



# 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**

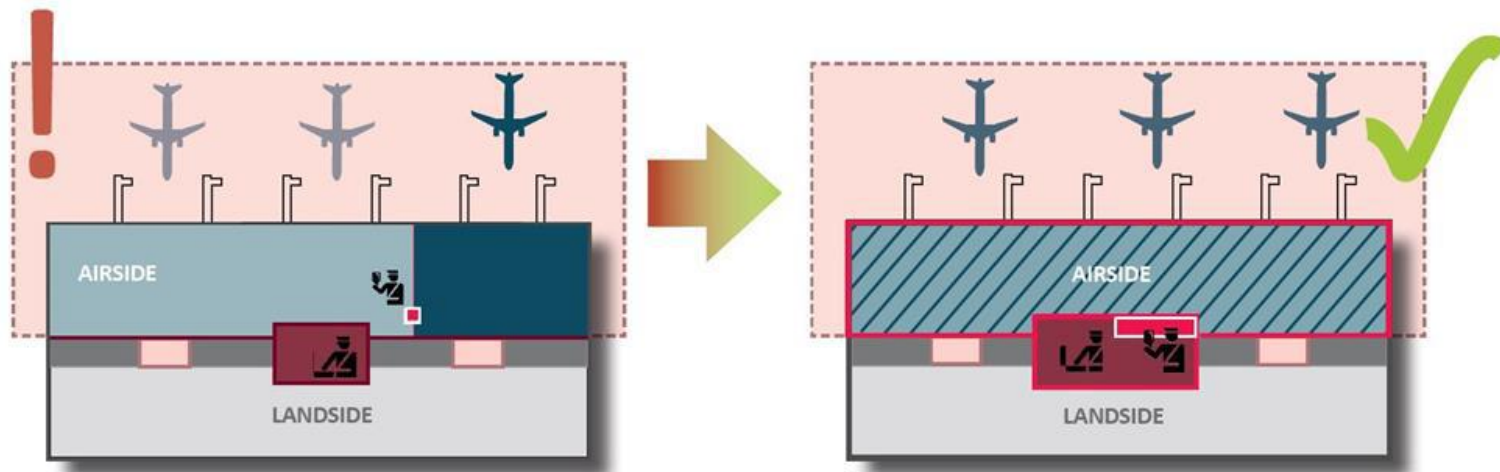
**The Swiss Cheese Model:** enchainment of failure events

analytical decomposition, statistics, human error, interactions, organizational aspect, ...

# Safety, Security and Privacy in Future Airports

## case: the Uniform Terminal Area Concept

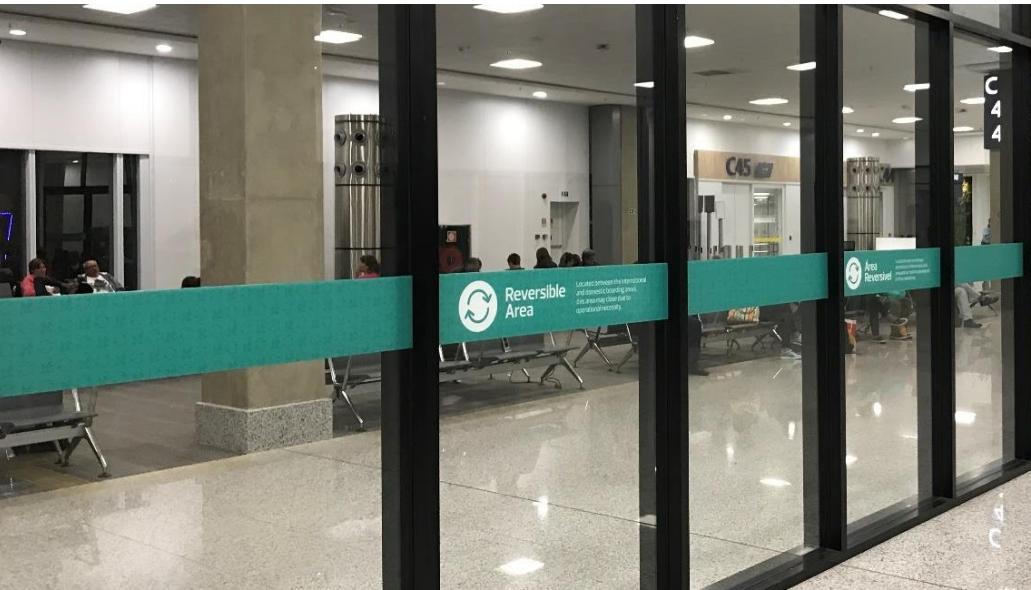
- The External border control problem
  - Regulatory **physical separation of passenger flows** in gate
    - Unnecessary cost and complexity
- **Modern technologies** for unbundling of passenger flows
  - Estimated benefits in capacity, workload, costs, service and security levels



# 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:

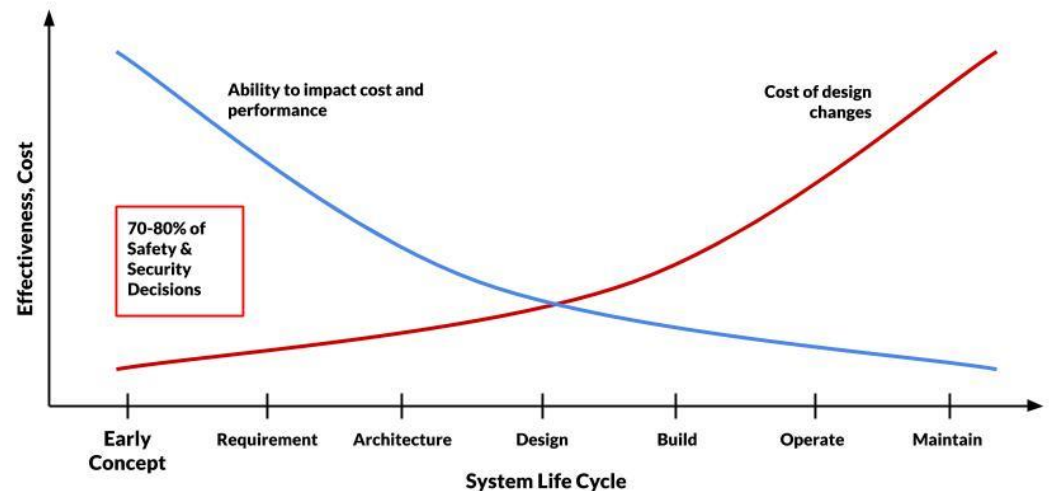
@Boarding

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

# Safety, Security and Privacy in Future Airports

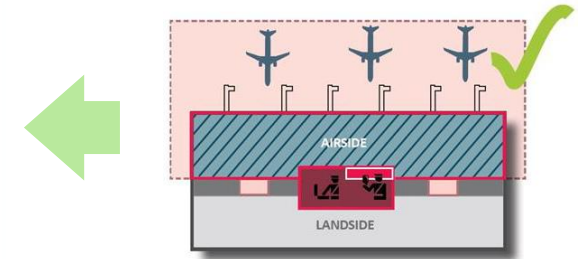
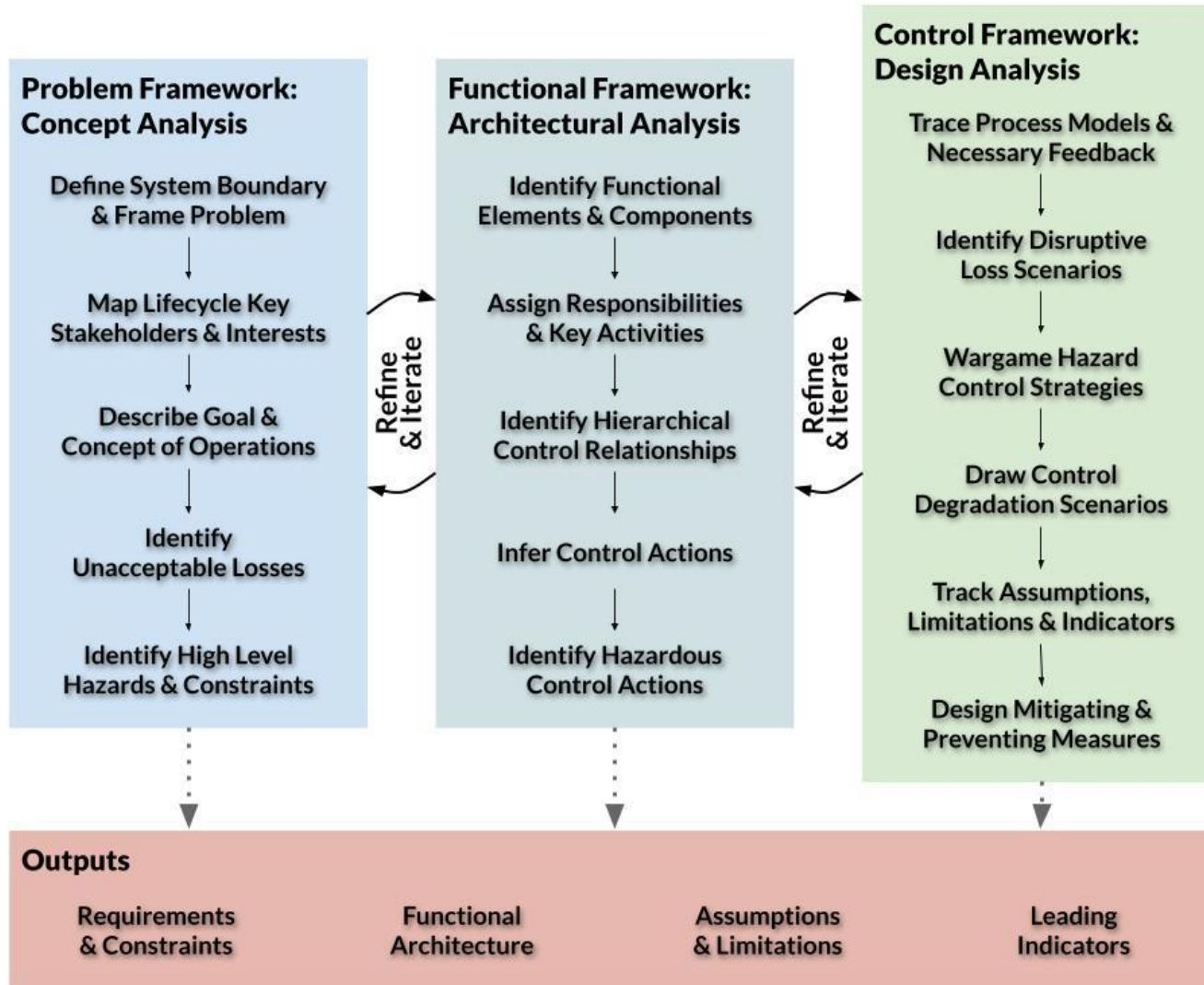
## case: the Uniform Terminal Area Concept

- Our project:
  - a **technical solution** must be defined & **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

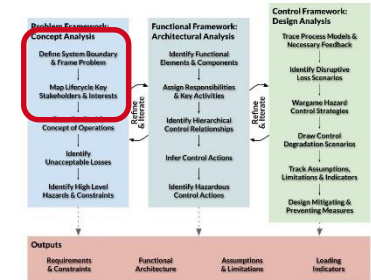
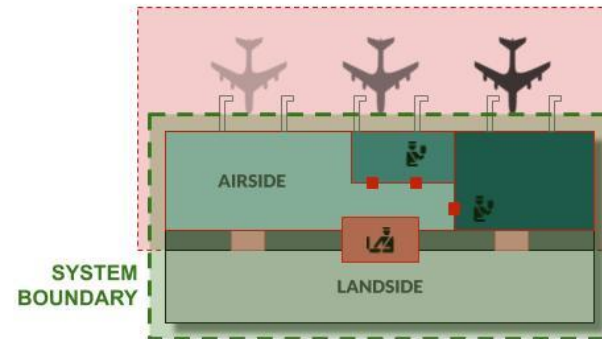
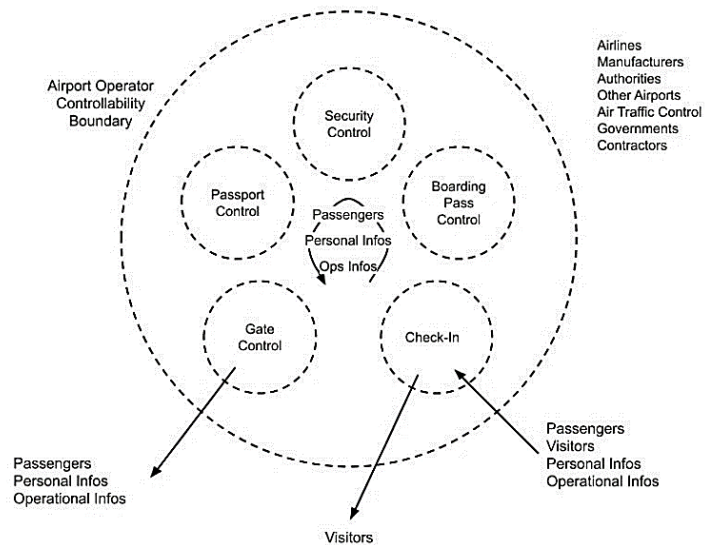
## how we are doing it





# Safety, Security and Privacy in Future Airports

## UTA case: concept analysis



### System of Interest (Sol)

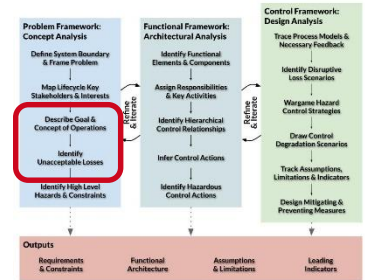
A system to promote **identity control and processing of passengers** in airport terminals by means of **allowing or not access** of passengers/users to controlled areas and keeping track of each passenger/user processing in each area during check-in, bag drop, boarding pass control, security control, 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

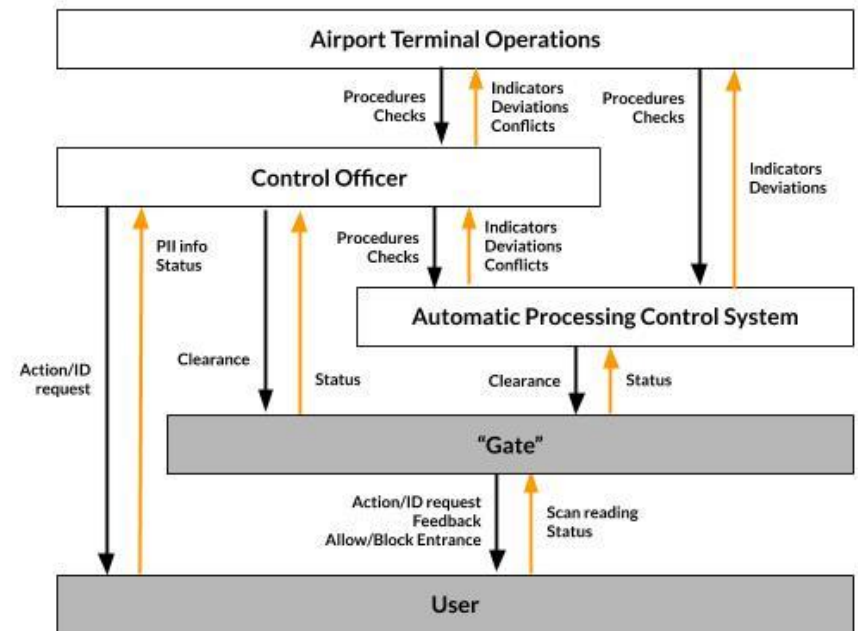
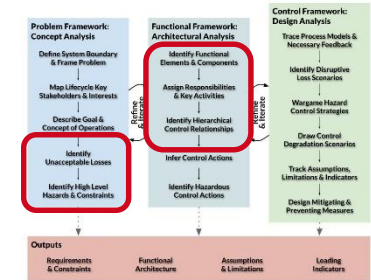
## UTA case: concept analysis

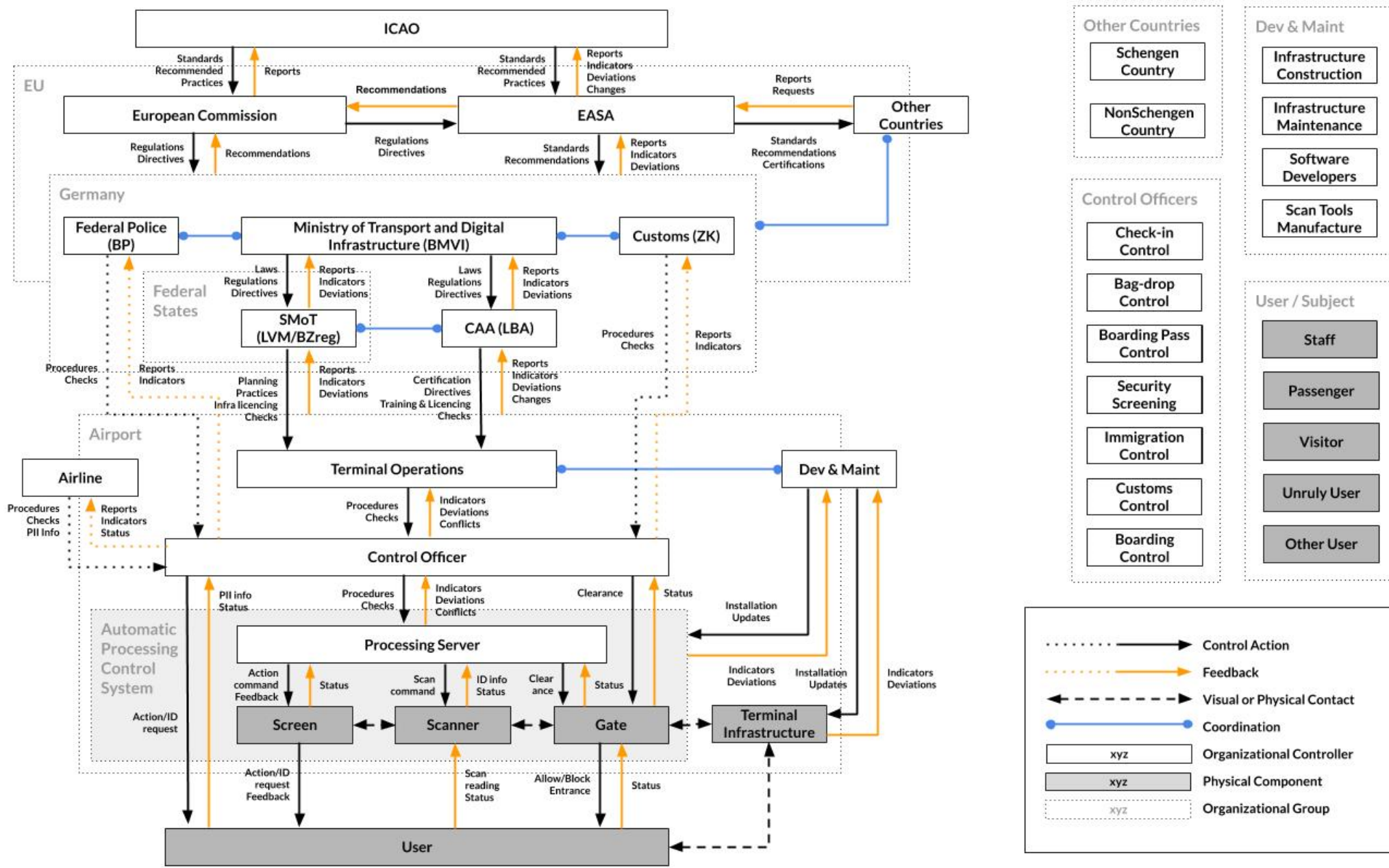
### Unacceptable Losses

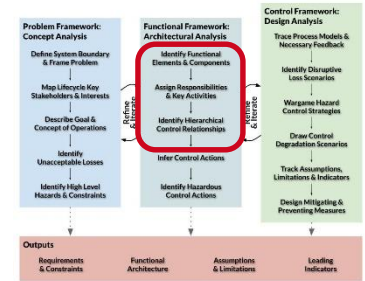
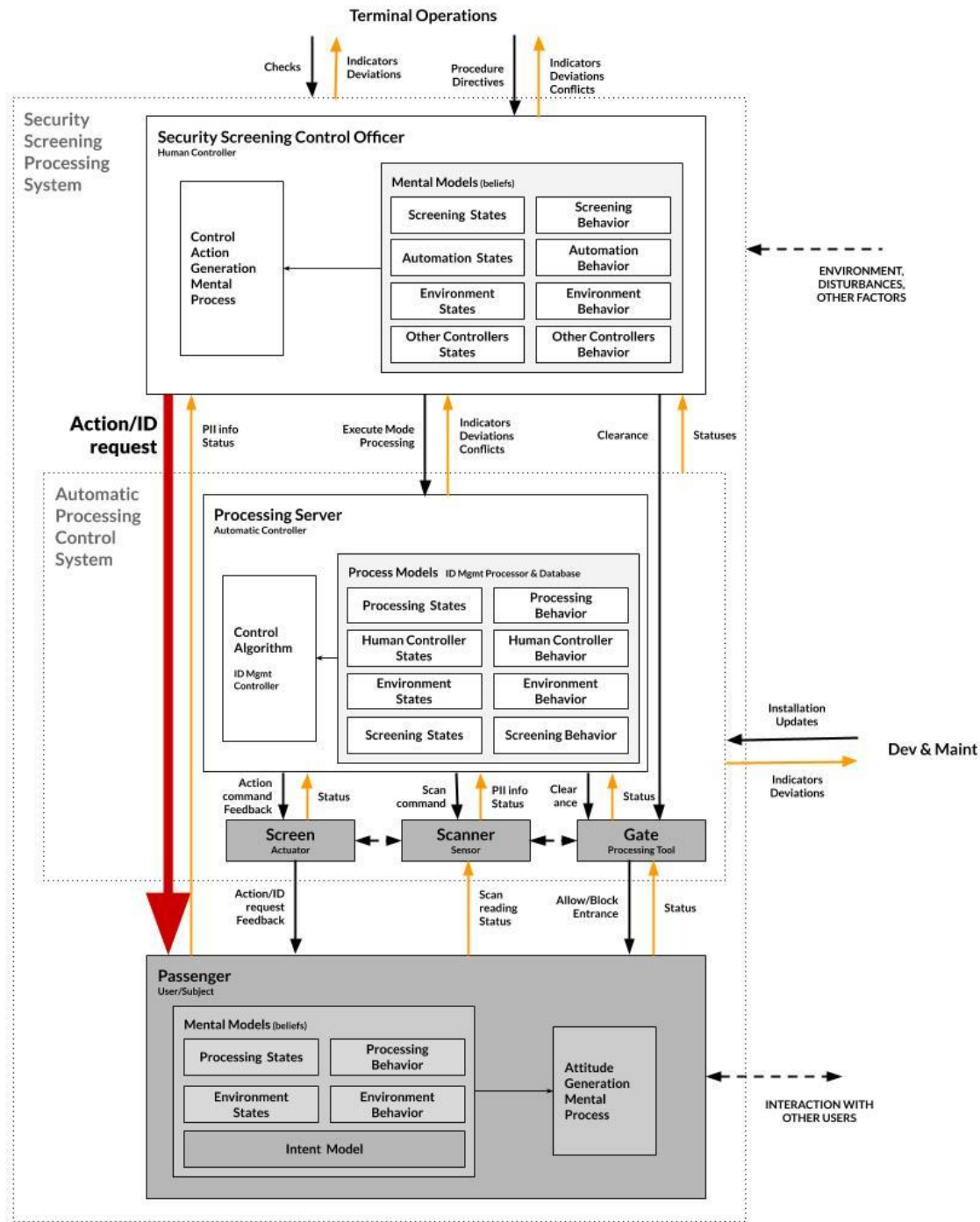
- L-1 loss of life, injury or health compromise
- L-2 damage to equipment or infrastructure
- L-3 disruption on processing or transport
- L-4 stain to reputation

### 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







## 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

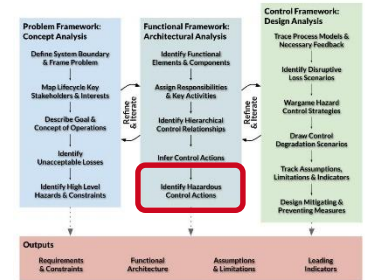
## UTA case: CA-2.5 example

### 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 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                               |

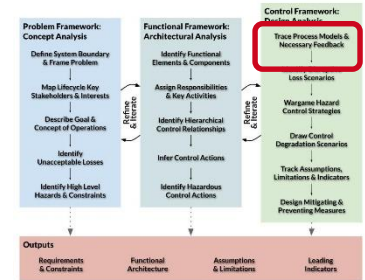
**processing function only, may also include security screening function (more privacy issues)**



# 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

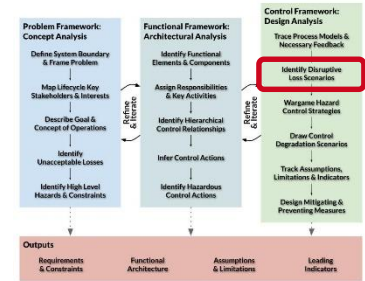
#### Process Model Variables & Values

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_entrapment	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**

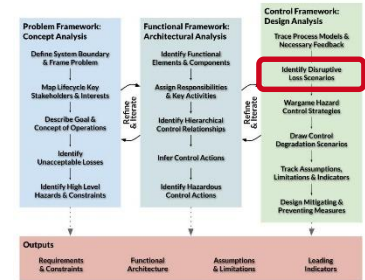
- > Officer believes Server is still controlling Processing and does not issue CA
- > PAX can be delayed, or interpret this lack of orientation as a „go forward“

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 is completed)
- 2: Control action improperly executed (e.g. user spoofs FR-check)



# Safety, Security and Privacy in Future Airports

## formal STPA

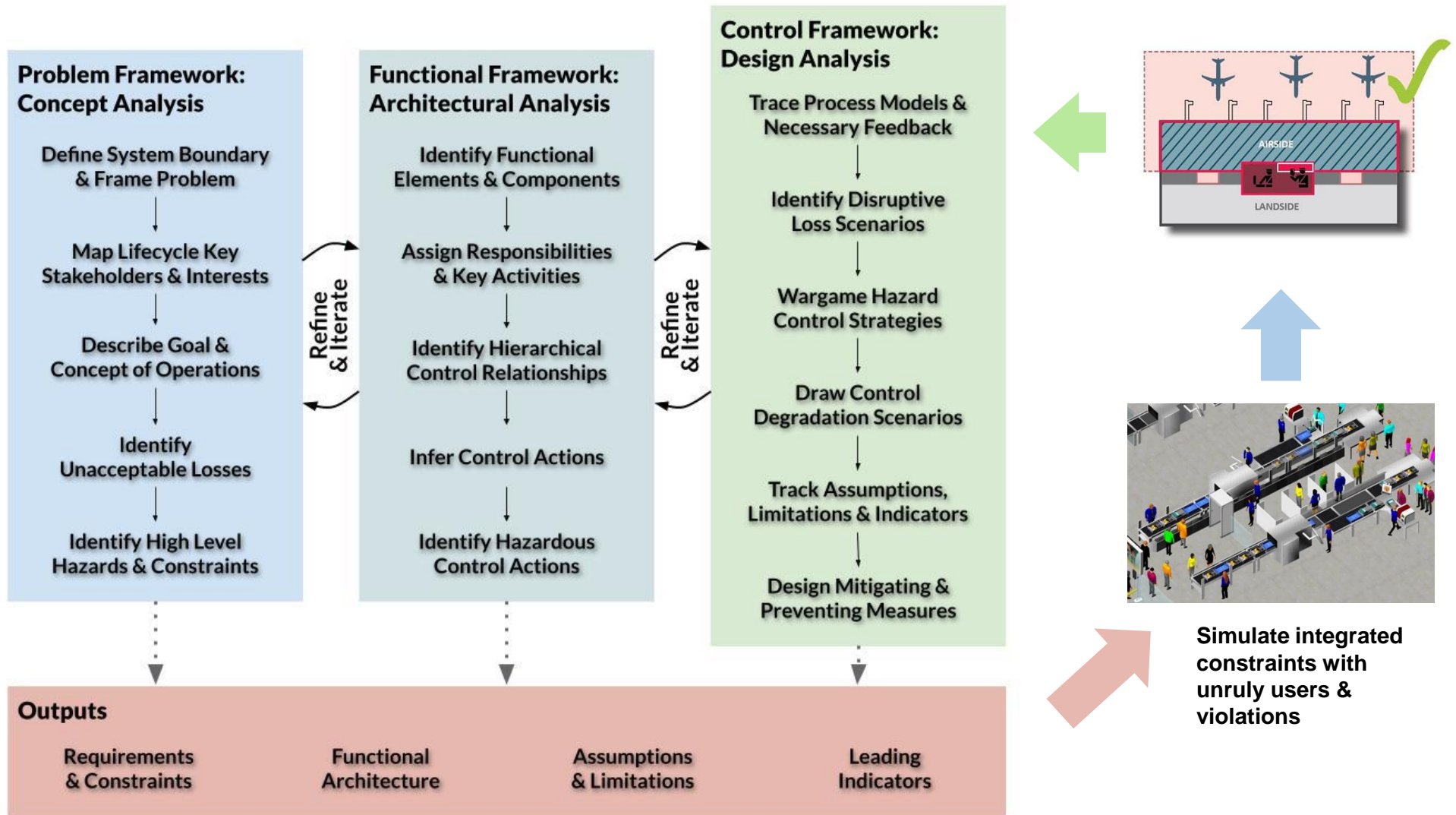
CA#	General	Specific	Controller	Verbal Form	Information For Controlled	Statement
CA1	Execute Processing	Security Screen commands	Security Screen	to execute proce	Processing Servt	Security Screening Co
CA1.1	Automation	Security Screen commands	Security Screen	to execute proce	Processing Servt	Security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

**Control Actions**

Related CA#	Controller	Verbal Action	Controlled	Info Action	HCA Type#	Type 1	Type 2	HCA#	Control	Rationale	Related HW	Related SW
CA2	Security Screen	request	Passenger	Action or ID	1 not providing	does not	-	HCA-2.1	when Server is in rct. of missing p[H1, H3]	[L3, L4]		
CA2	Security Screen	request	Passenger	Action or ID	2 proading	does	-	HCA-2.1	when Server is in rct. of missing p[H1, H3, H4, H5, H6, H7, H8, H9, H10, H11, H12, H13, H14, H15, H16, H17, H18, H19, H20, H21, H22, H23, H24, H25, H26, H27, H28, H29, H30, H31, H32, H33, H34, H35, H36, H37, H38, H39, H40, H41, H42, H43, H44, H45, H46, H47, H48, H49, H50, H51, H52, H53, H54, H55, H56, H57, H58, H59, H60, H61, H62, H63, H64, H65, H66, H67, H68, H69, H70, H71, H72, H73, H74, H75, H76, H77, H78, H79, H80, H81, H82, H83, H84, H85, H86, H87, H88, H89, H90, H91, H92, H93, H94, H95, H96, H97, H98, H99, H100, H101, H102, H103, H104, H105, H106, H107, H108, H109, H110, H111, H112, H113, H114, H115, H116, H117, H118, H119, H120, H121, H122, H123, H124, H125, H126, H127, H128, H129, H130, H131, H132, H133, H134, H135, H136, H137, H138, H139, H140, H141, H142, H143, H144, H145, H146, H147, H148, H149, H150, H151, H152, H153, H154, H155, H156, H157, H158, H159, H160, H161, H162, H163, H164, H165, H166, H167, H168, H169, H170, H171, H172, H173, H174, H175, H176, H177, H178, H179, H180, H181, H182, H183, H184, H185, H186, H187, H188, H189, H190, H191, H192, H193, H194, H195, H196, H197, H198, H199, H200, H201, H202, H203, H204, H205, H206, H207, H208, H209, H210, H211, H212, H213, H214, H215, H216, H217, H218, H219, H220, H221, H222, H223, H224, H225, H226, H227, H228, H229, H230, H231, H232, H233, H234, H235, H236, H237, H238, H239, H240, H241, H242, H243, H244, H245, H246, H247, H248, H249, H250, H251, H252, H253, H254, H255, H256, H257, H258, H259, H260, H261, H262, H263, H264, H265, H266, H267, H268, H269, H270, H271, H272, H273, H274, H275, H276, H277, H278, H279, H280, H281, H282, H283, H284, H285, H286, H287, H288, H289, H290, H291, H292, H293, H294, H295, H296, H297, H298, H299, H300, H301, H302, H303, H304, H305, H306, H307, H308, H309, H310, H311, H312, H313, H314, H315, H316, H317, H318, H319, H320, H321, H322, H323, H324, H325, H326, H327, H328, H329, H330, H331, H332, H333, H334, H335, H336, H337, H338, H339, H340, H341, H342, H343, H344, H345, H346, H347, H348, H349, H350, H351, H352, H353, H354, H355, H356, H357, H358, H359, H360, H361, H362, H363, H364, H365, H366, H367, H368, H369, H370, H371, H372, H373, H374, H375, H376, H377, H378, H379, H380, H381, H382, H383, H384, H385, H386, H387, H388, H389, H390, H391, H392, H393, H394, H395, H396, H397, H398, H399, H400, H401, H402, H403, H404, H405, H406, H407, H408, H409, H410, H411, H412, H413, H414, H415, H416, H417, H418, H419, H420, H421, H422, H423, H424, H425, H426, H427, H428, H429, H430, H431, H432, H433, H434, H435, H436, H437, H438, H439, H440, H441, H442, H443, H444, H445, H446, H447, H448, H449, H450, H451, H452, H453, H454, H455, H456, H457, H458, H459, H460, H461, H462, H463, H464, H465, H466, H467, H468, H469, H470, H471, H472, H473, H474, H475, H476, H477, H478, H479, H480, H481, H482, H483, H484, H485, H486, H487, H488, H489, H490, H491, H492, H493, H494, H495, H496, H497, H498, H499, H500, H501, H502, H503, H504, H505, H506, H507, H508, H509, H510, H511, H512, H513, H514, H515, H516, H517, H518, H519, H520, H521, H522, H523, H524, H525, H526, H527, H528, H529, H530, H531, H532, H533, H534, H535, H536, H537, H538, H539, H540, H541, H542, H543, H544, H545, H546, H547, H548, H549, H550, H551, H552, H553, H554, H555, H556, H557, H558, H559, H560, H561, H562, H563, H564, H565, H566, H567, H568, H569, H570, H571, H572, H573, H574, H575, H576, H577, H578, H579, H580, H581, H582, H583, H584, H585, H586, H587, H588, H589, H590, H591, H592, H593, H594, H595, H596, H597, H598, H599, H600, H601, H602, H603, H604, H605, H606, H607, H608, H609, H610, H611, H612, H613, H614, H615, H616, H617, H618, H619, H620, H621, H622, H623, H624, H625, H626, H627, H628, H629, H630, H631, H632, H633, H634, H635, H636, H637, H638, H639, H640, H641, H642, H643, H644, H645, H646, H647, H648, H649, H650, H651, H652, H653, H654, H655, H656, H657, H658, H659, H660, H661, H662, H663, H664, H665, H666, H667, H668, H669, H670, H671, H672, H673, H674, H675, H676, H677, H678, H679, H680, H681, H682, H683, H684, H685, H686, H687, H688, H689, H690, H691, H692, H693, H694, H695, H696, H697, H698, H699, H700, H701, H702, H703, H704, H705, H706, H707, H708, H709, H710, H711, H712, H713, H714, H715, H716, H717, H718, H719, H720, H721, H722, H723, H724, H725, H726, H727, H728, H729, H730, H731, H732, H733, H734, H735, H736, H737, H738, H739, H740, H741, H742, H743, H744, H745, H746, H747, H748, H749, H750, H751, H752, H753, H754, H755, H756, H757, H758, H759, H760, H761, H762, H763, H764, H765, H766, H767, H768, H769, H770, H771, H772, H773, H774, H775, H776, H777, H778, H779, H780, H781, H782, H783, H784, H785, H786, H787, H788, H789, H790, H791, H792, H793, H794, H795, H796, H797, H798, H799, H800, H801, H802, H803, H804, H805, H806, H807, H808, H809, H810, H811, H812, H813, H814, H815, H816, H817, H818, H819, H820, H821, H822, H823, H824, H825, H826, H827, H828, H829, H830, H831, H832, H833, H834, H835, H836, H837, H838, H839, H840, H841, H842, H843, H844, H845, H846, H847, H848, H849, H850, H851, H852, H853, H854, H855, H856, H857, H858, H859, H860, H861, H862, H863, H864, H865, H866, H867, H868, H869, H870, H871, H872, H873, H874, H875, H876, H877, H878, H879, H880, H881, H882, H883, H884, H885, H886, H887, H888, H889, H890, H891, H892, H893, H894, H895, H896, H897, H898, H899, H900, H901, H902, H903, H904, H905, H906, H907, H908, H909, H910, H911, H912, H913, H914, H915, H916, H917, H918, H919, H920, H921, H922, H923, H924, H925, H926, H927, H928, H929, H930, H931, H932, H933, H934, H935, H936, H937, H938, H939, H940, H941, H942, H943, H944, H945, H946, H947, H948, H949, H950, H951, H952, H953, H954, H955, H956, H957, H958, H959, H960, H961, H962, H963, H964, H965, H966, H967, H968, H969, H970, H971, H972, H973, H974, H975, H976, H977, H978, H979, H980, H981, H982, H983, H984, H985, H986, H987, H988, H989, H990, H991, H992, H993, H994, H995, H996, H997, H998, H999, H1000, H1001, H1002, H1003, H1004, H1005, H1006, H1007, H1008, H1009, H1010, H1011, H1012, H1013, H1014, H1015, H1016, H1017, H1018, H1019, H1020, H1021, H1022, H1023, H1024, H1025, H1026, H1027, H1028, H1029, H1030, H1031, H1032, H1033, H1034, H1035, H1036, H1037, H1038, H1039, H1040, H1041, H1042, H1043, H1044, H1045, H1046, H1047, H1048, H1049, H1050, H1051, H1052, H1053, H1054, H1055, H1056, H1057, H1058, H1059, H1060, H1061, H1062, H1063, H1064, H1065, H1066, H1067, H1068, H1069, H1070, H1071, H1072, H1073, H1074, H1075, H1076, H1077, H1078, H1079, H1080, H1081, H1082, H1083, H1084, H1085, H1086, H1087, H1088, H1089, H1090, H1091, H1092, H1093, H1094, H1095, H1096, H1097, H1098, H1099, H1100, H1101, H1102, H1103, H1104, H1105, H1106, H1107, H1108, H1109, H1110, H1111, H1112, H1113, H1114, H1115, H1116, H1117, H1118, H1119, H1120, H1121, H1122, H1123, H1124, H1125, H1126, H1127, H1128, H1129, H1130, H1131, H1132, H1133, H1134, H1135, H1136, H1137, H1138, H1139, H1140, H1141, H1142, H1143, H1144, H1145, H1146, H1147, H1148, H1149, H1150, H1151, H1152, H1153, H1154, H1155, H1156, H1157, H1158, H1159, H1160, H1161, H1162, H1163, H1164, H1165, H1166, H1167, H1168, H1169, H1170, H1171, H1172, H1173, H1174, H1175, H1176, H1177, H1178, H1179, H1180, H1181, H1182, H1183, H1184, H1185, H1186, H1187, H1188, H1189, H1190, H1191, H1192, H1193, H1194, H1195, H1196, H1197, H1198, H1199, H1200, H1201, H1202, H1203, H1204, H1205, H1206, H1207, H1208, H1209, H1210, H1211, H1212, H1213, H1214, H1215, H1216, H1217, H1218, H1219, H1220, H1221, H1222, H1223, H1224, H1225, H1226, H1227, H1228, H1229, H1230, H1231, H1232, H1233, H1234, H1235, H1236, H1237, H1238, H1239, H1240, H1241, H1242, H1243, H1244, H1245, H1246, H1247, H1248, H1249, H1250, H1251, H1252, H1253, H1254, H1255, H1256, H1257, H1258, H1259, H1260, H1261, H1262, H1263, H1264, H1265, H1266, H1267, H1268, H1269, H1270, H1271, H1272, H1273, H1274, H1275, H1276, H1277, H1278, H1279, H1280, H1281, H1282, H1283, H1284, H1285, H1286, H1287, H1288, H1289, H1290, H1291, H1292, H1293, H1294, H1295, H1296, H1297, H1298, H1299, H1300, H1301, H1302, H1303, H1304, H1305, H1306, H1307, H1308, H1309, H1310, H1311, H1312, H1313, H1314, H1315, H1316, H1317, H1318, H1319, H1320, H1321, H1322, H1323, H1324, H1325, H1326, H1327, H1328, H1329, H1330, H1331, H1332, H1333, H1334, H1335, H1336, H1337, H1338, H1339, H1340, H1341, H1342, H1343, H1344, H1345, H1346, H1347, H1348, H1349, H1350, H1351, H1352, H1353, H1354, H1355, H1356, H1357, H1358, H1359, H1360, H1361, H1362, H1363, H1364, H1365, H1366, H1367, H1368, H1369, H1370, H1371, H1372, H1373, H1374, H1375, H1376, H1377, H1378, H1379, H1380, H1381, H1382, H1383, H1384, H1385, H1386, H1387, H1388, H1389, H1390, H1391, H1392, H1393, H1394, H1395, H1396, H1397, H1398, H1399, H1400, H1401, H1402, H1403, H1404, H1405, H1406, H1407, H1408, H1409, H1410, H1411, H1412, H1413, H1414, H1415, H1416, H1417, H1418, H1419, H1420, H1421, H1422, H1423, H1424, H1425, H1426, H1427, H1428, H1429, H1430, H1431, H1432, H1433, H1434, H1435, H1436, H1437, H1438, H1439, H1440, H1441, H1442, H1443, H1444, H1445, H1446, H1447, H1448, H1449, H1450, H1451, H1452, H1453, H1454, H1455, H1456, H1457, H1458, H1459, H1460, H1461, H1462, H1463, H1464, H1465, H1466, H1467, H1468, H1469, H1470, H1471, H1472, H1473, H1474, H1475, H1476, H1477, H1478, H1479, H1480, H1481, H1482, H1483, H1484, H1485, H1486, H1487, H1488, H1489, H1490, H1491, H1492, H1493, H1494, H1495, H1496, H1497, H1498, H1499, H1500, H1501, H1502, H1503, H1504, H1505, H1506, H1507, H1508, H1509, H1510, H1511, H1512, H1513, H1514, H1515, H1516, H1517, H1518, H1519, H1520, H1521, H1522, H1523, H1524, H1525, H1526, H1527, H1528, H1529, H1530, H1531, H1532, H1533, H1534, H1535, H1536, H1537, H1538, H1539, H1540, H1541, H1542, H1543, H1544, H1545, H1546, H1547, H1548, H1549, H1550, H1551, H1552, H1553, H1554, H1555, H1556, H1557, H1558, H1559, H1560, H1561, H1562, H1563, H1564, H1565, H1566, H1567, H1568, H1569, H1570, H1571, H1572, H1573, H1574, H1575, H1576, H1577, H1578, H1579, H1580, H1581, H1582, H1583, H1584, H1585, H1586, H1587, H1588, H1589, H1590, H1591, H1592, H1593, H1594, H1595, H1596, H1597, H1598, H1599, H1600, H1601, H1602, H1603, H1604, H1605, H1606, H1607, H1608, H1609, H1610, H1611, H1612, H1613, H1614, H1615, H1616, H1617, H1618, H1619, H1620, H1621, H1622, H1623, H1624, H1625, H1626, H1627, H1628, H1629, H1630, H1631, H1632, H1633, H1634, H1635, H1636, H1637, H1638, H1639, H1640, H1641, H1642, H1643, H1644, H1645, H1646, H1647, H1648, H1649, H1650, H1651, H1652, H1653, H1654, H1655, H1656, H1657, H1658, H1659, H1660, H1661, H1662, H1663, H1664, H1665, H1666, H1667, H1668, H1669, H1670, H1671, H1672, H1673, H1674, H1675, H1676, H1677, H1678, H1679, H1680, H1681, H1682, H1683, H1684, H1685, H1686, H1687, H1688, H1689, H1690, H1691, H1692, H1693, H1694, H1695, H1696, H1697, H1698, H1699, H1700, H1701, H1702, H1703, H1704, H1705, H1706, H1707, H1708, H1709, H1710, H1711, H1712, H1713, H1714, H1715, H1716, H1717, H1718, H1719, H1720, H1721, H1722, H1723, H1724, H1725, H1726, H1727, H1728, H1729, H1730, H1731, H1732, H1733, H1734, H1735, H1736, H1737, H1738, H1739, H1740, H1741, H1742, H1743, H1744, H1745, H1746, H1747, H1748, H1749, H1750, H1751, H1752, H1753, H1754, H1755, H1756, H1757, H1758, H1759, H1760, H1761, H1762, H1763, H1764, H1765, H1766, H1767, H1768, H1769, H1770, H1771, H1772, H1773, H1774, H1775, H1776, H1777, H1778, H1779, H1780, H1781, H1782, H1783, H1784, H1785, H1786, H1787, H1788, H1789, H1790, H1791, H1792, H1793, H1794, H1795, H1796, H1797, H1798, H1799, H1800, H1801, H1802, H1803, H1804, H1805, H1806, H1807, H1808, H1809, H1810, H1811, H1812, H1813, H1814, H1815, H1816, H1817, H1818, H1819, H1820, H1821, H1822, H1823, H1824, H1825, H1826, H1827, H1828, H1829, H1830, H1831, H1832, H1833, H1834, H1835, H1836, H1837, H1838, H1839, H1840, H1841, H1842, H1843, H1844, H1845, H1846, H1847, H1848, H1849, H1850, H1851, H1852, H1853, H1854, H1855, H1856, H1857, H1858, H1859, H1860, H1861, H1862, H1863, H1864, H1865, H1866, H1867, H1868, H1869, H1870, H1871, H1872, H1873, H1874, H1875, H1876, H1877, H1878, H1879, H1880, H1881, H1882, H1883, H1884, H1885, H1886, H1887, H1888, H1889, H1890, H1891, H1892, H1893, H1894, H1895, H1896, H1897, H1898, H1899, H1900, H1901, H1902, H1903, H1904, H1905, H1906, H1907, H1908, H1909, H1910, H1911, H1912, H1913, H1914, H1915, H1916, H1917, H1918, H1919, H1920, H1921, H1922, H1923, H1924, H1925, H1926, H1927, H192			



# Safety, Security and Privacy in Future Airports design & verification cycle



# 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:
  - **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 & Constraints: outcomes can be **easily simulated**

# Thank you!

Idoaldo Lima,  
Max Schwienhorst,  
Johannes Reichmuth

[lima@via.rwth-aachen.de](mailto:lima@via.rwth-aachen.de)

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

