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

2020 MIT STAMP/STPA Workshop

Idoaldo Lima, Max Schwienhorst, Johannes Reichmuth

4 August 2020

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

DAAD

Safety, Security and Privacy in Future Airports
Proposal

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**

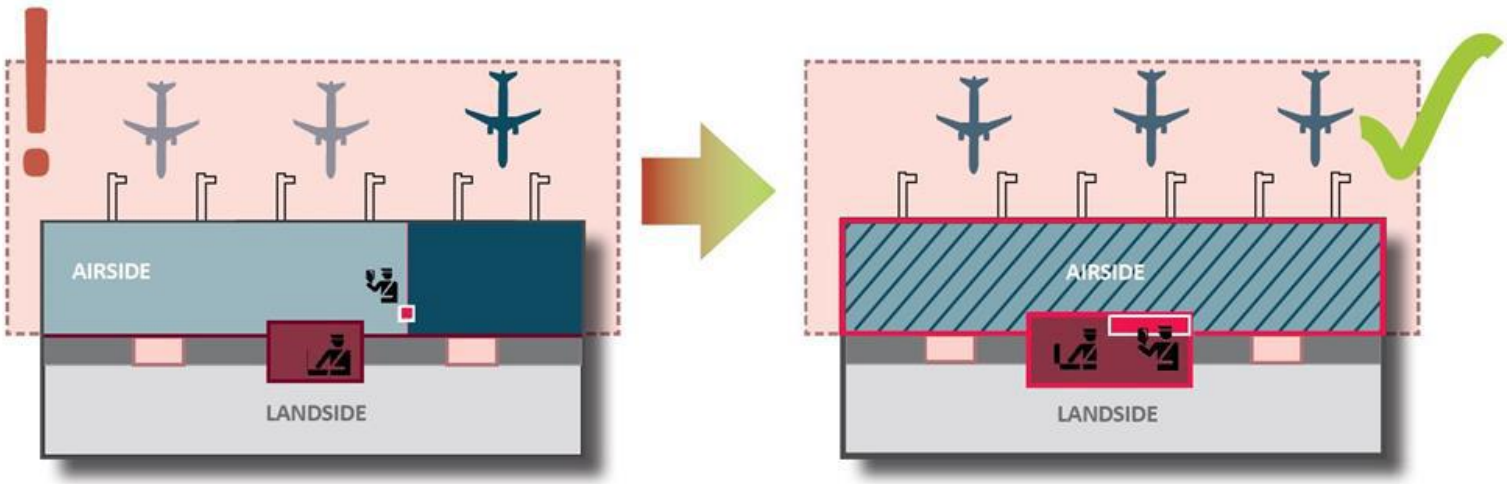
  The Swiss Cheese Model: enchainment of failure events

  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

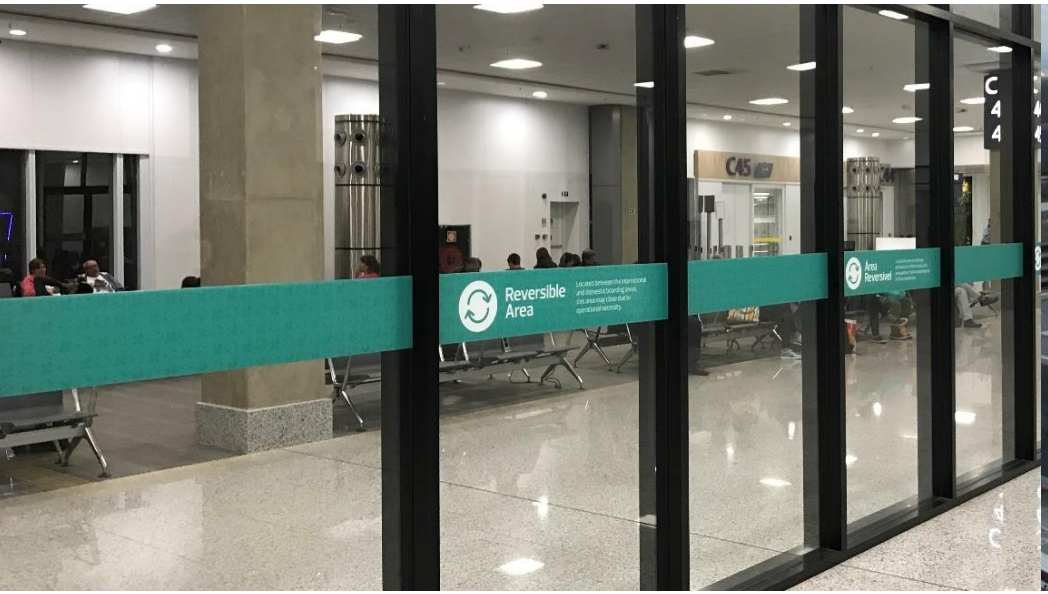
- **Modern technologies** for unbundling of passenger flows
  - Estimated benefits in capacity, workload, costs, service and security levels



possible solutions

- ***reversible gate areas***

(e.g. CGN, GIG)



- ***different floors or terminals***

(e.g. MUN, ATL)

Safety, Security and Privacy in Future Airports
case: the Uniform Terminal Area Concept

- 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:

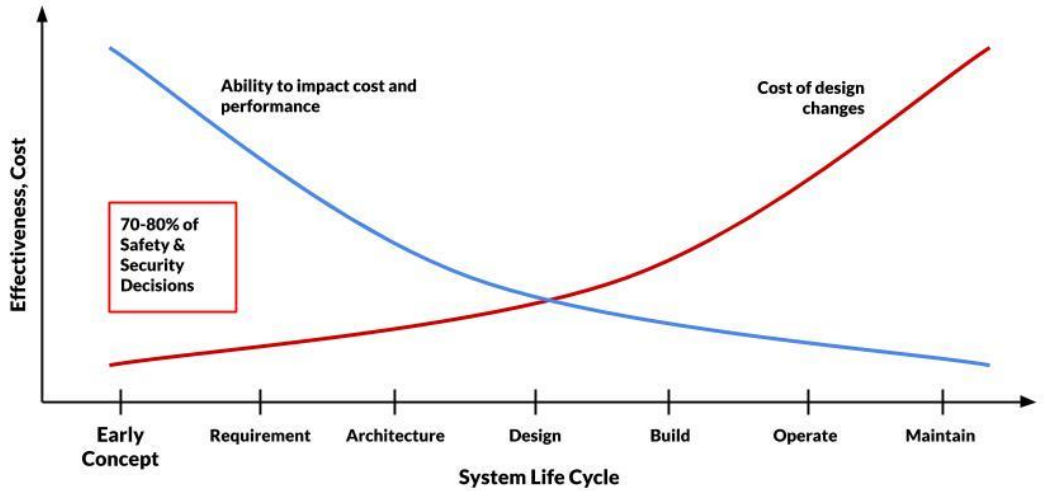
@Boarding

Check individual permission to enter the plane (boarding pass & emigration)

Safety, Security and Privacy in Future Airports
case: the Uniform Terminal Area Concept

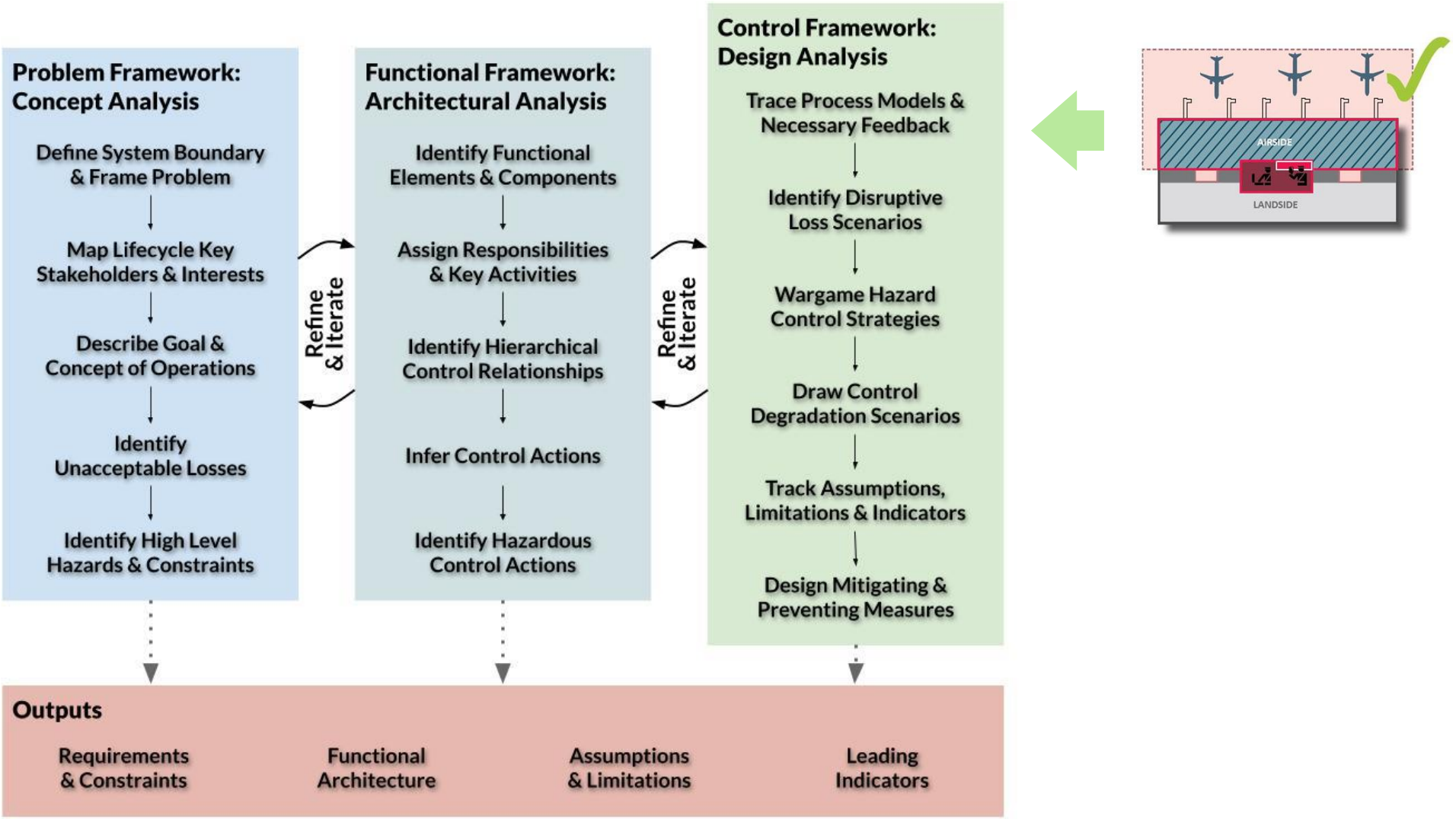
- Our project:
  - a **technical solution** must be defined **& constraned**
  - the **benefits** must be **quantified**
  - a **legal framework** must be established

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



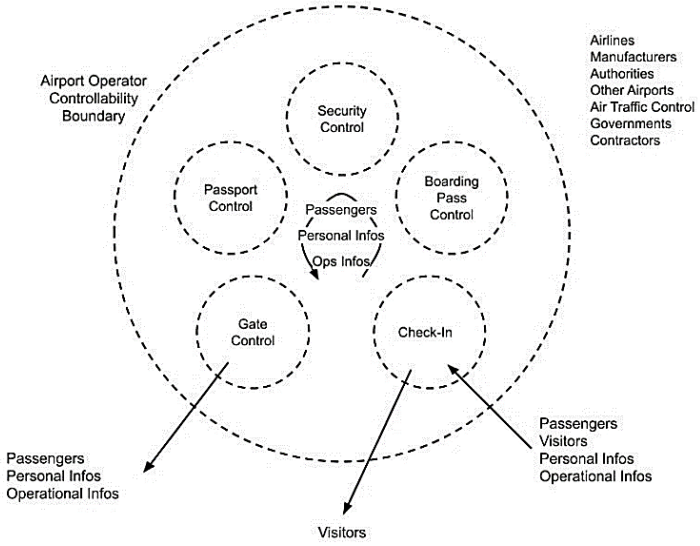
Safety, Security and Privacy in Future Airports

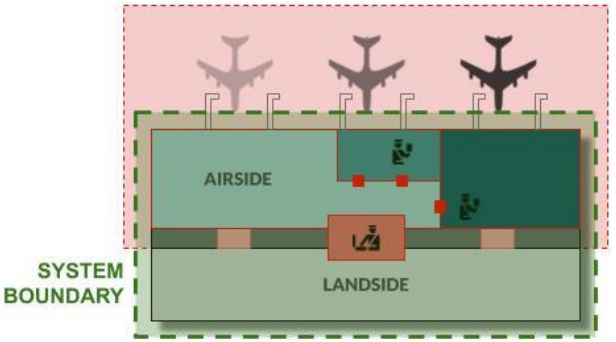
how we are doing it

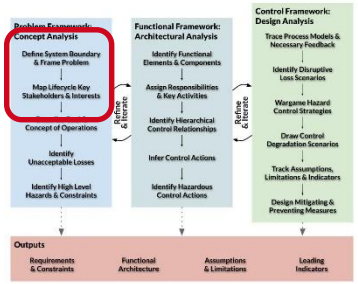


Safety, Security and Privacy in Future Airports

UTA case: concept analysis







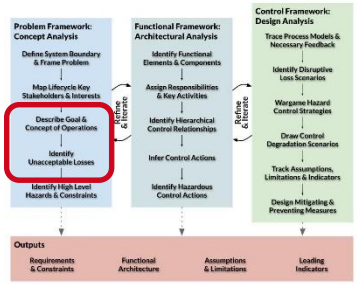
System of Interest (SoI)

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.

Safety, Security and Privacy in Future Airports
UTA case: concept analysis

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

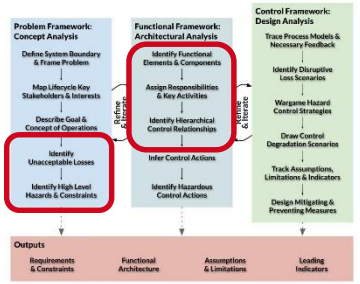
Obs.: due to unacceptable number or severity of safety, security or privacy issues qualification, quantification, and the act of unacceptance are made by responsible stakeholders

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

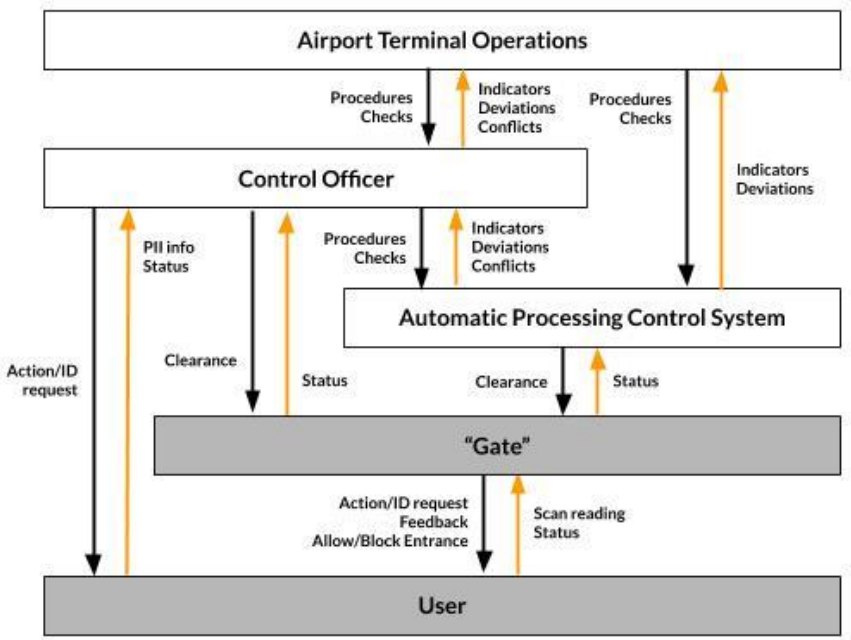
H-1 Equipment or procedure entraps user during processing

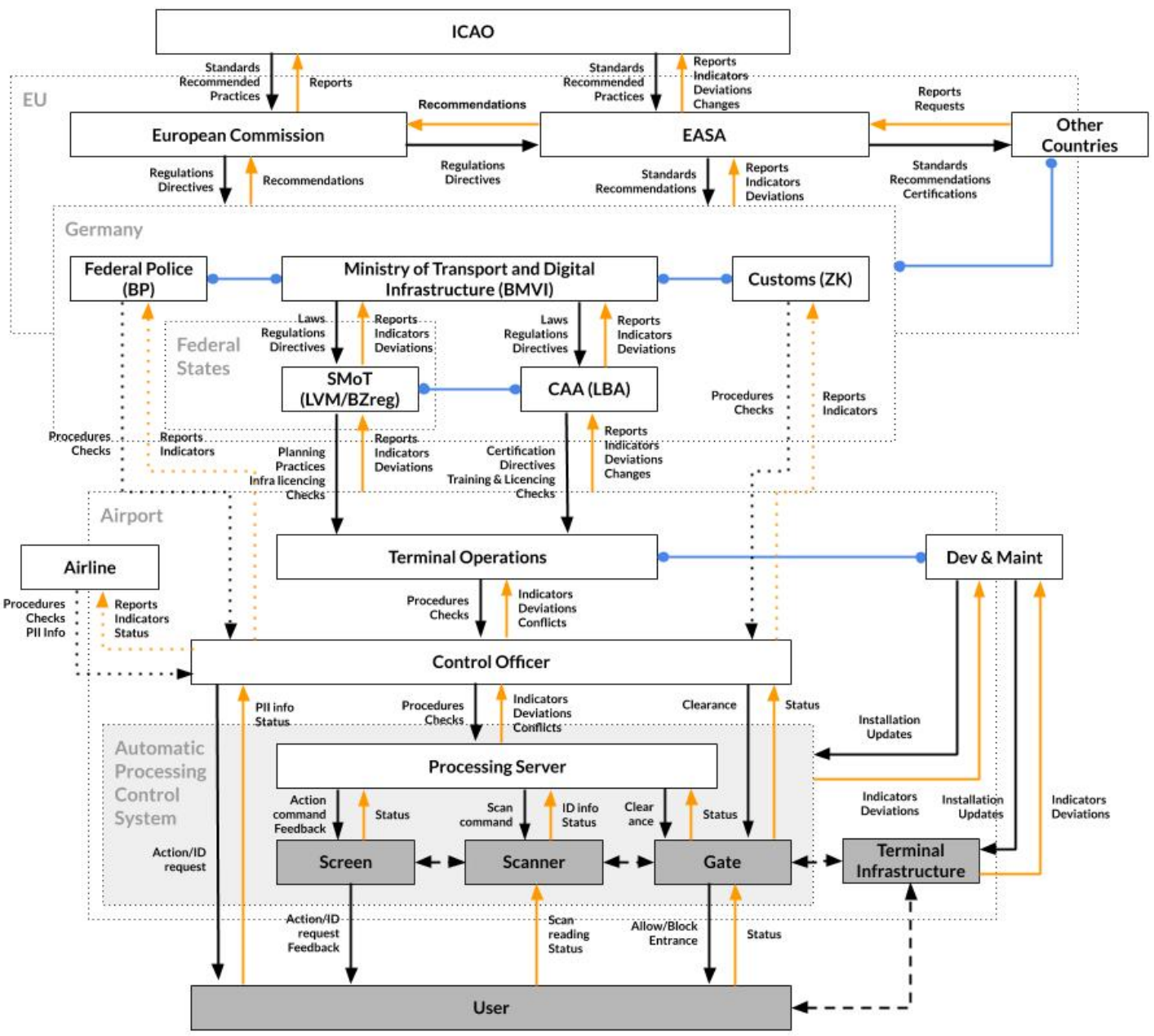
H-2 State or Dynamic leads to damages on physical component

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





Other Countries

- Schengen Country
- NonSchengen Country

Dev & Maint

- Infrastructure Construction
- Infrastructure Maintenance
- Software Developers
- Scan Tools Manufacture

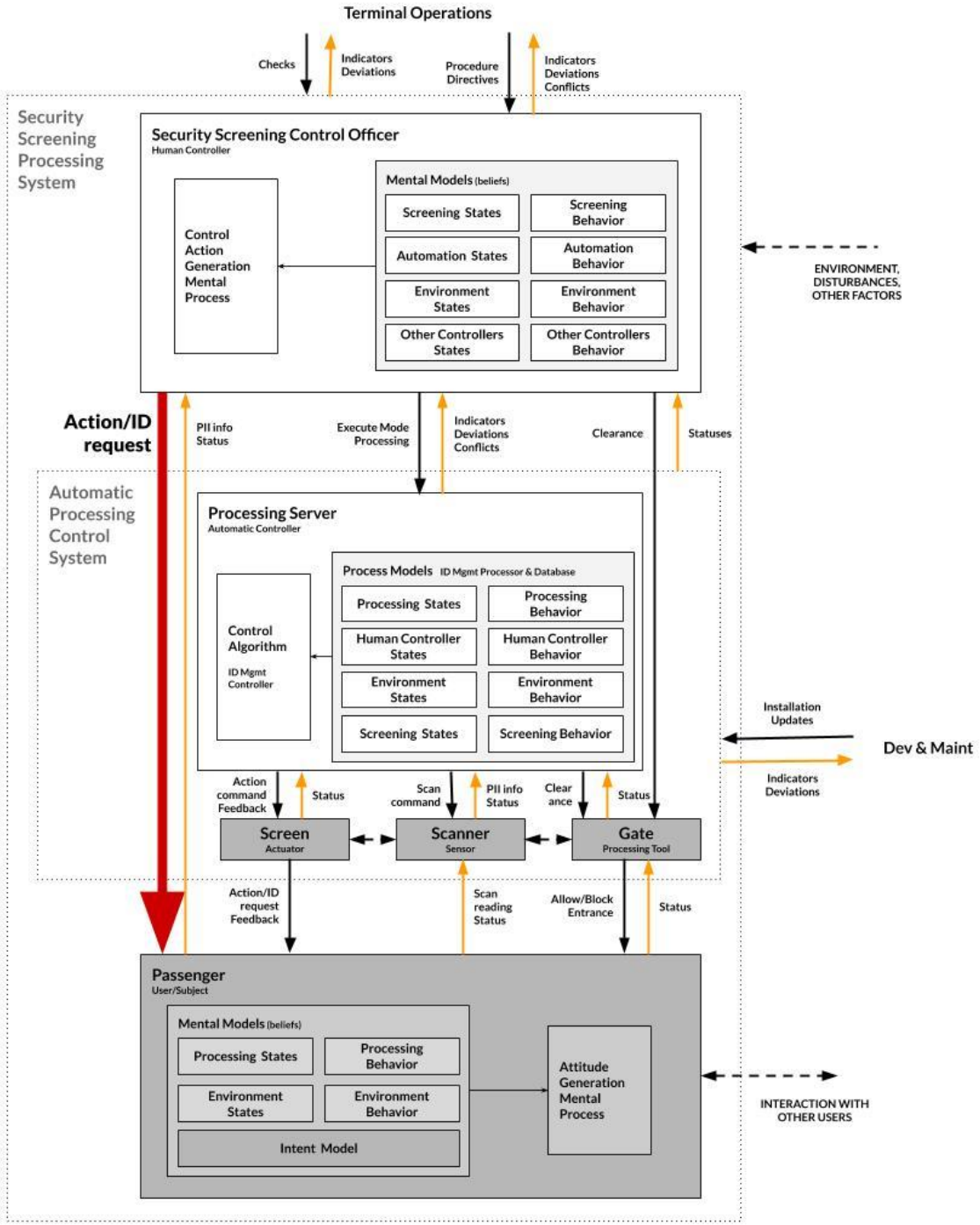
Control Officers

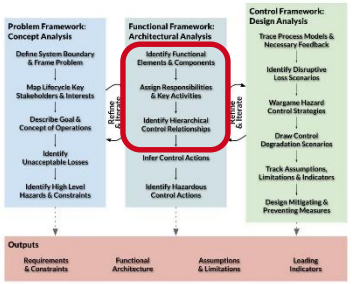
- Check-in Control
- Bag-drop Control
- Boarding Pass Control
- Security Screening
- Immigration Control
- Customs Control
- Boarding Control

User / Subject

- Staff
- Passenger
- Visitor
- Unruly User
- Other User

- Control Action
- Feedback
- Visual or Physical Contact
- Coordination
- xyz — Organizational Controller
- xyz — Physical Component
- xyz — Organizational Group





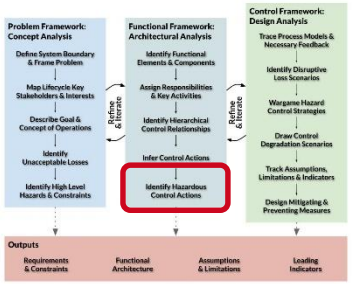
CA-2: Security Screening Control Officer request action or ID from Passenger.

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

Safety, Security and Privacy in Future Airports

UTA case: CA-2.5 example

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

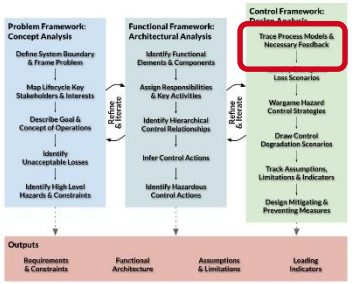
HCA-2.5-1.1	when Server is in Manual Mode, and FR-scanning is working
HCA-2.5-1.2	when PAX is not following Screen procedure
HCA-2.5-2.1	when Server is in Automatic Mode, and Server is correctly running
HCA-2.5-2.2	when ID check has already been approved
HCA-2.5-3.1	when PAX is not yet under ID-check procedure
HCA-2.5-3.2	when PAX has already gone though 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)

Safety, Security and Privacy in Future Airports

UTA case: CA-2.5 example

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

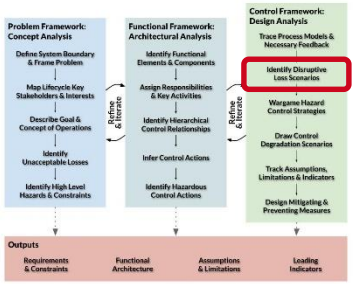
AND FR-ID-check must still be carried out

Process Model Variables & Values

Server_mode	Automatic/Manual
Server_function	working/not-working
Screen_function	working/not-working
Scann_function	working/not-working
Gate_mode	Server/Officer/Manual
Gate_function	working/not-working
Gate_occupation	free/occupied
Gate_'Door'-mode	open/closed
Gate_entrappment	free/entrapped
PAX_location	in-line/in-gate/in-controlled-area
PAX_attitude	moving/in position
PAX_procedure-compliance	compliant/not-compliant
PAX_ID-checking	TBD/under-eval/approved/not-approved/conflict
PAX_checklist_correctness	coherent/incoherent
PAX_checklist_execution	coherent/incoherent
[…]	

Safety, Security and Privacy in Future Airports
UTA case: HCA-2.5-1.1 example

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]

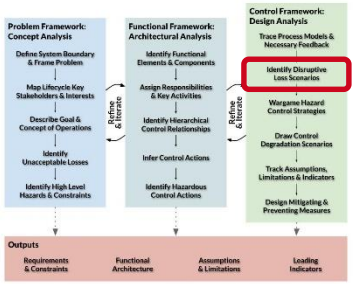
-> Server_function working/not-working **delayed**

-> 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

Safety, Security and Privacy in Future Airports
UTA case: for example

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)

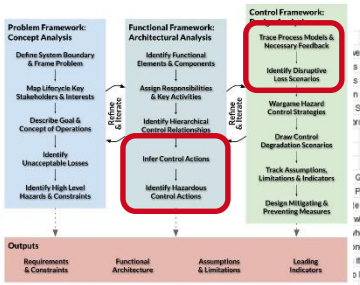
Safety, Security and Privacy in Future Airports
formal STPA

Control Actions

CA#	General	Specific	Controller	Verbal Form	Information For	Controlled	Statement
CA1	Execute Processing		Security Screeni	commands	to execute proce	Processing Serve	Security Screening Co
CA1.1		Automation	Security Screeni	commands	to execute proce	Processing Serve	Security Screening Co
CA1.2		Manual/Disable	Security Screeni	commands	to cease executi	Processing Serve	Security Screening Co
CA2	Request Action or ID				Action or ID	Passenger	Security Screening Co
CA2.1		Come forward	Security Screeni	request	to come forward	Passenger	Security Screening Co
CA2.2		Go back	Security Screeni	request	to go back	Passenger	Security Screening Co
CA2.3		Wait for Approval	Security Screeni	request	to wait for approv	Passenger	Security Screening Co
CA2.4		Present ID or Boa	Security Screeni	request	to present ID	Passenger	Security Screening Co
CA2.5		Facial ID Recog	Security Screeni	request	to present facial	Passenger	Security Screening Co
CA2.6		Answer enquiry	Security Screeni	request	to answer enquir	Passenger	Security Screening Co
CA2.7		Go through Gate	Security Screeni	request	to through Gate	Passenger	Security Screening Co
CA2.8		Go to previous pr	Security Screeni	request	to go to previous	Passenger	Security Screening Co
CA3	Display Command or Feedback		Processing Serve	command	to display	Screen	Processing Server con
CA3.1		Go forward	Processing Serve	command	to display 'go for	Screen	Processing Server con
CA3.2		Go back	Processing Serve	command	to display 'go bac	Screen	Processing Server con
CA3.3		Wait for Approval	Processing Serve	command	to display 'wait fo	Screen	Processing Server con
CA3.4		Present ID or Boa	Processing Serve	command	to display 'preser	Screen	Processing Server con
CA3.5		Facial ID Recog	Processing Serve	command	to display 'underg	Screen	Processing Server con
CA3.6		Wait for Assistan	Processing Serve	command	to display 'wait fo	Screen	Processing Server con

Hazardous Control Actions

Related CA#	Controller	Verbal Action	Controlled	Info Action	HCA Type#	Type 1	Type 2	HCA#	Context	Rationale	Related H#	Related
CA2	Security Screeni	request	Passenger	Action or ID	1: not providing	does not	-	HCA-2-1	when Server is in risk of missing fli		[H4.3]	[L3, L4]
CA2	Security Screeni	request	Passenger	Action or ID	2: providing	does	-	HCA-2-2.1	when Server is in potential conflict		[H1, H2, H3, H4]	[L1, L2,
CA2	Security Screeni	request	Passenger	Action or ID	2: providing	does	-	HCA-2-2.2	when Server is in M anual Mode, Pi		[H1, H2, H3, H4]	[L1, L2,
CA2	Security Screeni	request	Passenger	Action or ID	3: wrong timing	does	too early	HCA-2-3.1	when Server is in assuming the sy		[H1, H2, H3, H4]	[L1, L2,
CA2	Security Screeni	request	Passenger	Action or ID	3: wrong timing	does	too late	HCA-2-3.2	when Server is in assuming if there		[H1, H2, H3, H4]	[L1, L2,
CA2	Security Screeni	request	Passenger	Action or ID	3: wrong timing	does	in the wrong orde	HCA-2-3.3	when Server is in assuming if the p		[H1, H2, H3, H4]	[L1, L2,
CA2	Security Screeni	request	Passenger	Action or ID	4: wrong duratio	does	but stops it too s	NA		depends on the specific CA		
CA2	Security Screeni	request	Passenger	Action or ID	4: wrong duratio	does	but for too long	NA		depends on the specific CA		
CA2.1	Security Screeni	request	Passenger	to come forward	1: not providing	does not	-				[H4.3]	[L3, L4]
CA2.1	Security Screeni	request	Passenger	to come forward	1: not providing	does not	-				[H4.3]	[L3, L4]
CA2.1	Security Screeni	request	Passenger	to come forward	2: providing	does	-	HCA-2-1-2	when Gate is not potential conflict		[H1, H2, H3, H4]	[L1, L2,
CA2.1	Security Screeni	request	Passenger	to come forward	3: wrong timing	does	too early	HCA-2-1-3.1	when Gate is free there can only be		[H1, H2, H3, H4]	[L1, L2,
CA2.1	Security Screeni	request	Passenger	to come forward	3: wrong timing	does	too late	HCA-2-1-3.2	when PAX has already gone thoug		[H4.3]	[L3, L4]
CA2.1	Security Screeni	request	Passenger	to come forward	3: wrong timing	does	in the wrong orde	HCA-2-1-3.3	when the PAX pr assuming if the p		[H1, H2, H3, H4]	[L1, L2,
CA2.1	Security Screeni	request	Passenger	to come forward	4: wrong duratio	does	but stops it too s	HCA-2-1-4.1	when PAX has al assuming these		[H1, H2, H3, H4]	[L1, L2,
CA2.1	Security Screeni	request	Passenger	to come forward	4: wrong duratio	does	but for too long	HCA-2-1-4.2	when PAX has al PAX could misun		[H1, H2, H3, H4]	[L1, L2,
CA2.2	Security Screeni	request	Passenger	to go back	1: not providing	does not	-	HCA-2-2-1	when Gate is not security & privac		[H1, H2, H3, H4]	[L1, L2, L3, L4]
CA2.2	Security Screeni	request	Passenger	to go back	1: not providing	does not	-	HCA-2-2-1.2	when Gate is not threat related to		[H1, H2, H3, H4]	[L1, L2, L3, L4]
CA2.2	Security Screeni	request	Passenger	to go back	2: providing	does	-	HCA-2-2-2	when Gate is not potential conflict		[H1, H2, H3, H4]	[L1, L2, L3, L4]
CA2.2	Security Screeni	request	Passenger	to go back	3: wrong timing	does	too early	HCA-2-2-3.1	when Gate is free there can only be		[H1, H2, H3, H4]	[L1, L2, L3, L4]
CA2.2	Security Screeni	request	Passenger	to go back	3: wrong timing	does	too late	HCA-2-2-3.2	when PAX has already gone thoug		[H4.3]	[L3, L4]
CA2.2	Security Screeni	request	Passenger	to go back	3: wrong timing	does	in the wrong orde	HCA-2-2-3.3	when the PAX pr assuming if the p		[H1, H2, H3, H4]	[L1, L2, L3, L4]
CA2.2	Security Screeni	request	Passenger	to go back	4: wrong duratio	does	but stops it too s	HCA-2-2-4.1	when PAX has al assuming these		[H1, H2, H3, H4]	[L1, L2, L3, L4]
CA2.2	Security Screeni	request	Passenger	to go back	4: wrong duratio	does	but for too long	HCA-2-2-4.2	when PAX has al PAX could misun		[H1, H2, H3, H4]	[L1, L2, L3, L4]
CA2.3	Security Screeni	request	Passenger	to wait for approv	1: not providing	does not	-	HCA-2-3-1.1	when ID check is risk of security o		[H1, H2, H3, H4]	[L1, L2, L3, L4]
CA2.3	Security Screeni	request	Passenger	to wait for approv	1: not providing	does not	-	HCA-2-3-1.2	when PAX is not threat related to		[H1, H2, H3, H4]	[L1, L2, L3, L4]
CA2.3	Security Screeni	request	Passenger	to wait for approv	2: providing	does	-	HCA-2-3-2	when ID check h risk of missing fli		[H1, H2, H3, H4]	[L1, L2, L3, L4]



Feedbacks

Process Model Variables	Necessary Information	Feedback	Source	Sensor/Update
Server_mode	State, Behaviour Reference	Server Mode State	Server	Monitor
		Server Mode Transitioning Referen	higher level of hierarchy, training, e	Monitor, Training, Procedure
Server_function	State, Behaviour Reference	Server Functioning State	Server, hier level of hierarchy	Monitor, Training, Procedure
		Server Functioning Reference	higher level of hierarchy, training, e	Monitor, Training, Procedure
Screen_function	State, Behaviour Reference	Screen Functioning State	Server, Screen	Monitor, Visual-Screen
		Screen Functioning Reference	higher level of hierarchy, training, e	Monitor, Training, Procedure
Scann_function	State, Behaviour Reference	Scann Functioning State	Server, Scann	Monitor, Visual-Scann
		Scann Functioning Reference	higher level of hierarchy, training, e	Monitor, Training, Procedure
Gate_mode	State, Behaviour Reference	Gate Mode State	Server, Gate	Monitor, Visual-Gate
		Gate Mode Transitioning Referenc	higher level of hierarchy, training, e	Monitor, Training, Procedure
Gate_function	State, Behaviour Reference	Gate Functioning State	Server, Gate	Monitor, Visual-Gate
		Gate Functioning Reference	higher level of hierarchy, training, e	Monitor, Training, Procedure
Gate_occupation	State, Behaviour Reference	Gate Occupation State	Server, Gate, PAX	Monitor, Visual-Gate, Visual-PAX
		Gate Occupation Transitioning Ref	higher level of hierarchy, training, e	Monitor, Training, Procedure
Gate-Door_mode	State, Behaviour Reference	Gate Door Mode State	Server, Gate, Door	Monitor, Visual-Gate-Door
		Gate Door Mode Reference	higher level of hierarchy, training, e	Monitor, Training, Procedure
Gate-Door_function	State, Behaviour Reference	Gate Door Functioning State	Server, Gate, Door	Monitor, Visual-Gate
		Gate Door Functioning Reference	higher level of hierarchy, training, e	Monitor, Training, Procedure
Gate_entrapment	State, Behaviour Reference	Gate Entrapment State	Server, Gate, PAX	Monitor, Visual-Gate, Visual/Speak
		Gate Entrapment Reference	higher level of hierarchy, training, e	Monitor, Training, Procedure
PAX_location	State, Behaviour Reference	PAX Location State	Server, PAX, *Scann	Monitor, Visual/Speaking-PAX
PAX_attitude	State, Behaviour Reference	PAX Attitude State	Server, PAX, *Scann	Monitor, Visual/Speaking-PAX
		PAX Movement Reference	higher level of hierarchy, training, e	Monitor, Training, Procedure
PAX_procedure-compliance	State, Behaviour Reference	PAX Processing Procedure Compli	Server, PAX, *Scann	Monitor, Visual/Speaking-PAX
		PAX Processing Procedure Compli	higher level of hierarchy, training, e	Monitor, Training, Procedure
PAX_ID-checking	PII/NPII, State, Behaviour Referenc	PAX ID/PII/NPII	Server, PAX, PAX-ID	Monitor, ID
		PAX ID-checking State	Server, PAX, Scann	Monitor, ID
		PAX ID-checking Reference	higher level of hierarchy, training, e	Monitor, Training, Procedure

Causal Scenarios

HCA#	Statement	Causes	Cause#	Factors	Factor#	Scenarios	Scenario#	Contributors	Contributor#	H# & L#	CS#	Statement
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate contr	1	Flawed implemer	1	-	0	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.1.1.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate contr	1	Specified control	2	-	0	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.1.2.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate contr	1	Specified control	3	-	0	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.1.3.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Unsafe control in	2	-	0	-	0	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.2.0.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate proce	3	Controller receive	1	conflicting inform	1	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.3.1.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate proce	3	Controller receive	1	conflicts that ma	2	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.3.1.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate proce	3	Controller receive	2	controller is disal	1	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.3.2.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate proce	3	Controller receive	2	controller is miss	2	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.3.2.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate proce	3	Controller receive	2	process model is	3	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.3.2.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate proce	3	Controller receive	2	wrong process m	4	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.3.2.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate proce	3	Controller receive	2	feedback/informa	5	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.3.2.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate proce	3	Controller does n	3	feedback is never	1	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.3.3.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate proce	3	Controller does n	3	controller may as	2	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.3.3.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate proce	3	Controller	3	feedback is delay	3	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.3.3.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate proce	3	Controller	3	information receiv	4	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.3.3.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate proce	3	Necessary contro	4	does not exist in	1	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.3.4.	Security Screeni
2.5-1.1	Security Screeni	Unsafe Controller	1	Inadequate proce	3	Necessary contro	4	does not exist in	2	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-1.3.4.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info	1	conflicts that ma	1	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.1.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info	1	conflicts that ma	2	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.1.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info se	1	delays in commu	3	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.1.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info se	1	feedback/info ser	4	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.1.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info is	2	sensor failures	1	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.2.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info is	2	loss of power to f	2	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.2.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info is	2	inaccuracies in s	3	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.2.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info is	2	sensor errors or r	4	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.2.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info is	2	delays in sensor	5	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.2.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info is	2	incorrect configur	6	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.2.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info is	2	degradation or ch	7	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.2.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info is	2	unanticipated co	8	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.2.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info is	3	-	0	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.3.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Feedback or info	1	Feedback/info do	4	-	0	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.1.4.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Inadequate feedb	2	Sensor(s) respon	1	transmission erro	1	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.2.1.	Security Screeni
2.5-1.1	Security Screeni	Inadequate Feedb	2	Inadequate feedb	2	Sensor(s) respon	1	lost communicati	2	[H1, H2, H3, H4] [L1, L2, L3, L4]	CS-2.5-1.1-2.2.1.	Security Screeni

+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

Refine & Iterate

Functional Framework: Architectural Analysis

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

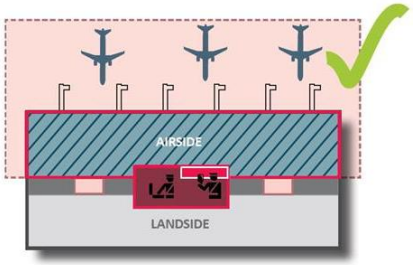
Refine & Iterate

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



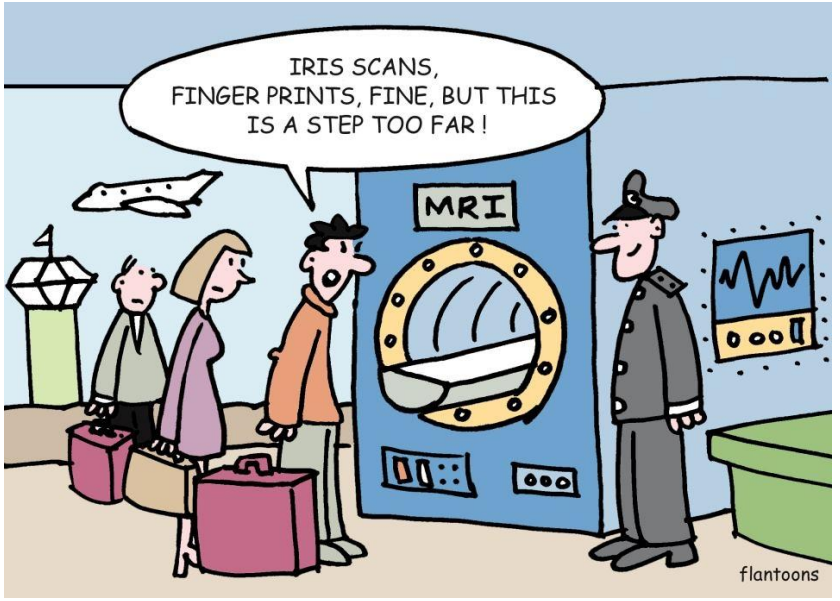
Simulate integrated constraints with unruly users & violations

Safety, Security and Privacy in Future Airports
insights & lessons learned

- **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:
  - **Iteractive 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!



Idoaldo Lima,

Max Schwienhorst,

Johannes Reichmuth

lima@via.rwth-aachen.de

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

DAAD