STPA for Safety, Security and Privacy in Smart Airport Terminal New Concepts

2020 MIT STAMP/STPA Workshop

Idaldo Lima, Max Schwienhorst, Johannes Reichmuth
4 August 2020

Institute of Transport Science
Chair of Air Transport and Airport Research
RWTH Aachen University
Better comprehend and constraint safety, security and privacy in future technology-intensive airport terminal operating concepts, through a System Theory based hazard analysis (using STPA), using the UTA departing passenger processing concept case study, and provide adequate constraints for this future system.
Safety, Security and Privacy in Future Airports

Motivation

1. Future airports are **tech-intensive critical infrastructures**
   Clear **technological push** for future systems
   more complex, integrated and software intensive

2. **No longer only safety** problems
   Leads to major concerns in terms of **security and privacy**
   e.g. user intent, personal data (PII), proprietary data (PD), non-recovery, reputation, critical scenarios, ...

3. Traditional understanding of hazard become **ineffective and obsolete**
   The **Swiss Cheese Model**: enchainment of failure events
   analytical decomposition, statistics, human error, interactions, organizational aspect, ...
Safety, Security and Privacy in Future Airports

Case: the Uniform Terminal Area Concept

- The External border control problem
  - Regulatory **physical separation of passenger flows** in gate
    - Unnecessary cost and complexity

- Modern technologies for unbundling of passenger flows
  - Estimated benefits in capacity, workload, costs, service and security levels
possible solutions

- **reversible gate areas**  
  (e.g. CGN, GIG)

- **different floors or terminals**  
  (e.g. MUN, ATL)
Main challenges:

- a **technical solution** must be defined
- the **benefits** must be quantified
- a **legal framework** must be established

### Step 1:
@Security Control
Enrollment of all departing PAX (facial recognition)

### Step 2:
(if applicable)
@Border Control
Updating the individual dataset regarding exit permission

### Step 3:
@Boarding
Check individual permission to enter the plane (boarding pass & emigration)
Safety, Security and Privacy in Future Airports

case: the Uniform Terminal Area Concept

- Our project:
  - a **technical solution** must be defined & **constrained**
  - the **benefits** must be **quantified**
  - a **legal framework** must be established

- **STPA** will yield constraint-basis for technical solutions and simulations and enable guidance to suitable legal framework **while** it is in conceptual phase
Safety, Security and Privacy in Future Airports

how we are doing it

**Problem Framework: Concept Analysis**
- Define System Boundary & Frame Problem
- Map Lifecycle Key Stakeholders & Interests
- Describe Goal & Concept of Operations
- Identify Unacceptable Losses
- Identify High Level Hazards & Constraints

**Functional Framework: Architectural Analysis**
- Identify Functional Elements & Components
- Assign Responsibilities & Key Activities
- Identify Hierarchical Control Relationships
- Infer Control Actions
- Identify Hazardous Control Actions

**Control Framework: Design Analysis**
- Trace Process Models & Necessary Feedback
- Identify Disruptive Loss Scenarios
- Wargame Hazard Control Strategies
- Draw Control Degradation Scenarios
- Track Assumptions, Limitations & Indicators
- Design Mitigating & Preventing Measures

**Outputs**
- Requirements & Constraints
- Functional Architecture
- Assumptions & Limitations
- Leading Indicators
System of Interest (SoI)
A system to promote identity control and processing of passengers in airport terminals by means of allowing or not access of passengers/users to controlled areas and keeping track of each passenger/user processing in each area during check-in, bag drop, boarding pass control, security control, passport/visa control and gate control (using biometrics/FR) in order to enable seamless passenger processing while maintaining profitable operations, minimizing risks to passengers, cargo, staff, equipment, infrastructure and society, protecting personal data (PII) and improving the airport's value and image as user-friendly.
Concept of Operations

Users: passengers, visitors, staff, airport operator

Likely Operation: proper access and processing control during (Check-in Online, Curbside, Landside Lounge,) Check-in Kiosk/Counter, Baggage Drop, Boarding Pass Control, Security Control, (Passport Control, Airside Lounge,) Gate Control, Aircraft Boarding, in this order

Key Assumptions: biometric automatic control will aid (or replace) the current system

Expected Capabilities: more capacity, assured safety, security, privacy, resilience, ...

Unacceptable Losses

L-1: loss of life, injury or health compromise
L-2: damage to equipment or infrastructure
L-3: disruption on processing or transport
L-4: stain to reputation

Obs.: due to unacceptable number or severity of safety, security or privacy issues qualification, quantification, and the act of unacceptance are made by responsible stakeholders
Safety, Security and Privacy in Future Airports
UTA case: concept analysis

Unacceptable Losses
L-1  loss of life, injury or health compromise
L-2  damage to equipment or infrastructure
L-3  disruption on processing or transport
L-4  stain to reputation

Hazards
H-1  Equipment or procedure entraps user during processing
H-2  State or Dynamic leads to damages on physical component
H-3  Unauthorized user is allowed through
H-4  Non-recovery from disruption / Recovery into a hazardous state
H-5  Unauthorized/unconsented disclosure/release of PII/PD
CA-2: Security Screening Control Officer request action or ID from Passenger.

CA-2.1  Come forward
CA-2.2  Go back
CA-2.3  Wait for Approval
CA-2.4  Present ID or Boarding Pass
CA-2.5  Undergo Facial ID Recog
CA-2.6  Answer enquiry
CA-2.7  Go through Gate
CA-2.8  Go to previous step
CA-2.5: Security Screening Control Officer requests Passenger to undergo facial ID recognition

1: not providing CA leads to hazard
2: providing CA leads to hazard
3: providing CA with wrong timing/order leads to hazard
4: providing CA with wrong duration leads to hazard

HCA-2.5-1.1 when Server is in Manual Mode, and FR-scanning is working
HCA-2.5-1.2 when PAX is not following Screen procedure
HCA-2.5-2.1 when Server is in Automatic Mode, and Server is correctly running
HCA-2.5-2.2 when ID check has already been approved
HCA-2.5-3.1 when PAX is not yet under ID-check procedure
HCA-2.5-3.2 when PAX has already gone through the Gate
HCA-2.5-4.1 when FR-screening is not yet completed
HCA-2.5-4.2 when FR-screening is long completed

processing function only, may also include security screening function (more privacy issues)
CA-2.5: Security Screening Control Officer requests Passenger to **undergo facial ID recognition**

**Decision Logic**

Issue CA-2.5 when:

- Server is in Manual Mode OR
- Server is not responding correctly OR
- PAX is not complying with Screen orientation

AND PAX is in the Gate

AND FR-ID-check is working

AND FR-ID-check must still be carried out

**Process Model Variables & Values**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server_mode</td>
<td>Automatic/Manual</td>
</tr>
<tr>
<td>Server_function</td>
<td>working/not-working</td>
</tr>
<tr>
<td>Screen_function</td>
<td>working/not-working</td>
</tr>
<tr>
<td>Scann_function</td>
<td>working/not-working</td>
</tr>
<tr>
<td>Gate_mode</td>
<td>Server/Officer/Manual</td>
</tr>
<tr>
<td>Gate_function</td>
<td>working/not-working</td>
</tr>
<tr>
<td>Gate_occupation</td>
<td>free/occupied</td>
</tr>
<tr>
<td>Gate_’Door’-mode</td>
<td>open/closed</td>
</tr>
<tr>
<td>Gate_entrapment</td>
<td>free/entrapped</td>
</tr>
<tr>
<td>PAX_location</td>
<td>in-line/in-gate/in-controlled-area</td>
</tr>
<tr>
<td>PAX_attitude</td>
<td>moving/in position</td>
</tr>
<tr>
<td>PAX_procedure-compliance</td>
<td>compliant/not-compliant</td>
</tr>
<tr>
<td>PAX_ID-checking</td>
<td>TBD/under-eval/approved/not-approved/conflict</td>
</tr>
<tr>
<td>PAX_checklist_correctness</td>
<td>coherent/incoherent</td>
</tr>
<tr>
<td>PAX_checklist_execution</td>
<td>coherent/incoherent</td>
</tr>
</tbody>
</table>
HCA-2.5-1.1: Security Screening Control Officer does not request Passenger to undergo facial ID recognition when Server is in Manual Mode, and FR-scanning is working [H1, H2, H3, H4] [L1, L2, L3, L4]

CS-2.5-1.1-1.3.3.3: Security Screening Control Officer does not request Passenger to undergo facial ID recognition when Server is in Manual Mode, and FR-scanning is working [HCA-2.5-1.1] due to its inadequate process model: Officer does not receive feedback status from Server when needed due to Server status feedback delay. [H1, H2, H3, H4] [L1, L2, L3, L4]

-> Server_function working/not-working delayed

-> Officer believes Server is still controlling Processing and does not issue CA
-> PAX can be delayed, or interpret this lack of orientation as a „go forward“

Might be a good idea to design a „door function“ for the Gate
HCA-2.5-1.1: Security Screening Control Officer does not request Passenger to undergo facial ID recognition when Server is in Manual Mode, and FR-scanning is working [H1, H2, H3, H4] [L1, L2, L3, L4]

Causal Scenarios

1: Hazardous Controller (Officer) Behavior
   1: Inadequate control algorithm (e.g. assumes user will wait for approval)
   2: Unsafe control input from another controller (e.g. missing coordination with Officer Supervisor)
   3: Inadequate process model (e.g. believes Server is in Automatic Mode and working fine)

2: Inadequate Feedback and Information (Status)
   1: Feedback or information not received (e.g. missing user procedure-compliance status)
   2: Inadequate feedback is received (e.g. FR-check is completed for the wrong user)

3: Inadequate Control Path (Screen/Verbal)
   1: Control action not received (e.g. screen does not request user to follow Officer instructions)
   2: Control action not forwarded (e.g. screen indicates FR-check is completed when it’s not)

4: Hazardous Controlled Process (Passenger/User) Behavior
   1: Control action not executed (e.g. user states/believes that FR-check in completed)
   2: Control action improperly executed (e.g. user spoofs FR-check)
Safety, Security and Privacy in Future Airports

Control Actions

Hazardous Control Actions

Control Actions

Hazardous Control Actions

+100 common SCs found at first run
Safety, Security and Privacy in Future Airports

design & verification cycle

Problem Framework: Concept Analysis
- Define System Boundary & Frame Problem
- Map Lifecycle Key Stakeholders & Interests
- Describe Goal & Concept of Operations
- Identify Unacceptable Losses
- Identify High Level Hazards & Constraints

Functional Framework: Architectural Analysis
- Identify Functional Elements & Components
- Assign Responsibilities & Key Activities
- Identify Hierarchical Control Relationships
- Infer Control Actions
- Identify Hazardous Control Actions

Control Framework: Design Analysis
- Trace Process Models & Necessary Feedback
- Identify Disruptive Loss Scenarios
- Wargame Hazard Control Strategies
- Draw Control Degradation Scenarios
- Track Assumptions, Limitations & Indicators
- Design Mitigating & Preventing Measures

Outputs
- Requirements & Constraints
- Functional Architecture
- Assumptions & Limitations
- Leading Indicators

Simulate integrated constraints with unruly users & violations
Safety & Security are most of the time **intertwined**

- Security & Privacy issues are **already critical from the beginning**
- **Resilience** (recovery from disturbance) should also be addressed
- User modeled as a **Controller with Intent** in process model
- **STRIDE & LINDDUN** classes integrated at **Wargaming**
- **Assumptions** are essential to ensure validity of the analysis

STPA application:

- **Interactive process**: between steps and design phases (questions raised)
- **Common Causes**: many scenarios are common and mitigatable by design
- Clear requirements: indicate also **paths for legal framework** change
- Process Models & Contraints: outcomes can be **easely simulated**
Thank you!

Idaldo Lima,
Max Schwienhorst,
Johannes Reichmuth

lima@via.rwth-aachen.de

Institute of Transport Science
Chair of Air Transport and Airport Research
RWTH Aachen University