010; TRB, 2012; TRB, 2014; Stocking et. al., 2009; Bellioti, 2010; Purnell, 2012; Murphy et. al., 2015) for finding the technical, security, and process related factors and SITA for the passenger related factors, preferences (SITA, 2016a) and trends (2016b) in airports.

Despite the fact that one airport is different from another in terms of size, complexity, and used technologies; we could interpret and highlight the general systems as described in the reports that are commonly used in various airports. The used guidelines, standards, and good practices that were reviewed and analyzed differed in terms of publisher (private/public), publication year, level of detail and used terminology, but each report described on a general level an aspect or viewpoint, related factors or elements, which were missing from other reports or were outdated i.e., despite the general available information regarding the airport process chains and technology dependencies, in some cases important key information was missing.

In total about, 300 possible airport technical elements and dependencies were found, which were related to the airport supervisory control and data acquisition (SCADA) type industrial control systems (ICS) and information technology (IT) systems which were not explicitly related to security countermeasure technologies. Additionally, about 100 other possible technical elements were found, which were more closely related to cargo, airside, and maintenance areas and their functions. Furthermore, some of the elements could have been decomposed into smaller subsystems, which have their own operational functions and purposes.

For disclosure and security reasons, the dependencies will not be listed, but in total, more than 400 possible airport technical elements, factors, and dependencies were found, with their corresponding area locations, human and security concerns. As a final result, for the purposes of this research, the airport technical elements that were not directly related to security, were omitted from the technical element listing as the boundary for the study was set on the case, which takes a passenger's point of view from arriving into the airport until their departure in a non-connected flight or transfer inside the Schengen area, which is an European Union (EU) agreement for free movement between the countries that signed the Schengen agreement (Bellioti, 2008).

Elements that were directly related to the passenger journeys and security technologies were outlined with their corresponding security and human concerns as shown in Table 3 in a generic format. These 24 elements are situated in the airport parking or landside, terminal, security checkpoint, and airside areas. The listed airport technologies range from biometric systems, CCTV, CUSS, common-use terminal equipment (CUTE) to advanced full-body scanners.

General airport related security threats and risks were identified to belong to environmental, personal, political, technical community, economic, and technical domains that affect the airports critical assets and some of the examples are chemical and biological attacks, improvised explosives devices, hurricanes or natural disasters, cyber-attacks, insider sabotages, and theft of items.

Then there is more passenger or human centered concerns (listed in Table 3) that might or might not have direct dependencies to risks and threats, but passenger experiences that might result in security threats ranging from maps and driving directions to the airport and inside it to real-time area traffic conditions, parking locations, security wait status, and conveyance. For further information regarding the airport security systems and threat types is mentioned in Appendix sections 1, 2, and 3.

Table 3. Technical listing

Technical Elements	Security and Human Concerns
Closed Circuit Television (CCTV)	Inadequate Monitoring of Proximity Events (Murphy et. al., 2015), passenger privacy,
Automated Vehicle Identification (AVI) / License Number Plate (LPR) System	Supply Chain Integrity (Murphy et. al., 2015), Inadequate Monitoring of Proximity Events (Murphy et. al., 2015)
Dynamic Signage / Wayfinding	May impact airlines dedicated use of static signage or the use of airline gate information displays, and thus may confuse the passengers (Bellioti, 2008), may confuse the passengers in wayfinding if they are aging or inexperienced (Bellioti, 2008)
Parking Access and Revenue Control (PARC) / Electronic Parking Toll (entry/exit stations)	Aging Devices (Murphy et. al., 2015), Proper functionality, Parking locations, rates, and status (Elizer et. al., 2012)
Common-Use Passenger Processing Systems (CUPPS)	Lack of Internal Control (Murphy et. al., 2015), Unintended Data Leak / Compromise (Murphy et. al., 2015), Less tenant autonomy (Bellioti, 2008)
Multi-User Baggage Information Display Systems (MUBIDS)	May require advanced scheduling of baggage carrousels (Bellioti, 2008)
Premise Distribution Systems (Wired/Wireless network)	May impact airlines current use of Wireless services
Baggage Screening System	Insider Threat (Murphy et. al., 2015), Aging Devices (Murphy et. al., 2015)
Resource and Gate Management Systems	Lack of Internal Control (Murphy et. al., 2015)
Escalators, Elevators, Moving Walkways	Passenger characteristics might cause concerns in the usability or conveyance (TRB, 2012)

Table 3. Technical listing - continued

Technical Elements	Security and Human Concerns
Common-Use Terminal Equipment (CUTE)	Might not be able to support general/airline wayfinding systems (Bellioti, 2008), less tenant autonomy / airlines lose some control over the use of their dedicated gates and ticket counters (TRB, 2008), significant change in airline operations / In a poorly implemented common use system (Bellioti, 2008), the ability to process passengers quickly through the check-in and bag-drop procedures only moves problems to the gate area, causing delays in boarding (Bellioti, 2008)
Common-Use Self Service (CUSS)	Check-in application for use by passengers on a single (kiosk) device, significant change in airline operations (Bellioti, 2008), usability and understandability, functionality might not be standardized for each self-service kiosk (TRB, 2008), speed and convenience (TRB, 2008),
Multi-User Flight Information Display System (MUFIDS)	Enable passengers to quickly locate flight information or the availability of real-time information pertaining to wait times and gate assignments / Flight status information (TRB, 2008; Elizer et. al., 2012), usability (TRB, 2008)
Biometric System	Unauthorized Physical Access (Murphy et. al., 2015), Insider Threat / Data Breach (Murphy et. al., 2015), Intentional Data Alteration, (Murphy et. al., 2015), Denial of Service (DoS) (Murphy et. al., 2015), privacy, slow down of the passenger movement and processing
Automated Wait Time (AWS)	Data Breach (Murphy et. al., 2015), Host Exploit (Murphy et. al., 2015), Intentional Data Alteration (Murphy et. al., 2015), Privacy (Murphy et. al. 2015), availability of real-time information pertaining to wait times / Security wait status (Bellioti, 2008; Elizer et. al., 2012)
Travel Document Checker (TDC) and Credential Authentication Technology / Boarding Pass Scanning System (CAT/BPSS)	Insider Threat / Data Breach (Murphy et. al., 2015), Intentional Data Alteration (Murphy et. al., 2015), Denial of Service (DoS) (Murphy et. al., 2015)
Explosive Trace Detection (ETD) and Bottle Liquid Scanner (BLS)	Inadequate detection of explosives (Berrick, 2003 - 2004), False positives
Access Gates (ADA, General)	Must provide equal access to services and movement (Bellioti, 2008)
Gate Information Display System (GIDS)	Malicious Code (Murphy et. al., 2015), Aging Devices, Usability and understandability (Gilger, 2006; TRB, 2008b)

Table 3. Technical listing - continued

Technical Elements	Security and Human Concerns
Advanced Technology (AT) X-Ray (components are entrance roller/scanning belt, queuing conveyor, queuing conveyor hood, dome, alarm bag cutout / manual diver roller (MDR), high speed conveyor, exit roller, bag stop, operator cart)	Lack of Internal Control (Murphy et. al., 2015), Inadequate detection of illegal items (Kutz, 2007), Smuggled dangerous items through the security checkpoint (Kutz, 2007), operator performance in detection of illegal items (Kutz, 2007), passenger satisfaction and experience, radiation exposure, passenger privacy
Access Control	Unauthorized Access (Murphy et. al., 2015), Unauthorized Physical Access (Murphy et. al., 2015), Insider Threat (Murphy et. al., 2015), Intentional Data Alteration (Murphy et. al., 2015), airport operator may require use of airport access control on airline controlled gates (Bellioti, 2008)
Walk Through Metal Detector (WTMD)	Inadequate Monitoring of Proximity Events (Murphy et. al., 2015), Inadequate detection of illegal items (Kutz, 2007)
Advanced Imaging Technology (AIT) (components are touch control operator panels, barriers)	Inadequate Monitoring of Proximity Events (Murphy et. al., 2015), Inadequate detection of illegal items (Kutz, 2007), user privacy, radiation exposure through or without human error,
Baggage Tag and Boarding Card printer	Boarding card and baggage tag produced in the case of low quality printers may not be readable by the equipment at the gate, or downstream in the airline system (Bellioti, 2008)

3 HUMAN-CENTERED SYSTEMS DESIGN IN AIRPORTS

Technology and their targeted goals, tasks, and context setting in airport security, in various cases include a middle-man or the human operator. Identifying how humans work in and behave in conjunction with their motives is imperative in finding human elements and factors related to airport security.

In this section, the aim is to understand the various design methods and tools in understanding the humans and their roles in the airport ecosystem and how to analyze the human-computer interactions in airports as part of the larger process by incorporating the design thinking steps so that innovative solutions could be acquired.

To describe humans and the computer interaction, this chapter has been segmented as subchapters, which will cover what innovation is, human-computer interaction, historical analysis of human-computer interaction, human-computer interaction security and design as an innovative approach in solving security problems. Since design and innovations in design could cross various disciplines and concerns, the primary focus is on the human-centered design methods.

3.1 Innovation by design

The term innovation or the act of innovating is by definition a set of processes and functionalities that take place at a particular place, where the end result is a new idea, device, or method (Oxford, 2016).

Although the term innovation is a high-level, generic, and abstract word, we can recognize at least two types of innovations. One is product innovation and another one is process innovation. Product innovations contain the development of new software products for example computers, sensors, microcontrollers, graphical user interfaces, technology that maintains internet, search engines, and office software's. Process innovations involve the development of new or improved methods, patterns, and processes of development that can somehow improve the existing ways of doing things, shorten development time, reduce costs, and/or improve quality (Wieringa, 2014).

Kamrani et. al. (2010) further categorized the innovations in the field computer science into four different segments, which are product innovation, process innovation, position innovation, paradigm innovation.

Deitwiler et. al. (2011) categorized the paths of innovation into a) new (inclusive, visionary/disruptive) b) existing (incremental/adaptive). The basis for the categorization is, because software, product, and other forms of design depend on innovation to meet growing and changing demands. High number of software products are based on incremental improvements in these days as they evolve version after another through new features that are introduced (or existing features that are improved) and can be considered as innovations.

In design based incremental innovation, the template or technical research questions are to improve a problem in a context by redesigning/designing an artifact that satisfies some requirements in order to help stakeholders to achieve their goals. This same approach can be applied to any other software related development (Wieringa, 2014). The process of design contains problem and decision making activity in uncertain and high penalty environment that needs and involves the application of some formal degree of logical problem analysis despite the complexity of the nature of design. As a consequence, design can involve a series of decisions between various design alternative (Hong, 2005).

Design by its core nature forces the designers to accept implicitly or explicitly the transformational nature of it. For example, requirements could be thought of as needs or driving forces and seeds that design transforms into a form that will guide and used to implement an artifact, plan, or process. Design could be thought of a reconstruction of the current situation to achieve some preferred situations. Also, the design process generates new ideas and is a highly creative activity that involves in bringing together various old and new concepts and factors to create something useful that has not previously existed e.g., innovative solutions (Hong, 2005).

In finding out how design can be used as a source of innovation and problem solving activity in the context of airport security, the next chapter will address how design can be used as an approach for solving security problems.

3.2 Design Thinking as an Innovation Approach for Solving Security Problems

Design is universal in scope and has no particular subject matter other than apart from what designers conceive it to be as a consequence of its applicability in any area of human experience (Buchanan, 1992). As a field of science, design research according to Cristopher Frayling (1994), can be categorized as a research into (activity itself), through, and for the art and design. Research into the design activity by itself has been the core focus for various researchers and design has been defined in many ways. Design is a process, a solution, a creative activity, an application of knowledge, invention, etc. (Löwgren & Stolterman, 2004; Walls et al., 1992; Eckroth et al., 2007; Ogot and Okudan-Kremer, 2004; Dym, 2006; Asimov, 1974; Vidosic, 1969, Freeman et. al., 2004). Nowadays authors of many papers related to design try to clarify and understand a design concept in order to understand better the innovation by itself (Bitard, 2005; Hobday et al., 2011; Johansson-Sköldberg et al., 2013; von Stamm, 2004; Liedtka, 2011).

The concept of design is thought as an innovation driver in one or another way was mentioned in works of many authors over the last 40 years (Cohen, 2014). Herbert Simon (1969) in his book "The Sciences of the Artificial", Robert McKim (1973) in his book "Experiences in Visual Thinking", and Rolf Faste (1981) in his book "Seeing it Different Ways: The Role of Perception in Design" were creating and developing a formal methodology for creatively analyzing complexity and complex system and actualizing or imaging concepts and ideas.

Design, according to various researchers (Treffinger et. al., 2006; Kuhn, 1962; Lakatos et. al., 1980; Simon, 1969), is a creative problem solving activity and can be described as more solution and result focused problem solving that is based on analyzing and synthesizing various ideas and concepts through divergent and convergent thinking, whereas problem focused research or natural science in general can be thought of an formal activity that contributes to the existing knowledge base around particular phenomenon and is accepted by the majority of the research community.

Owen (2006a; 2006b), stated that designers invent new patterns and concepts to address facts and possibilities, while scientist are more focused on facts in discovering patterns and insights and categorized them as finders and makers. Owen (2006a; 2006b) further elaborated that the finders (scientists) as people who exercise their creativity through discovery, understanding the nature of the problem, and finding explanations for problems and phenomena's, whereas makers (designers) demonstrate their creativity through synthesis, arrangements, patterns, compositions, and concepts that result in tangible inventions. Furthermore, Lawson (2005) in his empirical study of two different teams consisting of only scientists or architects in solving an architectural design problem, realized that the scientists were problem-focused, while the architects were more creative in their approach and focused on the solution i.e., the architects were solution-focused and their actions were directed on the preferred outcome based on intuition, while scientists adopted a more analytical approach to the problem domain.

On the other hand, Owen (2006a; 2006b) stated that the level of using design and science, must be balanced in than used alone as a source of advice. Also, Owen (2006a; 2006b) stated that the designers work as part of larger multi-disciplinary teams that possibly contains other designers and experts from other fields in the design activities. Likewise, Braha et. al. (1997) stated that design is more or less a collection of various different logically connected knowledge and disciplines and that in the design process, the designers "modify (due to bounded rationality) either the tentative (current) design, or the specifications, based on new information obtained in the current design cycle" to remove discrepancies. These multidisciplinary teams as stated by Harhoff et. al. (2003) have individuals with complementary capabilities that contribute in the design activity and thus come up with creative and innovative solutions i.e., participation in design thinking process does not require every participant to have background in design in order to come up with innovative solutions. This process of multi-disciplinary information and knowledge transfer through various means is on a general level referred to as learning.

According to Buchanan (1992), these design activities are explored by both the professional designers and non-designers and can be segmented in four broad areas e.g., symbolic and visual communication, material objects, activities and organized services, complex systems or environments for living, working, playing, and learning.

Furthermore, various design based models, frameworks, approaches, and processes exist in supporting the design activities and have been defined by different researchers as focusing on ergonomics, socio-technical systems design, cognitive modeling and programmable user models, user-centered and human-centered design, user-experience, and human-computer interaction (Ritter et. al., 2014). These design activities as mentioned by Buchanan (1992), have approached the physical objects or products from semantic, rhetorical, experience, action, sign, visual form, product expressiveness, part of larger systems, cycles and environments point of view. Additionally, in supporting design activities and approaches, a high number of methods and tools have been proposed in fostering innovation. For example, Alves et. al. (2013) identified 164 various design methods related to service design.

However, one of these design based models, namely design thinking, which was extended from human-centered design to take human needs and processes more into consideration, has received large amount of attention of various researchers and industry experts in producing innovative solutions as a result of its applicability into more complex problems (Johansson-Sköldberg et al., 2013; Liedtka, 2011; Owen, 2006a; Owen, 2016b; Tschimmel, 2012; Buchanan, 1992). The popularity of design thinking was based on its different non-linear approach from more methodical and linear design practices, because design of interrelated socio-technical systems in itself was considered as a non-linear process and the problems that designers faced were complex and there does not exist a clear determinacy of the possible path to be taken or solution (Buchanan, 1992).

Furthermore, in order to understand the nature of design thinking in more detail, Owen (2006a; 2006b) identified designers or those who are working on a design thinking domain to have characteristics like conditioned inventiveness, human-centered focus, environment-centered concerns, ability to visualize, tempered optimism, bias for adaptivity, predisposition toward multifunctionality, systemic vision, view of the generalist, ability to use language as a tool, affinity for teamwork, facility for avoiding necessity of choice, self-governing practicality, and the ability to work systematically with qualitative information.

Similarly, Brown (2009) pointed out at IDEO, factors such as where you innovate, how you innovate, and what you innovate as considerable design problems, which need to be taken into consideration on the organizational process and strategy level instead of narrowly focusing on tangible industrial products or objects and graphics in the design process. Hence, Brown (2009) suggested the application of design thinking as a way in "helping people to articulate the latent needs they may not even know they have" in an iterative step approach, which covers various design thinking related activities.

Increasing amount of companies and design practitioners are considering and advocating the application of design thinking practices in their innovation processes as possible driving factors for maintaining competitive advantage in rapidly changing markets, and academic field is trying to study the influence of design processes and methods on product development (Verganti, 2008; Nussbaum, 2004; Gemser and Leenders, 2001; Hertenstein et al., 2001; Lockwood, 2010). For example, in 1980's a design thinking methodology called the Six Sigma was introduced to Motorola, which was based on Japanese total quality management (TQM) practices, as a consequence of rising competition and changing market demands (Tennant, 2001).

Similarly, as stated by von Stamm (2004), "design is an essential component" in innovation development and innovation development brings larger market share and higher profits by supporting the problem solving activities in a wide range of business challenges. Additionally, Design Council (2004), has published a report and stated that 166 companies that were tracked over ten years, outperformed against London's Financial Times Stock Exchange (FTSE) 100 index, by 200%. Furthermore, Design Council (2007) conducted a survey on how design can contribute to business performance and to some extent; about half of the United Kingdom's (UK) businesses believe that design contributes to increased market share and turnover. Thus, for successful innovative activity there is a need of designers' involvement, and design process and methods implementation.

This type of design method and design thinking, takes a very human centered approach, which takes into account what humans need and by converting that need into usable demand.

Brown (2009), further elaborated that design thinking is focused on learning by making instead of thinking what to build, where we have shifted the service users from consumers (passive) to participants (active), which is also called participatory design, where the participants exchange knowledge, brainstorm new solutions and conduct rapid prototyping. The proposed steps to overcome the design problems are mentioned as shown in Table 4, which takes a divergent approach in creation of possible paths and choices and then convergent approach, where the team participants can make choices (Brown, 2009).

Table 4. Design steps

Steps	Description
Empathize	Understand the users from their point of view through field observations (environment interaction) and engagement.
Define	Define the user problem boundary. Compile a meaningful and actionable problem statement.
Ideate	Generate ideas. You ideate in order to transition from identifying problems to creating solutions for your users.
Prototype	Build a tangible/intangible prototype for refined idea representation.
Test	Get feedback from the customers/users, learn, and improve.

As mentioned by Brown (2009), at its core, design thinking process is an iterative process that enhances creativity to solve complex problems that differs from the traditional system design approaches by promoting thinking out of the box type of mindset instead of relying on pure statistics and definition of all problem parameters in forming a solution.

Also, since design thinking is an iterative process, the incremental prototyping and idea refinement allows some level of flexibility in the redefinition of the problem space based on customer or user feedback, which is a highly valued characteristic of design thinking especially in the company and organizational level, as a consequence of budgetary and resource constraints (Brown, 2009). Similarly, as stated by Tschimmel (2012), design thinking assumes that the designer has the ability to be analytical, empathic, rational, emotional, methodical, intuitive, and spontaneous in consideration of three interrelated factors, such as desirability (user's needs and wants), feasibility (availability of technological solutions and resources), and viability (the constraints and opportunities of business).

Thus, we can say that design by innovation (or design for innovation) can help to investigate the complex security problems from 3 different perspectives (Fig. 1), where the focus is not solely on the scientific/technical factors nor on the design. Innovation by design may only occur at the intersection of all three forces.

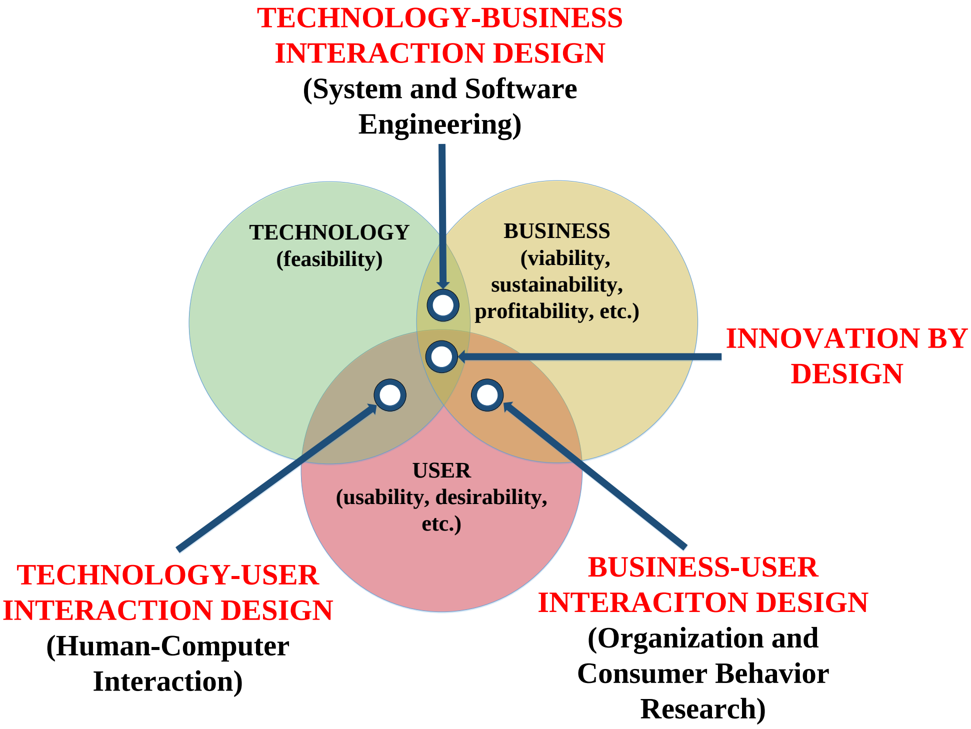

TECHNOLOGY-BUSINESS INTERACTION DESIGN
(System and Software Engineering)
TECHNOLOGY
(feasibility)
BUSINESS
(viability, sustainability, profitability, etc.)
INNOVATION BY DESIGN
USER
(usability, desirability, etc.)
TECHNOLOGY-USER INTERACTION DESIGN
(Human-Computer Interaction)
BUSINESS-USER INTERACITON DESIGN
(Organization and Consumer Behavior Research)

Fig. 1. The three perspectives of innovation by design (Brown, 2009; Tchimmel, 2012)

1. Business, which looks at the viability of the solution from the business-added values and viability. Questions we should answers include how much the problem is affecting the entire business ecosystem and what are the cost-benefits of the solution or service?
2. Technology explores the feasibility of new products or services. What is the most efficient technological platform to develop and deploy the service?
3. People judges/judging the accessibility and usability of the new products or services. Who will be using the system and why?

Various applications of design thinking has been extensively studied and proposed in complex-problems and areas as a possible innovative approach. These complex problems were formally defined as wicked problems by Rittel et. al. (1973) and is seen as a promising and innovative approach in the complex business environments (Simon, 1969; Rittel et. al., 1973, Buchanan, 1992). The ten characteristics of these wicked problems were formalized and identified as the following according to Rittel et. al. (1973):

1. There is no definite formulation of a wicked problem.
2. Wicked problems have no stopping rule.
3. Solutions to wicked problems are not true or false, but good or bad.
4. There is no immediate and ultimate test of a solution to a wicked problem.
5. Every solution to a wicked problem is one-shot operation; because there is no learn by trial and error, every attempt counts significantly.
6. Wicked problems do not have an enumerable set of potential solutions, nor is there a well-described set of permissible operations that may be incorporated into the plan.
7. Every wicked problem is essentially unique.
8. Every wicked problem can be considered to be a symptom of another problem.
9. Existence of a discrepancy representing a wicked problem can be explained in numerous ways. The choice of explanation determines the nature of the problems resolution.
10. The planner has no right to be wrong.

As can be seen from the ten characteristics of the wicked problems, the problems are difficult to solve and information might be incomplete, contradictory or changing. Furthermore, Buchanan (1992) extended the definition of wicked problem as the problem of conceiving and planning something that does not exist yet and suggested the use of design thinking and design methods as an approach in solving wicked problems. Hence, in decision making, there is a need of abductive reasoning in approaching the complex problems by connecting information together rapidly (Crouch et. al., 2012).

Reasons for applying design thinking in the complex problems or environments are various and design thinking has been increasingly used in the academia to solve wicked problems. Some of the reasons could be, because of the characteristics of complex problems that do not fall into the categorization of well-structured and ill-structured problems, as a consequence of scale of the problem, indeterminacy of scope, and not having a definite method in approaching the problem in finding a proper solution (Simon, 1973). From designers point of view, the application of design thinking methodology in the complex problems expands the scope from focusing in only visible and tangible products to the processes and ecosystems around the complex problems, through the incorporation of participatory design, empathy towards the possible stakeholders or users and thus taking responsibility in one's own design choices, cultural sensitivity, ideation and prototyping like use cases, storyboards, journey maps, service blueprints, etc. (Kolko, 2012; Brown, 2009).

Some examples of the application of design thinking in complex-problems are in areas like the maritime (Bateman, 2011), environment (UTS, 2014), and U.S. homeland security (Wyckoff, 2015). Additionally, Taiichi Ohno (1988) stated based on his work experience that many Toyota production line problems were caused by humans and emphasized the importance of company processes. Similarly, Eric Ries (2011), stated that most of the technical and process related problems are caused by humans one way or another and stressed the need to empathize the final end users of the designed products. The examples provided by Ohno (1988) and Ries (2011) possibly hint that there is a need for taking the whole processes around the technologies and particular problems into consideration since the design of technologies by nature take humans, organizational processes, and procedures into consideration instead of focusing on only individual product and system design and security concerns (see Appendix sections 4, 5, and 6 for more information on human-computer interaction design and concerns).

Design is becoming increasingly popular concept in technology-driven software industries. Today, software design is a driver of many innovations, but at the same time in software engineering, design is under-utilized and the understanding of software designer is more related to the term "programmer", even though these are both, clear examples of different, but crossing roles in software development process. Therefore it is necessary to achieve better understanding of professional designers' involvement in software development processes and phases, as well as integration of design methods and tools as facilitators of innovation for software development projects (Gemser et al., 2006).

4 PROPOSALS FOR HUMAN-CENTRIC DESIGN OF SECURITY SERVICES

Understanding the end user's needs is key to achieving design innovation, and the process to get there is design thinking. Employment of a team (researchers and designers), which is prepared for the identification of user requirements based on the fact what users want to achieve as a result of their interaction with a specific artifact, assures that even without asking users what they want, design will be able to satisfy even latent users' needs. This is the core of innovation. Thus, it is possible to create solutions, which can support users in ways they would never even think about by themselves. Due to collected data and its translation to the information for the support of user's decisions, attentional and financial resources are freeing up and can be spent on solving of previously hidden problems. Coordination of disparate systems and modification of processes will serve the satisfaction of user's wants and needs.

Several methods have been proposed for user-centric design and design thinking by various communities. As mentioned by Alves et. al. (2013), about 164 different design methods exists. The detailed description of these methods goes beyond the scope of this paper. In this writing this master's thesis, a research was conducted and a set of methods have been studied that have been reported as powerful and/or have been largely used in industry. In understanding how design can create new innovations, a qualitative case-study was conducted in the research. Table 5 describes the framework of proposed and different design methods and tools that have been used at each stage of a design process.

Table 5. Design Methods and Tools Used During the Course

Step	Tools/methods	Description
Empathize: Identify potential users, their needs and potential use of a service	Personas	A persona typically is a fictional name and a set of characteristics that describe a class of users. We differentiate between primary and secondary personas. The description include background, needs, attributes, behavior, personal profile (Cooper, 1999; Pruitt and Adlin, 2006).
	Touch-points	Touch-points has been used to identify the points of interaction between a service provider (security airport) and customer (Clatworthy, 2011; Brigman, 2013)

Table 5. Design methods and tools used during the Course - continued

Step	Tools/methods	Description
Empathize: Identify potential users, their needs and potential use of a service	User journey Maps	Students have made the customer journey map that describes the journey of a user through the representation of identified touch-points (Clatworthy, 2011; Brigman, 2013)
	Field Observation (User Shadowing)	This technique is used to understand real user's needs and their interaction with the world via the observation of potential users when interacting with the service. (del Real et al., 2006)
	User stories	User stories provided a short description of user's actions and needs for the facilitation of requirements management (Cohn, 2004)
	Task/workflow model	When appropriate, we also considered those techniques for modeling how users accomplish a task (E.g. a traveler crossing a security point, or security personnel checking the bags) (Ko et. al., 2009)
Inspire: Combine all possible ideas that could satisfy potential users' needs and problems that may occur	Affinity Diagramming	Affinity diagramming helped to organize uncertain ideas and thoughts about potential representation of the service (Maguire, 2001)
	Six Thinking Hats	Six Thinking Hats method was used for making group decisions by using different perspectives associated with the colors of the hats (De Bono, 1985): • Blue – thinking about subject, goals, decisions • White - what information is available, what are the facts? (neutral and objective thinking) • Red - intuitive and emotional reaction on a problem • Black – focusing on negative aspects – difficulties, weaknesses and dangers • Yellow – positive and optimistic approach • Green – creativity and thinking "out of a box" E.g. black hat – User will not be able to use the service because of software incompatibility issues
	Mind Mapping	A Mind map was used to visualize the ideas that occurred during usage of a "six thinking hats" method and their connections (E.g. dividing ideas in subcategories - navigation, security, notification, payments, etc.) (Davies, 2010).

Table 5. Design methods and tools used during the Course - continued

Step	Tools/methods	Description
Ideate: Come up with possible solutions for creating a security system and its usage	Brainstorming	Brainstorming served as a method for generating new ideas and creating solutions by collecting the opinions proposed by group members (Osborn, 1963)
	Storytelling	For collecting information about users it was proposed to the students to describe the real stories of user experience process (Parrish, 2006)
	Storyboarding	For the representation of the relationships between user actions and service elements, students had to make a graphical representation of user's actions in a particular order (Truong et al., 2006; Maguire, 2001; Madsen et. al., 1993).
Prototype**:** Build a low-fidelity prototype that illustrates your design concept	Mock-ups	Mockup of the user interface helped students to better illustrate the desired functionality of the service. (Nielsen, 1990; Ehn, et. al., 1991)
	Wireframes	Wireframes allowed students to do experimentation with visualization during the early stage of design (Snyder, 2003; Arnowitz, et al., 2010)
	Wizard of OZ	Wizard of OZ as a computer-based prototyping method, allowed students to create a prototype, in which the user's interaction with a simulated system could be controlled and guided (Maulsby et al., 1993)
Test: Return to other students (potential users), demonstrate your prototype and collect their opinion	Cognitive Walk-through	Before the system's implementation and without real users students had to find usability problems and simulate user's behavior step by step (Blackmon et al., 2002; Wharton et al., 1994; Nielsen, 1994) For that students were asked to answer the following questions (Wharton et al., 1994): - What is the use's goal at this step? - What kind of correct actions are available? - Does user understand that there is a correct action for this task? - Will user get an appropriate feedback to understand that the performed action was correct?
	Heuristic Evaluation	Heuristic evaluation assumes that several experts evaluate the prototype and determine flaws of the system and possible problems for users (Maguire, 2001; Nielsen, 1992)
	User-Oriented Usability Testing	Usability testing allows to evaluate the user's experience with the system by his direct involvement into the testing of the mission-critical tasks (Nielsen, 1994; Barnum et. al., 2001)

The first step of a process – “Empathize” – consists of developing a deep understanding of the users and stakeholders experiences and needs as well as defining the strategies to get them engaged. Analyzes of user’s needs, identification of problems and constructing a point of view on a future product are happening on a second step of the design process called “Define”

The goal of the second stage “Ideate” step is formulate the problem and to generate ideas and possible solutions can be new services that need to be developed, existing services that to be enhanced or even new policy that need to be implemented. On this step it is necessary to take into account mentioned three forces: business, technology and people. Innovations occur exactly at the intersections of the mentioned forces. These means that development of a successful product or service assumes satisfaction of all need and wants of users. And as a result company gets a competitive advantage.

“Prototyping” step assumes building a representation of chosen in previous step solutions that illustrate your design concept. On a “testing” phase the prototypes are evaluated by users, and according to the feedback some of the steps can be repeated in order to improve the solutions. All five steps of the design process are interconnected. This assumes the possibility and even necessity of coming back in the design process and makes improvements if needed.

Some of the mentioned methods described in Table 5, are supported by software tools. The following are the tools we have been using (Fig. 2 portrays the five stage process we proposed):

1. Balsamiq – “wireframing and mock up tool with a high focus on usability” – was used for the prototyping step of a design process
2. Online service “Bubbl.us” suited for brainstorming and mind mapping
3. Trello is a tool for collaboration tool. It was used to organize the design projects into boards, each board represent one security service being developed. Trello tells all the participants (all students enrolled in the course) what's being worked on, who's working on what, and where something is in a process, meaning which design

method is being used and how. It also a shared board to put online the prototypes being developed. Evaluators from outside the class can comment on the prototypes and even participate in the description of security problems and solutions.

4. Prezi, supplement Trello, as way to document the design concept in the format of an interactive design portfolio that includes the description of all the artifacts that were created during the entire innovation process (Fig. 2).

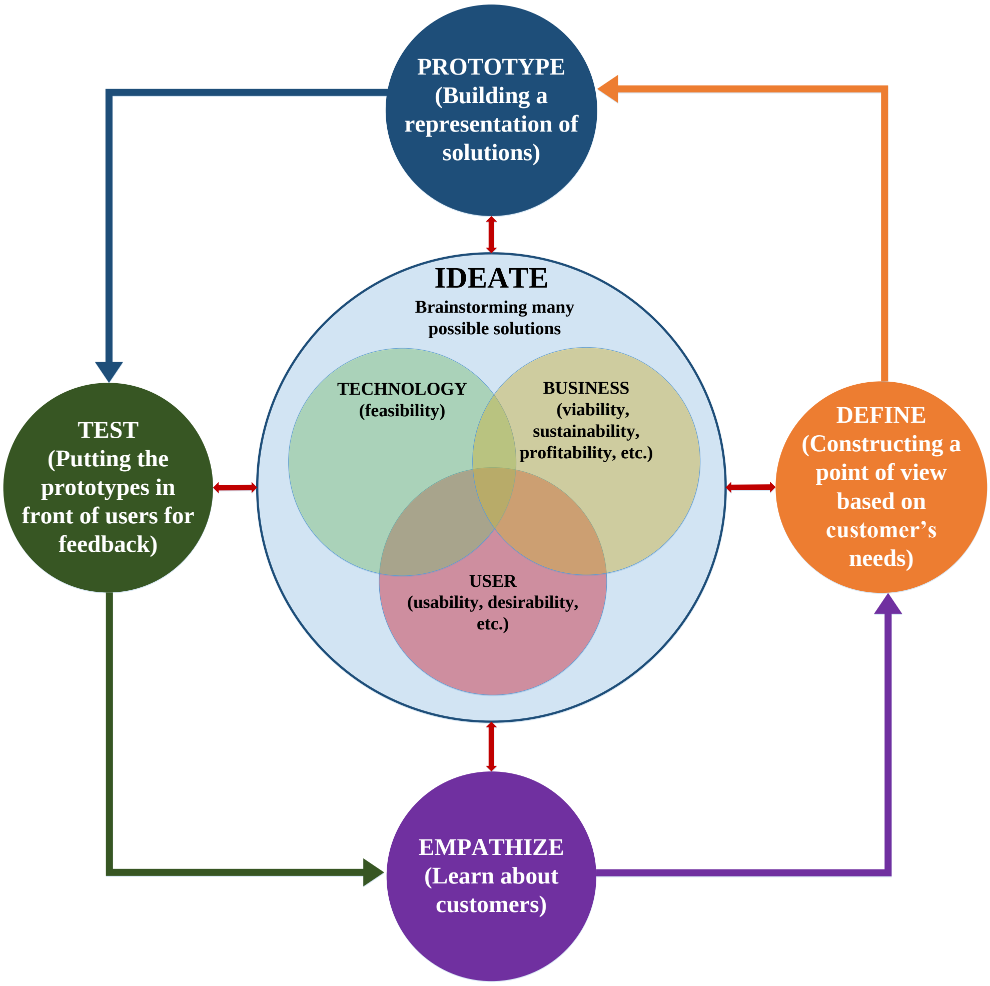

PROTOTYPE
(Building a representation of solutions)
IDEATE
Brainstorming many possible solutions
TECHNOLOGY
(feasibility)
BUSINESS
(viability, sustainability, profitability, etc.)
USER
(usability, desirability, etc.)
TEST
(Putting the prototypes in front of users for feedback)
DEFINE
(Constructing a point of view based on customer's needs)
EMPATHIZE
(Learn about customers)

Fig. 2. The Proposed 5on5 Process for Innovation by Design (Brown, 2009; Tchimmel, 2012)

In this section, various design thinking methods and tools in 5 different steps (empathize, inspire, ideate, prototype, and test) will be covered as possible enhancers of innovations. In order to demonstrate how various design methods could be used in different steps, 9 different methods and tools were selected based on their ability to communicate information between the possible team participants and their visualization techniques for this section. The context and case takes a look on how to design a particular security service like a CCTV for the airport security office. In the case demonstration, for the sake of this paper, a secondary research was conducted based on existing knowledge and sources in finding relevant data as a consequence of limited resources and options in conducting a real ethnographic research in airports for the proposed methods in 5 different steps (Table. 5).

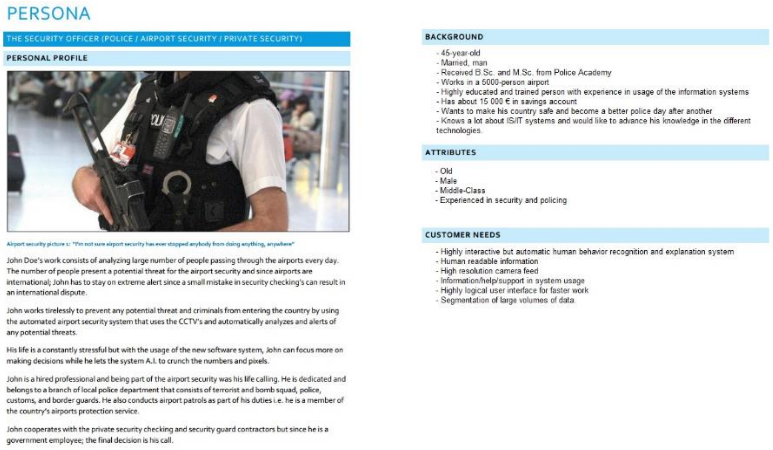
4.1 Persona

A persona typically is a fictional name and a set of characteristics that describe a class of users. We differentiate between primary and secondary personas. The descriptions include background, needs, attributes, behavior, picture, personal profile (Cooper, 1999; Pruitt et. al., 2006; Maguire, 2001).

The possible personas in airports could generally be categorized in two e.g., passengers, general public and airport staff (TSA, 2011). According to SITA (2016a; 2016b), passenger category could be further categorized as airport passenger persona types such as careful planners, hyper-connected, pampered, or open-minded adventurers. These passenger personas could be broken down into smaller and more detailed personas such as tech savvy, service seekers, physically impaired, frequent fliers, or first class fliers.

Similarly, the airport staff can be broken down into belonging to the airports own staff (maintenance, business related function support, and so on), tenants (airline staff), security officer, private security, and federal law enforcement officers (Purnell, 2012; TSA, 2011).

One hypothetical example description of one gathered persona is described in Fig. 3 and Fig. 4, where the persona description is based on a fictional airport security officer, despite the fact that airport security officers cannot be considered as airport customers, but they could be viewed as the possible customers and stakeholders i.e., personas for the CCTV system.



PERSONA

THE SECURITY OFFICER (POLICE / AIRPORT SECURITY / PRIVATE SECURITY)

PERSONAL PROFILE

Airport security picture 1: "I'm not sure airport security has ever stopped anybody from doing anything, anywhere"

John Doe's work consists of analyzing large number of people passing through the airports every day. The number of people present a potential threat for the airport security and since airports are international; John has to stay on extreme alert since a small mistake in security checking's can result in an international dispute.

John works tirelessly to prevent any potential threat and criminals from entering the country by using the automated airport security system that uses the CCTV's and automatically analyzes and alerts of any potential threats.

His life is a constantly stressful but with the usage of the new software system, John can focus more on making decisions while he lets the system A.I. to crunch the numbers and pixels.

John is a hired professional and being part of the airport security was his life calling. He is dedicated and belongs to a branch of local police department that consists of terrorist and bomb squad, police, customs, and border guards. He also conducts airport patrols as part of his duties i.e. he is a member of the country's airports protection service.

John cooperates with the private security checking and security guard contractors but since he is a government employee; the final decision is his call.

BACKGROUND

- 45-year-old
- Married, man
- Received B.Sc. and M.Sc. from Police Academy
- Works in a 5000-person airport
- Highly educated and trained person with experience in usage of the information systems
- Has about 15 000 € in savings account
- Wants to make his country safe and become a better police day after another
- Knows a lot about IS/IT systems and would like to advance his knowledge in the different technologies.

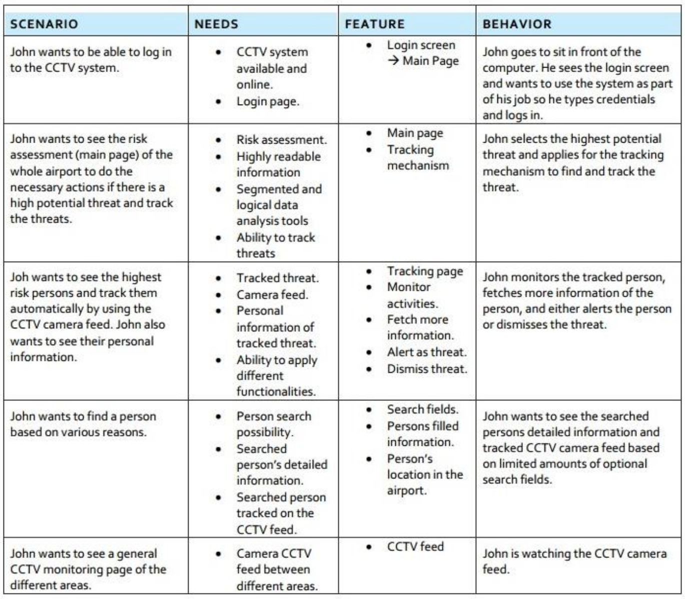
ATTRIBUTES

- Old
- Male
- Middle-Class
- Experienced in security and policing

CUSTOMER NEEDS

- Highly interactive but automatic human behavior recognition and explanation system
- Human readable information
- High resolution camera feed
- Information/help/support in system usage
- Highly logical user interface for faster work
- Segmentation of large volumes of data.

Fig. 3. Persona description



SCENARIO	NEEDS	FEATURE	BEHAVIOR
John wants to be able to log in to the CCTV system.	• CCTV system available and online. • Login page.	• Login screen → Main Page	John goes to sit in front of the computer. He sees the login screen and wants to use the system as part of his job so he types credentials and logs in.
John wants to see the risk assessment (main page) of the whole airport to do the necessary actions if there is a high potential threat and track the threats.	• Risk assessment. • Highly readable information • Segmented and logical data analysis tools • Ability to track threats	• Main page • Tracking mechanism	John selects the highest potential threat and applies for the tracking mechanism to find and track the threat.
Joh wants to see the highest risk persons and track them automatically by using the CCTV camera feed. John also wants to see their personal information.	• Tracked threat. • Camera feed. • Personal information of tracked threat. • Ability to apply different functionalities.	• Tracking page • Monitor activities. • Fetch more information. • Alert as threat. • Dismiss threat.	John monitors the tracked person, fetches more information of the person, and either alerts the person or dismisses the threat.
John wants to find a person based on various reasons.	• Person search possibility. • Searched person's detailed information. • Searched person tracked on the CCTV feed.	• Search fields. • Persons filled information. • Person's location in the airport.	John wants to see the searched persons detailed information and tracked CCTV camera feed based on limited amounts of optional search fields.
John wants to see a general CCTV monitoring page of the different areas.	• Camera CCTV feed between different areas.	• CCTV feed	John is watching the CCTV camera feed.

Fig. 4. Persona scenario description

4.2 Touchpoints and user journey mapping

Touch-points have been used to visually identify the points of interaction between a service provider and customer (Clatworthy, 2011; Brigman, 2013). The idea of using touchpoints is to identify the possible personas (customers or system users) and map the points in the user (persona) journey when they are engaging with the service or context ecosystem. The user journey maps are visualization methods used to describe the user experiences in using a particular services such as airports. Although, touchpoints and journey maps have a lot in common, these two should not be mixed with one another, since touchpoints only define all the points of interaction, while user journey maps visualize the user experience.

In our example, the persona (customer) journey mapping is used as a process model or diagram in illustrating the passenger persona for the CCTV monitoring of the whole passenger process from the moment they arrive in the terminal to the time they board their planes. Reasons for choosing this particular scenario is in understanding the whole ecosystem of the airport rather than focusing on only the security officer persona for which the case system is being designed. As can be seen in the Fig. 5, where a design participant is drawing possible touchpoints in relation to the user journey and drawing then compiled the final customer journey map with the team participants.

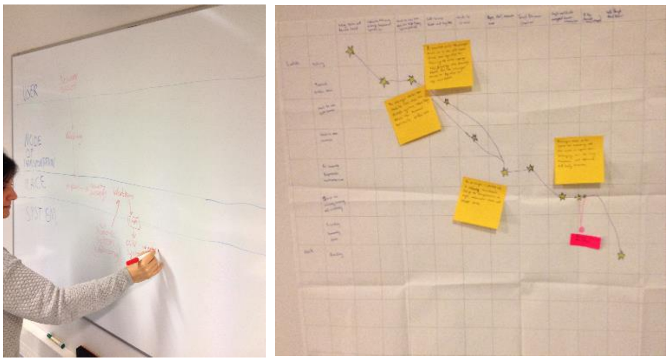


Fig. 5. Customer journey map

4.3 Task and work-flow models

Task-workflow models can be used in various ways to visualize the dependencies between the user and the system in a way that the functional dependencies and constraints will determine the path of possible outcomes (Ko et. al., 2009). In the case example as shown in the Fig. 6, we have the possible user functionalities in relation to the possible system generated choices and paths.

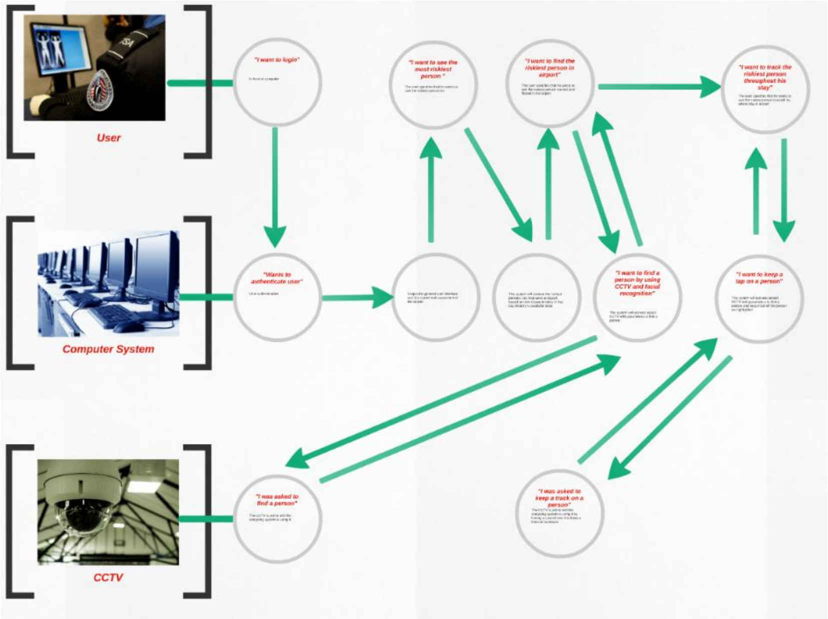

User
Computer System
CCTV
"I want to login"
"I want to see the most riskiest person "
"I want to find the riskiest person in airport"
"I want to track the riskiest person throughout his stay"
"Wants to authenticate user"
"I want to find a person by using CCTV and facial recognition"
"I want to keep a tap on a person"
"I was asked to find a person"
"I was asked to keep a track on a person"

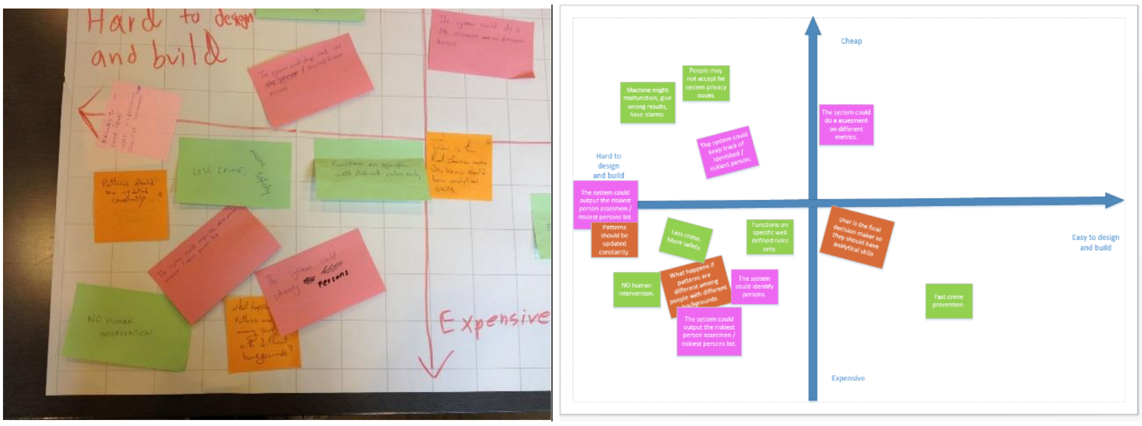
Fig. 6. Work-flow model

4.4 User stories

User stories are a way in describing possible functional points in the used system and aid in the understanding and prioritization of story dependencies (Cohn, 2004). For example, if we would be hypothetically designing a CCTV system for the airport security staff (only one persona), the user story would be like the following *"As a security system manager user, I can monitor different sections of the airport, see threats and their corresponding metrics, identify threats, track threats, and report threats"*.

4.5 Affinity diagramming

Affinity diagrams are used in the organization of new system structure by the designers and/or users (Maguire, 2001). How affinity diagramming occurs is that the potential designers and/or users write down the potential screens or functions on sticky notes and then organize the notes based on their concepts as shown in the Fig. 7, where the hypothetical problem domain or case is based on the improvement of the airport CCTV system.


Hard to design and build
Expensive
Less crime
No human intervention
Cheap
Hard to design and build
Easy to design and build
Expensive
Machine might malfunction, give wrong results, have alarms.
People may not accept he system privacy issues
The system could do a assesment on different metrics.
The system could keep track of identified / riskiest person.
The system could output the riskiest person assesmen / riskiest persons list.
Patterns should be updated constantly.
Less crime. More safety.
Functions on specific well defined rules only.
User is the final decision maker so they should have analytical skills
NO human intervention.
What happens if patterns are different among people with different backgrounds.
The system could identify persons.
The system could output the riskiest person assesmen / riskiest persons list.
Fast crime prevention.

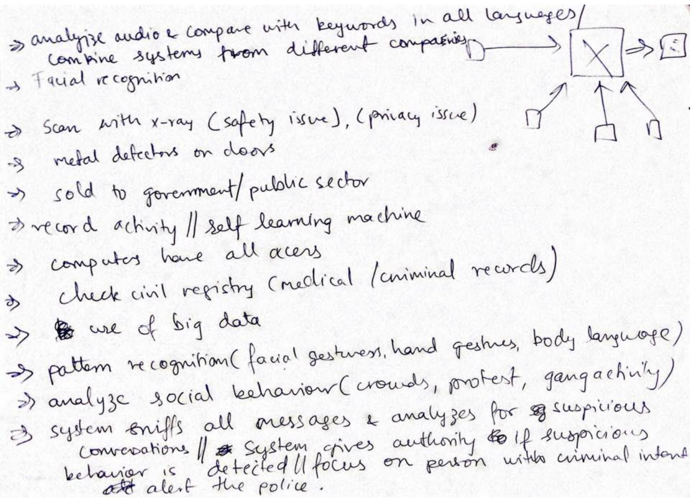
(a) (b)

Fig. 7. Affinity diagramming on paper (a) and later refined in digital form (b)

4.6 Brainstorming

According to Osborn (1963), brainstorming serves as a method for generating new ideas and creating solutions by collecting the opinions proposed by group members. These brainstorming sessions produce lists of various ideas that the participants contributed and can be later used in other problem solving or design processes (Osborn, 1963).

The basic rules of brainstorming is to defer from judgement, encourage wild ideas, build on the ideas of others, staying focused on the topic, having only one conversation at a time, being visual and have large amounts of ideas in terms of quantity. These ideas will be written on Post-it notes, large piece of paper or whiteboard (Osborn, 1963; Brown, 2009). An example of one our case study group's refined brainstorming list is show in Fig. 8.



⇒ analyze audio & compare with keywords in all languages/
combine systems from different companies
→ Facial recognition

⇒ Scan with x-ray (safety issue), (privacy issue)
⇒ metal detectors on doors
⇒ sold to government/ public sector
⇒ record activity // self learning machine
⇒ computers have all acces
⇒ check civil registry (medical /criminal records)
⇒ use of big data
⇒ pattern recognition(facial gestures, hand gestures, body language)
⇒ analyze social behavior(crowds, protest, gang activity)
⇒ system sniffs all messages & analyzes for suspicious conversations // System gives authority if suspicious behavior is detected // focus on person with criminal intent alert the police.

Fig. 8. Brainstorming list

The case study groups brainstorming ideation result is like the following. Let’s for example assume that the increasing amount of passenger flow through the airports in relation to the rising tension and crime needs to be monitored. The case takes a look on how to design a particular security service like a CCTV for the airport security officer.

The case example system is not the CCTV system itself, but an extension that will be integrated to the CCTV monitors. It scans the audio/video streams coming from the CCTVs and other possible devices and displays results on system user interface. The system interface also allows the user to execute commands to the ground security services. The main idea of the system is to be able to conduct pattern recognition and learn throughout its life cycle by storing and analyzing the collected data.

The system will be able to automatically recognize any suspicious behavior, alert of any high risk situations, track and identify anyone in the airport i.e. everything 'abnormal' is highlighted. The system learns normal patterns by just collecting data over one month or year. Who comes in and how they interact and leave the place. The system has predefined alarm rules for undesirable behavior. For example, if someone walks in a restricted ‘No Loitering’ area, the system will immediately alarm the security.

Measures how long a person will usually stay or walk. Measures and determines what is normal and what is not (behavior, etc.). The surveillance system is a combination of the following elements such as presently available CCTV cameras, a central server which collects and processes data real-time, system which enables authenticated users to view the analyzed data, and a control panel in the system to enable users to take necessary actions.

4.7 Mind map

The reasons for using mind mapping technique in understanding the airport security technologies as defined by Davies (2010) is the possibility of free-form visualization networked or connected concerns and concepts. In general terms, the aim of mind mapping is to find creative associations between ideas as shown in Fig. 9, where possible security technologies in between the passenger arrival to the airport and departure.

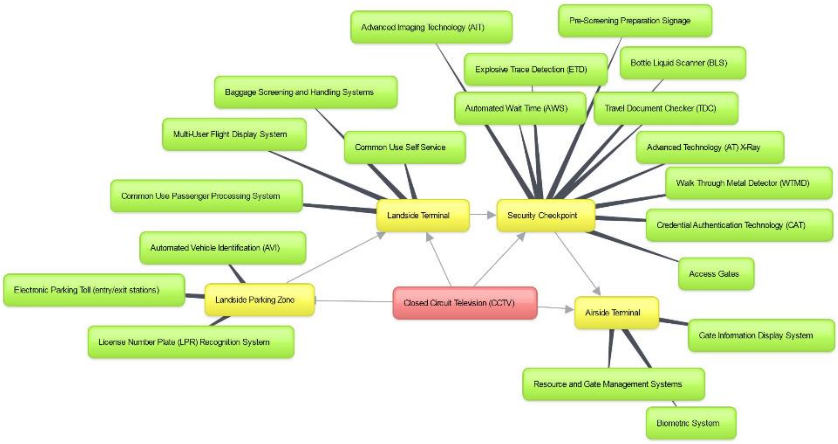

Advanced Imaging Technology (AIT)
Pre-Screening Preparation Signage
Explosive Trace Detection (ETD)
Bottle Liquid Scanner (BLS)
Baggage Screening and Handling Systems
Automated Wait Time (AWS)
Travel Document Checker (TDC)
Multi-User Flight Display System
Common Use Self Service
Advanced Technology (AT) X-Ray
Walk Through Metal Detector (WTMD)
Common Use Passenger Processing System
Landside Terminal
Security Checkpoint
Credential Authentication Technology (CAT)
Automated Vehicle Identification (AVI)
Access Gates
Electronic Parking Toll (entry/exit stations)
Landside Parking Zone
Closed Circuit Television (CCTV)
Airside Terminal
Gate Information Display System
License Number Plate (LPR) Recognition System
Resource and Gate Management Systems
Biometric System

Fig. 9. Mind map chart

4.8 Storytelling

According to Parrish (2006) storytelling is used for collecting information about users and to describe the real stories of user experience process. Furthermore, storytelling is used to gain empathy from customers or users point of view by creating vivid, descriptive, and logical stories for acquiring insight into the user’s experiences and humans in general instead of only focusing on the processes (Parrish, 2006).

The storytelling scenario was acquired for the passenger is based on authors own experience and standards about used technologies in airports (FAA, 2001-2009; Kutz et. al., 2007; Berrick, 2003; Berrick, 2004; TSA, 2004; TSA, 2006; TSA, 2011; TSA, 2012; Elizer et. al., 2012; Stocking et. al., 2009; Murphy et. al. 2015), but it follows a linear scenario and thus might not reflect a real dialog and passenger scenarios, which might reveal possible discoveries. The storytelling scenario in this hypothetical case is based on the CCTV example given in the previous design method descriptions. A possible note is that the storytelling scenario in this case in not based on the main persona, but the passengers that the CCTV is supposed to monitor.

A possible story telling scenario could be like the following. The passenger journey begins by *“arriving to or near the airports international departure flight terminal either by bus, car, taxi, or train. If the passenger arrives by car and wants a long-term parking service, the journey continues to this phases parking zone, where the first technical factor is the* *automated entry station. The passenger will get a parking coupon at the station/barrier, before entering into the parking space. If the CCTV cameras are installed in and around the parking zone, the car might be tracked with a license number plate recognition (LPR) or Automated Vehicle Identification (AVI) systems. When the car is parked in the parking zone, the passenger will move into the terminal building for international departing flights…"* The rest of the story telling is exemplified in Appendix section 7.

4.9 Mockups and wireframes

Wireframing and mock-ups are used in the visualization of the prototype (Arnowitz, 2010). Furthermore, prototyping is an experimentation activity and the prototype as the finished model of the product to be manufactured (Brown, 2009). The goal of prototyping process is based on acquiring feedback from potential stakeholders or users of some particular service, product, or system. In this papers particular case, the prototype is a possible software tool for the airport security as shown in the Fig. 10.

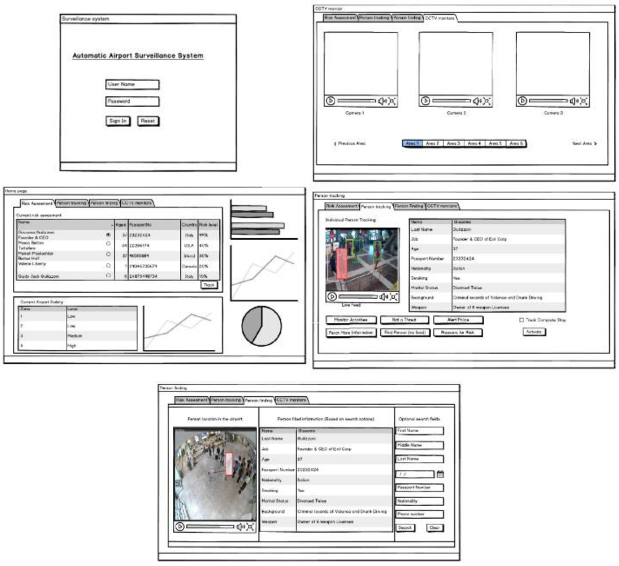


Fig. 10. Mockups and wireframes

In the Fig. 10, we have a simple mockups and wireframes, which were built to showcase a possible system information for the airport security officer, based on previously acquired empathize, inspire, and ideate steps.

5 CASE STUDY

5.1 Case-Study: Airport Security Systems and Services

Security in airports, especially International ones, have been largely discussed and many technology exit and are used in modern Airports today. However, it is a well-known fact that the humans and human experiences are the weakest concern in security.

In fact, all passengers and crew are required to go through security screening of some form prior to boarding commercial aircraft. These systems are a response to decades of hijacking and terrorists attempts worldwide. They attempt to limit what passengers can bring into an airplane cabin, in order to ensure the safety of the passengers and crew. They also try to increase awareness regarding objects left in common areas. Particular regulations vary internationally, but generally airport security is intended to keep people and airports safe when prospective threats exist. The experience of going through this screening process varies widely depending on many conditions. Regardless of the state of many of these conditions - the nature of security guards, the accuracy of the technologies involved at any given time, how busy the airport is - generally, passengers are stressed to an extent, because there are inflexible deadlines that customers must meet.

These rushing situations create non-satisfied travelers and can lead to some security breaches. The link between user experience and security technologies or technologies in general has been closely studied academically and is known as HCISec, which is also referred to as HCI-SEC or Human Computer Interaction Security (Appendix sections 4, 5, and 6 explain the HCI and HCISec concepts in more detail).

Hence, security professionals should be fully aware of the fact that while they need to give utmost precedence to system security, they cannot overlook user experience. They must ascertain that only authorized users have access to the system and also make sure that users are safe in the knowledge that their information is safe online and they can continue to safely use it. As a consequence, there is a need for more innovative solutions and approaches in designing the airport processes and ecosystem in conjunction with the SCADA ICS’s, passenger processing systems, and security systems.

In researching into how design thinking can be utilized to improve the airport security and user experience, a case study was formed for a course, which lasted for 2 months. The course located in Lappeenranta University of Technology. Table 6 shows the different services, which were developed by 5 group of students, in addressing the security and user experience factors. All the study group participants had a background in computer science and were either PhD or masters students with diverse range of skills and specializations.

The preliminary rules for the case study group were to follow the weekly instructions for design steps and methods e.g., empathize (persona, touch-points, user journey maps, field observation, user stories), inspire (affinity diagramming, six thinking hats, affinity mapping), prototype (mock-ups, wireframes, prototypes, Wizard of OZ), and test (cognitive walk-through, heuristic evaluation, user-oriented usability testing).

Table 6. Service descriptions and covered problems

Service	Security problems addressed	User experience targeted
Surveillance system The system acts as a security device and suitable for locations with CCTV cameras installed. The system scans the audio/video streams coming from the CCTVs and displays results on a system's user interface. The system interface also allows the user to execute commands to the ground security services. The main idea of the system is to be able to do a pattern recognition and learn throughout its life cycle by storing and analyzing the collected data.	Recognition of any suspicious behavior, alerts of high risk situations, tracking and identifying of anyone in the airport (i.e. everything 'abnormal' is highlighted)	Convenient travelling without unnecessary personal extra security checks
Travel Smart A mobile application is able to guide a user from his current location to the airport and then to the boarding on a plane, including necessary managements needed for boarding and travelling	Specific security issues of different airports in different countries (e.g. cultural differences, border rules)	Convenient trip, avoiding any unexpected incidents (e.g. traffic jams, lack of necessary documentation)
Airapp The system guides a traveler to various airports and their immigration and security checkpoints till the traveler reaches his final destination.	Small security issues and overcrowding of immigration and security checkpoints	Convenient trip avoiding immigration problems

Table 6. Service descriptions and covered problems - continued

Service	**Security problems addressed**	**User experience targeted**
CoAIR (Citizen Observation Airport). The application aim to empower citizens to report and classify issues at airports in exchange for prizes available at the shops of the airports. The idea is to use the power of the crowd to monitor possible security issues at airports.	Monitoring of mostly small incidents	Pleasant gifts for accomplishing easy, but useful task
Uber for Airport The basic service that UIA offers is taxi-like pick up service that customers can order inside the airports and it delivers the customer from one point to another point inside the airport. The advantage of using UIA is that the delivery service consists also all the security checks and baggage check-ins. UIA provides additional services, like tailored assistance services for elderly people and children.	Security issues connected to people travelling with children	Extremely easy and relaxing movement within the airport for elderly people and families with children

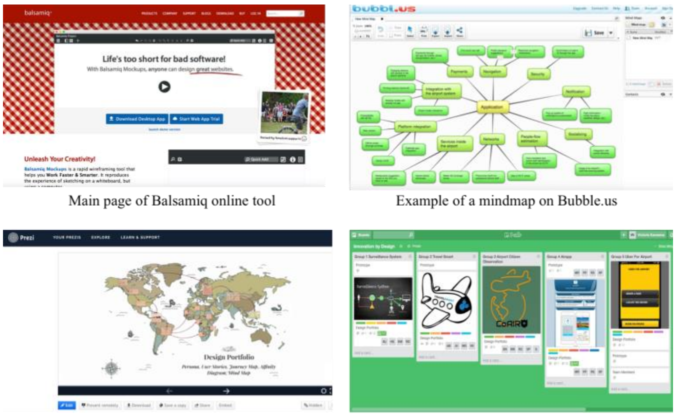
5.2 Lessons Learned From the Case Study

In total, 32 students participated in the project and they were organized in 5 groups. Each group comprised 5-7 students. Ideally, group should be six people in a group, as each person was playing one specific role in making decisions using six thinking hats method. The project has been running in 12 weeks, each week we organized a workshop of 2 hours. Students were asked to collect and report information about airport security either via the Internet, ether social media or from friends that have been travelling across the airports. Also, all of the case study team participants have been traveling through the Helsinki-Vantaa Airport on various occasions and as a consequence, have some form of image and understanding of their airport experience.

In the beginning of the case study and course workshops, the students had high eagerness in applying design thinking and design methods for their proposed problems or services, but on some level, there was general vagueness of the wanted end results, and hazy or inconsistent terminology used for design tools and methods in the available academic articles and books, industry practitioner guides and so on. As a consequence, a clear cut breakdown of methods and tools were given for each design step, where the constraining factors were that the workshop teams, were not allowed to proceed on the next design steps and design methods without proper guidance or until all of the teams had achieved the same level of preparedness. This approach was highly successful in terms of the proper flow of the given task completion in teams.

For some of the tasks (e.g. for mind mapping, brainstorming) students from different groups were mixed and had to share their opinion on proposed by other group members' ideas and solutions, and their interconnections. In general, all of the team participants were productive and all of the proposed design method artifacts were produced.

To facilitate and support more efficiently in the entire process, we used Trello. Fig. 11 portrays the user interface of the online platform Trello. In Trello it was possible to manage the vide variety of tasks including the collection of the design portfolios of all 5 groups, letting all members of a particular group be involved in managing of their group's portfolio, letting members of other groups to comment and evaluate colleagues' work, and make the evaluation of work easier for the professor.



Main page of Balsamiq online tool

Example of a mindmap on Bubble.us

Presentation on Prezi.com

Trello Interface

Fig. 11. Examples of used online software tools

After completing the five steps of design process, we conducted a survey. In one of the questions students were asked to evaluate their experience of methods implementation. Thus, the results of a question about the different design methods usefulness for each stage of a design process are shown in Fig. 12.

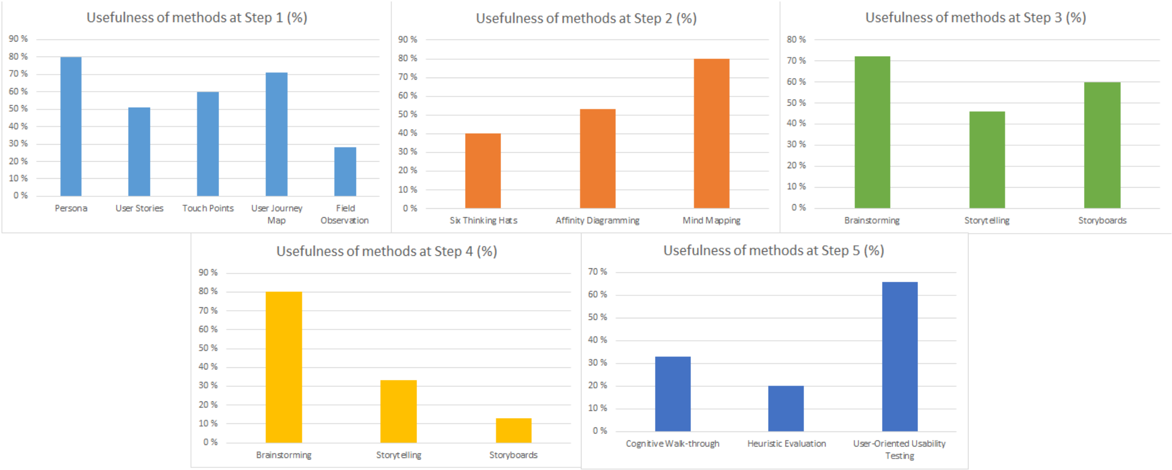


Fig. 12. Students’ perception of methods’ ease of use and usefulness

Fig. 12 displays the following pattern:

- Step 1 – “Persona” and “User Journey Maps” seemed to the most suitable and important for the decision-making process;
- Step 2 – “Mind Mapping” was the easiest method for combining different ideas by students’ opinion;
- Step 3 – “Brainstorming” and “Storyboards” turned out to be most useful for coming up with possible solutions for creating a security system;
- Step 4 – “Mock-up” was evaluated as the most suitable and easiest method for prototyping;
- Step 5 – “User-Oriented Usability Testing” was leading amongst other methods for the testing step of a design process.

The students were asked about the different tools that have been using. Most of the students had the opinion that Prezi and Trello were suitable tools for presenting and managing their design portfolio as well as to collecting more feedback from other groups about their design concept. Opinions on prototyping phase and Balsamic usage were controversial. Half of the students decided that it is a good tool, and another half proposed other resources, which could be used on this step of design process. Those are “proto.io”, “marvelapp”, and “InVision”.

6 CONCLUSION AND FUTURE WORK

In this research, the theory was that security technology have to be designed with human mindset, meaning the active involvement of all stakeholders is imperative. Users and other stakeholders can or should be designers and innovators, meaning they can co-create or contribute significantly to the development and validation of new security services and technologies.

In the proposed approach, the argument was that security concerns are problems that need to be solved through the usage of human-centered design methods and tools if we want to design and build security technologies that serve the people and their actual needs.

These human-centered design concepts, methods, and tools were used in our research to brainstorm and collectively develop solutions and technology to mentioned problems. Nowadays the idea of innovations facilitated by design process and design methods becomes more and more solid. Design thinking brings to the product and service developers the opportunity to be innovatively active and consequently become more competitive.

In the proposed five-stage process for innovation by design, called 5on5, various design methods to identifying and solving security problems was exemplified. The paper illustrated the applicability and add-values of this process using a case study of creating security services for airports by travelers, with travelers and for travelers. The conducted case-study showed how design methods and innovation by design process can support new ideas development. User-experience driven design for innovation assumes users' explicit engagement in the design process for a good reason, as the outcome of this engagement brings a lot of opportunities and benefits. By prioritizing the passengers as one of the most important elements in the airport security design, we can convert the needs into demand.

We have to understand that the airport security is initially based on the fact that there exists some threats that endanger the passenger's journey process. Hence, the whole security system should be designed in a way to show passengers that they do need such a system to have a safe journey. The airport security system should be thought of as a service system that provides services to the passengers. The main challenge in incorporating design thinking into the airport security context is how to turn the system into a demand by the passengers, without compromising security. In order to reach such a goal, the system should be designed in way that positions the humans as the first priority. However, in ordinary airport security systems, each passenger is considered as a potential terrorist until proven to be the opposite. This random classification of passengers makes it very hard to attract the passengers and show them that this system is exactly made for the passengers themselves.

Design methods provide to the users the opportunity to be involved in the design process quite easily. This involvement requires little time for educating people for being able to implement some design methods and tools for innovation creation or just to be a useful resource for product evaluation and testing.

For the developers and other stakeholders', innovation by design process and design methods and tools usage ensures more productive and creative work outcome. Design thinking is a user-centric approach that more and more becomes a solution for solving engineering and business problems. It is an important factor for success that provides an opportunity to set the right goals and to use the right methods for their achievement.

Designing a new system should be done in a way to assure the acceptance of whoever was supposed to use this system in the future. The ideas should be held beyond the individuals, which mean that all stakeholder groups should be taken into consideration all together when designing a certain system through observation.

If we are talking about the airport security system and about the human factors in particular, we should be thinking about all the contributors to this system through empathizing and learning from them, since the end goal is the improvement of user-experience, without compromising security. Fast prototyping and experimentation techniques, methods and tools in design and design thinking can aid us in understanding, evaluating and implementing the end user product.

Design thinking in an organizational context, promotes a collaborative design process between the various experts in achieving ideation so that services would not be designed and implemented as siloed products, but as part of the whole portfolio of services. Furthermore, design thinking can aid in understanding the business service users in a more insightful way. By synthesizing the known information and having an end goal (what is it that the organization wants to learn), we can use design methods as tools in acquiring insight and discovery. On the other hand, design thinking also promotes discovery without knowing the wanted end goal by aiding in understanding some particular phenomena or area of concern.

Based on the literature study, we can acknowledge the fact that passenger journeys in the airports are never under any particular federal or organizations complete control. The various organizations could vary from software to industrial control systems providers.

Thus, design in a complex environment like in airports needs a cross-organizational and stakeholder effort and cooperation so that various points of view, expertise and inputs are taken into consideration in confirming and disconfirming the facts and design choices.

By nature, design thinking forces the multi-disciplinary teams to take the whole problem domain or ecosystem into consideration and creatively come up with new innovative solutions not only in the form of individual products, but the whole business model, which also has bigger impact on the passengers.

Design thinking, expands the context and focus from a single activity set to a larger activity set. In the context of the airport security, it's not just about boarding the plane, but the whole experience of passengers buying their ticket all the way through terminal, boarding, claiming their baggage, and leaving the airports.

By taking the larger context (business, technology, and people) into consideration, innovation by design will occur both on the organizational process and product level, which brings customer value and new market opportunities. In our case study, we found that novice teams, were able to quickly adopt various design methods and tools in fostering new and innovative ideas through collaboration.

Despite the fact that all of the study participants had background in computer science, the students were able to split their roles, take a divergent approach in gathering large amounts of academic literature and industry standards, which were cross-disciplinary in nature, generate ideas and take a convergent approach in synthesizing information and prototyping their ideas in 12 weeks. In our case study, we noticed that there was a correlation between the student teams, independently generated knowledge and information in the design ideation step with the industry practitioner’s generated information available online. The various teams were able to quickly find knowledge, which was accumulated and refined in an iterative way, which resulted in prototypes at the end of each iteration.

Based on the current findings, the acknowledgeable fact is that design and design thinking can aid in the human-centered design for user experience, without compromising the security layers, but it cannot be used alone in fully designing the airport security system. Design methods should be used with other methodologies, tools, and technologies so that more comprehensive, complete, and safer solutions could be acquired as design is merely concerned with human experience related usability, experience, and human induced security cause-effect related concerns.

For future research, we propose similar case studies, which would have real world multi-disciplinary expertise participating in the whole design process in casting light on how these various methods could be further refined to fit the real world cases in designing security services and technologies. In this future case study, the proposed approach would be to use the mentioned 5on5 design steps and the corresponding design methods and tools in a workshop type of environment.

REFERENCES

1. AIAA (2013) A Framework for Aviation Cybersecurity. Available at: https://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf (Accessed: 1 November 2016).
2. Airports Council International (2014) We need to talk about cyber-security. Available at: http://www.airport-business.com/2014/06/need-talk-cyber-security/ (Accessed: 8 November 2016).
3. Alves, R. and Nunes, N.J. (2013) 'Towards a Taxonomy of Service Design Methods and Tools', Berlin: Springer Berlin Heidelberg. pp. 215–229.
4. Arnowitz, J., Arent, M. and Berger, N. (2010) Effective prototyping for software makers. 1st edn. San Francisco, CA: Morgan Kaufmann.
5. Asimov, M. (1974) 'A Philosophy of Engineering Design', in Rapp, F. (ed.) Contributions to a Philosophy of Technology: Studies in the Structure of Thinking in the Technological Sciences. Dordrecht, Holland: Reidel Publishing Company, pp. 150–157.
6. Aviation Safety Network (2016) ASN aircraft accident Ford Tri-Motor registration unknown Arequipa airport (AQP). Available at: http://aviation-safety.net/database/record.php?id=19310221-0 (Accessed: 8 November 2016).
7. Barnum, C.M. and Dragga, S. (2001) Usability testing and research. New York: Allyn & Bacon.
8. Bateman, S. (2011) 'Solving the "Wicked Problems" of maritime security: Are regional forums up to the task?', CONTEMPORARY SOUTHEAST ASIA, 33(1), p. 1. doi: 10.1355/cs34-1a.
9. BBC (1976) 1976: Israelis rescue Entebbe hostages. Available at: http://news.bbc.co.uk/onthisday/hi/dates/stories/july/4/newsid_2786000/2786967.stm (Accessed: 8 November 2016).
10. BBC (2001) History of airliner hijackings. Available at: http://news.bbc.co.uk/2/hi/south_asia/1578183.stm (Accessed: 8 November 2016).
11. BBC (2011) Moscow bombing: Carnage at Russia's Domodedovo airport. Available at: http://www.bbc.com/news/world-europe-12268662 (Accessed: 8 November 2016).
12. BBC (2015) Afghan Taliban kill dozens at Kandahar airport. Available at: http://www.bbc.com/news/world-asia-35043938 (Accessed: 8 November 2016).

13. BBC (2016a) Brussels explosions: What we know about airport and metro attacks. Available at: http://www.bbc.co.uk/news/world-europe-35869985 (Accessed: 8 November 2016).
14. BBC (2016b) Istanbul Ataturk airport attack: 41 dead and more than 230 hurt. Available at: http://www.bbc.co.uk/news/world-europe-36658187 (Accessed: 8 November 2016).
15. Bellioti, R. (2008) ACRP Synthesis 8: Common Use Facilities and Equipment at Airports. Washington, D.C.: Transportation Research Board of the National Academies.
16. Berrick, C.A. (2003) Aviation security: Efforts to measure effectiveness and strengthen security programs. Available at: http://www.gao.gov/assets/120/110523.pdf (Accessed: 3 November 2011).
17. Berrick, C.A. (2004) Aviation security: Further steps needed to strengthen the security of commercial airport perimeters and access controls. Available at: http://www.gao.gov/assets/250/242812.pdf (Accessed: 1 November 2011).
18. Bitard, P. and Basset, J. (2008) Mini Study 05 – Design as a tool for Innovation: A Project for DG Enterprise and Industry. Available at: http://ec.europa.eu/DocsRoom/documents/4394/attachments/1/translations/en/renditions/pdf. (Accessed: 9 November 2016).
19. Blackmon, M.H., Polson, P.G., Kitajima, M. and Lewis, C. (2002) 'Cognitive walkthrough for the web', CHI '02 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Minneapolis, MN, 25 April 2002. New York: ACM. pp. 463–470.
20. Bowen, P., Hash, J. and Wilson, M. (2006) Information Security Handbook: A Guide for Managers. Gaithersburg: National Institute of Standards and Technology.
21. Braha, D. and Maimon, O. (1997) 'The design process: Properties, paradigms, and structure', IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, 27(2), pp. 146–166. doi: 10.1109/3468.554679.
22. Brigman, H. (2013) TOUCHPOiNT POWER! Get & Keep More Customers, Touchpoint by Touchpoint. 1st edn. William Henry Publishing.
23. Brown, T. (2009) Change by Design: how design thinking can transform organizations and inspire innovation. New York, NY: HarperCollins Publishers.
24. Buchanan, R. (1992) 'Wicked Problems In Design Thinking', Design Issues, 8(2), pp. 5–21. doi: 10.2307/1511637.

25. Clatworthy, S. (2011) ‘Service innovation through touch-points: Development of an innovation toolkit for the first stages of new service development’, International Journal of Design, 5(2), pp. 15–28.

26. Cohen, R. (2014) Design thinking: A unified framework for innovation. Available at: http://www.forbes.com/sites/reuvencohen/2014/03/31/design-thinking-a-unified-framework-for-innovation/#796ed44856fc (Accessed: 9 November 2016).

27. Cohn, M. (2004) User stories applied: For agile software development. Addison-Wesley Professional.

28. Cooper, A. (1999) The inmates are running the asylum: Why high-tech products drive us crazy and how to restore the sanity. Indianapolis, IN: Sams Publishing.

29. Crilly, R. (2014) Karachi airport attack: Taliban gunmen terror attack leaves 28 dead. Available at: http://www.telegraph.co.uk/news/worldnews/asia/pakistan/10885752/Karachi-airport-attack-Taliban-gunmen-terror-attack-leaves-28-dead.html (Accessed: 8 November 2016).

30. Crouch, C. and Pearce, J. (2012) Doing research in design. London: Berg Publishers.

31. Cutler, V. (2009) ‘Use of threat image projection (TIP) to enhance security performance’, Proceedings 43rd Annual 2009 International Carnahan Conference on Security Technology (ICCST 2009). Zurich: Institute of Electrical and Electronics Engineers (IEEE). pp. 46–51.

32. Davies, M. (2010) ‘Concept mapping, mind mapping and argument mapping: What are the differences and do they matter?’, Higher Education, 62(3), pp. 279–301. doi: 10.1007/s10734-010-9387-6.

33. de Bono, E. (1985) Six thinking hats .. An essential approach to business management from the Crator of lateral thinking. Boston: Little Brown and Company.

34. del Real, P., Tomico, O., Pons, L. and Lloveras, J. (2006) ‘Designing Urban Furniture Through User’s Appropriation Experience: Teaching Social Interaction Design’, DS 38: Proceedings of E&DPE 2006, the 8th International Conference on Engineering and Product Design Education. Salzburg, Austria: pp. 39–44.

35. Denning, P., Comer, D.E., Gries, D., Mulder, M.C., Tucker, A.B., Turner, A.J. and Young, P.R. (1988) ‘Computing as a discipline: Preliminary report of the ACM task

force on the core of computer science', ACM SIGCSE Bulletin, 20(1). doi: 10.1145/52965.52975.

36. Design Council (2004) The Impact of Design on Stock Market Performance. Available at: https://www.gdc.net/sites/default/files/attachments/static-pages/impact2004.pdf.
37. Design Council (2007) The Value of Design Factfinder report. Available at: https://www.designcouncil.org.uk/sites/default/files/asset/document/TheValueOfDesignFactfinder_Design_Council.pdf.
38. Detweiler, M. and Friedland, L. (2011) 'Design Innovation for Enterprise Software', Orlando, FL: Springer-Verlag Berlin Heidelberg. pp. 408–414.
39. Detweiler, M. and Friedland, L. (2011) 'Design Innovation for Enterprise Software', Orlando: Springer. pp. 408–414.
40. DeWitt, A.J. and Kuljis, J. (2006) 'Is usable security an oxymoron?', interactions, 13(3), p. 41. doi: 10.1145/1125864.1125889.
41. Dym, C.L. (2006) 'Engineering Design: So Much to Learn', Journal of Engineering Education, 22(3), pp. 422–428.
42. ECAC (2014) Six decades of civil aviation: 2005-2015. Available at: https://www.ecac-ceac.org/2005-2015?p_p_id=58&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_58_struts_action=%2Flogin%2Fforgot_password6.AIAA. (2013.). A Framework for Aviation (Accessed: 8 November 2016).
43. Eckroth, J., Aytche, R. and Amoussou, G.-A. (2007) 'Toward a science of design for software-intensive systems', SoD '07 Proceedings of the 2007 Symposium on Science of Design. Arcata, CA, 24 March 2007. New York: ACM. pp. 40–41.
44. Ehn, P. and Kyng, M. (1991) 'Cardboard computers: mocking-it-up or hands-on the future', in Greenbaum, J. and Kyng, M. (eds.) Design at work: cooperative design of computer systems. Hillsdale, NJ: L. Erlbaum Associates, pp. 169–196.
45. Elias, B. (2009) Airport Passenger Screening: Background and Issues for Congress. Available at: https://www.fas.org/sgp/crs/homesec/R40543.pdf (Accessed: 4 November 2016).
46. Elizer, J. and Marshall, R. (2012) ACRP Report 70: Guidebook for Implementing Intelligent Transportation Systems Elements to Improve Airport Traveler Access

Information. Washington, D.C.: Transportation Research Board of the National Academies.

47. Engelbart, D.C. (1962) Augmenting Human intellect: A Conceptual Framework. Menlo Park, CA: Stanford Research Institute.
48. European Comission (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Available at: https://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf (Accessed: 11 June 2016).
49. European Comission (2015) Special Eurobarometer 423: Cyber Security Report. Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf (Accessed: 4 November 2016).
50. Faste, R. (1981) 'Seeing it Different Ways: The Role of Perception in Design', IDSA Papers, Industrial Designers Society of America, McLean, VA, pp. 83–86.
51. Feakin, T. (2011) Insecure Skies? Challenges and Options for Change in Civil Aviation Security. Available at: https://rusi.org/sites/default/files/201103_op_insecure_skies.pdf.
52. Flechais, I., Sasse, M.A. and Hailes, S.M.V. (2003) 'Bringing Security Home: A process for developing secure and usable systems', NSPW '03 Proceedings of the 2003 workshop on New security paradigms. Ascona, Switzerland: ACM. pp. 49–57.
53. Frayling, C. (1994) Research in Art and Design. 1st edn. London: Royal College of Art.
54. Freeman, P. and Hart, D. (2004) 'A science of design for software-intensive systems', Communications of the ACM, 47(8), p. 19. doi: 10.1145/1012037.1012054.
55. Gemser, G. and Leenders, M.A.A.M. (2001) 'How integrating industrial design in the product development process impacts on company performance', Journal of Product Innovation Management, 18(1), pp. 28–38. doi: 10.1111/1540-5885.1810028.
56. Gemser, G., Jacobs, D. and Ten Cate, R. (2006) 'Design and competitive advantage in technology-driven sectors: The role of usability and aesthetics in Dutch IT companies 1', Technology Analysis & Strategic Management, 18(5), pp. 561–580. doi: 10.1080/09537320601019719.
57. Gilger, M. (2006) 'Addressing information display weaknesses for situational awarenessAddressing information display weaknesses for situational awareness', MILCOM'06 Proceedings of the 2006 IEEE conference on Military communications. Washington, D.C.: IEEE Press. pp. 3635–3641.

58. Group, A.S.I., Interaction, C.-H., Group, C.D. and Hewett, T. (1992) ACM SIGCHI curricula for human-computer interaction. New York: Association for Computing Machinery.

59. Grover, J. (2016) Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates. Available at: Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates (Accessed: 22 November 2016).

60. Hanington, B.M., Martin, B. and Hannington, B. (2012) Universal methods of design: 100 ways to research complex problems, develop innovative ideas, and design effective solutions. Gloucester, MA, United States: Rockport Publishers.

61. Harhoff, D., Henkel, J. and von Hippel, E. (2003) ‘Profiting from voluntary information spillovers: How users benefit by freely revealing their innovations’, Research Policy, 32(10), pp. 1753–1769. doi: 10.1016/s0048-7333(03)00061-1.

62. Hertenstein, J.H., Platt, M.B. and Brown, D.R. (2001) ‘Valuing design: Enhancing corporate performance through design effectiveness’, Design Management Journal (Former Series), 12(3), pp. 10–19. doi: 10.1111/j.1948-7169.2001.tb00548.x.

63. Hobday, M., Boddington, A. and Grantham, A. (2011) ‘An innovation perspective on design: Part 1’, Design Issues, 27(4), pp. 5–15. doi: 10.1162/desi_a_00101.

64. Hofer, F. and Wetter, O. (2012) ‘Operational and human factors issues of new airport security technology—two case studies’, Journal of Transportation Security, 5(4), pp. 277–291. doi: 10.1007/s12198-012-0096-5.

65. Hong, Z. (2005) Software Design Methodology. 1st edn. Burlington: Butterworth-Heinemann.

66. Hürriyet Daily News (2013) Virus attack strikes at both Istanbul airports. Available at: http://www.hurriyetdailynews.com/virus-attack-strikes-at-both-istanbul-airports.aspx?pageID=238 (Accessed: 8 November 2016).

67. Jacobson, S.H., Virta, J.L., Bowman, J.M., Kobza, J.E. and Nestor, J.J. (2003) ‘Modeling aviation baggage screening security systems: A case study’, IIE Transactions, 35(3), pp. 259–269. doi: 10.1080/07408170304372.

68. Johansson-Sköldberg, U., Woodilla, J. and Çetinkaya, M. (2013) ‘Design thinking: Past, present and possible futures’, Creativity and Innovation Management, 22(2), pp. 121–146. doi: 10.1111/caim.12023.

69. Johnston, J., Eloff, J.H.P. and Labuschagne, L. (2003) ‘Security and human computer interfaces’, Computers & Security, 22(8), pp. 675–684. doi: 10.1016/s0167-4048(03)00006-3.
70. Kamrani, K.A. (2010) Engineering Design and Rapid Prototyping. Edited by A. E. Nasr. New York: Springer.
71. Kawakita, J. (1982) The original KJ method. Tokyo: Kawakita Research Institute.
72. Kay, A. and Goldberg, A. (1977) ‘Personal dynamic media’, Computer, 10(3), pp. 31–41. doi: 10.1109/c-m.1977.217672.
73. Ko, R.K.L., Lee, S.S.G. and Wah Lee, E. (2009) ‘Business process management (BPM) standards: A survey’, Business Process Management Journal, 15(5), pp. 744–791. doi: 10.1108/14637150910987937.
74. Kolko, J. (2012) Wicked Problems: Problems Woth Solving. Austin, Texas: ac4d.
75. Kuhn, T.S. (1962) ‘The structure of scientific revolutions’, American Journal of Physics, 31(7), p. 554. doi: 10.1119/1.1969660.
76. Kutz, G.D. and Cooney, J.W. (2007) Aviation security: Vulnerabilities exposed through covert testing of TSA’s passenger screening process: Testimony before the Committee on Oversight and Government Reform, House of Representatives. Available at: http://www.gao.gov/assets/120/118618.pdf.
77. Lakatos, I., Worrall, J. and Currie, G. (1980) The methodology of scientific research programmes: Philosophical papers: Volume 1. Cambridge: Cambridge University Press.
78. Lawson, B. (2005) How designers think: The design process demystified. 4th edn. Oxford: Elsevier/Architectural.
79. Lazarick, R. and Cammaroto, R. (2001) Recommended Security Guidelines for Airport Planning, Design and Construction. Washington, D.C.: Federal Aviation Administration.
80. Leng, R.C. (2009) Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems. Washington, D.C.: Federal Aviation Administration.
81. Licklider, J.C.R. (1960) ‘Man-computer Symbiosis’, IRE Transactions on Human Factors in Electronics, HFE-1(1), pp. 4–11. doi: 10.1109/thfe2.1960.4503259.
82. Liedtka, J. (2011) ‘Learning to use design thinking tools for successful innovation’, Strategy & Leadership, 39(5), pp. 13–19. doi: 10.1108/10878571111161480.
83. Lockwood, T. (2014) Design thinking: Integrating innovation, customer experience and brand value. Edited by Thomas Lockwood. New York: Allworth Press.

84. Löwgren, J. and Stolterman, E. (2004) Thoughtful interaction design: A design perspective on information technology. Cambridge, MA: The MIT Press.
85. Madsen, K.H. and Aiken, P.H. (1993) ‘Experiences using cooperative interactive storyboard prototyping’, Communications of the ACM, 36(6), pp. 57–64. doi: 10.1145/153571.163268.
86. Maguire, M. (2001) ‘Methods to support human-centred design’, International Journal of Human-Computer Studies, 55(4), pp. 587–634. doi: 10.1006/ijhc.2001.0503.
87. Maulsby, D. (1993) ‘Prototyping an Intelligent Agent through Wizard of Oz’, CHI ’93 Proceedings of the INTERACT ’93 and CHI ’93 Conference on Human Factors in Computing Systems. Amsterdam, Netherlands, 29 April 1993. New York: ACM. pp. 277–284.
88. McAnulty, D.M. and Fobes, J.L. (1995) Test and evaluation plan for Screener Proficiency Evaluation and Reporting System (SPEARS) threat image projection. Available at: http://www.tc.faa.gov/its/worldpac/techrpt/ar95126.pdf (Accessed: 5 November 2016).
89. McKim, R.H. (1973) Experiences in Visual Thinking. Brooks/Cole Publishing Co.
90. Meredith, L. (2010) Malware implicated in fatal Spanair plane crash. Available at: http://www.nbcnews.com/id/38790670/ns/technology_and_science-security/ (Accessed: 8 November 2016).
91. Murphy, R.J., Sukkarieh, M., Haass, J. and Hriljac, P.M. (2015) ACRP Report 140: Guidebook on best practices for airport cybersecurity. Washington, D.C.: Transportation Research Board of the National Academies.
92. Myers, B.A. (1998) ‘A brief history of human-computer interaction technology’, interactions, 5(2). doi: 10.1145/274430.274436.
93. Newell, A., Perlis, A.J. and Simon, H.A. (1967) ‘Computer science’, Science, 157(3795), pp. 1373–1374. doi: 10.1126/science.157.3795.1373-b.
94. Nielsen, J. (1990) ‘Paper versus computer implementations as mockup scenarios for heuristic evaluation’, INTERACT ’90 Proceedings of the IFIP TC13 Third Interational Conference on Human-Computer Interaction. Amsterdam, Amsterdam, Netherlands: North-Holland Publishing. pp. 315–320.

95. Nielsen, J. (1992) ‘Finding usability problems through heuristic evaluation’, CHI ’92 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Monterey, CA, 7 May 1992. New York: ACM. pp. 373–380.

96. Nielsen, J. (1994) ‘Usability inspection methods’, CHI ’94 Conference Companion on Human Factors in Computing Systems. Boston, MA, 28 April 1994. New York: ACM. pp. 413–414.

97. NIST (2015) Guide to Industrial Control System (ICS) Security. 2nd edn. Gaithersburg: National Institute of Standards and Technology.

98. Nussbaum, B. (2004) ‘The Power of Design’, BusinessWeek, Cover Story (May), .

99. Ogot, M. and Okudan-Kremer, G. (2004) Engineering Design: A Practical Guide. Victoria, Canada: Trafford Publishing.

100. Ohno, T. (1988) Toyota production system: Beyond large-scale production. Cambridge, MA: Productivity Press.

101. Osborn, A.F. (1963) Applied Imagination: Principles and Procedures of Creative Problem-Solving. 3rd edn. New York: Charles Scribner’s Sons.

102. OTA (1984) Airport System Development. Washington, D.C.: U.S. Congress, Office of Technology Assessment.

103. Owen, C.L. (2006a) ‘Design Thinking: Notes on Its Nature and Use’, Design Research Quarterly, 2(1), pp. 16–27.

104. Owen, C.L. (2006b) Design Thinking: Driving Innovation. Illinois: Institute of Design, Illinois Institute of Technology.

105. Oxford (2016) ‘Innovation’, in Oxford Dictionary. Available at: http://www.oxforddictionaries.com/definition/english/innovation (Accessed: 8 November 2016).

106. Parrish, P. (2006) ‘Design as storytelling’, TECHTRENDS TECH TRENDS, 50(4), pp. 72–82. doi: 10.1007/s11528-006-0072-7.

107. Patricio, L., Fisk, R.P., Falcao e Cunha, J. and Constantine, L. (2011) ‘Multilevel service design: From customer value constellation to service experience Blueprinting’, Journal of Service Research, 14(2), pp. 180–200. doi: 10.1177/1094670511401901.

108. Pruitt, J. and Adlin, T. (2006) The persona lifecycle: Keeping people in mind throughout product design. San Francisco: Morgan Kaufmann.

109. Purnell, J., Hough, R., White, R., Gonzalez, S., Haley, F. and Hyde, M. (2012) ACRP Report 59: Information Technology Systems at Airports - A Primer. Washington, D.C.: Transportation Research Board of the National Academies.

110. Reid, T. (1985) Essays on the intellectual powers of man. Edited by A D Woozley. United States: Lincoln-Rembrandt Pub.

111. Ries, E. (2011) The lean startup: How today's entrepreneurs use continuous innovation to create radically successful businesses. New York: Crown Publishing Group, Division of Random House.

112. Rittel, H.W.J. and Webber, M.M. (1973) 'Dilemmas in a general theory of planning', Policy Sciences, 4(2), pp. 155–169. doi: 10.1007/bf01405730.

113. Ritter, F.E., Churchill, E.F. and Baxter, G.D. (2014) Foundations for designing user-centered systems: What system designers need to know about people. United Kingdom: Springer-Verlag New York.

114. Saltzer, J.H. and Schroeder, M.D. (1975) 'The protection of information in computer systems', Proceedings of the IEEE, 63(9), pp. 1278–1308. doi: 10.1109/proc.1975.9939.

115. Sasse, M.A., Brostoff, S. and Weirich, D. (2001) 'Transforming the "Weakest Link" — a Human/Computer Interaction Approach to Usable and Effective Security', BT Technology Journal, 19(3), pp. 122–131.

116. Simon, H.A.A. (1969) The sciences of the artificial. 1st edn. Cambridge, MA: MIT Press.

117. Simon, H.A.A. (1973) 'The structure of ill structured problems', Artificial Intelligence, 4(3-4), pp. 181–201. doi: 10.1016/0004-3702(73)90011-8.

118. SITA (2016a) 'The Future Is Connected', Air Transportation Industry Insights.

119. SITA (2016b) 'The Passenger IT Trends Survey', Air Transport Industry Insights.

120. Smith, S.W. (2003) 'Humans in the loop: Human-computer interaction and security', IEEE Security & Privacy Magazine, 1(3), pp. 75–79. doi: 10.1109/msecp.2003.1203228.

121. Snyder, C.A. (2003) Paper Prototyping: The fast and easy way to design and refine user interfaces. San Diego, CA: Morgan Kaufmann.

122. Stephano, A.L. and Groth, D.P. (2011) 'Useable security: Interface design strategies for improving security', CCS '06 13th ACM Conference on Computer and Communications Security 2006. Alexandria, VA: ACM. pp. 278–29.

123. Stocking, C., DeLong, J., Braunagel, V., Healy, T. and Loper, S. (2009) ACRP Report 13: Integrating Airport Information Systems. Washington, D.C.: Transportation Research Board of the National Academies.

124. Tassi, R. (2009) Design activities. Available at: http://www.servicedesigntools.org (Accessed: 9 November 2016).

125. Tennant, G. (2001) Six sigma: SPC and TQM in manufacturing and services. Aldershot: Ashgate Publishing.

126. Theofanos, M.F. and Pfleeger, S.L. (2011) ‘Guest editors’ introduction: Shouldn’t all security be usable?’, IEEE Security & Privacy Magazine, 9(2), pp. 12–17. doi: 10.1109/msp.2011.30.

127. TRB (2008) ACRP Report 10: Innovations for Airport Terminal Facilities. Washington, D.C.: Transportation Research Board of the National Academies.

128. TRB (2010) ACRP Report 25: Airport Passenger Terminal Planning and Design Volume 1. Washington, D.C.: Transportation Research Board of the National Academies.

129. TRB (2012) ACRP Report 67: Airport Passenger Conveyance Systems Planning Guidebook. Washington, D.C.: Transportation Research Board of the National Academies.

130. TRB (2014) ACRP Report 101: Best Practices Manual for Working in Or Near Airport Movement Areas. Washington, D.C.: Transportation Research Board of the National Academies.

131. Treffinger, D.J., Isaksen, S.G., Stead-Dorval, B.K. and Stead-Doval, B.K. (2006) Creative problem solving: An introduction, 4th edition. 4th edn. Waco, TX: Prufrock Press.

132. Truong, K.N., Hayes, G.R. and Abowd, G.D. (2006) ‘Storyboarding: an empirical determination of best practices and effective guidelines’, DIS ’06 Proceedings of the 6th conference on Designing Interactive systems. University Park, PA, June 2006. New York: ACM. pp. 12–21.

133. TSA (2004) Security Guidelines for General Aviation Airports. Washington, D.C.: Transportation Security Administration.

134. TSA (2006) Security Checkpoint Layout Design / Reconfiguration Guide. Washington, D.C.: Transportation Security Administration.

135. TSA (2011) Recommended Security Guidelines for Airport Planning, Design and Construction. Washington, D.C.: Transportation Security Administration.

136. TSA (2012) Checkpoint Design Guide (CDG) Revision 4.0. Washington, D.C.: Transportation Security Administration.

137. Tschimmel, K. (2012) 'Design Thinking as an effective Toolkit for Innovation', Proceedings of The XXIII ISPIM Conference 2012. Barcelona, Spain, 20 June 2012. Barcelona, Spain: ISPIM. .

138. UTS (2014) Solving wicked problems in Alaska using design thinking. Available at: http://www.uts.edu.au/research-and-teaching/our-research/institute-sustainable-futures/news/solving-wicked-problems-alaska (Accessed: 9 November 2016).

139. Walls, J.G., Widmeyer, G.R. and El Sawy, O.A. (1992) 'Building an information system design theory for vigilant EIS', Information Systems Research, 3(1), pp. 36–59. doi: 10.1287/isre.3.1.36.

140. Verganti, R. (2008) 'Design, meanings, and radical innovation: A Metamodel and a research agenda', Journal of Product Innovation Management, 25(5), pp. 436–456. doi: 10.1111/j.1540-5885.2008.00313.x.

141. Wharton, C., Rieman, J., Lewis, C. and Polson, P. (1994) 'The cognitive walkthrough method: a practitioner's guide', in Nielsen, J. and Mack, R.L. (eds.) Usability inspection methods. New York: John Wiley & Sons, pp. 105–140.

142. Whitten, A. (1999) 'Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0', SSYM'99 Proceedings of the 8th conference on USENIX Security Symposium - Volume 8. Berkeley: USENIX. pp. 14–14.

143. Vidosic, J.P. (1969) Elements of Design Engineering. New York: John Wiley & Sons.

144. Wieringa, R.J. (2014) Design Science Methodology. London: Springer.

145. von Stamm, B. (2004) 'Innovation-what's design got to do with it?', Design Management Review, 15(1), pp. 10–19. doi: 10.1111/j.1948-7169.2004.tb00145.x.

146. Wyckoff, K. (2015) Solving Homeland Security's Wicked Problems: a Design Thinking Approach. Naval Postgraduate School. Monterey, CA. .

147. Yee, K.P. (2002) 'User Interaction Design for Secure Systems', ICICS '02 Proceedings of the 4th International Conference on Information and Communications Security. Singapore: Springer-Verlag. pp. 278–290.

APPENDIX 1. Analysis of Present Threats and Risks

In the present day various factors can contribute or pose a threat/risk to airport security, which needs to be taken into consideration. In general, security incidences can be segmented into crime, natural disasters like fires and floods, malicious attacks, espionage, internal attacks or sabotage, malfunctions and unintentional human errors or accidents.

There are various examples in the aviation history, where the airport security mechanisms were in place, but were not triggered to prevent accidents from happening. However, in the first occurrence of aviation related attacks, the aviation security mechanisms were not advanced enough to counter the risks, since the policies and standards were developed to only encounter the known threats and risks (Grover, 2016).

For this reason, theoretical non-empirical qualitative study was conducted on some of the earliest aviation related incidences, which were can be seen in Table 7 (does not contain every single incident that occurred before, middle, and after the incidences).

Table 7. Historical analysis of aviation threats (Aviation Safety Network, 2016; BBC, 2001; BBC, 2016c)

Date	Incident
21th February 1931	Stand-off between the pilot (Byron Richards) and armed revolutionary soldiers
23th July 1968	Hijacking incident of El Al plane from Rome and diverted to Algiers, which is told to be the longest hijacking incident in the aviation history. Lasted 40 days.
4th July 1976	100 Israeli/jewish passengers in an Air France flight, were rescued by Israeli commandos from the palestinian militias and Ugandan soldiers after one week from the start of the incident.
13th October 1977	Lufthansa 181 Flight 181 from Son Sant Joan Airport to Frankfurt International Airport hijacking incident by 4 member group, which was part of the Popular Front for the Liberation of Palestine

(continues)

APPENDIX 1. (continues)

Some of the examples of the recent aviation related attacks are mentioned are listed in the Table 8, which does not contain all of the occurrences of such attacks.

Table 8. Recent attacks in the aviation (BBC, 2016a; BBC, 2016b; BBC, 2011; Crilly, 2014; BBC, 2015; BBC, 2001)

Date	Airport	Location	Used Techniques
28th June 2016	Istanbul Ataturk International Airport	Landside Area (Parking), Main Terminal	automatic weapons, improvised explosives devices,
22th March 2016	Brussels Zaventem Airport	Main Terminal (Check-In Area)	improvised explosives devices
24th January 2011	Moscow Domodedovo	Main Terminal	improvised explosives device
8th June 2014	Jinnah International Airport	Cargo area, VIP area	masking (police uniforms), suicide vests, rocket propelled grenades, automatic weapons
8th December 2015	Kandahar International Airport	Airside (Airfield)	automatic weapons, human shields
11th September 2001	Logan International Airport, Newark Liberty International Airport, Washington Dulles International Airport		Plane hijacking, Insider Threat / Masking, Planes as weapons of mass destruction tool, maces, tear gas, pepper sprays, sharp items, multi-function hand tools

As can be seen from the Tables 7 and 8, targeting airports and aviation has a symbolic value and thus they are under constant attacks. The reasons of targeting airports ranges from politics to malicious intents since the first recorded attack in the 1930’s. The targeting of airports and the used methods took a more intensive turn during the years 1970’s and 1980s, as the reasons and methods shifted from political statements and hijackings to bombings (Feakin, 2011). About 47 bombs were successfully placed on aircrafts between the 1970’s and 1980’s. There are passengers, airport and airline staff from various different countries, which are used as targets as the airport architectural layout is closed and humans (continues) are confined inside different, but small spaces (TSA, 2011). Also, airports usually have security checks inside the terminal building, which means that attackers have time and the opportunity to attack on buses, trains, parking areas, and pre-security terminal building, where people are at the most vulnerable position (TSA, 2004; TSA, 2006; TSA, 2011). Additionally, airports do not tend to keep the federal law enforcement officers (LEO) at every site as the presence of security and LEO officers might have a negative impact on the airport atmosphere and passenger experience (TSA, 2012).

In addition to growing number of terrorist related attacks and threats, there has been a growing interest on the cybersecurity threats in airports as the aviation industry heavily relies on computer systems on its ground and flight operations, where some systems are highly safety-critical e.g., related to aircraft in flight, operationally important and directly impacts the airport services and thus the reputation and financial stability of airports (Leng, 2009).

Furthermore as the information systems become further interdependent and the critical systems shift increasingly towards technological solutions cyber security concerns become more important in understanding the cyber security loops. Some examples of past cyber security attacks have been listed in Table 9 (Leng, 2009; Meredith, 2010; Dogan News Agency, 2013).

Table 9. Cyber-attacks

Date	**Airport**
2006	FAA’s remote maintenance monitoring system was connected to the less-secure mission support network, which created security exposure to ATC operations
2006	A virus attack originating from the internet spread from administrative networks to ATC networks, forcing FAA to shut down a portion of its ATC systems in Alaska
2008	Hackers took over FAA computers in Alaska, becoming FAA “insiders”. By taking advantage of FAA’s interconnected networks, hackers later stole FAA’s

(continues)

APPENDIX 1. (continues)

Table 9. Cyber-attacks - continued

Date	Airport
2008	enterprise administrator's password in Oklahoma, installed malicious codes with the stolen password, and compromised FAA’s domain controller in its Western Pacific Region. About 40,000 user IDs, passwords, and other information used to control a portion of the FAA mission-support network was stolen
2008	Spanair flight 5022, crashed after take-off in Madrid-Barajas Airport as a consequence of an malware infected aircraft system
2009	Hackers compromised an FAA public-facing Web application computer on the Internet and used it as a conduit to enter an FAA internal database server
2013	Cyber-attack in Istanbul Ataturk and Sabiha Gökcen airports causing flight delays and shutdown of the passport control system

In order to minimize or prevent further attacks and risks, a thorough understanding and information of airport systems and subsystems need to be acquired. This serves as a structure in the airport security related technologies and process chain analysis to see the security and technology dependencies in the present moment and map previously conducted attacks and methods of targeting airports in the anticipation of future threats in the design of security systems in relation to passenger or human experiences in general.

APPENDIX 2. SCADA and ICS Security and Usability

In this appendix, the threats and risk points have been segmented into two categories e.g., supervisory control and data acquisition (SCADA) industrial control system (ICS) security risks, so that the complexity of the airport ecosystem can be demonstrated.

Airports contain various types of supervisory control and data acquisition (SCADA) and industrial control systems (ICS) (Stouffer et. al., 2008; Murphy et. al., 2015). In securing the airport perimeter, organizations like FAA (Lazarick et. al., 2001) and TSA (2012a) have implemented various initiatives in strengthening the airport security, but the effectiveness of these initiatives has not been closely addressed.

In general, the airport security is focused on the checkpoint screening as a primary security mechanism in minimizing risks. The security checkpoint officers check the passengers for prohibited items like firearms, knifes, gasoline, lighter fluid, disabling chemicals like chlorine and liquid bleach. Also, the security officials are advised to look for suspicious behavior and combination of items, which may be used as weapons. The passenger screening process is made of security officers, technology, and standard operating procedures (TSA, 2012a).

In measuring and the effectiveness of airport security, various efforts have been conducted by organizations like GAO. For example, GAO has published diverse range of reports in measuring the effectiveness and vulnerabilities of general airport security and security checkpoints by taking human and technical factors in the security screening into consideration (Berrick, 2003; Berrick, 2004; Kutz et. al., 2007). Similarly, various researches like Sheldon et. al. (2001), Skorupski (2016), and Hofer et. al. (2012) have studied the human performance in operating the airport security technologies and possible human-computer interaction security loopholes. Also, as mentioned by Elias (2009) in his CRS Report for Congress named "Airport Passenger Screening: Background and Issues for Congress"; there is a need for more detailed analysis and improvement of human performance in operating the safety-critical systems. For example, according to Kutz et. al. (2007), the human performance related vulnerabilities were investigated

(continues)

through covert testing by the transportation security agency (TSO). The results showed that the covert TSO's were able to smuggle items through the security checkpoint, which could have been used as weapons or improvised explosives devices if combined. Also, some standard procedure related erroneous behavior was seen in the security checkpoint officers, which could lower the user experience and create a level of tension.

In measuring and strengthening the human performance, there are some promising technologies like Threat Image Projection (TIP) (Cutler et. al., 2009), Screener Proficiency Evaluation and Reporting System (SPEARS) (Fobes et. al., 1995), but these systems exist as training tools rather than evaluating and strengthening the system loopholes themselves.

From cybersecurity point of view, various airport stakeholders are increasingly reliant on computers and electronic devices. Cyber and computer-based security incidents are dramatically increasing yearly across the world in number and sophistication. Due to airport visibility and exposure, disruption of the essential operations of airlines and airports could feasibly be the subject of a cyber-attack by cyber terrorists, where the result could be the loss of confidential data, disruption to operations and critical infrastructure, costly recoveries, and degraded reputation. Cyber-attacks will stem from diverse sources and will have a range of possible targets, including civilian, commercial and military systems to damage critical services as airports rely more on computing technology such as desktop computers, servers, network devices, flight information display systems (FIDS), airfield lighting controls, heating and ventilation systems, baggage handling systems, access control devices among other technologies.

The serious cyber security threats posed by cyber-attacks have certainly been well recognized by many stakeholders in the global civil aviation community (Leng, 2009; Murphy et. al., 2015). Airports core infrastructure supports various different functions that are critical for the efficiency and effectiveness of the air transport system, but not all of the airports have implemented cyber-security systems that would protect and control those operations and all related features i.e., even though many may have security

(continues)

APPENDIX 2. (continues)

measures in place, cyber terrorists may consider this as a perfect opportunity to attack the airports in many different ways, where the most ‘desirable’ exposed parts could be public wireless hotspots; the baggage systems; main airport websites, and so on (Murphy et. al., 2015).

Furthermore, airports are particularly vulnerable to internal and external cyber threats and attacks from criminals, terrorists, or foreign actors. Apart from the traditional IT infrastructure such as the email and the Internet, several potential targets for cyber-attacks exist within the realm of internal airport operations like access control and perimeter intrusion systems, IT enabled aircraft systems, radar systems, ground radar, network-enabled baggage systems, wireless and wired network systems, supervisory control and data acquisition (SCADA)-type industrial control systems (ICS) (Stouffer et. al., 2008; Murphy et. al., 2015).

APPENDIX 3. Cybersecurity Threats and Concerns

Beyond physical security at airports, cyber threats to the internal airport operations are emerging to be a primary concern especially with the increasing use of mobile applications and mobile hardware. Furthermore, bring your own devices (BYOD) like smartphones and tablets are a common sight in workplaces. This trend is also catching up at airports where not only the airport passengers, but even the airport tenants, staff and contractor wish to bring their own devices into the workplace. However, if these devices interact with enterprise systems (such as e-mail and VPN access) they can potentially be used secretly gather confidential information or introduce viruses. Airports typically rely on SCADA-type industrial control systems for utilities, baggage systems, and business processes such as facility management. Due to their limited or lack of internet access, SCADA-type systems may appear to be more secure, but they too are vulnerable to cyber threats (Murphy et. al., 2015).

Also, various airports are facing a growing internal threats and attacks. For example, airport personnel could have a more easy access to airport systems and destroy, steal airport data, sell or leak sensitive information, or harm the systems intentionally. At first, leakage or destruction of data does not translate into risky or threat scenarios, but if this data is modified or some of the sensitive or safety-critical data reaches an unknown or malicious third party, could be disastrous not only for the airport, but also for the interconnected airports (or the whole civil aviation industry) as airports are seen as holding a symbolic status and act as gateways in and out of the countries.

As mentioned before, civil aviation is one of the high value targets likely to be selected by cyber terrorists and incidents may result in long lasting effects for any small to large sized airport. Also, loss of operations for any period of time would be crucial, in terms of costs. The same goes for reduced throughput. For example, loss of operation in hold baggage systems, could lead to unknown scenarios on the passenger side, and operational productivity would drastically drop on the airports side. As a consequence, to tackle the cyber and information security threats, there are many activities ongoing in from different institutions and bodies aiming at spreading awareness of cyber-attacks and how (continues) to protect businesses. In 2013, for example, the European Commission released a policy document called Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (European Commission, 2013), with a legislative proposal in strengthening the security of EU's information systems to encourage economic growth by inviting industries to take actions at the national level in order to protect their business and to have harmonized cyber-security measures among all Member State airports in the EU. Additionally, European Commission released a survey of the cyber security situation in 2015, which showed the increasing concern of the rising cyber security attacks and threats targeting at personal and enterprise information (European Commission, 2015).

Similarly, National Institute of Standards and Technology (NIST) published a Guide for Conducting Risk Assessments for Information Technology (NIST, 2012) and Framework for Improving Critical Infrastructure Cybersecurity report based on the Executive Order 13636 directed by President Obama (NIST, 2014) not to mention various of other reports before, in between and after related to cyber and information security.

Furthermore, the European Civil Aviation Conference (ECAC, 2014) has a research group, which works on cyber security threats to civil aviation. ECAC's final work reports consist of state of the art review of cyber security to tackle the cyber threats, good practice frameworks on Cyber Threats to Civil Aviation that considers recent developments in cyber-security and a cyber-threats, building a framework for establishing best practices (ECAC, 2014). Likewise, The American Institute of Aeronautics and Astronautics (AIAA) has published different frameworks and reports to address the cyber security threats and reducing cyber-attacks on critical aviation information systems (CIAS) (AIAA, 2013).

Further, Transportation Research Board (TRB) in U.S. is one of the seven program units of the National Academies of Science, Engineering, and Medicine that is aiming to develop Airport Cyber-security Best Practices among other airport related elements (Murphy et. al., 2015). In the following section, in order to understand and model the airport human-computer interaction security factors, the report will go through various

(continues)

APPENDIX 3. (continues)

levels of cyber security threats in a brief manner, because it is important to recognize the cyber security risks and threats so that it would be easier to establish a cyber-security related strategies and objectives.

In understanding the human-computer interaction related security factors, one must understand that cyber and information security threats affect a wide range of systems ranging from SCADA (Stouffer et. al., 2008), CIAS (AIAA, 2013), to IT (Murphy et. al., 2015). The wide variety of system types could range from heating and air conditioning (HVAC) to check-in and passenger screening technologies. Security threats can emerge from any point in the world as the airport IT systems are becoming more integrated and thus exposed with the outside world, not to mention that they can also occur in close proximity to the systems. As a consequence, to tackle the cyber security threats, the origin of the threats (person, machine) must be known in relation to the path of the attacker or threat to exploit the vulnerability so that proper models in possible countermeasures, recovery, and respond can be drawn.

To acquire information and data regarding the cyber security factors, NIST (2014) published a "Framework for Improving Critical Infrastructure Cybersecurity", where the core of the framework consisted of knowing the organization functions (identify, protect, detect, respond, and recover), categories, subcategories, and information references like standards, guidelines, and practices. Furthermore, the provided viewpoints for different organization levels were segmented as Tiers. These Tiers are defined as Tier 1, Tier 2, Tier 3, and Tier 4, where on every Tier the concerns were based on Risk Management Process, Integrated Risk Management Program, and External Participation. The wanted results are the identification of threats to airports data and systems, actors like hackers and insiders, motives to carry out the threats, vectors or channels that are used by attackers to reach the vulnerabilities in the organization's, targets like IT and SCADA systems, inventory of the potential targets, likelihood estimation of attacks, estimated impact of vulnerabilities, vulnerability of an systems that could be exploited, and a prioritization of the vulnerabilities. Additionally, the results contain cyber security related protections, detection, response, and

(continues)

APPENDIX 3. (continues)

recovery based procedures, policies, countermeasures, best practice guidelines, and so on. In assessing the risk factors in the airport information system; guidelines published by NIST (2012) in their “Guide for Conducting Risk Assessments” were used. The risks assessment of organization information systems can be categorized as Tier 1 (organization), Tier 2 (mission / business processes), and Tier 3 (information systems), where the concernable factors are exposure of information systems in the mission / business processes or vice versa, where the organization works as the vector or path to the mission / business processes. In acquiring information for various organizational Tiers, the possible generic model proposed by NIST (2012) as following:

1. Identify threat source (with characteristics like capability, intent, and targeting for adversarial threats), which initiates (likelihood of initiation) the
2. Threat event (sequence of actions, activities, or scenarios), which exploits (likelihood of success)
3. Vulnerability with severity in the context of
4. Conditions with pervasiveness
5. Security controls (planned / implemented) with effectiveness causing with a degree of
6. Adverse impact with risk as a combination of impact and likelihood, which produces an organization risk.

The various possible cyber security threats as mentioned by NIST (2012) in their “Guide for Conducting Risk Assessments” for assessing the company processes in relation to their IT systems and threats and later extended to the context of airport security by Murphy et. al. (2015) in their “Guidebook on best practices for airport cybersecurity” is show in the Table 10. A comprehensive listing will not be generated as it is out of this master’s thesis scope, but the listing will serve as an example of the complexity and safety-critical nature of the airport ecosystem, the used information technology, and industrial control systems, which means that there is a need for taking all the possible dependencies in airport into consideration, when designing or re-designing a particular service or system.

(continues)

APPENDIX 3. (continues)

Table 10. Cyber security threats (Murphy et. al., 2015)

Threat category	**Examples and concerns**
Confidentiality breach	Intentional or unintentional access to personally identifiable information and material
Counterfeit hardware	Compromisation of critical systems
Data breach	Malwares that extract valuable information
Delayed Technology Refresh	Degraded performance, aging equipment
Denial of Service (DoS)	Unavailable resources and systems
Host Exploit	exploitation of poorly conFig.d systems
Inadequate Monitoring of Proximity Events	Failure to monitor events in the airport proximity
Ineffective Disposal	Theft/scavenging of discarded systems
Ineffective Testing	Software integrity attacks
Insider Threat	Subverted individuals in organization causing harm, revealing critical/sensitive information and so on.
Insider Threat / Data Breach	Compromisation of mission-critical information
Intentional Data Alteration	Data vandalization, modification, deletion
Intentional data theft	Direct malware attack
Internal Threat	Robbery of property
Lack of Internal Control	Insecure tenant environment
Malicious Code	Information system code modification
Organized Campaign	Acquisition of specific information
Phishing	False front organization / person
Physical Exploit	Cyber-physical attack on facilities
Social Engineering	Tailgating, persuasion, emails, phones
Supply Chain Integrity	Compromisation of software and hardware
Third Party	Aging devices from same supplier
Unauthorized Access (host, network, app)	Compromisation of critical facilities and data
Unauthorized Backdoor	Inhibit intrusion detection and auditing
Unauthorized Host Access	Counterfeit certificates
Unauthorized Network Access	Compromise traffic/data movement
Unauthorized Physical Access	Bypassing card- and badge-based systems
Unauthorized Reconnaissance	access sensitive data/information

(continues)

APPENDIX 3. (continues)

Table 10. Cyber security threats (Murphy et. al., 2015) - continued

Threat category	Examples and concerns
Unintended Data Compromise	expose, disclose, mishandling
Unintended Data Leak	incorrect privileges and/or data leak
Vishing	voice system social engineering technique

APPENDIX 4. Historical Roots of HCI

Human-Computer Interaction studies have their roots in the early computer science related developments in computer graphics, operating systems, and human factors in machine interactions, ergonomics, industrial engineering and cognitive psychology (Hewett et. al., 1992).

There is no direct point in time, when the term HCI became known as a field of study and discipline, but it rose into the mainstream with the advancement of technology and innovations, where the focus of research and commercialization shifted from human-hardware interaction to human-computer interaction (emergence of user interfaces) in the early 1980's. As a consequence, various works were published. For example, Myers (1998) mentioned J. C. R. Licklider (1960) who theorized in his "Man-Computer Symbiosis", that in the future, humans and computers would live in a symbiosis and as a consequence, they would be dependable on each other, but both humans and computers would have their own separable functions and constraints.

Other equally recognizable contributions to the discipline were "Personal Dynamic Media" (Kay et. al., 1977) and "Augmenting Human Intellect: A Conceptual Framework" (D. C. Engelbart, 1962), where the core focus was on how through the augmented human intellect, we can gain comprehension and solutions in previously insoluble problems. Engelbart (1962) also mentioned that in order for a man to approach a complex problem situation, to gain comprehension to suit his particular needs, and to derive solutions to ever increasing complexity and problems in the work, there is a need for augmenting the human intellect through the useful means.

As mentioned by Myers (1998) few notable technological innovations and important works in the past that gave rise to human-computer interaction are ubiquitous direct manipulation interfaces (manipulatable and visible screen object, with physical pointing devices), direct manipulation of graphics (Light Handles), AMBIT/G (interface techniques, iconic representations, gesture recognition, dynamic menus and selectable items), icons, "What You See Is what You Get (WYSIWYG)" interfaces and editors, mouse, multiple (continues)

APPENDIX 4. (continues)

tiled and overlapping windows, applications, text editing, spreadsheets, hypertext, World Wide Web, Computer-Aided Design (CAD) tools, gesture recognition, multimedia (hypermedia, raster graphics, text, speech, video), three-dimensionality (3D) systems, virtual reality, augmented reality, computer-supported cooperative work, user interface (UI) tools, and interface builders. Few of the known examples of the research based and later commercialized major technologies are shown in Table 11.

Table 11. Innovations in HCI (Myers, 1998)

University Research Started	**Corporate Research Started**	**Commercial Productization Started**	**Technologies**
1960	1970	1980	Direct Manipulation of Graphical Objects
1965	1970	1980	Mouse
1960	1973	1980	Windows
1960	1973–1974	1980	Text Editing
1960	1977–1979	1986–1987	Hypertext
1963–1964	1956–1957	1976–1977	Gesture Recognition

APPENDIX 5. Human-Computer Interaction

Human-Computer Interaction (HCI), "is a discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them" (Hewett et. al., 1992) i.e., HCI is focused on interaction between humans and computers, which can lead to a vast, but specific topics in the interaction.

Furthermore, HCI is an interdisciplinary field of study, where the emphasis is on (not restricted to) computer science, psychology, sociology, anthropology, and industrial design (see Table 12) (Hewett et. al., 1992). Additional or other disciplines, might also serve as supporting fields of sciences depending on the perspective. As a consequence, to analyze and examine the HCI factors in a certain environment will require knowledge in more than one discipline for example computer science. For this report's purpose, the emphasis on computers, embedded systems and human interaction with these systems.

Table 12. HCI related disciplines (Hewett et. al., 1992)

Discipline	**Concerns**
Computer Science	Application design and engineering of human interfaces
Psychology	The application of theories of cognitive processes and the empirical analysis of user behavior
Sociology and Anthropology	Interactions between technology, work, and organization
Industrial design	Interactive products

Few examples, of HCI related special concerns are human-computer interactions and joint performance of tasks by humans and machines, communication structure between human and machines, human capabilities in using machines (learnability of interfaces), algorithms and programming of the interfaces itself, engineering concerns that arise in designing and building interfaces, the process of specification, design, and implementation of interfaces, and design trade-offs (Hewett et. al., 1992) i.e., all possible aspects that relate to the interaction between humans and computers. HCI as a subfield in computer

(continues)

science discipline can be described according to ACM (Denning, et al., 1988) report as “the systematic study of algorithmic process that describe and transform information: their theory, analysis, design, efficiency, implementation, and application.” i.e., users interacting with the system, which leads to algorithmic decomposition of the various business processes. Also, according to Newell et. al. (1967), computer science is the study of complex, varied and rich phenomena surrounding computers.

As a consequence, we can describe the employed computer systems existing within a larger context and organization, where in order to have a purposeful and functional system, we have fit human, technical, and work aspects of the system in specific situations together so that we take human learning, system tailorability, human information processing, communication, physical characteristics of users, input and output devices (interfaces) and dialogs into considerations (see Table 13) (Hewett et. al., 1992). For these reasons, we can describe HCI as the study of humans, human processes, computers, embedded systems and applications as only subsystems of the whole system of systems.

Table 13. Content of HCI (Hewett et. al., 1992)

Content Areas
The Nature of HCI • (Meta-) Models of HCI • Points of view like communication, agent, paradigm, tool paradigm, the work-centered point of view, human and their corresponding tasks and system division, supervisory control • Objectives like productivity or user empowerment • History and intellectual roots
Use and Context of Computers • Human Social Organization and Work like points of view in industrial engineering and operations research, models of human activity like opportunistic planning and open procedure, models of small-groups and organizations, models of work/workflow/cooperative activity, office work, socio-technical systems or human organization as adaptive open system and mutual impact of computer systems on work and vice versa, computer systems for group tasks, quality of work life and job satisfaction

(continues)

APPENDIX 5. (continues)

Table 13. Content of HCI (Hewett et. al., 1992) - continued

• Application Areas like characterization of application areas to individual, group, paced, and unpaced. Documentation-oriented interfaces like text-editing, document formatting, illustrators, spreadsheets, and hypertext. Communication oriented interfaces, Design Environments, On-Line tutorial systems and help systems, Multimedia information kiosks, Continuous control systems, Embedded systems • Human-Machine Fit and Adaptation like alternate techniques for achieving fit, nature of adaptive systems, system selection, system adaptation, user selection, user adaptation, user guidance
Human Characteristics • Human Information Processing like characteristics of the human as a processor of information, models of cognitive architecture, phenomena and theories of memory, phenomena and theories of perception, phenomena and theories of attention and vigilance, phenomena and theories of problem solving, phenomena and theories of learning and skill acquisition, phenomena and theories of motivation, users conceptual models, models of human action, human diversity (disabled populations) • Language, Communication, Interaction. For example, language as a communication and interface medium, aspects of language, formal models of language, pragmatic phenomena of conversational interaction, language phenomena, specialized languages, interaction reuse • Ergonomics like human anthropometry in relation to workspace design, arrangement of displays and controls / link analysis, human cognitive and sensory limits, sensory and perceptual effects of CRT and other display technologies, control design, fatigue and health issues, furniture and lighting design, temperature and environmental noise issues, design for stressful or hazardous environments, design for the disabled
Computer System and Interface Architecture • Input and Output Devices like surveys, mechanics of particular devices, human and computer performance characteristics, devices for the disabled, handwriting and gestures, speech input, eye tracking, exotic devices like EEG and other biological signals. • Dialogue Techniques like dialogue inputs (selection, discrete parameter specification, continuous control), input techniques (keyboard techniques, mouse-based techniques, pen-based techniques, voice-based technique), dialog type and techniques like alphanumeric techniques, form filling, menu selection, icons and direct manipulation, generic functions, natural language, navigation and orientation in dialogues, error management, multimedia and non-graphical dialogues (speech input, speech output, voice mail, video mail, active documents), agents and AI techniques, multi-person dialogue,

(continues)

APPENDIX 5. (continues)

Table 13. Content of HCI (Hewett et. al., 1992) - continued

real-time response issues, manual control theory, supervisory control / automatic systems / embedded system, standard, look and feel intellectual property protection, • Dialogue Genre like interaction metaphors, content metaphors, persona / personality / point of view, workspace models, transition management, relevant techniques from other media, style and aesthetics, • Computer Graphics • Dialogue Architecture
Development Process • Design Approaches • Implementation Techniques • Evaluation Techniques • Example Systems and Case Studies
Project Presentations and Examinations

As can be seen in Table 13, HCI uses knowledge from various supporting disciplines (depending on the perspective) where in the machine side we have concerns related to computer graphics, operating systems, programming languages, and development environment and on the human side we have communication theory, graphic and industrial design disciplines, linguistics, social sciences, cognitive psychology, and human performance. As a result, we can say that the goals of HCI are to examine the humans directly manipulating an interface, whether physical or graphical in nature to further develop some particular system or subset of systems. Some of the general criteria for successful HCI were described by Johnston et al. (2003) as shown in Table 14.

Table 14. Criteria for a successful HCI Johnston et al. (2003)

No.	Criteria	Description
2	Visibility of system status	User must be able to observe the internal state of the system. This can be achieved by the system providing correct feedback within a reasonable time.
3	Match between system and the real world	An HCI which uses real-world metaphors is easier to learn and understand. This will assist a user in figuring out how to successfully perform tasks
4	User control and freedom	System functions are often chosen by mistake. The user will then need a clearly marked exit path
5	Consistency and standards	Words, situations and actions need to be consistent and have the same meaning. A list of reserved words can assist in this area

(continues)

APPENDIX 5. (continues)

Table 14. Criteria for a successful HCI Johnston et al. (2003) –continued

6	Error prevention	It is obviously best to prevent errors in the first place through careful design. However, errors do occur and they need to be handled in the best possible way.
7	Recognition rather than recall	The user should not have to remember information from one session to another. Rather, the user should be able to 'recognize' what is happening.
8	Flexibility and efficiency of use	The system should be efficient and flexible to use. Productivity should be increased a a user learns a system. The system should not control the user; rather, the user should dictate which events will occur. The system should be suitable for new and power users.
9	Aesthetic and minimalist design	Information which is irrelevant should not be bombarded with information and options.
10	Help users recognize, diagnose and recover from errors	Errors messages need to be clear and suggest a solution
6	Error prevention	It is obviously best to prevent errors in the first place through careful design. However, errors do occur and they need to be handled in the best possible way.
7	Recognition rather than recall	The user should not have to remember information from one session to another. Rather, the user should be able to 'recognize' what is happening.

APPENDIX 6. Human-Computer Interaction Security

Until now, few of the known examples of the research based and later commercialized major technologies were described. Human-Computer Interaction Security (HCISec) as mentioned by Johnston et al. (2003) means “the part of a user interface which is responsible for establishing the common ground between a user and the security features of a system. HCISec is human computer interaction applied in the area of computer security”. In a sense, HCISec is an extension of HCI, where instead of only focusing on making the human-computer interaction more users friendlier, easy to learn and efficient, the focus is also on the security aspects.

The scope and focus of interest in human-computer interaction security could be related to authentication (biometric systems, passwords), security operations (threat and risk detection, intrusion detection, vigilance, policies and practices) and development of secure systems. The concept of usable security or usability security is rooted in the early advancements and research into computer security and protection of information and data for example one of the early publications in the field of information security was published by Jerome H. Saltzer and Michael D. Schroder (1975) in their “The Protection of Information in Computer Systems” journal.

According to Sasse et. al. (2003), one of the concerns in HCI-S is that the security communities tend to implement and design the systems based on the occurred threats and risks as a consequence of budgetary limitations. This has also lead to an assumption that the costs associated with early savings in the implemented security mechanisms lead to later costs in terms of used resources to maintain the secure system.

Also, Ka-Ping Yee (2002) noted in his “User Interaction Design for Secure Systems” that security of any system depends on human operation and configuration based on the outputted information for the users so that users can make decisions and based on their interpretations provide input for the system. Additionally, Ka-Ping Yee (2002) emphasized the trend among system designers that improved security degrades the usability and vice-versa.

(continues)

APPENDIX 6. (continues)

Similarly Johnston et al. (2003) identified six factors related to the HCI-S concerns namely conveyance of security, visibility of system status, learnability, aesthetic and minimalist design, satisfaction, and trust which could be taken into account when designing a system, where safety factors need to be taken into account.

However, everyone in the academia does not share the notion that usable and secure systems exist. For example, Dewitt et. al. (2006) mentioned that some systems cannot be considered both usable and secure at the same time, but emphasized the early stage of the current HCI-SEC research.

Likewise, according to Smith (2003) there is a known problem though in the field of HCI-S like how to make computer systems friendlier, while maximizing the security aspects. For example, how to design and implement a safety-critical system, where the users have to remember long, regularly changeable, complex, unique passwords (not repeatable) in addition to not being allowed to write them down. As a consequence, security concerns have a negative impact on the usability. As a result, system engineers need to balance and optimize between friendliness, usability and security so that inadequate user interfaces do not result in security loops and high security mechanism do not result in a bad user interface.

Even with a strong security mechanism in place, the system can become insecure since the users could find the system too difficult to be used in a correct way (Whitten, 1999) and as a consequence leads to security loopholes in the used system and associated systems through inadequate security system configuration in terms of functionality like firewalls, encryption and access controls (Stephano et. al., 2006), due to reasons like poor usability design in security aspects for example hard to use interfaces (small input devices/interfaces, combinatory user ID and password authentication) and understandability of the given interface information (asterisk display format for login information) (Steofanos et. al., 2011). Similarly, in the airport context the long waiting lines in airport checkpoints is a source of unsatisfied travelers.

(continues)

It is a well-known problem that security and usability are into conflicts when deploying a new a new security technology in airports. Maintaining an acceptable compromise between these factors is not an easy task. As a consequence, a system that is secure but difficult to use and learn will not be used. A system that supports a high level of usability but is not secure will not be used either. Therefore, usability and security should be designed in harmony and a tradeoff between these two factors should be explicitly considered.

Thus, the focus on the humans as important elements in the whole process link has to be taken also into consideration as part of the designed system in order to make it safe so that security and usability would not be regarded as two opposite goals in the system design, especially when the problem space takes into account various systems, where the systems have been designed as single points in the whole process chain to achieve a particular goal for example in the airport context.

We can say that whether our focus would be in designing systems for the passengers or the airport security; the important concept is the study of how the humans closely interact with IT systems to achieve a particular goal.

Although, HCI has its limitations in that it is based on incremental improvement and design of one particular systems visual design, interaction design, and usability rather than taking a complete organizational viewpoint of the business processes and other technologies; it has its own purpose in the layered approach in the context of design thinking. Furthermore, while human-computer interaction and security enhance incremental, creative and innovative solutions; design thinking approach could affect the whole organizational processes.

We could argue that the gap between the human-computer interaction, human-computer interaction security, and design thinking, could mean that these three could be complementary tools and methods in achieving the highest performance, usability, and security as shown in the Fig. 13, despite the fact that there are similar tasks in design thinking and human-computer interaction design.

(continues)

APPENDIX 6. (continues)

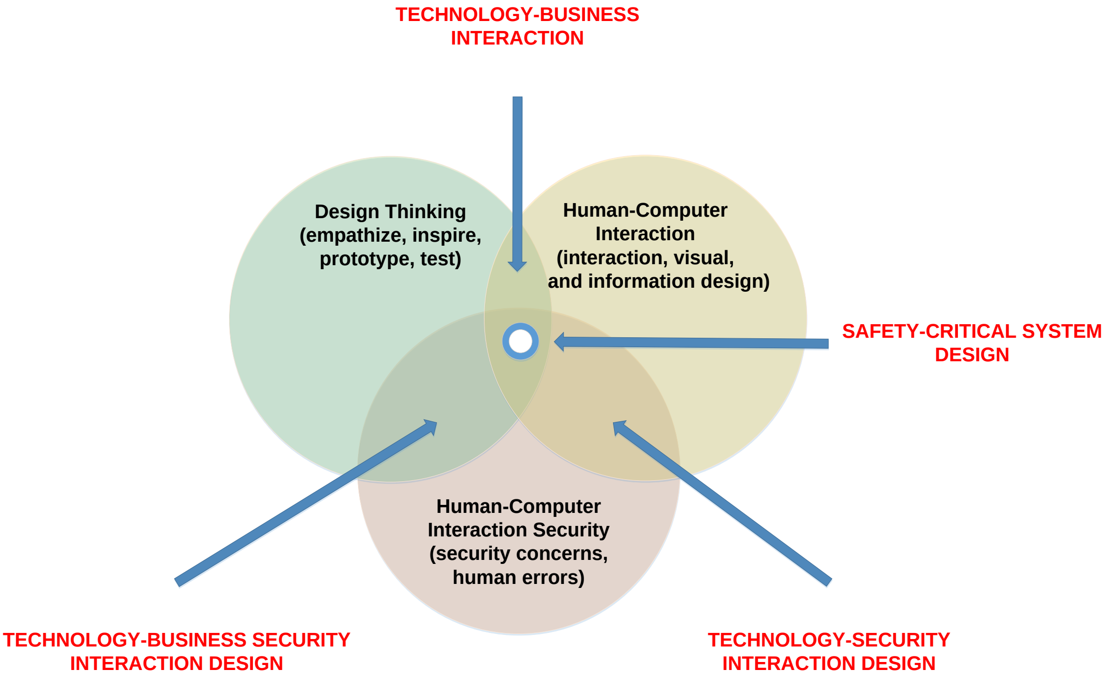

TECHNOLOGY-BUSINESS INTERACTION
Design Thinking (empathize, inspire, prototype, test)
Human-Computer Interaction (interaction, visual, and information design)
SAFETY-CRITICAL SYSTEM DESIGN
Human-Computer Interaction Security (security concerns, human errors)
TECHNOLOGY-BUSINESS SECURITY INTERACTION DESIGN
TECHNOLOGY-SECURITY INTERACTION DESIGN

Fig. 13. Three Design Methodology Approach

APPENDIX 7. Passenger Story Telling

A possible story telling scenario could be like the following. The passenger journey begins by arriving to or near the airports international departure flight terminal either by bus, car, taxi, or train. If the passenger arrives by car and wants a long-term parking service, the journey continues to this phases parking zone, where the first technical factor is the automated entry station. The passenger will get a parking coupon at the station/barrier, before entering into the parking space. If the CCTV cameras are installed in and around the parking zone, the car might be tracked with a license number plate recognition (LPR) or Automated Vehicle Identification (AVI) systems. When the car is parked in the parking zone, the passenger will move into the terminal building for international departing flights.

When arriving in the terminal building different general factors and elements that are not directly related to passenger journeys are ATMs, money exchange desks, shops, travel services (tax free refunds etc.), cafeterias/restaurants, lavatories, regional tourist information desks, airport information desks, airport travel cargo (airfreight and messenger services), taxi service desks, lounges, congress areas, elevators, escalators, moving walkways, people mover systems, Wi-Fi, and wayfinding systems. Diverse range of passengers might have different priorities and needs for the usage of the airport services, but the assumption for this case report is that the first thing that the passenger will want to do is to look up for their flights check-in time for luggage handover and boarding pass from the multi-user flight information display system (MUFIDS). Meanwhile, when the passenger has entered the building; he or she is being monitored by the closed circuit television (CCTV) system throughout their stay in the airport building, which is used for surveillance and transmits video through cameras to operator monitors and/or digital video recorders. When the check-in time has started, the passenger will be notified by the passenger paging system and there is two ways how the passenger can proceed. The two different ways are through personal service counters or self-service kiosks.

In the case of personal service counters, the passenger moves on to the queue for the check-in counter. In the check-in desk, the passenger moves to put the luggage's on the conveyor belt (handled by baggage handling or reconciliation, sortation, and tracking (continues) system) and hands out the passport for the human operator (airline staff or handling agent). The human operator checks the weight of the baggage, prints out the baggage tags with the baggage tag printer (BTP) and the boarding cards with the common use terminal equipment (CUTE), which provides the capability of multi-tenant operating environment i.e., the system feels and looks like the tenants own IT systems. The boarding cards will be given to the passenger, which will be used to proceed through the security checkpoint and into the airplane. Meanwhile, the baggage handling system has a point, where the baggage is checked for explosives, dangerous materials and illegal equipment by the baggage screening system.

For an automated service, the passenger moves in front of a self-service kiosk. The passenger will choose the airline company and type the e-ticket information on the screen, where the output will be printed boarding passes and baggage tags, which the passenger will attach to their luggage.

Afterwards, the passenger moves on to the self-service baggage drop / baggage drop off kiosk, where the first action is to have the boarding card scanned by the automated machine. The passenger moves on to put the baggage on the conveyor belt for weighting and scans the baggage tag either with the help of the airport or airline employees or independently. When the luggage’s are moving on the conveyor belts, they are managed by the baggage handling system (BHS), which sorts the baggage based on tags and diverts them to their intended destinations.

When the passenger has received their boarding cards and handed their luggage’s, the next step for the passenger is to move through the SCCP. The first element that the passenger will encounter before the security checkpoint is the automated wait time (AWT) system. The AWT system provides passengers the average time that takes to go through the security checkpoint either on-screen or/and available on mobile phones, tablets, and other browser enabled devices. The elements in the AWT system are sensors, wait time servers, and flat panel TV screens.

(continues)

APPENDIX 7. (continues)

Afterwards, the passenger proceeds to the pre-screening preparation instruction zone. The passenger is instructed in the pre-screening preparation zone for the SSCP by using signage, posters, instructional videos, and staff to provide a more calming environment and efficient screening.

Then, the passenger has to go through the travel document checker (TDC) device before queuing for the security checkpoint. There is also an alternative passenger flow, which will be covered later and are called ADA/access gates. The elements in the pre-screening preparation zone are signs, posters, instructional videos, staff, and passengers. After the pre-screening preparation zone, the passenger moves to the queue.

In the queue, the passengers stand in line in front of the security checkpoint (non-sterile side). The queue parameter is managed by barrier, -single, or -double strap queuing stanchion lanes from the TDC to the checkpoint. The elements in queue are stanchions and passengers. In the end of the queue, the passenger encounters the divest tables and bin carts with additional signs with instructions.

The passenger uses bin carts (gray containers) located at front and end of each checkpoint lane, to divest themselves of their personal belongings such as purses, carry-on bags, backpacks, laptops, shoes, jackets, etc. Divest tables are used for bins to be put side-by-side. When the passenger has unloaded their personal belongings from their carry-on baggage in the bin carts; they will move (with assistance or by themselves) the bin carts on the x-ray machines entrance roller and slowly move the bin carts to the automated queuing conveyor (hooded) and scanning belt, which will slowly move the bin cart to the X-Ray’s dome from non-sterile side to the sterile side. On the operator's (staff) side the monitors (workstation) that will show the bag content and cabinets for further trace examination are located. The position of the cabinets and workstation is manufacturer and model specific, but typically two monitors, keyboard, pc tower, and cabinets are included in every model. Also, next to the operator workstation, the Manual Divert Roller (MDR) is located that is used for suspicious bag pull, when an alarm is triggered that will be taken to the

(continues)

APPENDIX 7. (continues)

secondary screening area for further investigation. The elements in the x-ray screening phase are the x-ray machine, operator workstations, cabinets, x-ray operators (staff), other assisting staff, and passengers.

When the passenger has unloaded their belongings and bags for X-Ray machine screening; they will have to move through the walk through metal detector (WTMD), which is used for screening passengers for potential weapons and hazardous items. If the WTMD alarm is triggered, the passenger will be screened manually with hand-held metal detectors and staff. By moving the hand-held metal detector close to a passenger's body, the staff can accurately locate sources of conductive materials that may be on/in the passenger's body. When conductive material is detected, the hand-held metal detector will alarm. The responsibility of the staff is to judge whether the alarm was something to be suspicious about, investigate and determine the cause of it. If the staff is still suspicious of the passengers, the staff will move the passenger to a containment room. The elements in the walk through metal detector screening are WTMD, passengers, staff for manual search (hand-held metal detector).

If the passenger has suspicious characteristics and/or the walk through metal detector alarmed, the passenger could be taken into a containment/private room for further screening. Containment rooms are located near the security checkpoints that are used to contain and isolate the passenger for further private / thorough screening and investigation and the elements are containment/private rooms, staff, and the passenger.

If the passengers had their bag alarmed in the x-ray screening, they will move to a secondary screening area from this phase. The secondary screening area is required for passengers that had a bag that alarmed in the primary screening area. This particular area is situated either at the end of the screening lane or at the sides. This area can have Mobile Security Cabinets, which are secured and vented that contain Explosive Trace Detection (ETD) equipment and Bottle Liquid Scanners (BLS) and bag search tables, but the equipment might not necessarily be inside the mobile cabinets, which are secured and vented that contain Explosive Trace Detection (ETD) equipment and Bottle Liquid Scanners (BLS) and bag search (continues)

APPENDIX 7. (continues)

tables, but the equipment might not necessarily be inside the mobile cabinets. The elements in the secondary screening area are ETDs, BLSs, mobile security cabinets, and bag search tables.

There is also another element in the airports for passengers and staff, which is called ADA and/or Access gates. Access Gates are used to separate the sterile from non-sterile areas and limit the access between different roles working in the airports. ADA/Access gates are also used to provide a more direct traverse for passengers with disabilities (wheelchair passengers, passengers requiring special assistance, and passengers with pacemakers) and staff (free travel path that is clear of passengers. The access gates can be operated only by the authorized personnel with authorization/authentication rights. When the passenger is clear of the body and carry-on baggage screening, they will move to compose their belongings from the x-ray conveyor belt bins and proceed to the egress seating area for further composing of their belongings and leave the security checkpoint from the exit lanes.

After the security checkpoint, the passengers are on the sterile side of the airport and can access their flight specific gates. On some flights, for example in European Union from a Schengen to a Non-Schengen destination and back will have a mandatory passport control in which case, the passenger will have to move through the control to get to their flight specific gates, where there can be staff (border control) with their own workstations and systems to authenticate the passengers and the motives. Whether the case has a passport control or not the passenger will move near the boarding gates, where the boarding on the flight will occur. From the airlines point of view the process of how the gates are assigned is through the resource and gate management system, which allocates gates and passenger processing resources to airline tenants. Before the passenger boards the plane, the boarding pass/card, will be checked and validated by the desk counter staff manually or by using a travel document checker (TDC) and the CUTE system. One half of the boarding card will be teared (which has the seat and related flight information) and given to the passenger, before he/she moves into the aircraft.