Discussion on STPA validation, replicability and analyst bias

2021 MIT STAMP/STPA Workshop

Idoaldo Lima

30 June 2020

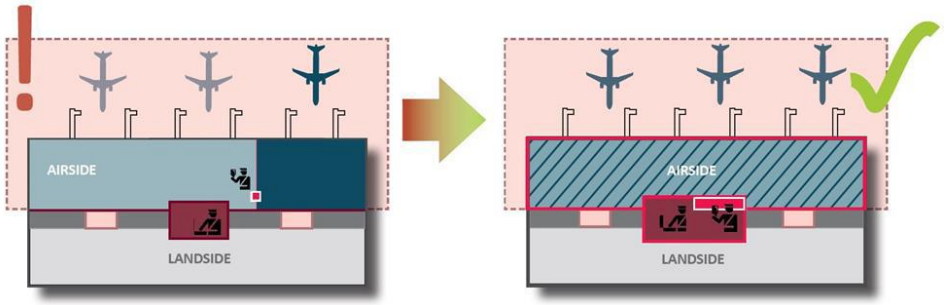
Institute of Transport Science
Chair of Air Transport and Airport Reserach
RWTH Aachen University

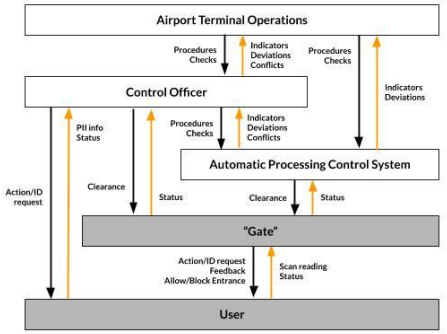
DAAD

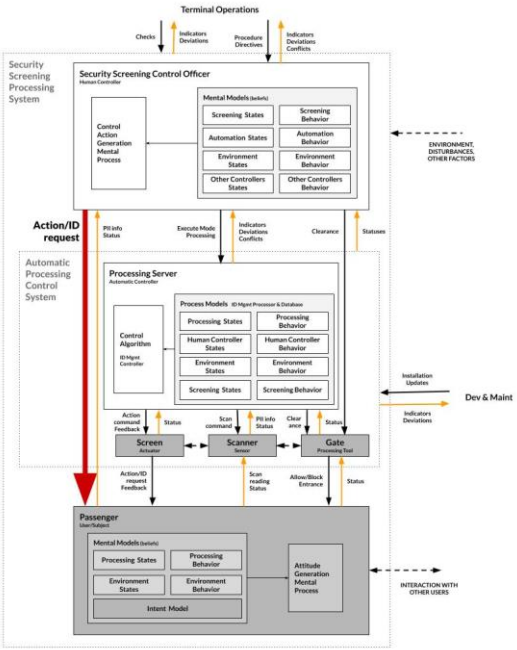
STPA validation, replicability and analyst bias

Previous work and context

http://psas.scripts.mit.edu/home/wp-content/uploads/2020/08/Airport-Terminal-Safety-Security-Privacy.pdf







Main take-aways:

- Safety & Security tend to be intertwined
- Path for legal framework change indicated
- Process Models & Contraints: easely simulated
- **Assumptions** are essential to ensure **validity** of the analysis

STPA validation, replicability and analyst bias
Analyst bias

STPA includes input from the from both **method- and topic-expert**'s perspectives and experiences

Beware of the **possibility of analyst bias**

https://www.researchgate.net/figure/Scenario-of-scatterplot-scaling-Bob-finds-a-pattern-of-interest-in-a-small-scatterplot_fig3_335133122

STPA validation, replicability and analyst bias
Replicability study

for our application “STPA applied for Safety, Security and Privacy Issues in Smart Airport Terminal New Concepts”

A Master’s student in our institute with similar background was given:

- ***Introduction***: our STPA approach and Uniform Terminal Areas (UTAs)
- ***Materials***: tutorials and examples of STPA and on our case study
- ***Goal***: develop an STPA analysis for safety, security and privacy issues in the use of biometrics for processing of passengers at airport terminals with UTAs
- ***Flow up***: Discussion of questions and review of the various development steps for ca. 4 months

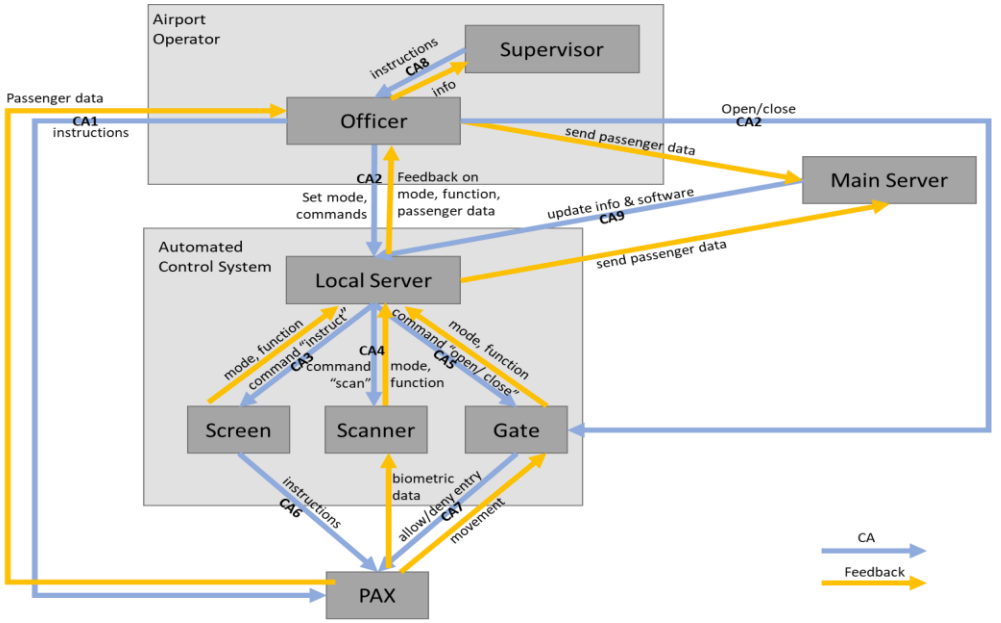
STPA validation, replicability and analyst bias
Replicability study

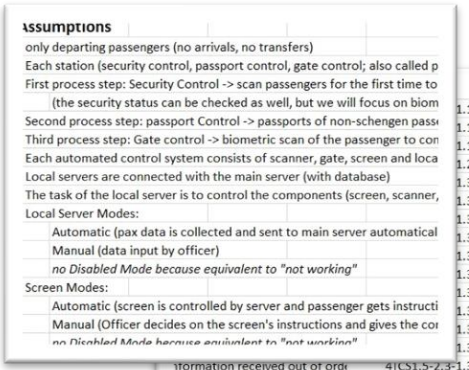
Relatively similar:

- control actions and constraints
- causal scenarios

Valuable intel obtained:

- different ways to model system and interactions
- levels of detail
- some different assumptions
- **implied assumptions** identified
  - Original analysis enhanced
  - Next step: Expert inteviews





ssumptions

only departing passengers (no arrivals, no transfers)
Each station (security control, passport control, gate control; also called p
First process step: Security Control -> scan passengers for the first time to
(the security status can be checked as well, but we will focus on biom
Second process step: passport Control -> passports of non-schengen passe
Third process step: Gate control -> biometric scan of the passenger to con
Each automated control system consists of scanner, gate, screen and loca
Local servers are connected with the main server (with database)
The task of the local server is to control the components (screen, scanner,
Local Server Modes:
Automatic (pax data is collected and sent to main server automatical
Manual (data input by officer)
no Disabled Mode because equivalent to "not working"
Screen Modes:
Automatic (screen is controlled by server and passenger gets instructi
Manual (Officer decides on the screen's instructions and gives the cor
no Disabled Mode because equivalent to "not working"

	Comment/ Statement	Hazard#	Loss#	Causal Scenario
1.1.1.0	*Officer thinks he* The officer is nc	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
1.1.2.0	*control algorithr* The control algc	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
1.1.3.0	*e.g. control algo* The specified cc	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
1.2.0.0	*e.g. command o* The supervisor c	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
1.3.1.1	*Officer receives* The officer rece	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
1.3.1.2	*Officer receives* The officer rece	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
1.3.2.1	*Officer doesn't r* The officer rece	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
1.3.2.2	*Officer doesn't k* The officer rece	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
1.3.2.3	*Officer interpret* The officer rece	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
1.3.2.4	*Officer interpret* The officer rece	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
1.3.2.5	*e.g. officer think* The officer rece	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
1.3.3.1	*Officer doesn't r* The officer does	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
1.3.3.2	*will only lead to* The officer does	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
1.3.3.3	*Officer receives* The officer does	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t
	does not apply b -	-	-	-
	scanner feedbac The necessary fe	[H3, H4, H5]	[L1, L2, L3, L4]	The officer requests t

formation received out of orde	4 CS1.5-2.3-1.3.3.4
oes not exist in the control stru	1 CS1.5-2.3-1.3.4.1

STPA validation, replicability and analyst bias
Lessons Learned

We can infer from this experience that:

For a different group of analysts to **properly replicate an STPA analysis** and its results. They have to **understand the assumptions beheind** the analysis!

- Avoid **analyst bias** though clear assumptions
- **Validaty** of the results is enhanced with assumptions
- Either public or confidential projects
- Essential also for **leading indicators**

Thank you!

Idoaldo Lima

lima@via.rwth-aachen.de

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