EASA
European Aviation Safety Agency

Final Report EASA_REP_RESEA_2016_1

Research Project:

Impact Assessment of Cybersecurity Threats

An agency of the European Union

PAGE INTENTIONALLY LEFT BLANK

Disclaimer

This study has been carried out for the European Aviation Safety Agency by an external organization and expresses the opinion of the organization undertaking the study. It is provided for information purposes only and the views expressed in the study have not been adopted, endorsed or in any way approved by the European Aviation Safety Agency. Consequently it should not be relied upon as a statement, as any form of warranty, representation, undertaking, contractual, or other commitment binding in law upon the European Aviation Safety Agency.

Ownership of all copyright and other intellectual property rights in this material including any documentation, data and technical information, remains vested to the European Aviation Safety Agency. All logo, copyrights, trademarks, and registered trademarks that may be contained within are the property of their respective owners.

Reproduction of this study, in whole or in part, is permitted under the condition that the full body of this Disclaimer remains clearly and visibly affixed at all times with such reproduced part.

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

1 INTRODUCTION

1.1 PURPOSE OF THE DOCUMENT

The main objective of the IACT project is to develop a knowledge base for the impact assessment of security threat on the safety of flight operations with a focus on cyber-security threats to a number of critical aircraft systems.

The purpose of the current document is to present the design and the results of the flight simulations exercises performed within the activity in the DLR facilities, using the DLR simulator.

The design of the flight simulator exercises includes:

- The definition of the flight plan scenario;
- The definition of the threat scenarios;
- The simulation plan;
- The technical details concerning the implementation of the GNSS-based threat within the simulator, including the specification of the additional functionalities / modules / interfaces developed within the activity.

The results of the flight simulations exercises include

- the analysis of the pilots' behavior during the exercises;
- the pilots feedback after the exercises;
- some suggestions for procedures for threat mitigation.

1.2 SCOPE OF THE PROJECT

The scope of the project encompasses the preliminary risk assessment at system and aircraft levels for potential cyber-attacks to the Flight Management System (FMS) and to the Global Navigation Satellite System (GNSS) receiver, including GBAS and SBAS augmentations.

The work is conducted considering generic functional architectures for aircraft systems and does not encompass the development of detailed system architecture. The assessment covers the analysis of potential failure cases and the characterization of potential impact for flight operations (covering all flight phases), while considering the main (existing) mitigations at the level of flight crews working methods and operational procedures.

1.3 TERMS, DEFINITIONS AND ABBREVIATED TERMS

1.3.1 ACRONYMS AND ABBREVIATIONS

ACARS	Aircraft Communication Addressing and Reporting System
ADIRU	Air Data and Inertial Reference Unit
AGL	Above Ground Level
AIP	Aeronautical Information Publication
AMM	Aircraft Maintenance Manual
AOC	Airline Operations Center

APCH	Approach
AP	Auto Pilot
APV	Approach Procedure with Vertical guidance
ARR	Arrival
ATC	Air Traffic Control
ATM	Air Traffic Management
CAT	Category
CG	Center of Gravity
CLB	Climb
CM	Crew Member
CRZ	Cruise
DA	Decision Altitude
DEP	Departure
DES	Destination
EFB	Electronic Flight Bag
FD	Flight Director
FCOM	Flight Crew Operating Manual
FMGC	Flight Management and Guidance Computer
FMS	Flight Management System
FOM	Field Operations Manual
GBAS	Ground Based Augmentation System
GLS	GBAS Landing System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GTSM	GNSS Threat Simulator Module
IACT	Impact Assessment of Cybersecurity Threats
IC	Interface Computer
IFR	Instrument Flight Rules
INS	Inertial Navigation System
IOS	Instructor Operator Station
ISA	International Standard Atmosphere
LPV	Localizer Performance with Vertical guidance
MCDU	Multipurpose Control and Display Unit
MOC	Minimum Obstacle Clearance
MSL	Mean Sea Level
NCD	No Computed Data
NM	Nautical Mile
OPS	Operations
PF	Pilot Flying
PFD	Primary Flight Display
PM	Pilot Monitoring
QRH	Quick Reference Handbook
RNAV	Area Navigation
RNP	Required Navigation Performance
RWY	Runway

SBAS	Satellite Based Augmentation System
SID	Standard Instrument Departure
SOP	Standard Operating Procedure
TO	Take Off
TS	Threat Scenarios
VOR	VHF Omni-directional radio Range
W&B	Weight and Balance

1.4 REFERENCES

1.4.1 APPLICABLE DOCUMENTS

[AD.1] EASA.2016.HVP.10: Tender Documents Part I

[AD.2] EASA.2016.HVP.10: Tender Documents Part I

[AD.3] EASA.2016.HVP.10: Tender Documents Part II

[AD.4] EASA.2016.HVP.10: Tender Documents Part III

[AD.5] Section A of Qascom proposal in response to EASA.2016.HVP.10: EASA-QASC-IACT-A-AD

[AD.6] EUROCAE, 132/ ED-202A – Airworthiness Security Process Specification

[AD.7] Section B – Technical and Professional Capacity, EASA-QASC-IACT-B-TPC V1.0, of Qascom proposal in response to tender EASA.2016.HVP.10

[AD.8] Section B – Technical Offer, EASA-QASC-IACT-B-TPC V1.0, of Qascom proposal in response to tender EASA.2016.HVP.10

[AD.9] G. Gamba, L. Canzian and R. Geister, "D1 – Survey report", v1.00, 2017.

[AD.10] R. Geister, J.-P. Buch, G. Gamba and L. Canzian, "D2 – Report on FMS Threat Assessment", v1.00, 2017.

[AD.11] G. Gamba, L. Canzian, R. Geister and J.-P. Buch, "D3 – Report on GNSS Threat Assessment", v1.00, 2017.

1.4.2 REFERENCE DOCUMENTS

[RD.1] FAA, "Instrument Flying Handbook (FAA-H-8083-15B)", 2012.

1.5 OVERVIEW OF THE DOCUMENT

The document is structured as follows:

- Chapter 2 defines the flight plan;
- Chapter 3 defines the threat scenarios;
- Chapter 4 defined the simulation plan;
- Chapter 5 describes how the GNSS-based threat have been implemented within the simulator;
- Chapter 6 reports the test outcomes and provides suggestions for procedures for threat mitigation;
- Chapter 7 concludes the document with some final remarks and suggestions for the future.

2 FLIGHT PLAN DEFINITION

2.1 SCENARIO OVERVIEW

The simulation flight scenario represents a short distance flight starting from holding point A13 of runway 26R at Munich Airport and ending after the aircraft comes to a complete stop on runway 27R of Hanover Airport. This scenario is depicted in Figure 2-1, which shows also the phases at which different Threat Scenarios (TS) could be activated. Zoomed views of such scenario are also shown in Figure 2-2 and Figure 2-3.

The flight departs Munich to the north via the INPUD2N RNAV / GPS departure route and climbs to FL300. The arrival at Hanover is flown via the ELNAT4P arrival route which ends at Leine (DLE) VOR. From DLE VOR the approach is continued on runway 27R of Hanover Airport. The estimated flight time is 1:09 h. The departure and approach paths are defined by excerpts from the AIP Germany that will also be used for pilot information during the simulations.

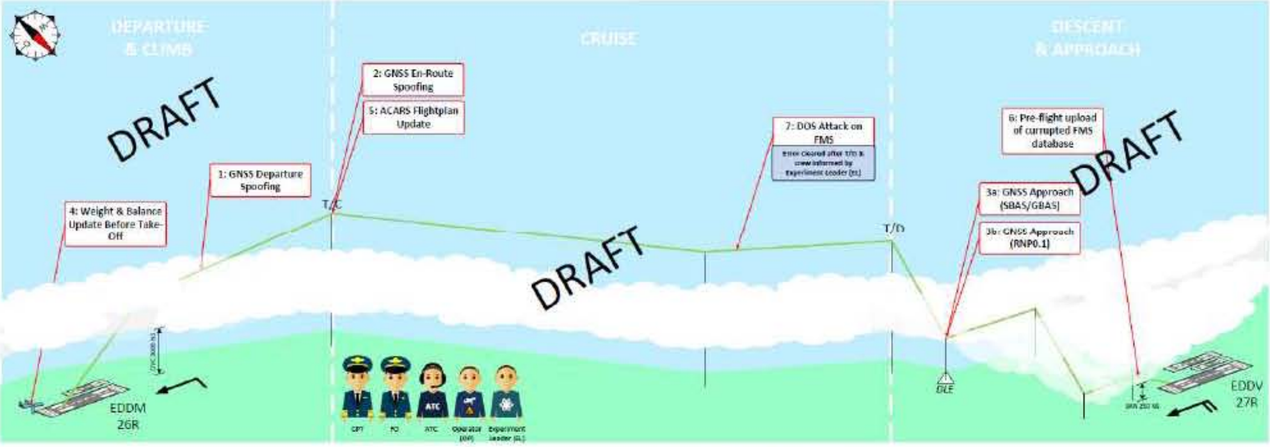

DEPARTURE & CLIMB
CRUISE
DESCENT & APPROACH
DRAFT
DRAFT
DRAFT
4: Weight & Balance Update Before Take-Off
1: GNSS Departure Spoofing
2: GNSS En-Route Spoofing
5: ACARS Flightplan Update
T/C
7: DOS Attack on FMS
Error cleared after T/D & crew informed by Experiment Leader (EL)
T/D
6: Pre-flight upload of currupted FMS database
3a: GNSS Approach (SBAS/GBAS)
3b: GNSS Approach (RNP0.1)
EDDM
26R
CPT
FO
ATC
Operator (OP)
Experiment Leader (EL)
DLE
EDDV
27R

Figure 2-1: Overview of the flight scenario.

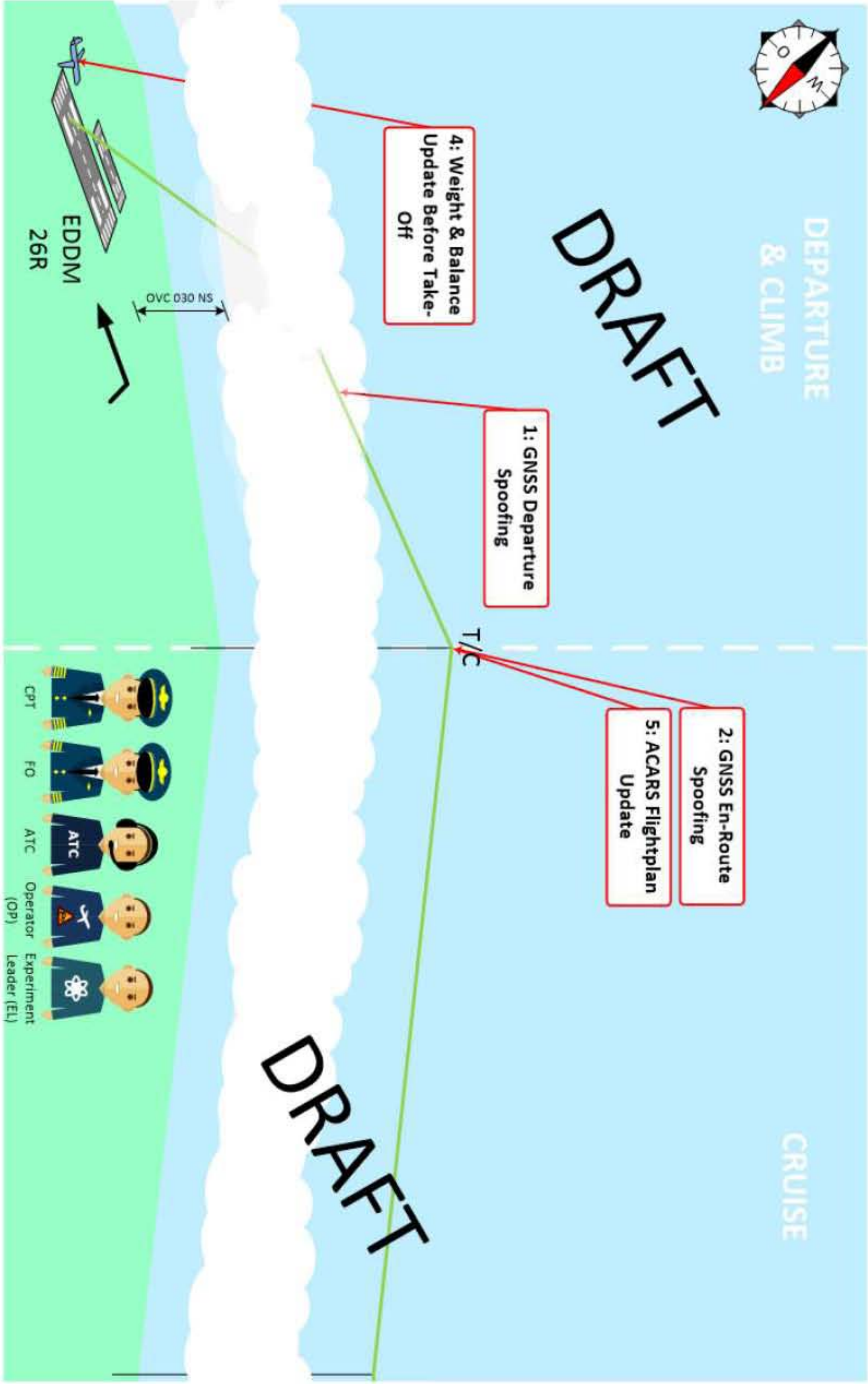

DEPARTURE & CLIMB
CRUISE
DRAFT
4: Weight & Balance Update Before Take-Off
1: GNSS Departure Spoofing
2: GNSS En-Route Spoofing
5: ACARS Flightplan Update
T/C
EDDM 26R
OVC 030 NS
CPT
FO
ATC
Operator (OP)
Experiment Leader (EL)
DRAFT

Figure 2-2: Flight scenario zoom showing the Departure, Climb and initial Cruise phases.

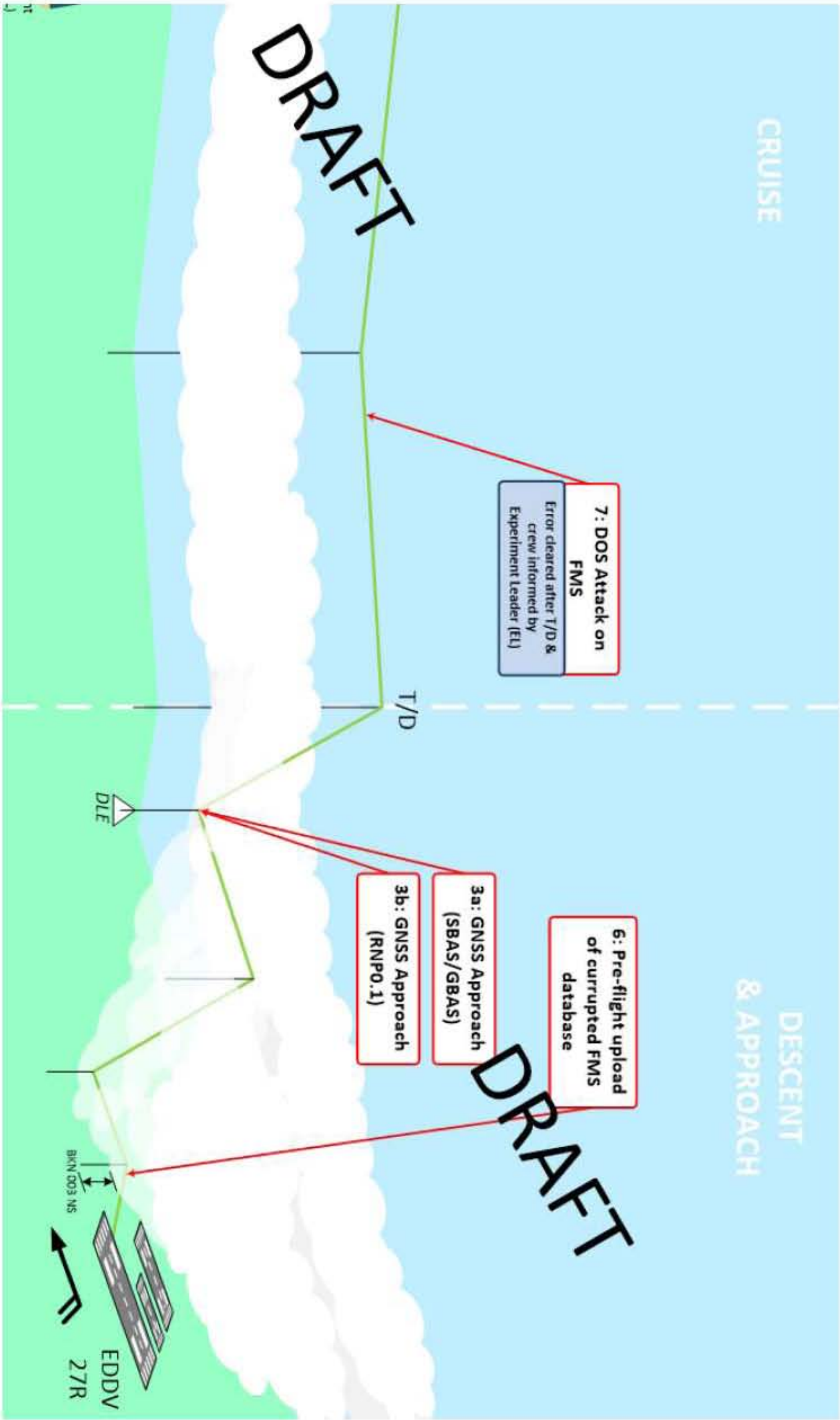

CRUISE
DESCENT
& APPROACH
7: DOS Attack on FMS
Error cleared after T/D & crew informed by Experiment Leader (EL)
T/D
DLE
3a: GNSS Approach (SBAS/GBAS)
3b: GNSS Approach (RNP0.1)
6: Pre-flight upload of currupted FMS database
BKN 003 NS
EDDV
27R

Figure 2-3: Flight scenario zoom showing the final Cruise, Descent, and Approach phases.

2.2 FILED FLIGHT PLAN

The filed flight plan, i.e., without any falsified waypoint, is provided in Table 2-1.

Waypoint	Route	wDir	wSpd	TAS [kts]	Track	GS [kts]	DIST [NM]	ETE [min]	Fuel [kg]	
RW26R EDDM	Altitude [ft/FL]	Temp	Temp Dev		WCA			ETO [min]	EFR [kg]	
	INPUD2N	256°	5	250	311°	247	5.0	1.5	165	Departure
DM066	4700							1.5	6713	
	INPUD2N	256°	5	330	346°	329	13.2	2.7	270	
DM065	FL113							4.2	6443	
	INPUD2N	256°	5	342	339°	341	6.2	1.1	96	
INPUD	FL114							5.3	6347	
	Y102	256°	5	400	342°	399	35.2	5.7	415	
UPALA	FL242							11.0	5933	Climb
	Z109	256°	5	425	350°	426	22.5	3.3	202	
RODOG	FL282							14.3	5731	
	Z109	256°	5	437	352°	438	18.0	2.5	133	
BAMAS	FL300							16.8	5597	Enroute
	Z109	256°	5	437	359°	438	11.7	1.6	69	
EBESI	FL300							18.4	5528	
	Z109	256°	5	437	359°	438	18.8	2.6	110	
PIBAD	FL300							21.0	5419	
	Z109	256°	5	437	327°	436	19.8	2.6	113	
BAMKI	FL300							23.6	5305	
	UL602	256°	5	437	296°	434	12.3	1.6	70	
TAMEB	FL300							25.3	5236	
	UL602	256°	5	437	296°	434	12.4	1.7	73	
ROBEL	FL300							27.0	5162	Descent
	UL602	256°	5	411	330°	409	31.8	4.4	123	
KEMAD	FL260							31.4	5039	
	UP605	256°	5	402	003°	403	4.9	0.6	5	
ELNAT	FL246							32.0	5034	Approach
	ELNAT4P	256°	5	371	006°	372	16.0	2.5	21	
WERRA	FL193							34.5	5013	
	ELNAT4P	256°	5	316	006°	317	24.1	4.1	38	
NORTA	FL118							38.6	4976	
	ELNAT4P	256°	5	263	019°	265	23.1	4.9	57	
DLE	3600							43.5	4919	Initial Approach
	RNP27R	256°	5	198	023°	201	10.2	2.6	69	
DV611	3000							46.1	4850	
	RNP27R	256°	5	196	318°	194	4.0	1.1	50	
DV612	3000							47.2	4800	Final Approach
	RNP27R	256°	5	174	273°	169	4.0	1.2	44	
RW27R EDDV	3000							48.4	4756	

Table 2-1: Filed flight plan.

2.3 DEPARTURE AIRPORT

In order to focus on the essential scenario flight, the taxi phase is skipped and the aircraft is already positioned at holding point A13 of runway 26R in Munich. The position is depicted in Figure 2-4 with the coordinates and true heading given in Table 2-2.

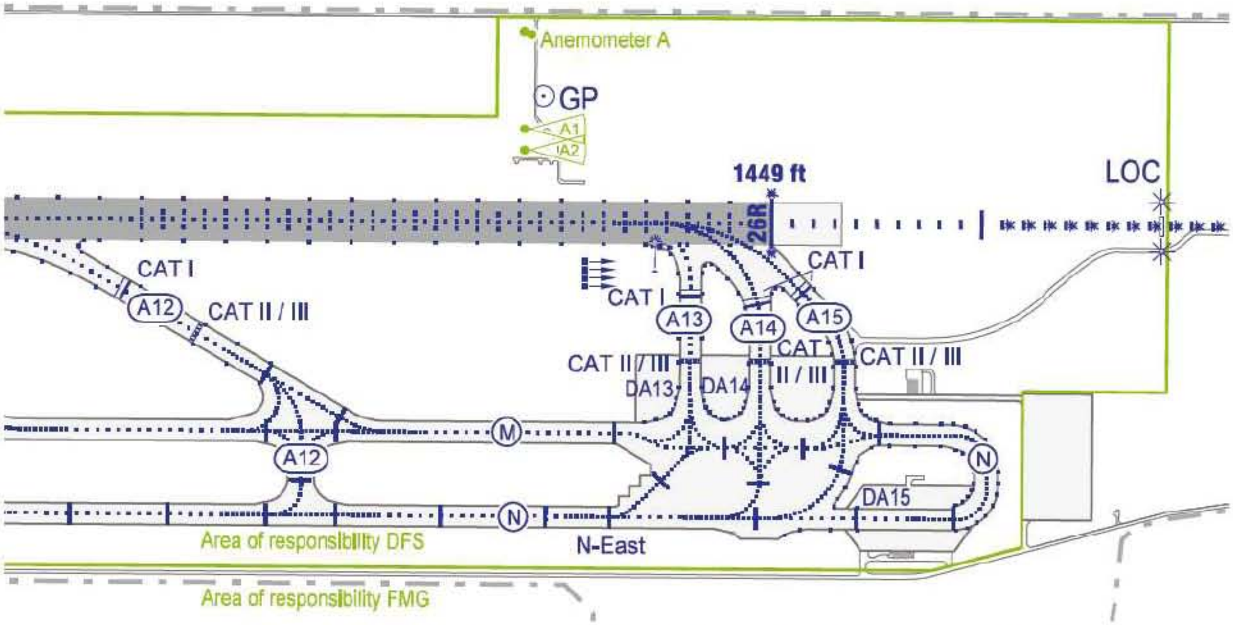


Figure 2-4: The aircraft is positioned at holding point A13 of runway 26R in Munich.

Variable	Value
Latitude	48.3656°
Longitude	11.8198°
True heading	353°

Table 2-2: Coordinates and true heading of the aircraft at holding point A13.

2.4 DEPARTURE ROUTE

The RNAV (GPS) SID INPUD2N is used for departure, which is depicted in Figure 2-5 (source: AIP Germany).

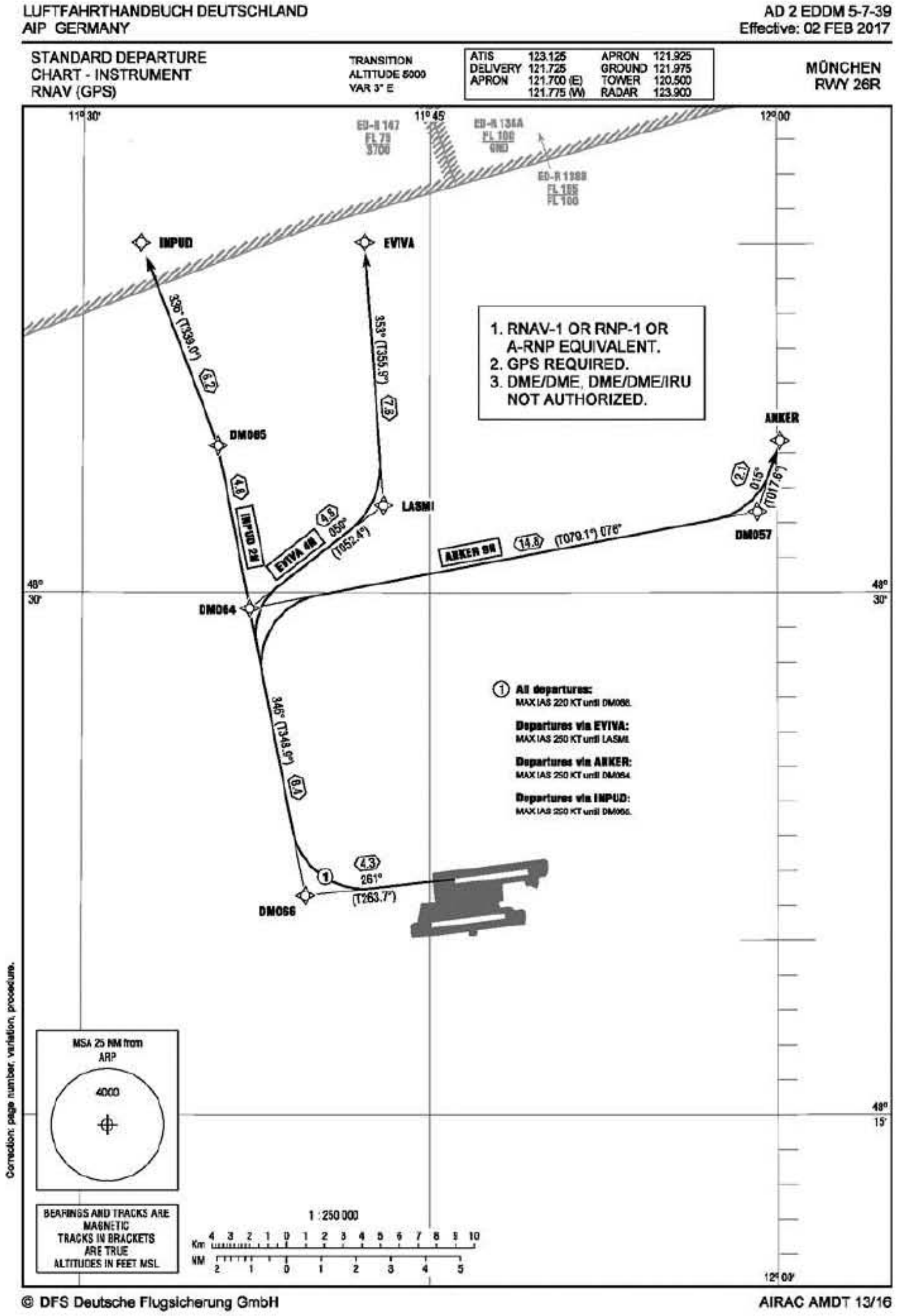
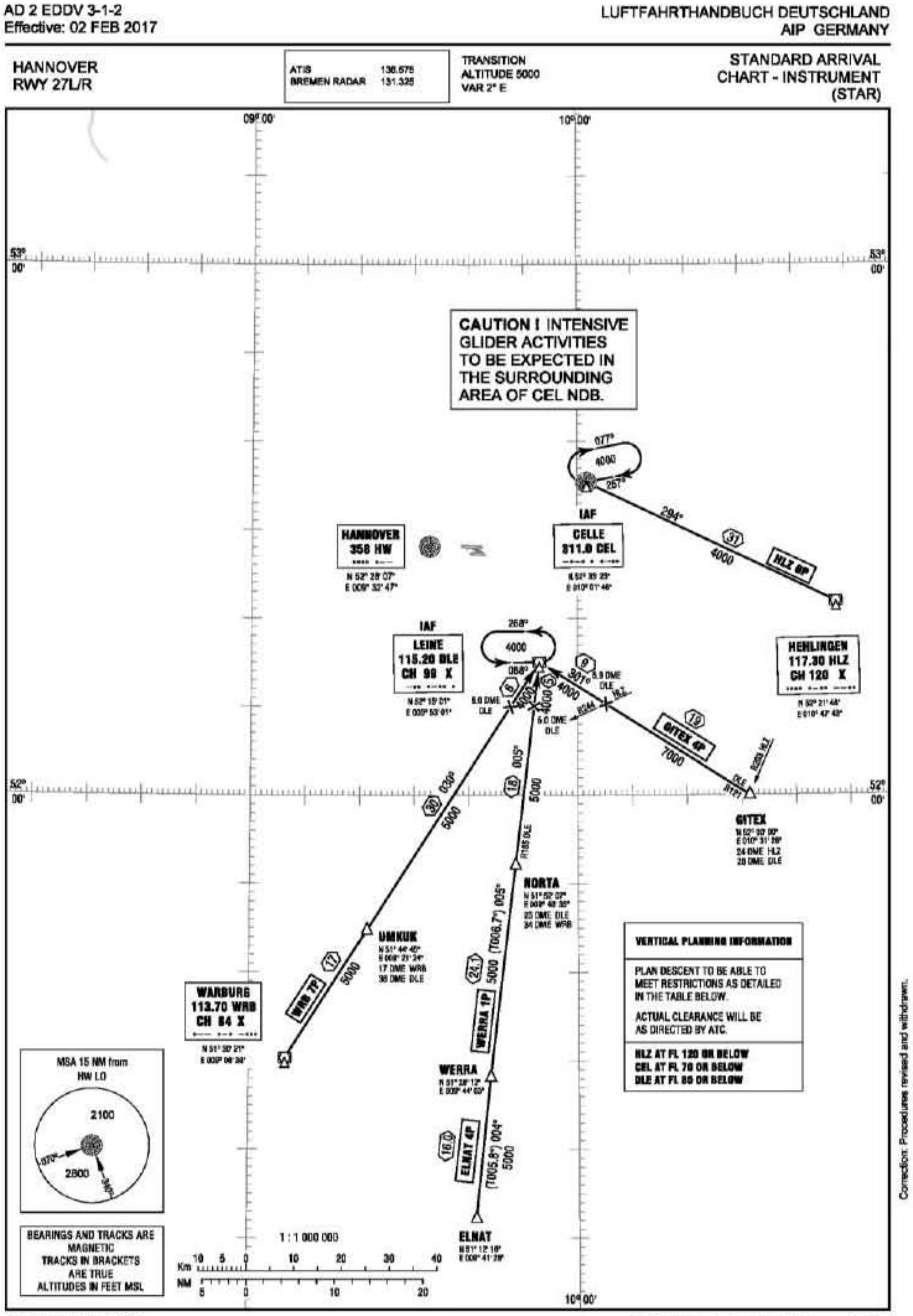


Figure 2-5: RNAV (GPS) standard departure chart showing the used INPUD2N departure.

2.5 ARRIVAL ROUTE

For the transition between en-route and approach the arrival route ELNAT4P is used, which is depicted in Figure 2-6 (source: AIP Germany).



VERTICAL PLANNING INFORMATION

PLAN DESCENT TO BE ABLE TO MEET RESTRICTIONS AS DETAILED IN THE TABLE BELOW.

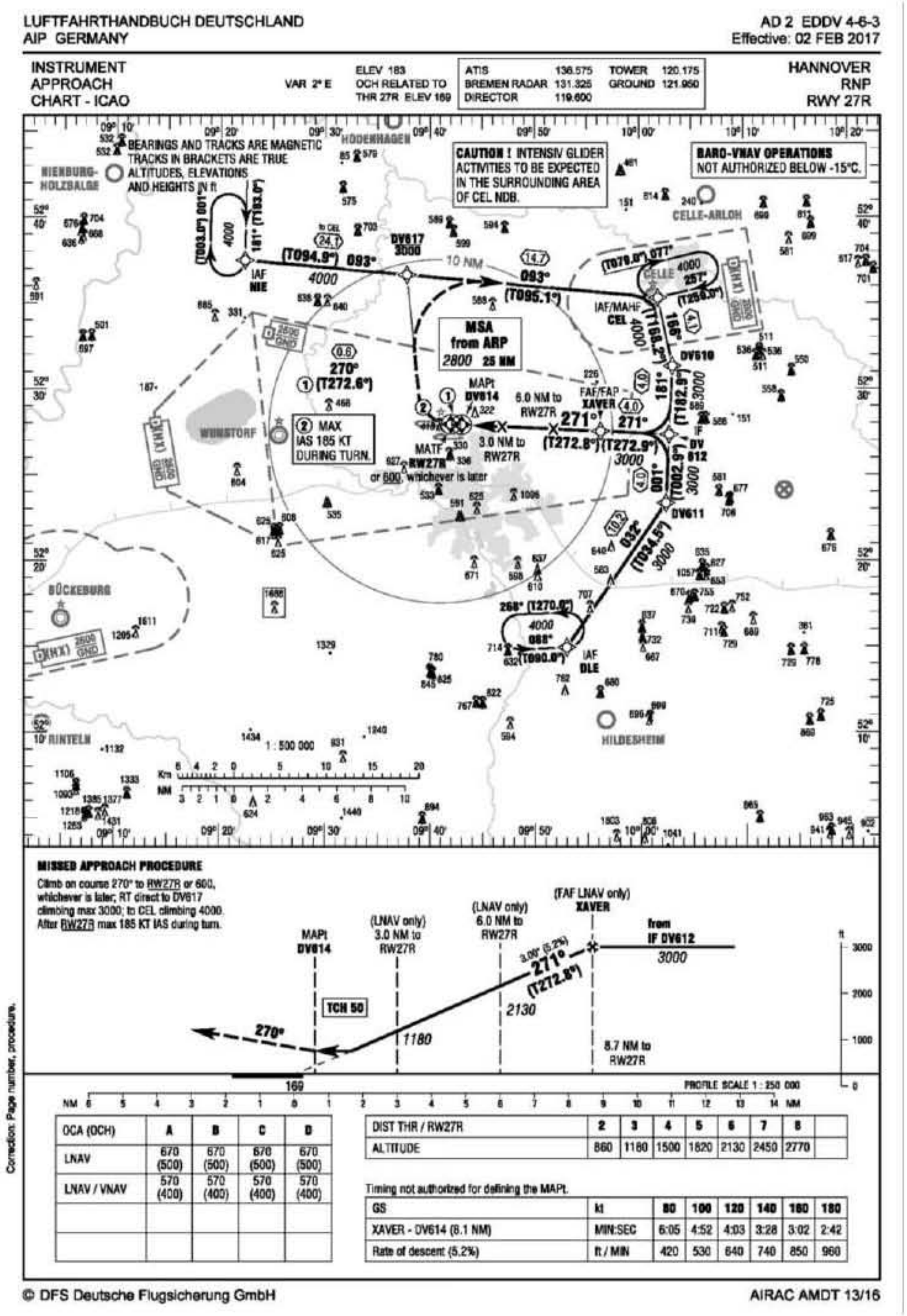
ACTUAL CLEARANCE WILL BE AS DIRECTED BY ATC.

HLZ AT FL 120 OR BELOW
CEL AT FL 70 OR BELOW
DLE AT FL 80 OR BELOW

Figure 2-6: Standard Instrument Arrival Route ELNAT4P.

2.6 APPROACH ROUTE

The RNP RWY 27R approach, which is depicted in Figure 2-7 (source: AIP Germany), is used as basis for the creation of the project specific GBAS, SBAS and RNP 0.1 approaches.



LUFTFAHRTHANDBUCH DEUTSCHLAND
AIP GERMANY

AD 2 EDDV 4-6-3
Effective: 02 FEB 2017

INSTRUMENT
APPROACH
CHART - ICAO

VAR 2° E

ELEV 183
OCH RELATED TO
THR 27R ELEV 169

ATIS	136.575	TOWER	120.175
BREMEN RADAR	131.325	GROUND	121.950
DIRECTOR	119.600		

HANNOVER
RNP
RWY 27R

BEARINGS AND TRACKS ARE MAGNETIC
TRACKS IN BRACKETS ARE TRUE
ALTITUDES, ELEVATIONS
AND HEIGHTS IN ft

CAUTION ! INTENSIV GLIDER ACTIVITIES TO BE EXPECTED IN THE SURROUNDING AREA OF CEL NDB.

BARO-VNAV OPERATIONS
NOT AUTHORIZED BELOW -15°C.

MISSED APPROACH PROCEDURE
Climb on course 270° to RW27R or 600, whichever is later; RT direct to DV617 climbing max 3000; to CEL climbing 4000. After RW27R max 185 KT IAS during turn.

OCA (OCH)	A	B	C	D
LNAV	670 (500)	670 (500)	670 (500)	670 (500)
LNAV / VNAV	570 (400)	570 (400)	570 (400)	570 (400)

DIST THR / RW27R	2	3	4	5	6	7	8	
ALTITUDE	860	1180	1500	1820	2130	2450	2770	

Timing not authorized for defining the MAPt.

GS	kt	80	100	120	140	160	180
XAVER - DV614 (8.1 NM)	MIN:SEC	6:05	4:52	4:03	3:28	3:02	2:42
Rate of descent (5.2%)	ft / MIN	420	530	640	740	850	960

Correction: Page number, procedure.

© DFS Deutsche Flugsicherung GmbH

AIRAC AMDT 13/16

Figure 2-7: Arrival chart used as basis for the approaches.

2.7 ARRIVAL AIRPORT

The flight is planned to land on runway 27R of Hanover Airport. The simulation is stopped once the aircraft comes to a complete stop on the runway. The ground chart is given in Figure 2-8 (source: AIP Germany).

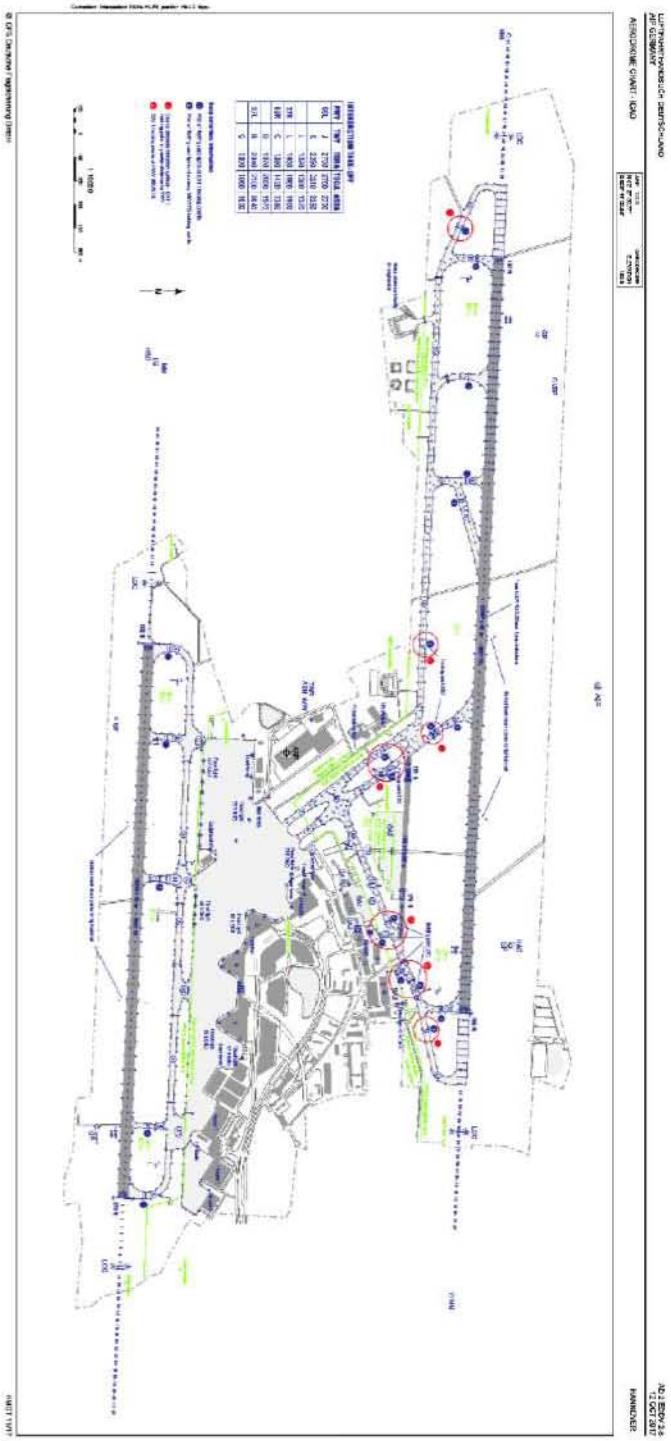


Figure 2-8: Ground chart of Hanover Airport.

2.8 LOCAL AND GLOBAL WEATHER SITUATION

The weather is utilized as a scenario element in the way that for the approach in Hanover the weather masks the position and altitude deviations introduced by the GNSS and FMS attack events. Specifically, the weather in Hanover is chosen to have broken clouds with a base of 300 ft Above Ground Level (AGL). Since the flown approaches have a minimum descent altitude of 250 ft AGL, the visual position and altitude deviations are masked until the aircraft breaks out of the clouds close to the ground. The weather at the departure airport Munich is far less critical with a cloud base of 3000 ft AGL, which is also the global could coverage along the whole flight.

The wind situation is generally calm with four to five knots at ground level, blowing from a westerly direction. The temperature is simulated according to the standard atmosphere (ISA+0) and therefore there is no need for a temperature compensation for the baro-referenced approaches.

3 THREAT SCENARIO DEFINITION

3.1 GENERAL REMARKS

The test person is the monitoring pilot in order to determine if the failure/attack is detected. DLR staff is the flying pilot. DLR staff does not actively contribute to problem detection and solution finding but supports the pilot monitoring on request.
Up to three different attacks on a representative flight are included, for the benefit of not giving away the true intention of the simulator trials to the participating pilots. Indeed, the pilots are invited under a false pretext to prevent them from being vigilant for cyber-attacks.

3.2 THREAT SCENARIOS OVERVIEW

TS ID	TS type	Attack Feasibility	Impact	Flight phase	Description
1	GNSS	Medium • GNSS signal not authenticated • Aircraft dynamic fast-changing • ATC always available Strict protection level limits	High • Short separation from obstacles and other aircrafts • ATC overloads may affect scheduling and support of other departures / arrivals	Departure	Spoofing of the GNSS position of the aircraft during departure. This causes a lateral displacement w.r.t. the actual GNSS based departure route.
2	GNSS	High • GNSS signal not authenticated • Aircraft dynamic slowly-changing • ATC not always available, in particular along oceanic routes • Loose protection level limits	Medium • Large separation from obstacles and from other airways	En-Route	Spoofing of the GNSS position of the aircraft during departure. This causes a lateral displacement w.r.t. the actual GNSS based en-route route.
3	GNSS / SBAS / GBAS spoofing	Medium • GNSS signal not authenticated • Aircraft dynamic fast-changing • ATC always available • Strict protection level limits	High • Short separation from obstacles and other aircrafts • ATC overloads may affect scheduling and support of other departures / arrivals • Runway misalignments during GNSS-based approaches (in particular for procedures exploiting GNSS also for vertical navigation) may lead to a	Approach	Spoofing of the GNSS or GNSS-SBAS or GNSS-GBAS position of the aircraft during approach. This causes a lateral and vertical displacement w.r.t. the actual GNSS based approach route. CAT I operations, with associated weather

			missed approach or to an hazardous landing		conditions, are considered.
4	Weight & Balance update before Take-Off	Medium • ACARS transmission not necessarily secured • Very small dataset • Information about values are publicly obtainable	High • W&B critical especially during T/O • Out of bounds trim setting can lead to loss of control • Auto-computed Green Dot, S, F, VAPP speeds depend directly on takeoff (and estimated landing) weight. Possible confusion about FMGC vs. FAC weight.	Take-Off	ACARS update of W&B. Before take-off, wrong mass and CG information as well as T/O speeds are received. This leads to a miss-trim of aircraft
5	Flight plan update in flight	Medium • ACARS transmission not necessarily secured • Information about values are publicly obtainable	Medium • Wrongful waypoints could lead to increased workload • ATC acts as safety net	En-Route	ACARS flight plan update in flight with new waypoints. This leads to a deviation of the flied and desired route
6	Upload of corrupted database	Low • Proprietary knowledge of FMS format required • Access to database provider IT infrastructure or to cockpit required • Knowledge of company procedures and destinations required	High • During approach, a wrongful flight path could lead into terrain • ATC overloads may affect scheduling and support of other departures / arrivals (indeed during approach ATC constantly maintains the flight path monitor of the aircraft under control and once ATC realized that the aircraft is conducting a wrong approach it intervenes to help pilots to recover and maintain safety parameters)	Approach	Wrong GNSS approach is loaded into the FMS database. IT-attack on database server of database provider. Corrupt database is loaded into both FMS. SBAS/RNP approach is carried out onto wrong waypoints during close to CAT I weather. Lateral displacement and vertical displacement
7	Denial of service attack on FMS	Low • Attacker would have to be on board and access to the FMS network which is usually decoupled from the cabin • Attacker is very likely to be detected • Extensive knowledge of FMS installed required	High • Attack could lead to double FMS failure • This will increase pilot's workload significantly • Navigation functions are deteriorated, no machine support for flight planning available • ATC as safety net	En-Route	Hacking of FMS in flight leads to double FMS failure. Total loss of both FMS

Table 3-1: Overview of the Threat Scenarios.

3.3 THREAT SCENARIOS TEST MATRIX

In each flight scenario there is a total of three different attacks on the aircraft, for the benefit of not giving away the true intention of the simulator trials to the participating pilots. Indeed, the pilots are invited under a false pretext to prevent them from being vigilant for cyber-attacks.

The scenario compositions of the seven planned simulation runs are defined in Table 3-2. It is important to remark that the table contains an empty column for the GNSS spoofing attack during the climb phase and for the SBAS/GBAS spoofing attack. In fact, these attacks were initially foreseen for the simulator trials (and for this reason the description of these attacks is present in chapters 3.4.1.2 and 3.4.3.1), but after a preliminary assessment with the simulator they were not considered for the trials, other scenarios were considered more relevant.

Scenario Number	**DEP & CLB**		**CRZ**			**DES & APCH**		
	W&B	**GNSS Spoof**	**GNSS Spoof**	**ACARS FPln**	**FMS DOS**	**DB hack**	**SBAS/GBAS Spoof**	**RNP 0.1 Spoof**
1	X			X		X		
2	X			X		X		
3	X				X	X		
4	X				X	X		
5	X		X			X		
6	X		X			X		
7	X		X					X

Table 3-2: Test matrix defining the TS that are incorporated in the different scenario runs.

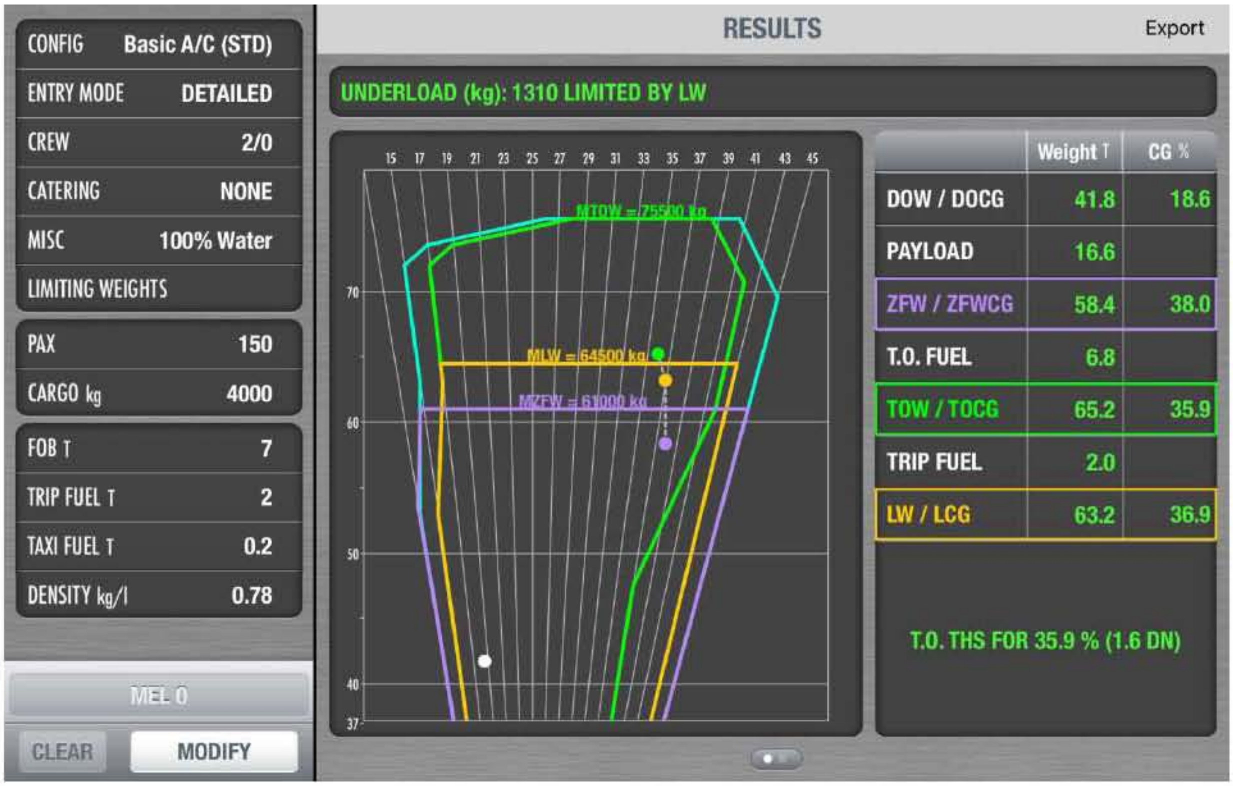
3.4 SCENARIO DESCRIPTION

3.4.1 DEPARTURE AND CLIMB PHASE

The scenario is chosen to start from the holding point position due to scenario time and simulator constraints, leaving out the taxi phase from the gate to the holding point. At the start of the scenario the aircraft is positioned at the holding point A13 of runway 26R of Munich airport. Due to simulator constraints the engines are already running with the aircraft being configured for takeoff. The crew is briefed to perform their departure briefing at the holding point position.

The Weight and Balance (W&B) data computed with the Loadsheet iOS app is given in Figure 3-1. At the holding point the aircraft has a mass of 65.2 tons and a center of gravity of 35.9%. The accompanying weight distribution is given in Figure 3-2.

During this phase of flight the flight crew either experiences an ACARS weight and balance update prior to takeoff or a GNSS spoofing during the departure. These two events are described and defined in the following subchapters.



CONFIG	Basic A/C (STD)
ENTRY MODE	DETAILED
CREW	2/0
CATERING	NONE
MISC	100% Water
LIMITING WEIGHTS	
PAX	150
CARGO kg	4000
FOB T	7
TRIP FUEL T	2
TAXI FUEL T	0.2
DENSITY kg/l	0.78

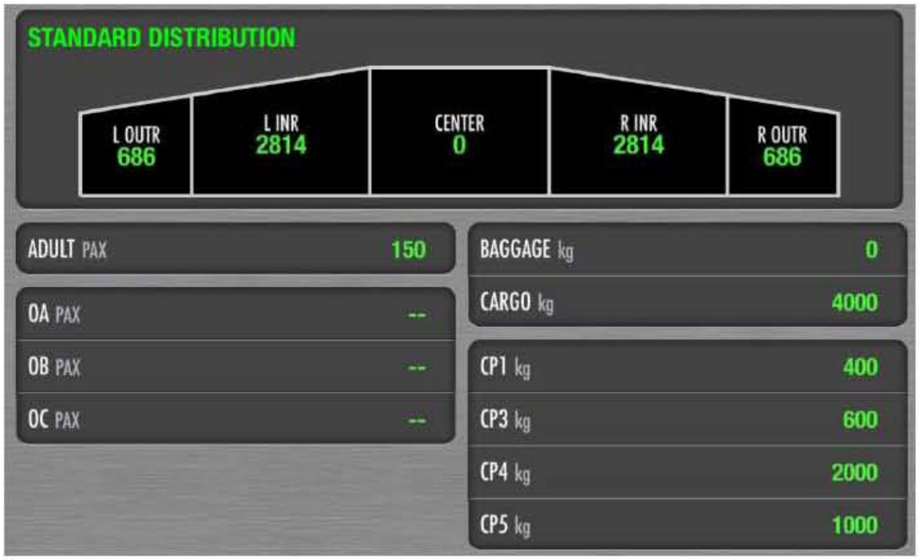
RESULTS

UNDERLOAD (kg): 1310 LIMITED BY LW

	Weight T	CG %
DOW / DOCG	41.8	18.6
PAYLOAD	16.6	
ZFW / ZFWCG	58.4	38.0
T.O. FUEL	6.8	
TOW / TOCG	65.2	35.9
TRIP FUEL	2.0	
LW / LCG	63.2	36.9

T.O. THS FOR 35.9 % (1.6 DN)

Figure 3-1: Weight & balance for the scenario flight.



STANDARD DISTRIBUTION

L OUTR	L INR	CENTER	R INR	R OUTR
686	2814	0	2814	686

ADULT PAX	150
OA PAX	--
OB PAX	--
OC PAX	--

BAGGAGE kg	0
CARGO kg	4000
CP1 kg	400
CP3 kg	600
CP4 kg	2000
CP5 kg	1000

Figure 3-2: Weight distribution.

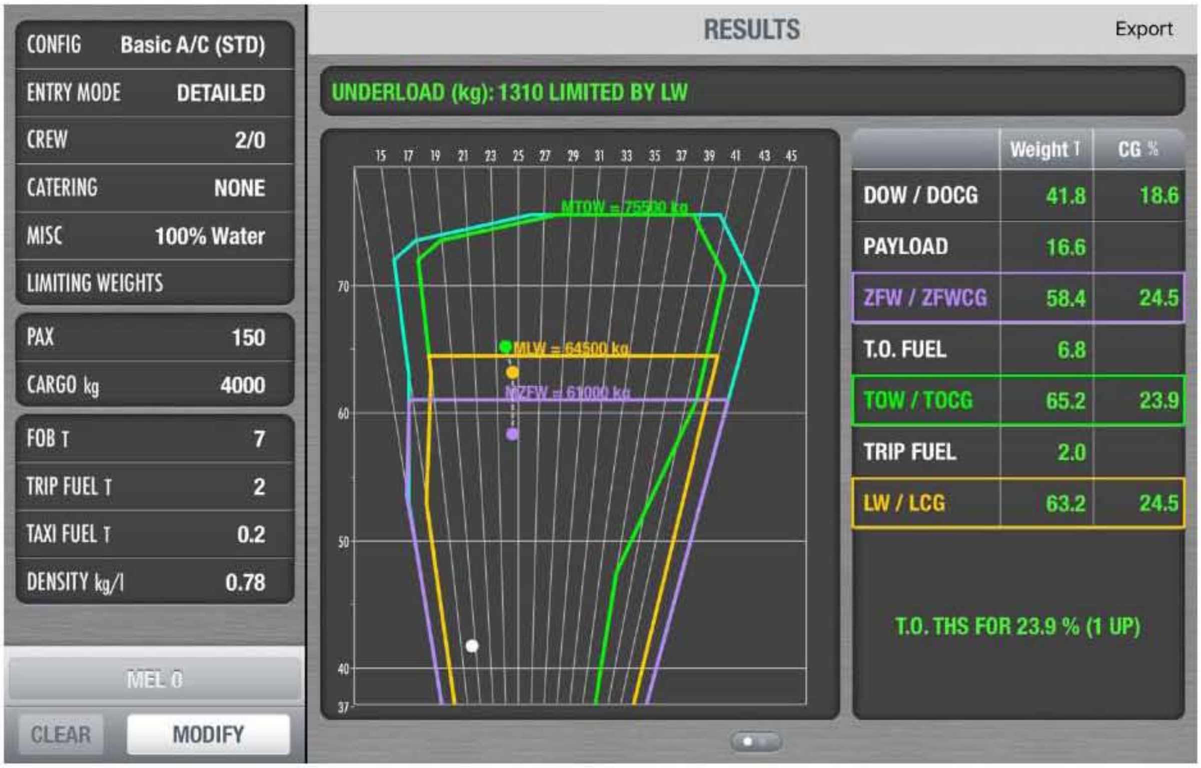
3.4.1.1 DEFINITION OF THE ACARS WEIGHT & BALANCE UPDATE EVENT

The threat scenario TO TS-1 is described in [AD.10] as:

TO TS-1: An attacker on the ground possesses the ACARS addresses of multiple aircraft and transmits falsified load sheet data via ACARS to the aircraft. On-board, the data is received, either by a print out or directly in the FMS. The worst condition for a take-off would be an aft CG and additionally a nose up trim. The elevator of the aircraft would, at certain values, lose the ability to pitch down the aircraft and that could result in an uncontrollable aircraft state. The attack would occur during the preflight phase but the results would become present in the take-off phase. Therefore, the scenario will be assigned to the take-off phase.

Attack: As shown in Figure 3-1 the aircraft has an aft center of gravity (CG). For the attack a falsified W&B with a forward CG is generated as it is given in Figure 3-3 and Figure 3-4. This falsified information is then sent by the attacker to the aircraft via ACARS. Although the computed takeoff weight has not changed, due to the falsified weight distribution the trim setting is 1° up instead of 1.6° down. This leads to a destabilization of the departure flight path. The printout that will be generated by the aircraft's printer is shown in Figure 3-5.

Timing: As the AVES cockpit does not feature a printer the printout is handed to the crew by the simulator operator when the pilots have taken their seats in the simulator and the simulation is about to start.



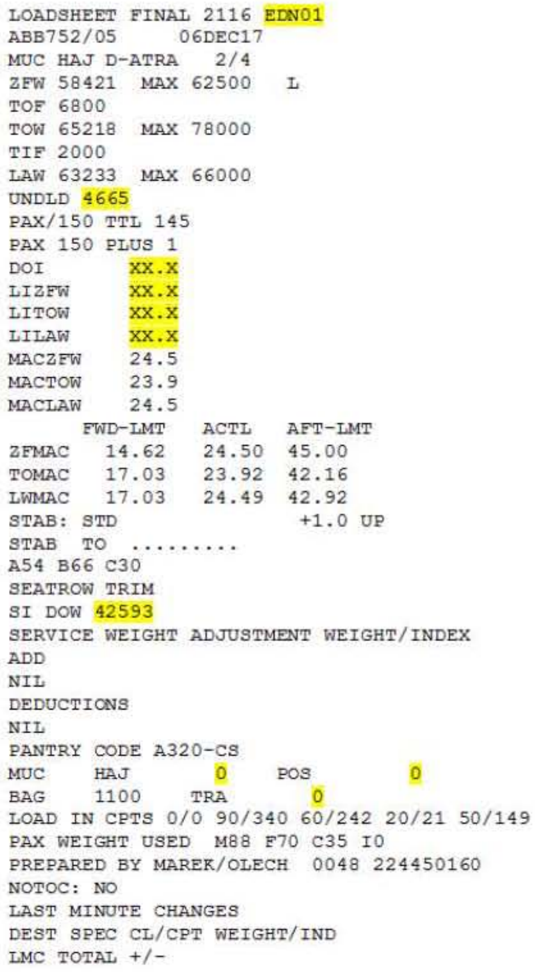
CONFIG	Basic A/C (STD)
ENTRY MODE	DETAILED
CREW	2/0
CATERING	NONE
MISC	100% Water
LIMITING WEIGHTS	
PAX	150
CARGO kg	4000
FOB T	7
TRIP FUEL T	2
TAXI FUEL T	0.2
DENSITY kg/l	0.78

UNDERLOAD (kg): 1310 LIMITED BY LW

	Weight T	CG %
DOW / DOCG	41.8	18.6
PAYLOAD	16.6	
ZFW / ZFWCG	58.4	24.5
T.O. FUEL	6.8	
TOW / TOCG	65.2	23.9
TRIP FUEL	2.0	
LW / LCG	63.2	24.5

T.O. THS FOR 23.9 % (1 UP)

Figure 3-3: Falsified Weight & Balance data used for the attack TO TS-1.



```
LOADSHEET FINAL 2116 EDN01
ABB752/05      06DEC17
MUC HAJ D-ATRA   2/4
ZFW 58421  MAX 62500   L
TOF 6800
TOW 65218  MAX 78000
TIF 2000
LAW 63233  MAX 66000
UNDLD 4665
PAX/150 TTL 145
PAX 150 PLUS 1
DOI         XX.X
LIZFW       XX.X
LITOW       XX.X
LILAW       XX.X
MACZFW      24.5
MACTOW      23.9
MACLAW      24.5
      FWD-LMT   ACTL   AFT-LMT
ZFMAC   14.62   24.50  45.00
TOMAC   17.03   23.92  42.16
LWMAC   17.03   24.49  42.92
STAB: STD               +1.0 UP
STAB  TO  .........
A54 B66 C30
SEATROW TRIM
SI DOW 42593
SERVICE WEIGHT ADJUSTMENT WEIGHT/INDEX
ADD
NIL
DEDUCTIONS
NIL
PANTRY CODE A320-CS
MUC    HAJ        0    POS        0
BAG    1100    TRA        0
LOAD IN CPTS 0/0 90/340 60/242 20/21 50/149
PAX WEIGHT USED  M88 F70 C35 I0
PREPARED BY MAREK/OLECH  0048 224450160
NOTOC: NO
LAST MINUTE CHANGES
DEST SPEC CL/CPT WEIGHT/IND
LMC TOTAL +/-
```

Figure 3-5: ACARS printout of falsified W&B data.

3.4.1.2 DEFINITION OF THE GNSS DEPARTURE SPOOFING EVENT

The GNSS threat scenario DEP TS-1 is considered for the departure phase. Specifically, the GNSS spoofing attack operates on the lateral position of the aircraft, with the goal of slowly diverging the lateral aircraft navigation with respect to the actual trajectory, up to the point in which the aircraft exits from the protected area.

Figure 3-6 illustrates the concept behind a lateral spoofing attack. If the attacker emulates a position that is on the right side of the aircraft with respect to the flight plan trajectory, then the pilot believes to be too on the right with respect to the flight plan trajectory, hence he applies a heading correction toward the left side. At this point, if the attacker continuously emulates a spoofed position that is on the right side with respect to the actual aircraft position and if the offset continuously increases, then the pilot follows a spoofed trajectory that slowly diverges from the flight plan trajectory toward the left side. Indeed, by following this trajectory the spoofed positions are compatible with the flight plan trajectory, hence the pilot believes to follow the correct course. This illustration is simplified, since it neglects effects such as the fusion of the GPS spoofed position with the inertial data (i.e., the GPIRS position solution), the actual actions performed by the pilots (e.g., position cross-check, control of the aircraft heading, etc.), and the dynamic model behind the aircraft motion; in fact, the impact of these effects have been evaluated during the simulation exercises. Nevertheless, this illustration is helpful to understand what could potentially happen during a spoofing attack and to design a spoofing attack.

For a departure phase an RNP 1 route is considered. For these types of routes, the lateral protected area is equal to Lp = 2 NM either side of the track [AD.10]. The DEP TS-1 spoofing attack is designed such that the GNSS spoofed position laterally diverges from the aircraft position of a total of $\Delta = 2 \cdot Lp = 4$ NM, from the beginning to the end of the attack. Since the attack lasts for 8 minutes, this implies that the spoofed position is computed using a lateral drift of 30 NM / hour with respect to the actual aircraft position. It is important to remark that this drift is significantly larger than the common drifts suffered by INS systems, which range from few hundredths of NM / hour for the best INS systems to few NM / hour for smaller and less expensive systems [RD.1].

The target value $\Delta = 2 \cdot Lp$ is selected such that the final point of the spoofed trajectory is significantly outside the protected area. In this way, in case the pilots “blindly” follow the indications provided by the GNSS-based navigation mode, the actual aircraft position at the end of the departure phase is expected to be outside the protected area, even considering that the GPIRS navigation solution is a fusion among the spoofed GNSS position and the aircraft inertial data.

Attack: The attack changes the GNSS position computed by the GNSS receivers. Specifically, the spoofed position laterally drifts of 30 NM / hour from the beginning of the attack to the end of the departure phase. The aircraft position at the end of the departure phase is expected to be outside the protected area, in case the aircraft is navigated following the GPIRS position solutions computed by the ADIRUs.

Timing: The attack starts 1 minute after having reached the waypoint DM066, i.e., after about 2.5 minutes since the beginning of the flight. It will last for 8 minutes, shortly before the beginning of the climb phase (see the flight plan in Table 2-1).

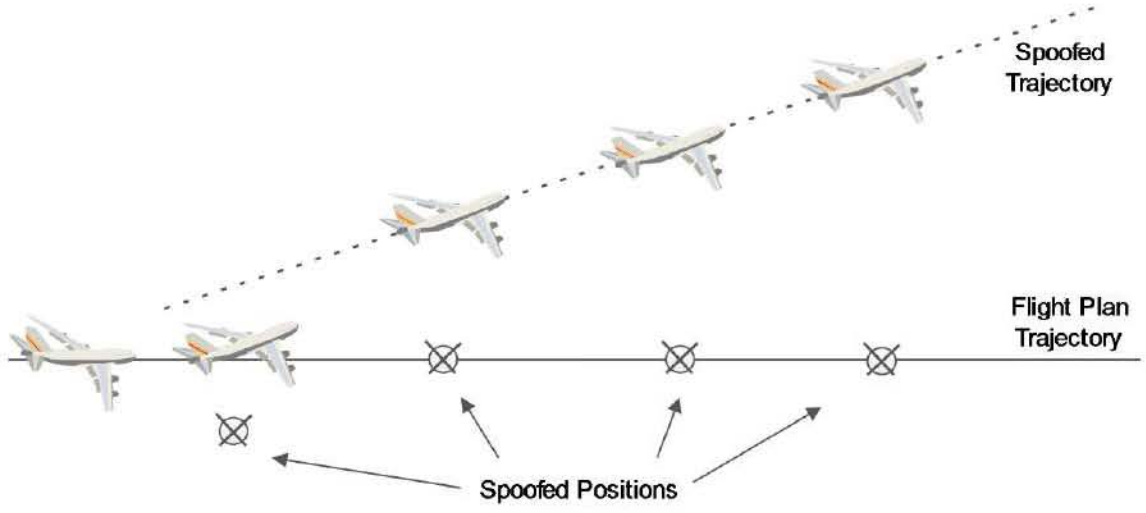


Figure 3-6: Illustration of an aircraft trajectory during a spoofing attack.

3.4.2 CRUISE PHASE

The cruise flight phase starts when the aircraft reaches its cruise flight level of FL300. This phase of flight contains four different threat scenarios that are refined in this chapter. For an increased comparability of the different experimental runs, where the threat scenarios are altered according to the test matrix given in Table 3-2, all of the threat scenarios will be triggered at the same physical location, i.e., when the aircraft passes the en-route IFR waypoint EBESI.

3.4.2.1 DEFINITION OF THE GNSS ENROUTE SPOOFING EVENT

The GNSS threat scenario EN-R TS-1 is considered for the en-route phase. Similarly to the departure phase, also in this case the GNSS spoofing attack operates on the lateral position of the aircraft, with the goal of slowly diverging the lateral aircraft navigation with respect to the actual trajectory, up to the point in which the aircraft exits from the protected area.

For the AVES sim, when GPS PRIMARY is available, the navigation performance in the en-route phase is RNP-1. For these types of routes the lateral protected area is equal to Lp = 2 NM either side of the track [AD.10]. The EN-R TS-1 spoofing attack is designed such that the GNSS spoofed position laterally diverges from the aircraft position of a total of $\Delta = 2 \cdot Lp = 4$ NM, from the beginning to the end of the attack. Since the attack lasts for 9 minutes, this implies that the spoofed position is computed using a lateral drift of 26.67 NM / hour with respect to the actual aircraft position. It is important to remark that this drift is significantly larger than the common drifts suffered by INS systems, which range from few hundredths of NM / hour for the best INS systems to few NM / hour for smaller and less expensive systems [RD.1].

The target value $\Delta = 2 \cdot Lp$ is selected such that the final point of the spoofed trajectory is significantly outside the protected area. In this way, in case the pilots “blindly” follow the indications provided by the GNSS-based navigation mode, the actual aircraft position at the end of the departure phase is expected to be outside the protected area, even considering that the GPIRS navigation solution is a fusion among the spoofed GNSS position and the aircraft inertial data.

Attack: The attack changes the GNSS position computed by the GNSS receivers. Specifically, the spoofed position laterally drifts of 26.67 NM / hour from the beginning of the attack to the end of the en-route phase. The aircraft position at the end of the en-route phase is expected to be outside the protected area, in case the aircraft is navigated following the GPIRS position solutions computed by the ADIRUs.

Timing: The attack starts 30 seconds after having reached the waypoint BAMAS, i.e., after about 17.3 minutes since the beginning of the flight. It will last for 9 minutes, shortly before the beginning of the descent phase (see the flight plan in Table 2-1).

3.4.2.2 DEFINITION OF THE ACARS FLIGHTPLAN UPDATE EVENT

The threat scenario EN R TS-11 is described in [AD.10] as:

EN-R TS-11: An attacker on the ground possesses the ACARS addresses of multiple aircraft and transmits falsified flight plan data to an aircraft. The attacker would need to know the departure and the arrival airport and have an idea of the used route to tailor the attack to the actual flight path but the data is easily obtainable through observation. The pilots would accept the new flight plan and deviate laterally from their desired path.

Attack: The attack changes the en-route part of the flight plan between the IFR waypoint EBESI to a more easterly trajectory, including a change of the proposed arrival route that is changed from the original ELNAT4P to the GITEX4P arrival. The air traffic control sector affected by the attack is shown in Figure 3-7.

Timing: The bogus FMGC flight plan update transmitted by the attacker via ACARS and printed out on the aircraft's printer is handed out to the crew by the simulator operator after the aircraft has entered the ATC sector "EDMM_FRKU_1 FL266 – FL315" approximately 12:27 minutes after takeoff. When the attack is triggered the aircraft is approximately eight minutes of flight time away from the bogus flight plan changes. The ACARS printout that is handed to the crew is shown in Figure 3-8.

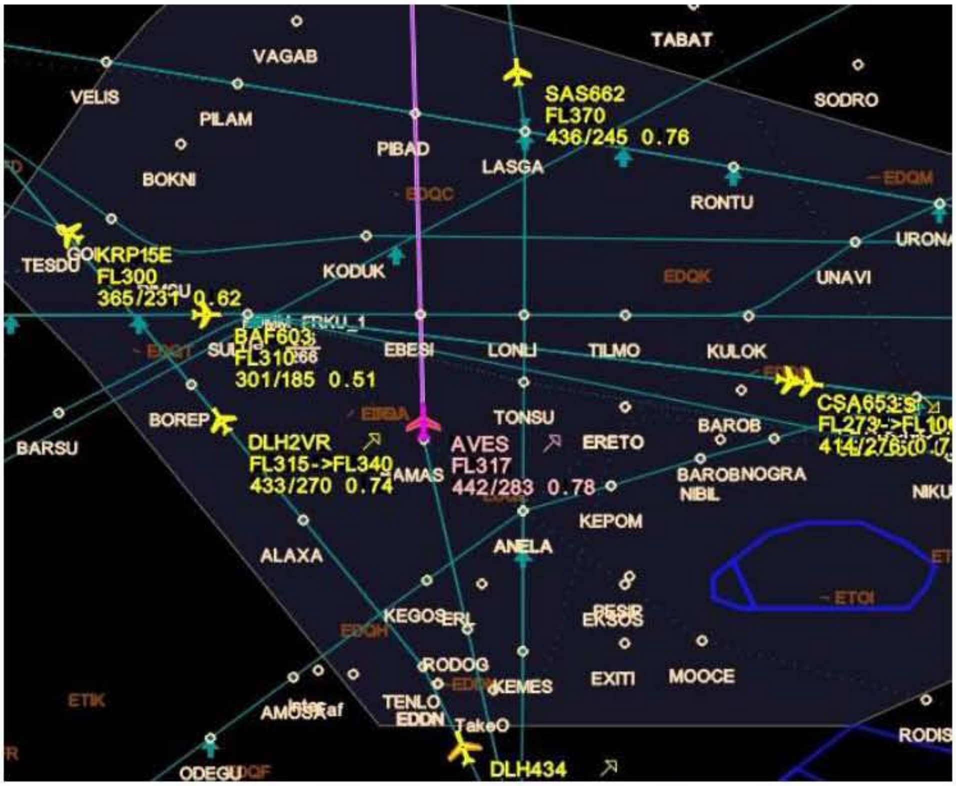
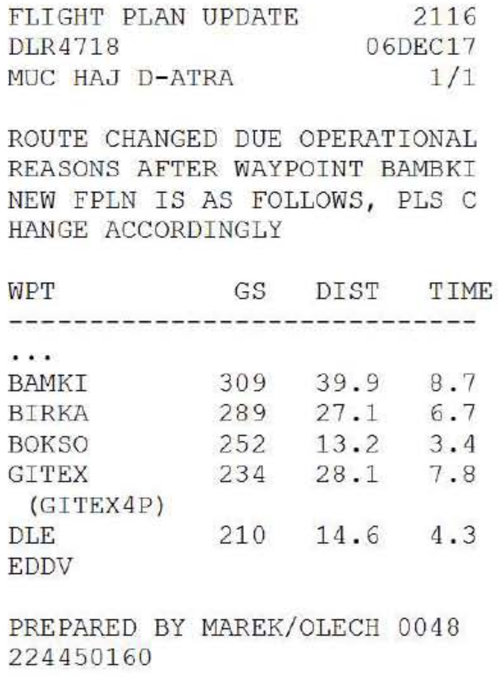


Figure 3-7: Flight plan change location.



```
FLIGHT PLAN UPDATE          2116
DLR4718                  06DEC17
MUC HAJ D-ATRA               1/1

ROUTE CHANGED DUE OPERATIONAL
REASONS AFTER WAYPOINT BAMBKI
NEW FPLN IS AS FOLLOWS, PLS C
HANGE ACCORDINGLY

WPT          GS   DIST   TIME
-----------------------------
...
BAMKI        309   39.9   8.7
BIRKA        289   27.1   6.7
BOKSO        252   13.2   3.4
GITEX        234   28.1   7.8
 (GITEX4P)
DLE          210   14.6   4.3
EDDV

PREPARED BY MAREK/OLECH 0048
224450160
```

Figure 3-8: Bogus ACARS flight plan update that is handed to the crew.

3.4.2.3 DEFINITION OF THE DOS ATTACK EVENT

The threat scenario EN R TS-12 is described in [AD.10] as:

EN-R TS-12: An attacker on board of the aircraft is able to access an interface to the FMS. The attacker starts a denial of service (DoS) attack so that the FMS is not responding in freezes at 100% task load. The complete functionality is lost. No flight planning via MCDU is possible nor is a map displayed. Independent navigation systems (VOR, DME…) are with backup display systems are still available. This situation will lead to an increased workload in the cockpit due to increased communication activities between the pilots and with ATC. In addition, paper navigation and/or ATC guided navigation will be required.

Attack: On the triggering of the DOS attack the MCDU screen freezes and the system does not react to pilot inputs. Additionally, the map on the navigation display (ND) disappears with the "MAP" flag showing up in the ND. An example of the resulting ND is given in Figure 3-9.

Timing: The DOS attack is triggered with the aircraft passing the IFR waypoint EBESI. This point of time is chosen so that all threat scenarios of the cruise flight phase are triggered at the same point of time, which is expected to increase the comparability of the different scenario elements. The DOS attack is held for a time of 180 seconds.

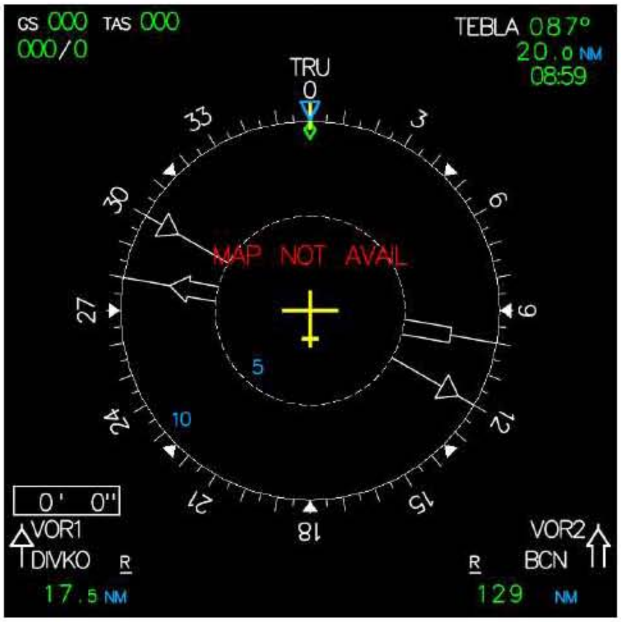


Figure 3-9: Navigation display (ND) showing the MAP NOT AVAIL flag.

3.4.3 DESCENT AND APPROACH PHASE

The descent and approach flight phase begins when the aircraft descends from its cruise flight level. This part of the flight contains three different cyberattacks on the aircraft that are described in the following subchapters.

3.4.3.1 SBAS/GBAS APPROACH EVENT

For a SBAS/GBAS-based approach the GNSS threat scenarios ARR TS-2 and ARR TS-3 are considered.

SBAS-based approaches are part of the RNP APCH procedures. Specifically, an SBAS-based approach is a Localizer Performance with Vertical guidance (LPV) approach, a type of Approach Procedure with Vertical guidance (APV) in which the vertical guidance is provided by the GNSS-based position solution. LPV is a non-precision approach, nevertheless it allows to fly up to a DA of 200-250 feet, similarly to a Category I precision approach.

GBAS-based approaches are instead performed through a GBAS Landing System (GLS), they are not Performance Based Navigation (PBN) approaches. GBAS allows to fly Category I (200' ≤ DA < 250'), Category II (100' ≤ DA < 200'), and Category III (DA < 100') precision approaches, and it will eventually support landings all the way down to the runway surface.

Though SBAS and GBAS are different types of approaches, they are treated in the same way during the simulation exercises. Indeed, they have several commonalities, for example they both allow to fly up to a DA of 200-250 feet and, most of all, in both cases the vertical guidance is provided through the GNSS-based position solution. Because of this, in the considered SBAS/GBAS threat scenario the spoofing attack operates both on the lateral and on the vertical position of the aircraft, with the goal of slowly diverging the lateral and vertical aircraft navigation with respect to the actual trajectory, up to the point in which the aircraft exits from the protected area, both laterally and vertically.

Concerning the lateral deviation, it is important to remark that a pure later deviation becomes less intense after a turn, because a component of the lateral deviation becomes projected on the longitudinal path. As an extreme case, a pure later deviation becomes a pure longitudinal deviation after a 90° turn. Since some turns are foreseen during the approach phase (in fact, the landing runway is orienting in the east-west direction, whereas the en-route path is towards the south-north direction), it is convenient to apply a longitudinal drift in addition to the lateral drift, in order to guarantee a certain lateral deviation also after the turns.

The final approach leg of a RNP APCH procedure is RNP 0.3, with a lateral protected area of Lp = 0.95 NM either side of the track [AD.10]. The spoofing attack is designed such that the GNSS spoofed position laterally and longitudinally diverges from the aircraft position of a total of $\Delta_{lat} = 2 \cdot Lp = 1.9$ NM, from the beginning to the end of the attack. Since the attack lasts for 12 minutes, this implies that the spoofed position is computed using a lateral drift of 9.5 NM / hour and a longitudinal drift of 9.5 NM / hour with respect to the actual aircraft position. The target value $\Delta_{lat} = 2 \cdot Lp$ is selected such that the final point of the spoofed trajectory is significantly outside the protected area. In this way, in case the pilots "blindly" follow the indications provided by the GNSS-based navigation mode, the actual aircraft position at the end of the departure phase is expected to be outside the protected area, even considering that the GPIRS navigation solution is a fusion among the spoofed GNSS position and the aircraft inertial data.

Concerning the vertical deviation introduced by the spoofing attack, for an RNP APCH procedure the MOC can be as low as $MOC_{min} = 75$ m [AD.10]. The spoofing attack is designed such that the GNSS spoofed position vertically diverges from the aircraft position of a total of $\Delta_{ver} = MOC_{min} = 75$ m, from the beginning to the end of the attack. Since the attack lasts for 12 minutes, this implies that the spoofed position is computed using a vertical drift of 6.25 m / minute with respect to the actual aircraft position. It is important to remark that the GNSS spoofed position must be at a higher altitude than the aircraft actual altitude, in order for the pilot to correct the aircraft trajectory and fly at an altitude below the planned one. The value $\Delta_{ver} = MOC_{min}$ is selected such that the final point of the spoofed trajectory could be very close to the vertical limit of the primary protection area. In addition, it is important to remark that the considered MDA is 250 feet, corresponding to 75 m, equal to the considered Δ_{ver}. Hence, in case the pilots "blindly" follow the indications provided by the GNSS-based navigation mode, the aircraft altitude could be extremely close to the ground level before reaching the runway.

Attack: The attack changes the GNSS position computed by the GNSS receivers. Specifically, the spoofed position drifts laterally of 9.5 NM / hour, longitudinally of 9.5 NM / hour, and vertically of 6.25 m / minute, from the beginning of the attack to the end of the approach phase. The aircraft position at the end of the approach phase is expected to be outside the protected area and at a dangerously low altitude, in case the aircraft is navigated following the GPIRS position solutions computed by the ADIRUs.

Timing: The attack starts 30 seconds after having reached the waypoint WERRA, i.e., after about 35 minutes since the beginning of the flight. It lasts for 12 minutes, shortly before the beginning of the final approach phase (see the flight plan in Table 2-1).

3.4.3.2 GNSS RNP 0.1 APPROACH EVENT

For a GNSS RNP 0.1 approach the GNSS threat scenario ARR TS-1 is considered. RNP 0.1 is part of the RNP AR APCH procedures. These procedures allow to perform an Approach Procedure with Vertical guidance (APV), in which the vertical guidance is provided by an altimeter (Baro VNAV). Hence, the GNSS-based position solution is only exploited for lateral guidance. For this reason, in this threat scenario, similarly to the departure and en-route phases, the GNSS spoofing attack operates on the lateral position of the aircraft, with the goal of slowly diverging the lateral aircraft navigation with respect to the actual trajectory, up to the point in which the aircraft exits from the protected area.

It is important to remark that a pure later deviation becomes less intense after a turn, because a component of the lateral deviation becomes projected on the longitudinal path. As an extreme case, a pure later deviation becomes a pure longitudinal deviation after a 90° turn. Since some turns are foreseen during the approach phase (in fact, the landing runway is orienting in the east-west direction, whereas the en-route path is towards the south-north direction), it is convenient to apply a longitudinal drift in addition to the lateral drift, in order to guarantee a certain lateral deviation also after the turns.

In an RNP 0.1 route the lateral protected area is equal to Lp = 0.2 NM either side of the track [AD.10]. The AR-R TS-1 spoofing attack is designed such that the GNSS spoofed position laterally diverges from the aircraft position of a total of $\Delta = 2 \cdot Lp = 0.4$ NM, from the beginning to the end of the attack. Since the attack lasts for 12 minutes, this implies that the spoofed position is computed using a lateral drift of 2 NM / hour and a longitudinal drift of 2 NM / hour with respect to the actual aircraft position, similar to common drifts suffered by small and cheap INS systems [RD.1].

The target value $\Delta = 2 \cdot Lp$ is selected such that the final point of the spoofed trajectory is significantly outside the protected area. In this way, in case the pilots "blindly" follow the indications provided by the GNSS-based navigation mode, the actual aircraft position at the end of the departure phase is expected to be outside the protected area, even considering that the GPIRS navigation solution is a fusion among the spoofed GNSS position and the aircraft inertial data.

Attack: The attack changes the GNSS position computed by the GNSS receivers. Specifically, the spoofed position drifts laterally of 2 NM / hour and longitudinally of 9.5 NM / hour from the beginning of the attack to the end of the approach phase. The aircraft position at the end of the approach phase is expected to be outside the protected area, in case the aircraft is navigated following the GPIRS position solutions computed by the ADIRUs.

Timing: The attack starts 30 seconds after having reached the waypoint WERRA, i.e., after about 35 minutes since the beginning of the flight. It lasts for 12 minutes, shortly before the beginning of the final approach phase (see the flight plan in Table 2-1).

3.4.3.3 CORRUPTED DATABASE EVENT

The threat scenario ARR TS-15 is described in [AD.10] as:

ARR TS-15: An attacker is able to access the servers of an FMS database provider. The final approach segment data of one or several approaches are altered. Specifically, the data for an SBAS (EGNOS) approach is changed. The attacker was able to lower the threshold height so that the glide path leads into the ground way before the real runway. The aircraft concludes an approach in poor weather conditions with a cloud ceiling around 250ft. The attacker was able to change the data so that the aircraft reaches that altitude before the actual runway starts.

Attack: The attacker manages to generate an FMS database with a falsified threshold height for the approach to runway 27R of Hanover airport. The nominal threshold height for this runway was 169 ft MSL before the attacker set it to 0 ft MSL, while leaving the altitude of the final approach fix XAVER of 3000 ft AGL unchanged. This changed geometry leads to a potential ground contact approximately 0.5 NM in front of the threshold of runway 27R.

Timing: As the corrupted database has to be loaded into the FMS, this attack must be performed before the actual flight. The corrupted database is an identical copy of the nominal AVES simulator FMS dataset, except for the threshold altitude of runway 27R of Hanover Airport.

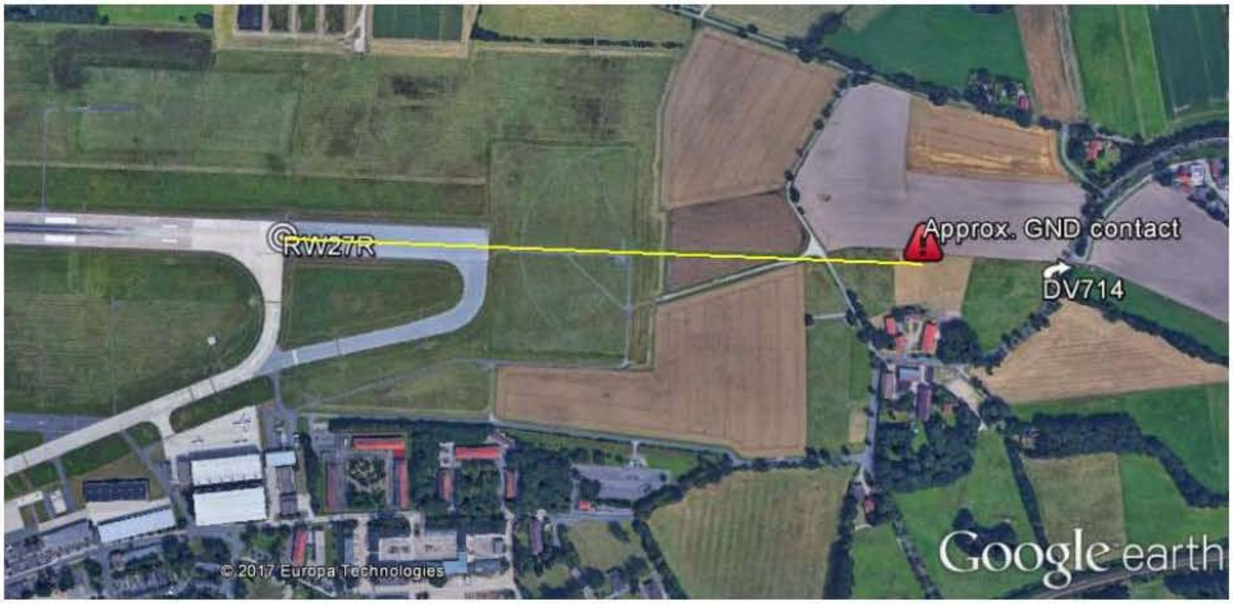


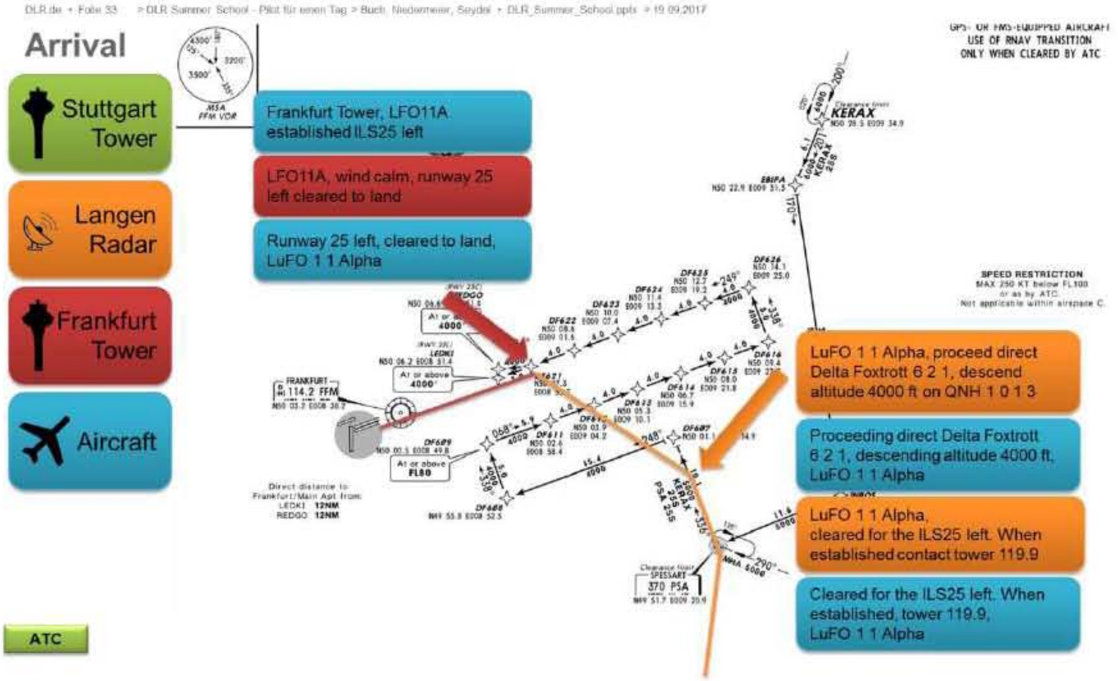
Figure 3-10: The lowered threshold height leads to a potential ground contact approximately 0.5 NM (yellow line) before the threshold, shortly after passing the missed approach point DV714.

4 SIMULATION PLAN

4.1 ATC SCRIPT

The ATC script defines how the ATM controller works. The basic idea is described in the following:

- 2 controllers
  - 1st one is the actor controller and controls departure and approach parts of the flight and is provided by the experiment personnel;
  - 2nd one controls the en-route part of the flight and belongs to the experiment participants as the consequences of aircraft cyberattacks on the ATM system shall also be examined (detection of route deviations/violations and decision-making during attack situations).
- The clearances of the first of these controllers have been scripted to reduce unnecessary variability over the different experimental runs. This also compensates changes in experiment personnel over the experiment period, e.g., when a controller is not available on all experiment runs.
- An example of such a script is given in Figure 4-1 from a different experiment. Basically, ATC clearances are written directly into the navigational charts. These are provided at the ATC workstation for the controller who acts as actor. The script is integrated according to the considered scenario, based on the appropriate navigational charts.



DLR.de • Folie 33 > DLR Summer School - Pilot für einen Tag > Buch, Niedermeier, Seydel • DLR_Summer_School.pptx > 19.09.2017

Arrival

Frankfurt Tower, LFO11A established ILS25 left

LFO11A, wind calm, runway 25 left cleared to land

Runway 25 left, cleared to land, LuFO 1 1 Alpha

LuFO 1 1 Alpha, proceed direct Delta Foxtrott 6 2 1, descend altitude 4000 ft on QNH 1 0 1 3

Proceeding direct Delta Foxtrott 6 2 1, descending altitude 4000 ft, LuFO 1 1 Alpha

LuFO 1 1 Alpha, cleared for the ILS25 left. When established contact tower 119.9

Cleared for the ILS25 left. When established, tower 119.9, LuFO 1 1 Alpha

GPS- OR FMS-EQUIPPED AIRCRAFT USE OF RNAV TRANSITION ONLY WHEN CLEARED BY ATC

SPEED RESTRICTION MAX 250 KT below FL100 or as by ATC. Not applicable within airspace C.

Direct distance to Frankfurt/Main Apt from: LEDKI 12NM REDGO 12NM

Figure 4-1: Sample of an ATC script used in a different AVES experiment.

4.2 ACTOR PILOT SCRIPT

The role of the pilot acting has been scripted in a way that the general behavior is the same for all experimental runs. DLR staff is the pilot flying. DLR staff does not actively contribute to problem detection and solution finding but support the pilot monitoring on request.

- General before Take-Off check list;
- Normal Take-off with standard callouts;
- If falsified W/B is not detected, this might lead to a crash. If so, then scenario is reset;
- Activation of autopilot after reaching acceleration altitude and climb speed/thrust;
- Check list.

Basic rules of thumb have considered to help the DLR staff pilot to behave consistently, even in the dynamically changing scenario environment.

4.3 SIMULATOR PREPARATION

4.3.1 FAMILIARIZATION SCENARIO

Within the familiarization scenario, the airline pilot was the pilot flying. Two ILS approaches were flown, one with a planned go-around and a manual landing after a traffic pattern. The DLR staff was the pilot monitoring.

4.3.1.1 ENVIRONMENT SETUP

The simulation environment for the familiarization was Frankfurt airport (EDDF) during good weather conditions.

4.3.1.2 AIRCRAFT SETUP

The aircraft simulator were set up normally with two different weights for the two approaches all within the normal envelope of the aircraft.

4.3.2 EXPERIMENT SCENARIO

During the experiments, flights were conducted from Munich (EDDM) to Hanover (EDDV). The flights had the same setup in terms of fuel, weather and flight plan. However, the three cyber-attacks that were simulated were changed during the trials. The airline pilots were the pilot monitoring in this case and DLR staff was the pilot flying.

4.3.2.1 ENVIRONMENT SETUP

The environment was a standard aircraft with a scheduled flight from Munich to Hanover within nominal operating conditions. The flight was operated in IMC with appropriate weather conditions.

4.3.2.2 AIRCRAFT SETUP

The aircraft was set up according to normal operations with enough fuel to conduct the flight safely and plenty of reserve fuel. All systems were operating properly to conduct a normal flight.

4.4 CREW SCENARIO BRIEFING

This chapter contains all briefing information the crew received before the simulation run. The briefing is split into two parts:

1. The general simulator briefing containing information about the experimental run, giving a false clue to the pilots about the experiments intention and excluding cybersecurity matters. Also included in this part is a safety instruction for the AVES simulator and relevant differences that are to be expected in AVES when compared to the real world, including a short familiarization flight in the simulator. This familiarization flight consists of a visually flown traffic pattern at another airport than the ones used during the later experiment. The briefing was performed in the AVES briefing room, the familiarization flight was performed in AVES. After the familiarization flight the crew came back to the briefing room again for the following flight briefing.
2. The flight briefing, containing information about the planned flight from Munich to Hanover. Relevant information like weather, weight and balance and the flight route were presented to the crew. Afterwards the crew had sufficient time to perform a self-briefing with the provided information.

4.4.1 GENERAL SIMULATOR INFORMATION

A general safety briefing for the simulator was conducted and the limitations of the simulator were described. Some of these limitations are: non-certified software, not fully implemented MCDU pages (not relevant for flight) and some differences in the presentation of map information on the displays.

4.4.2 FLIGHT BRIEFING

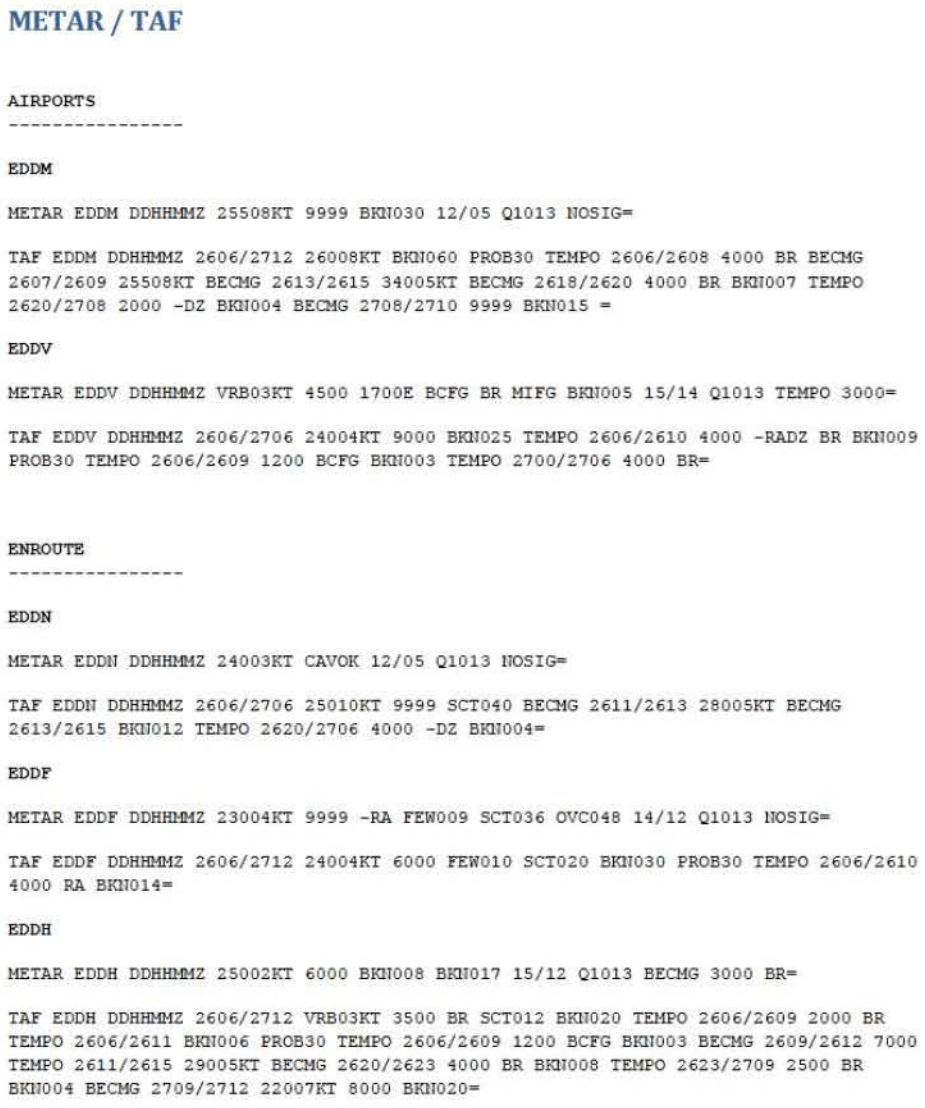
For each test flight, the general flight briefing was conducted. It was the same for each trial.

4.4.2.1 GENERAL FLIGHT INFORMATION

For each flight, a short operational briefing was given in form of a Power Point presentation. Afterwards, the documents for the flight were handed to the pilots. The briefing included the departure and destination airports, as well as the flight plan. In addition, the performance calculation including fuel quantity and the weight and balance were presented to the airline pilots.

4.4.2.2 WEATHER BRIEFING

The weather briefing was the same for all flight trials. It was according to Figure 4-2. It was good enough to conduct a non-precision RNP approach but bad enough not to spot the altered approach path before the minimum descent height.



METAR / TAF

```
AIRPORTS
----------------

EDDM

METAR EDDM DDHHMMZ 25508KT 9999 BKN030 12/05 Q1013 NOSIG=

TAF EDDM DDHHMMZ 2606/2712 26008KT BKN060 PROB30 TEMPO 2606/2608 4000 BR BECMG
2607/2609 25508KT BECMG 2613/2615 34005KT BECMG 2618/2620 4000 BR BKN007 TEMPO
2620/2708 2000 -DZ BKN004 BECMG 2708/2710 9999 BKN015 =

EDDV

METAR EDDV DDHHMMZ VRB03KT 4500 1700E BCFG BR MIFG BKN005 15/14 Q1013 TEMPO 3000=

TAF EDDV DDHHMMZ 2606/2706 24004KT 9000 BKN025 TEMPO 2606/2610 4000 -RADZ BR BKN009
PROB30 TEMPO 2606/2609 1200 BCFG BKN003 TEMPO 2700/2706 4000 BR=


ENROUTE
----------------

EDDN

METAR EDDN DDHHMMZ 24003KT CAVOK 12/05 Q1013 NOSIG=

TAF EDDN DDHHMMZ 2606/2706 25010KT 9999 SCT040 BECMG 2611/2613 28005KT BECMG
2613/2615 BKN012 TEMPO 2620/2706 4000 -DZ BKN004=

EDDF

METAR EDDF DDHHMMZ 23004KT 9999 -RA FEW009 SCT036 OVC048 14/12 Q1013 NOSIG=

TAF EDDF DDHHMMZ 2606/2712 24004KT 6000 FEW010 SCT020 BKN030 PROB30 TEMPO 2606/2610
4000 RA BKN014=

EDDH

METAR EDDH DDHHMMZ 25002KT 6000 BKN008 BKN017 15/12 Q1013 BECMG 3000 BR=

TAF EDDH DDHHMMZ 2606/2712 VRB03KT 3500 BR SCT012 BKN020 TEMPO 2606/2609 2000 BR
TEMPO 2606/2611 BKN006 PROB30 TEMPO 2606/2609 1200 BCFG BKN003 BECMG 2609/2612 7000
TEMPO 2611/2615 29005KT BECMG 2620/2623 4000 BR BKN008 TEMPO 2623/2709 2500 BR
BKN004 BECMG 2709/2712 22007KT 8000 BKN020=
```

Figure 4-2: Weather Briefing during the Experiments

5 IMPLEMENTATION OF THE GNSS THREATS

5.1 AVES ARCHITECTURE OVERVIEW

The AVES simulation is performed on a distributed simulation network comprising a multitude of computers (see Figure 5-1). It has a centralized communication structure with the Interface Computer (IC) being the source and destination for all simulation data, i.e. each software module gets its input data from the IC and returns its computed data to the IC. All of the communication except for some infrastructural ones is performed using UDP connections.

All simulation software was produced at DLR with the overall focus on human factors experiments and flight experiment preparation mostly dealing with flight performance and flight dynamics analyses with DLR's research aircraft fleet. The following list summarizes a short statement for all major simulation modules used within the basic AVES simulation.

- **Aircraft Model:** The aircraft model containing the flight performance and flight dynamics is based on flight test data gathered with DLR's research aircraft and resembles the aircraft behavior with a high accuracy for a wide flight envelope. For research, a variety of different aircraft models can be used in AVES.

- **System Simulation:** The system simulation comprises the simulation of all systems that cannot be assigned to the other four major simulation modules mentioned here. It creates the functionality behind all cockpit switches. The basic software design consideration behind the system simulation was to focus on reproducing the correct system logic and behavior for the pilot by using the official system documentation from DLR's aircraft (FCOM, FOM, QRH, AMM) augmented with comments from DLR's test pilots and data from accident reports that sometimes reveal the correct system behavior that is opposing to the aircraft documentation.
- **Visual System:** For the simulation of the outside vision a visual database was generated using satellite images (taken by DLR) on top of a terrain model. The visual database contains the area of Germany exclusively.
- **Sound Simulation:** The sound simulation comprises generic transport aircraft noise which is augmented by type specific sounds (e.g., warning sounds, power transfer unit sound, etc.).
- **Motion System:** The motion system uses a 6 degree-of-freedom electro-pneumatically driven Stewart platform for simulating forces and is provided with acceleration values from the aircraft model.
- **Simulator Runtime Environment:** The runtime environment contains all elements that are needed to either let the simulation run or control it (e.g., start, stop, hold). The Interface Computer (IC) that holds and distributes all simulation data to all simulation modules or the Instructor Operator Station (IOS) are two prominent members of the simulator runtime environment.

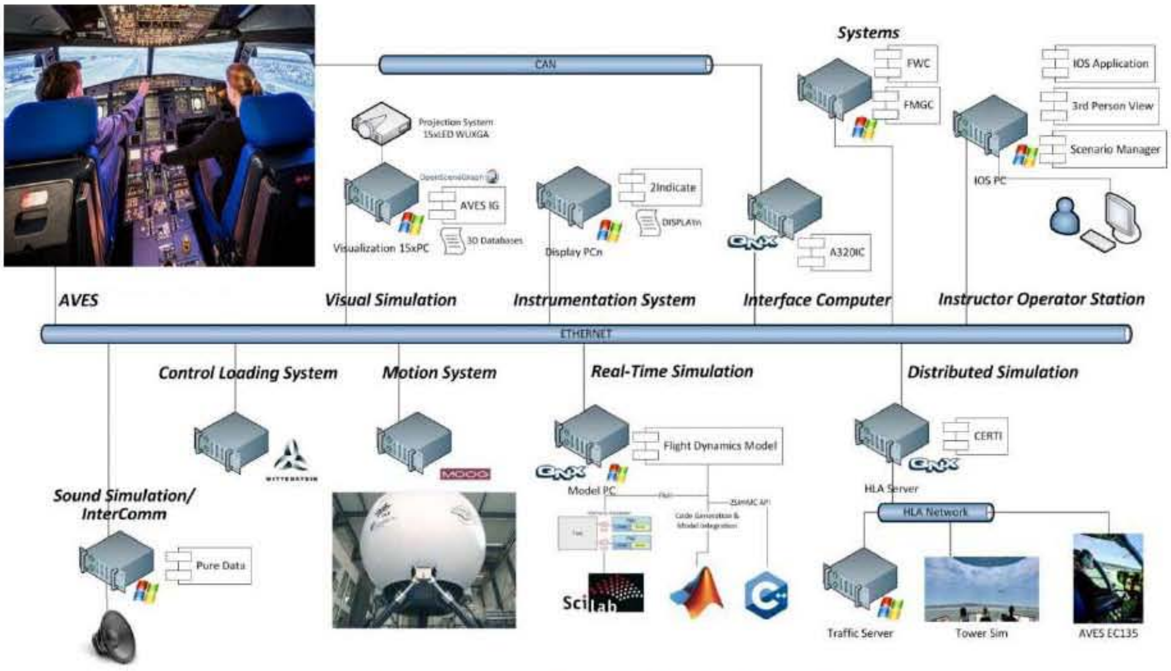


Figure 5-1: AVES Simulator Infrastructure.

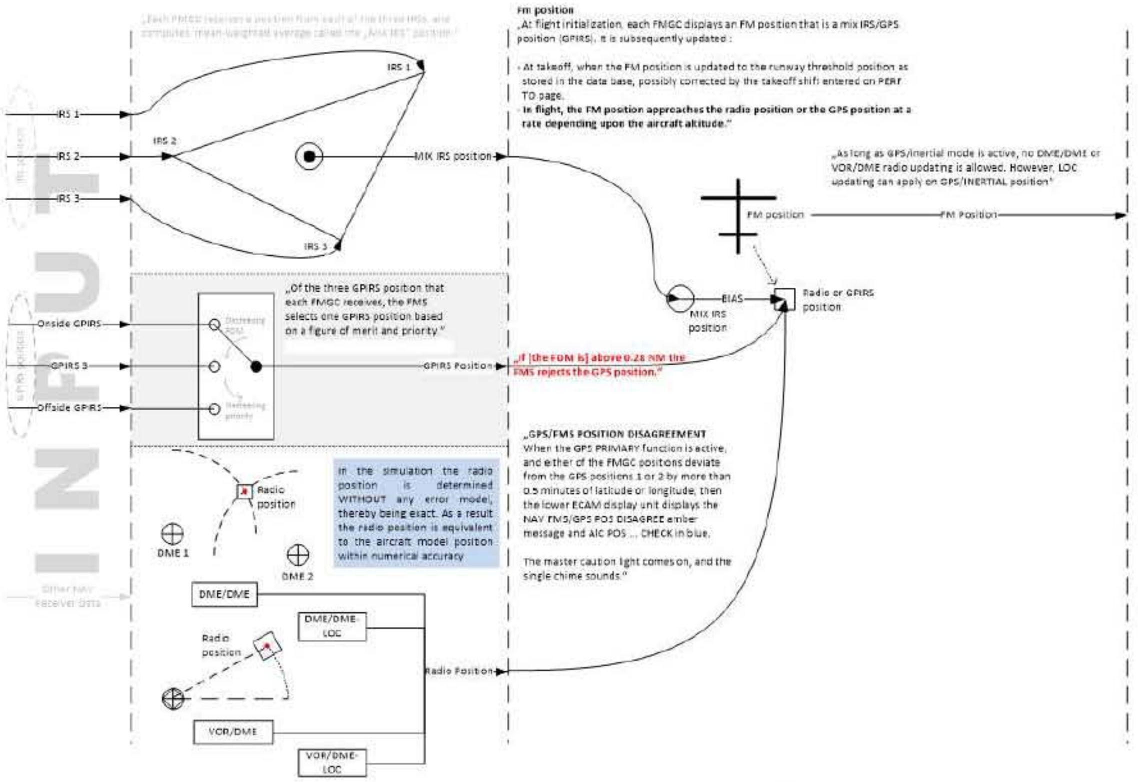
5.2 UPDATES TO THE AVES NAVIGATION MODES

In modern airliners the Flight Management System (FMS) uses a hybrid aircraft position generated from different navigation sources. These sources comprise at least one inertial, one radio, and one GNSS position. The quality and integrity of the navigation sources define the way the hybrid aircraft position is generated, i.e., which sources are used.

The IRS position (Inertial Reference System) is the fundamental navigation source without which no navigation mode exists. Whenever GNSS is “available and reasonable” it is used as a primary navigation source, filtered with the inertial data in order to increase the resolution, accuracy, integrity, availability and continuity. While primarily using GNSS, the position gets additionally updated in case of an ILS approach using the localizer signal. As soon as the GNSS position is voted unreasonable it gets rejected. In its place it is used the radio position, in case its error is lower than the IRS position error, otherwise the IRS position.

The GNSS-based cyberattack with the highest security threat is represented by a spoofed GNSS signal that is still voted “reasonable” by the aircraft's system computing the hybrid aircraft position. Indeed, if a spoofing attack is not performed correctly the GNSS signal is rendered invalid and it gets rejected, which means that the falsified GNSS position has no effect on the aircraft's navigation capabilities. Therefore, the analyses performed within the current activity is based on a spoofing attack where the spoofing itself is not detected by the aircraft's systems, possibly with the exception of some warnings / messages that are temporary activated by the spoofing attack. For this reason, the AVES navigation modes have been updated implementing the GNSS-based navigation modes in a realistic way, modelling measurement errors, threats, position fusion, associated messages and warnings, etc. Instead, concerning the radio position, it is determined without any error model, hence it is directly computed from the equations of motion of the aircraft. The navigation modes implemented by the FMGC of the AVES simulator are illustrated in Figure 5-3.

Figure 5-2: navigation mode selection [RD.2], GNSS-based modes are highlighted.



„Each FMGC receives a position from each of the three IRSs, and computes 'mean-weighted average called the „MIX IRS" position."

FM position
„At flight initialization, each FMGC displays an FM position that is a mix IRS/GPS position (GPIRS). It is subsequently updated :

- At takeoff, when the FM position is updated to the runway threshold position as stored in the data base, possibly corrected by the takeoff shift entered on PERF TO page.
- **In flight, the FM position approaches the radio position or the GPS position at a rate depending upon the aircraft altitude."**

„As long as GPS/inertial mode is active, no DME/DME or VOR/DME radio updating is allowed. However, LOC updating can apply on GPS/INERTIAL position"

„Of the three GPIRS position that each FMGC receives, the FMS selects one GPIRS position based on a figure of merit and priority."

„If [the FOM is] above 0.28 NM the FMS rejects the GPS position."

„GPS/FMS POSITION DISAGREEMENT
When the GPS PRIMARY function is active, and either of the FMGC positons deviate from the GPS positions 1 or 2 by more than 0.5 minutes of latitude or longitude, then the lower ECAM display unit displays the NAV FMS/GPS POS DISAGREE amber message and A/C POS ... CHECK in blue.

The master caution light comes on, and the single chime sounds."

In the simulation the radio position is determined WITHOUT any error model, thereby being exact. As a result the radio position is equivalent to the aircraft model position within numerical accuracy

Figure 5-3: Navigation modes implemented by the FMGC of the AVES simulator.

5.3 GNSS THREAT SIMULATOR MODULE

Within the current activity a special module, the GNSS Threat Simulator Module (GTSM), has been developed by Qascom in order to emulate the outputs of the GNSS receivers and of the ADIRUs during a GNSS spoofing attack.

The GTSM module, delivering the corrupted GNSS and GPIRS data, has been incorporated into the AVES simulation infrastructure as depicted in Figure 5-4 and Figure 5-5. In particular, Figure 5-5 shows that the GTSM module receives data from the Interface Computer (IC) and the FMGCs modules of the AVES simulator, and sends data to the IC. Hence, three new interfaces have been defined for the data communication: one for the communication FMGC→GTSM, one for the communication IC→GTSM, and one for the communication GTSM→IC. These interfaces are detailed in chapter 5.4.

Figure 5-9 depicts a high level view of an aircraft control model. The pilot (or autopilot) represents a controller, which applies control signals (steering, thrust control, etc.) based on the error between a reference trajectory (the flight plan) and the estimated actual trajectory. The control signals modify the aircraft motion, depending on the flight dynamic system. This, in turn, modifies the actual trajectory, the estimated trajectory, the trajectory error, the new control signals, and so on. Assuming the instruments estimating the actual trajectory (e.g., GPS, INS, ground aids, etc.) are properly working, this control loop is stable and allows to properly navigating an aircraft. A GNSS spoofing attack has the goal of impacting the aircraft navigation capabilities by falsifying the trajectory estimation process, hence inducing the controller to apply inappropriate control signals.

The GTSM module emulates GNSS threats by implementing the "Trajectory Estimation" block of the control system represented in Figure 5-9, both in absence and in presence of spoofing events. Specifically, the functionalities of the GTSM module are illustrated in Figure 5-10. It outputs eight different positions, belonging to three different types:

1. Two GPS positions: the outputs of the two GPS receivers in the AVES simulator, they are affected by instrument error models and by spoofing, in case of a spoofing event;
2. Three IRS positions: the outputs of the three inertial reference system in AVES simulator; they are affected by drifts caused by inertial data instrument error models;
3. Three GPIRS positions: the outputs of the three ADIRUs in the AVES simulator, they are computed by fusing, through Kalman filters, the GPS positions with the IRS positions (in nominal conditions GPIRS1 = GPS1 + IRS1, GPIRS2 = GPS2 + IRS2, GPIRS3 = GPS1 + IRS3).

In case of a spoofing event, a relative spoofing trajectory file is loaded and the offset positions contained within this file are sequentially added to the actual aircraft trajectory, in order to emulate the outputs of the GNSS receivers during a spoofing event. This may also include temporary unavailability of the GNSS position solution, during which the GNSS outputs are set to NCD (No Computed Data). The spoofed trajectory defined in the loaded file is relative in the sense that it contains position offsets that must be applied to the actual aircraft trajectory.

The architecture represented in Figure 5-10 is referred to as "semi-closed loop" in the D3 document [AD.11]. This name comes from the fact that the GNSS threat implemented with this architecture requires a spoofer capable of continuously estimating the aircraft position (as opposed to an open loop architecture in which the aircraft position must be estimated only at the beginning of the attack), but the relative spoofed trajectory is pre-computed, it does not depend on the actual aircraft trajectory (as opposed to a closed loop architecture in which the relative spoofed trajectory is a function of the actual aircraft trajectory). More details concerning these architectures, including pros and cons, are provided in the D3 document [AD.11].

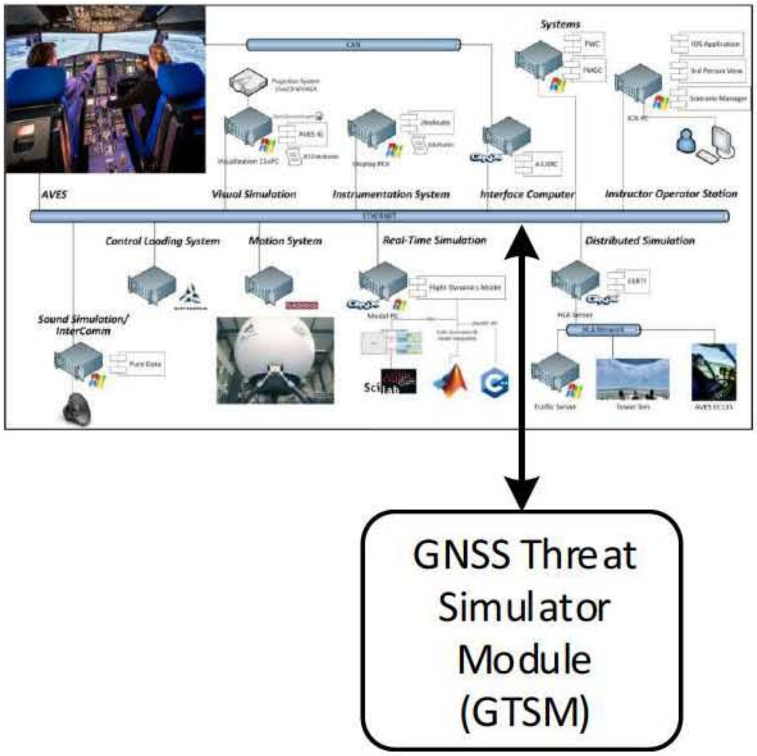


Figure 5-4: GTSM module incorporated into the AVES simulation infrastructure.

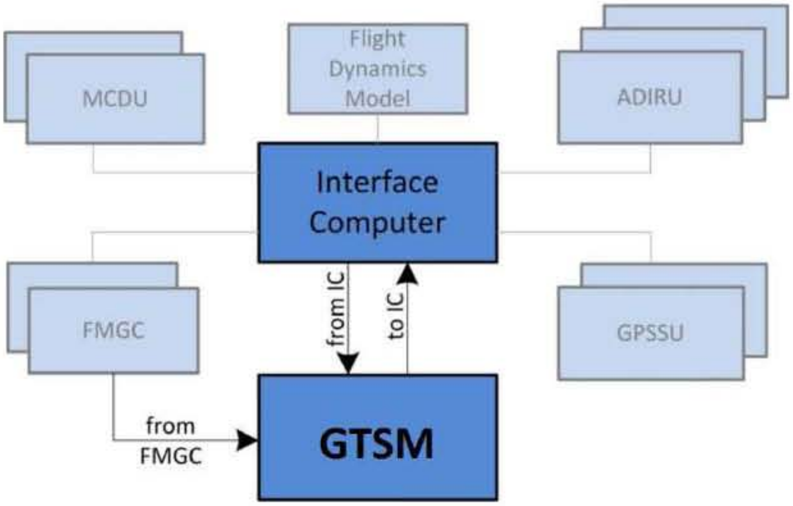


Figure 5-5: The GTSM module communicates with the IC and the FMGCs modules of the AVES simulator.

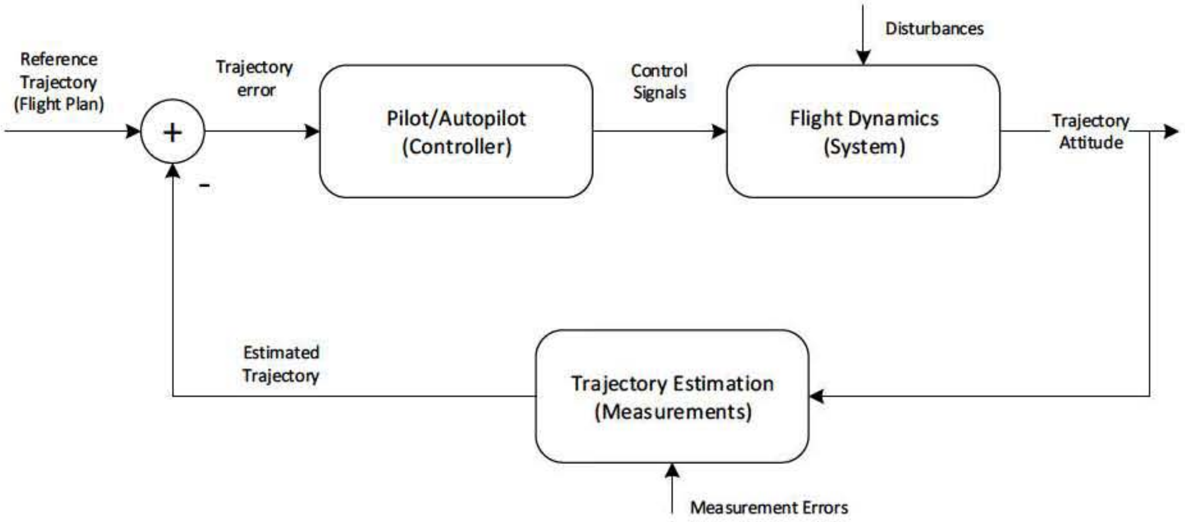


Figure 5-6: High level aircraft control model.

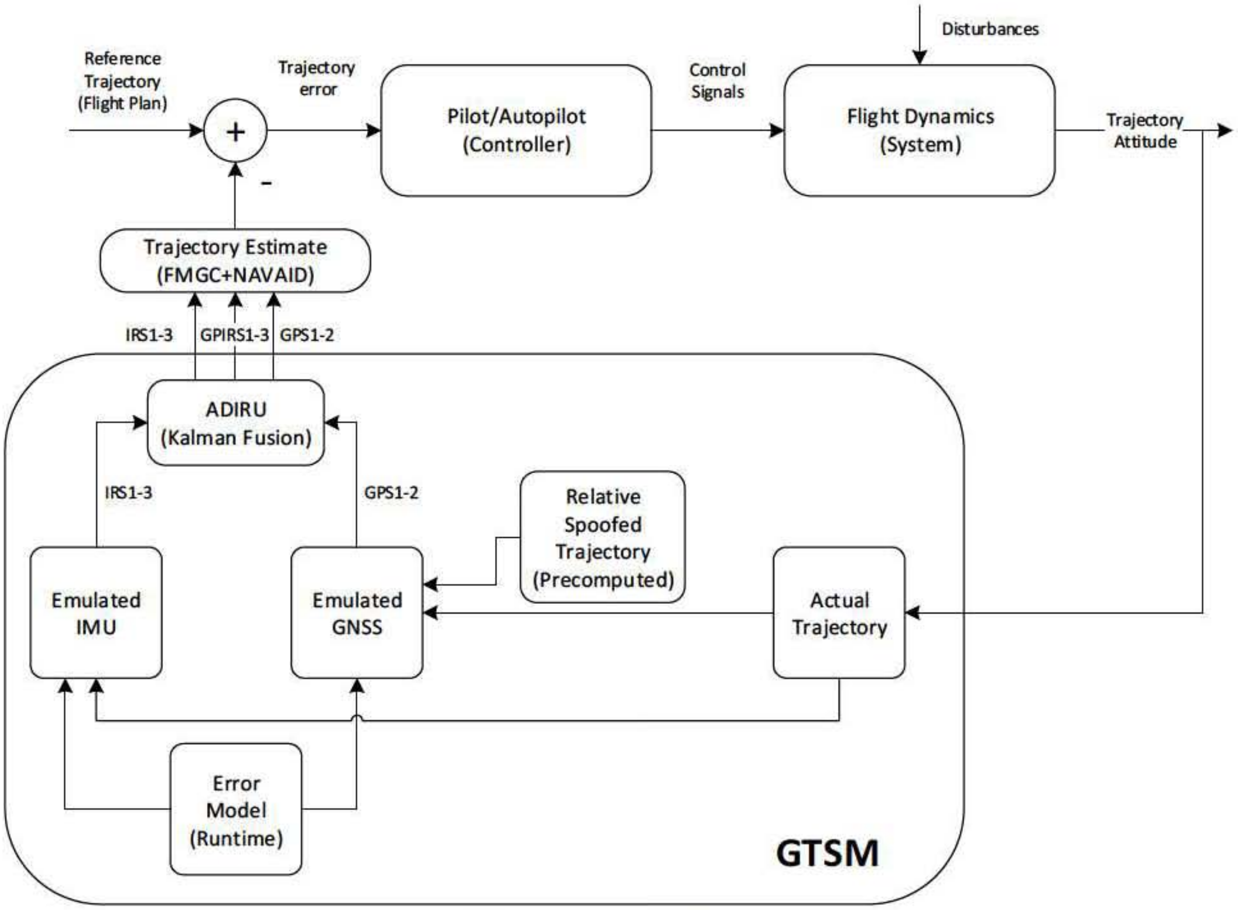


Figure 5-7: Functionalities of the GTSM module.

5.4 INTERFACE DEFINITION

In order to produce corrupted position information the GTSM module is provided with the aircraft position, attitude, translational accelerations, and rotatory velocities. These values come directly from the dynamic equations modelling the aircraft motion, thereby representing the true values used in the simulation, i.e., the true position, attitude, translational accelerations and rotatory velocities.

The GTSM module performs its position computation, including the impact of the signal spoofing, as explained in chapter 5.3, and returns to the IC module of the AVES simulator two GPS positions (GPS 1 and 2), three IRS positions (IRS1, 2, and 3) and three GPIRS positions (GPIRS 1, 2, and 3; corresponding to ADIRU 1, 2, and 3), including also additional information such as the GPS navigation mode, figure of merit, etc. Figure 5-8 represents a high level view of the interface between the AVES simulator and the GTSM module.

The coordinate system convention adopted for the data exchange are those used in traditional flight mechanics, depicted in Figure 5-9. The geodetic system is a right-hand coordinate system with the index g and is located at the aircraft's center of gravity: the z_g-axis points towards the gravitational force orienting both the x_g and y_g axes parallel to the surface of the earth, with x_g pointing to true north and y_g pointing eastwards. The second coordinate system used is the body-fixed coordinate system (index b), with its axes fixed to the aircraft: x_g is pointing to the nose and parallel to an aircraft reference line (usually the seat/floor rails), y_g pointing to the right wing and z_g completing the right-hand coordinate system.

The Euler angles ϕ for roll, θ for pitch, and Ψ for heading are defined between the body-fixed and geodetic coordinate system. The roll angle ϕ is the angle between the plane $x_g y_g$ and y_b and positive for right bank. The pitch angle θ is measured between the plane $x_g y_g$ and x_b and is positive in the pitch up direction. The heading Ψ is measured between the plane $x_g z_g$ and x_g and represents the true heading.

The variables contained in the interface from IC to the GTSM contain information about the accelerations from the aircraft motion model. An accelerometer measures the specific acceleration (force) b acting on a probe mass according to the formula below with, u, v, and w being the velocities along the x, y, and z axes:

$$\begin{bmatrix} b_x \\ b_y \\ b_z \end{bmatrix}_b = \begin{bmatrix} \dot{u} \\ \dot{v} \\ \dot{w} \end{bmatrix}_b - \begin{bmatrix} -\sin\theta \\ \sin\phi\cos\theta \\ \cos\phi\cos\theta \end{bmatrix}$$

The signals contained in the IC to GTSM interface are in the following relation to these measured accelerations:

$$\begin{bmatrix} navLonAcceleration \\ navLateralLoadFactor \\ navVerticalLoadFactor \end{bmatrix} = \begin{bmatrix} b_x \\ b_y/g \\ -b_z/g \end{bmatrix}$$

For example, for a stationary aircraft on ground with the artificial bank and roll angle of $\phi = 15°$ and $\theta = 10\,°$, the following equations are valid ($g = 9.81\frac{m}{s^2}$):

$$\begin{bmatrix} navLonAcceleration \\ navLateralLoadFactor \\ navVerticalLoadFactor \end{bmatrix} = \begin{bmatrix} 1.7035m/s^2 \\ -0.2549 \\ 0.9513 \end{bmatrix} = \begin{bmatrix} b_x \\ b_y/g \\ -b_z/g \end{bmatrix}$$

$$\begin{bmatrix} b_x \\ b_y \\ b_z \end{bmatrix} = \begin{bmatrix} navLonAcceleration \\ navLateralLoadFactor \cdot g \\ -navVerticalLoadFactor \cdot g \end{bmatrix} = \begin{bmatrix} 1.7035\, m/s^2 \\ -2.5004\, m/s^2 \\ -9.3318\, m/s^2 \end{bmatrix}$$

All the variables in the interface are given in SI units:

- angles in radians;
- angular velocities in rad/s;
- angular accelerations in rad/s²;
- distances in m;
- velocities in m/s;
- accelerations in m/s²;

The GTSM input and output interfaces are detailed in the following subchapters.

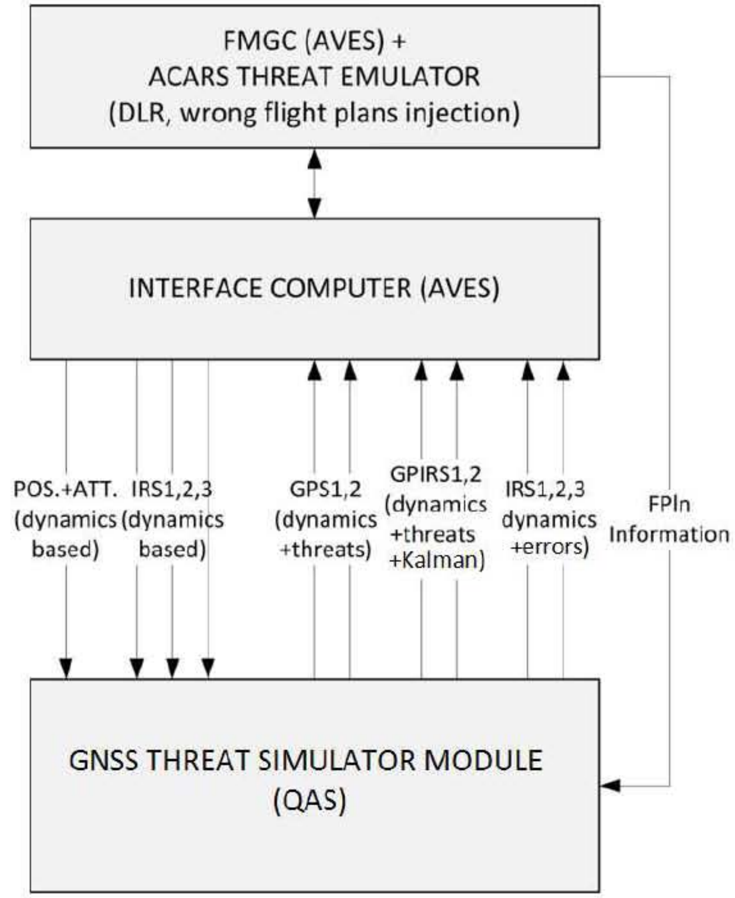

FMGC (AVES) +
ACARS THREAT EMULATOR
(DLR, wrong flight plans injection)
INTERFACE COMPUTER (AVES)
POS.+ATT. (dynamics based)
IRS1,2,3 (dynamics based)
GPS1,2 (dynamics +threats)
GPIRS1,2 (dynamics +threats +Kalman)
IRS1,2,3 dynamics +errors)
FPln Information
GNSS THREAT SIMULATOR MODULE
(QAS)

Figure 5-8: High level view of the interface between the AVES simulator and the GTSM module.

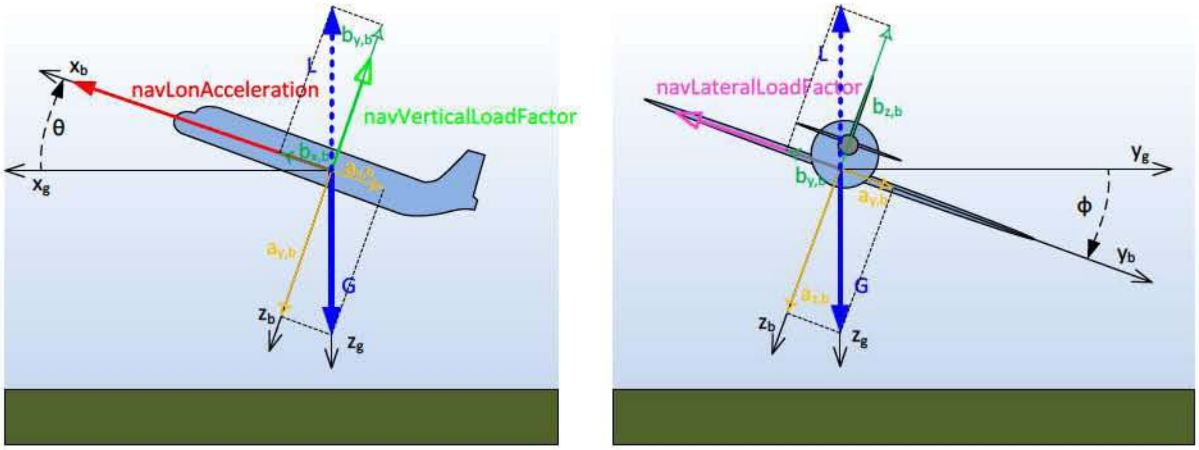
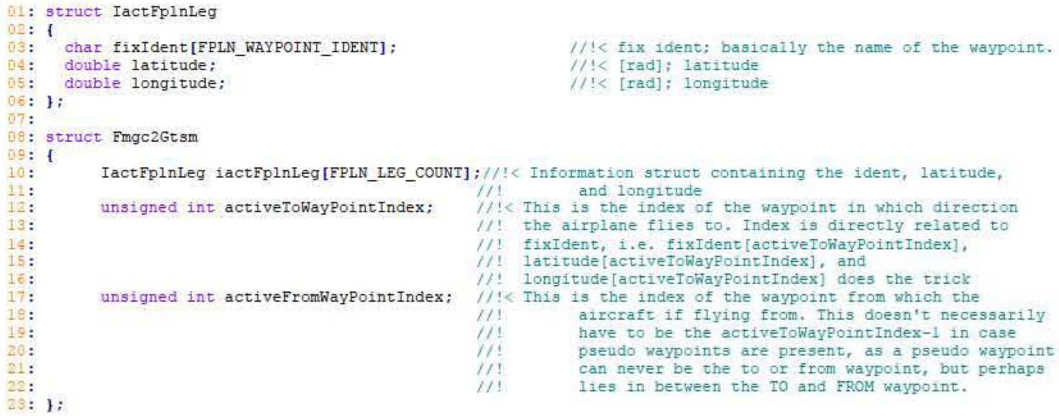


Figure 5-9: Definition of the coordinate systems, angles, acceleration, and load factors used for data exchange among the AVES simulator and the GTSM module.

5.4.1 GTSM INPUT INTERFACE

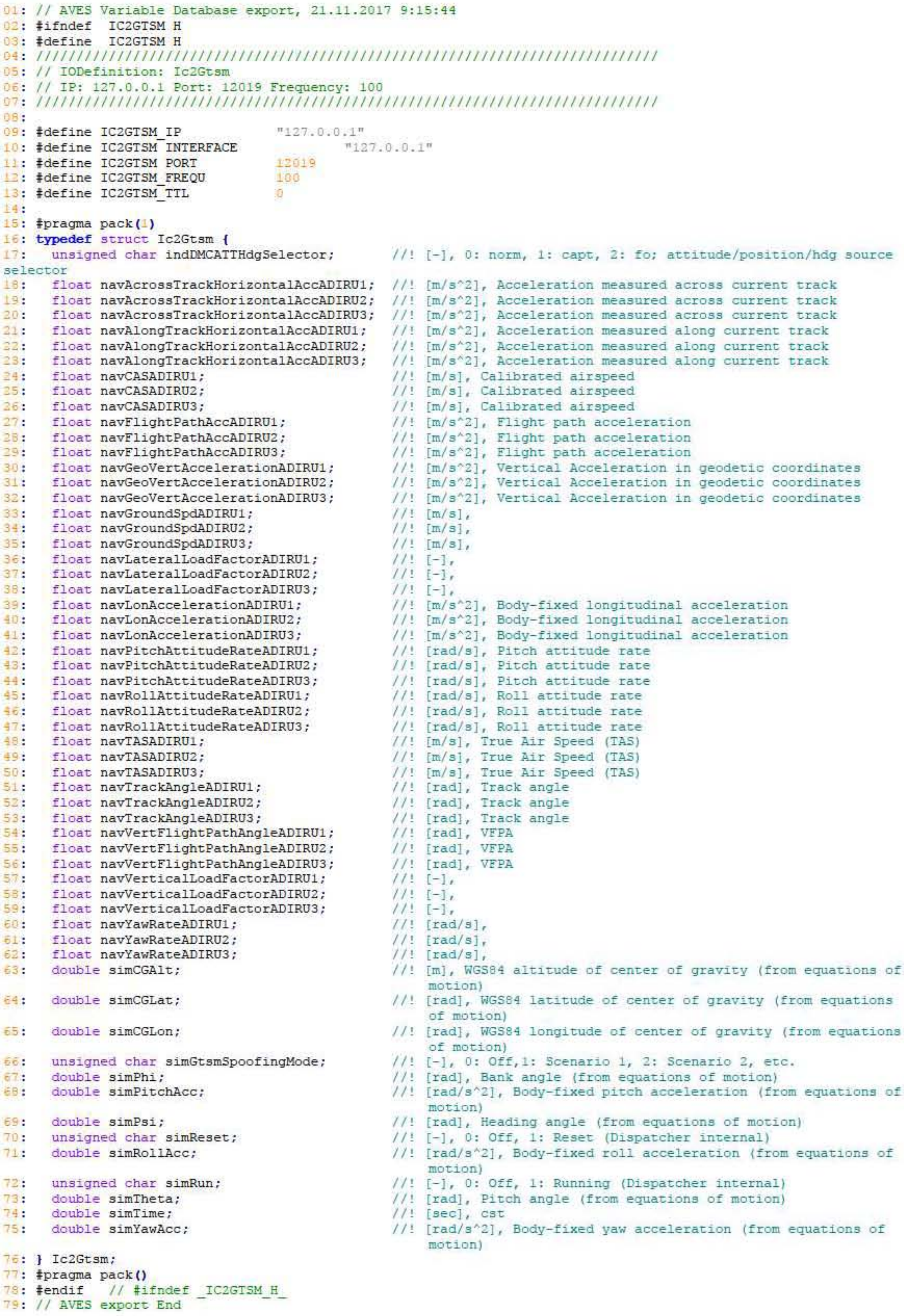
The GTSM receives data from two different sources. In the GTSM sample project all input data is accessible through a central storage object called dataCont (short for data container) from within the GTSM class. The two different input sources are combined in dataCont under newDataIn. The two sources and their definitions are given below:

1. **[dataCont.newDataIn.ic]:** The Interface Computer (IC) for all parameters belonging to the dynamic simulation, including data to control the simulation (e.g. run/reset signals). It is defined by the interface class Ic2Gtsm that itself is defined in the file Ic2Gtsm.h and given in Figure 5-11.
2. **[dataCont.newDataIn.fmgc]:** The FMGC interface gets the flight plan information, containing the ident, latitude, and longitude of every waypoint (sometimes also referred to as "leg") in the flight plan. Additionally, the ID of the waypoint the aircraft is flying to (TO waypoint) and the waypoint the aircraft is coming from (FROM waypoint). The interface is defined by the struct Fmgc2Gtsm that itself is defined in the file DataContainerGtsm.h. The struct definition is given below in Figure 5-10. The flight plan information is given as an array of type IactFplnLeg with a size of 200 units (a flight plan may hold 200 waypoints maximum) containing the ident (or "name") of the waypoint, its latitude and longitude. The provided flight plan is used in the FMGC, meaning that any update to the FMGC flight plan (e.g., by the pilots) directly affects the flight plan information received by the GTSM. It may happen that there are waypoints with a latitude and longitude of "0". This can happen when a waypoint is not defined per latitude and longitude (e.g., radius and distance to a fix) and the FMGC has not yet resolved the latitude and longitude through the waypoint definitions. It also can happen if the waypoint is a flight plan discontinuity, which is a special type of waypoint indicating breaks in the flight plan.



```
struct IactFplnLeg
{
  char fixIdent[FPLN_WAYPOINT_IDENT];                  //!< fix ident; basically the name of the waypoint.
  double latitude;                                     //!< [rad]; latitude
  double longitude;                                    //!< [rad]; longitude
};

struct Fmgc2Gtsm
{
      IactFplnLeg iactFplnLeg[FPLN_LEG_COUNT];//!< Information struct containing the ident, latitude,
                                             //!        and longitude
      unsigned int activeToWayPointIndex;    //!< This is the index of the waypoint in which direction
                                             //!  the airplane flies to. Index is directly related to
                                             //!  fixIdent, i.e. fixIdent[activeToWayPointIndex],
                                             //!  latitude[activeToWayPointIndex], and
                                             //!  longitude[activeToWayPointIndex] does the trick
      unsigned int activeFromWayPointIndex;  //!< This is the index of the waypoint from which the
                                             //!        aircraft if flying from. This doesn't necessarily
                                             //!        have to be the activeToWayPointIndex-1 in case
                                             //!        pseudo waypoints are present, as a pseudo waypoint
                                             //!        can never be the to or from waypoint, but perhaps
                                             //!        lies in between the TO and FROM waypoint.
};
```

Figure 5-10: FMGC to GSTM interface definition.

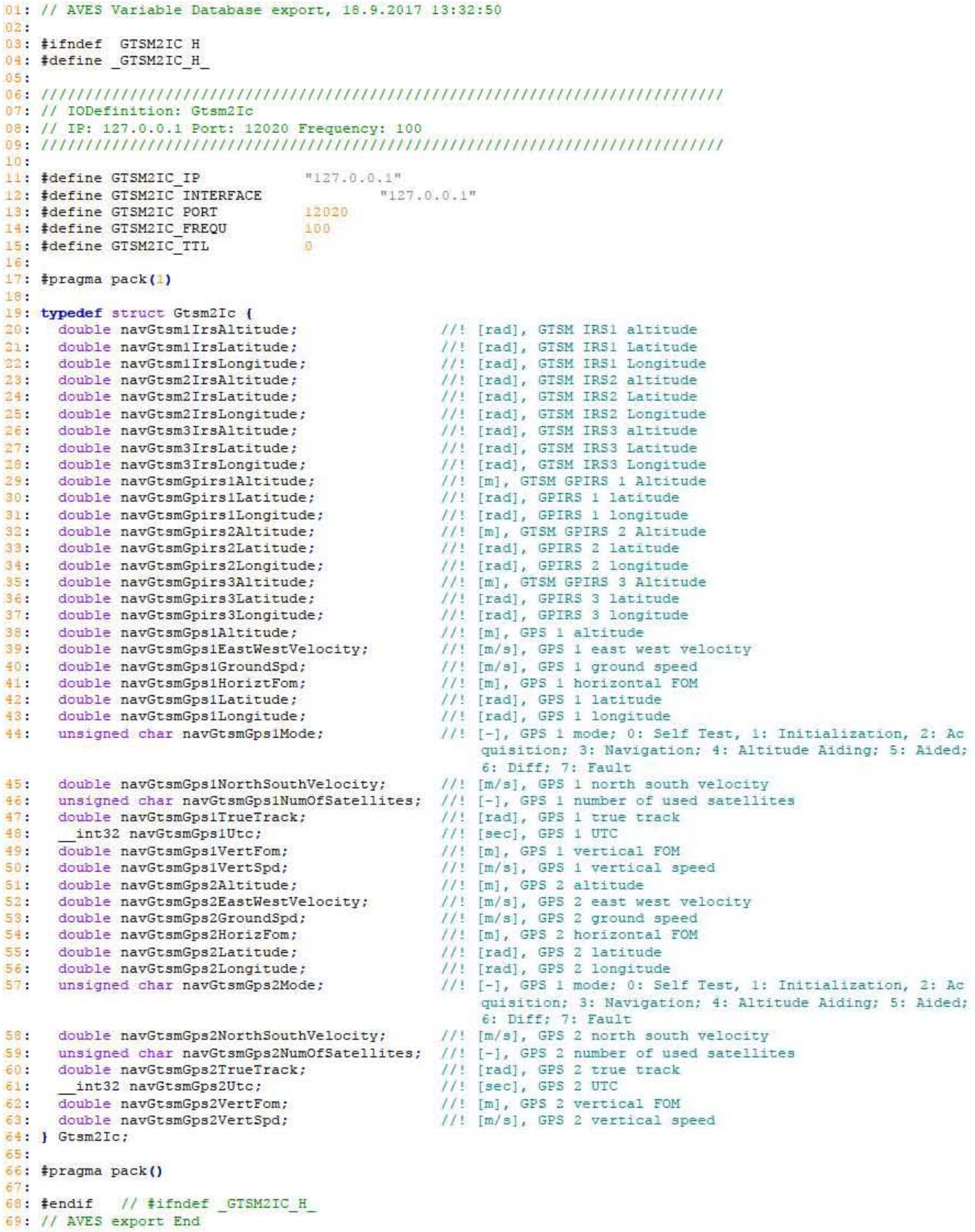


```
// AVES Variable Database export, 21.11.2017 9:15:44
#ifndef  _IC2GTSM_H_
#define  _IC2GTSM_H_
//////////////////////////////////////////////////////////////////////////////
// IODefinition: Ic2Gtsm
// IP: 127.0.0.1 Port: 12019 Frequency: 100
//////////////////////////////////////////////////////////////////////////////

#define IC2GTSM_IP                "127.0.0.1"
#define IC2GTSM_INTERFACE                 "127.0.0.1"
#define IC2GTSM_PORT              12019
#define IC2GTSM_FREQU             100
#define IC2GTSM_TTL               0

#pragma pack(1)
typedef struct Ic2Gtsm {
  unsigned char indDMCATTHdgSelector;       //! [-], 0: norm, 1: capt, 2: fo; attitude/position/hdg source
selector
  float navAcrossTrackHorizontalAccADIRU1;  //! [m/s^2], Acceleration measured across current track
  float navAcrossTrackHorizontalAccADIRU2;  //! [m/s^2], Acceleration measured across current track
  float navAcrossTrackHorizontalAccADIRU3;  //! [m/s^2], Acceleration measured across current track
  float navAlongTrackHorizontalAccADIRU1;   //! [m/s^2], Acceleration measured along current track
  float navAlongTrackHorizontalAccADIRU2;   //! [m/s^2], Acceleration measured along current track
  float navAlongTrackHorizontalAccADIRU3;   //! [m/s^2], Acceleration measured along current track
  float navCASADIRU1;                       //! [m/s], Calibrated airspeed
  float navCASADIRU2;                       //! [m/s], Calibrated airspeed
  float navCASADIRU3;                       //! [m/s], Calibrated airspeed
  float navFlightPathAccADIRU1;             //! [m/s^2], Flight path acceleration
  float navFlightPathAccADIRU2;             //! [m/s^2], Flight path acceleration
  float navFlightPathAccADIRU3;             //! [m/s^2], Flight path acceleration
  float navGeoVertAccelerationADIRU1;       //! [m/s^2], Vertical Acceleration in geodetic coordinates
  float navGeoVertAccelerationADIRU2;       //! [m/s^2], Vertical Acceleration in geodetic coordinates
  float navGeoVertAccelerationADIRU3;       //! [m/s^2], Vertical Acceleration in geodetic coordinates
  float navGroundSpdADIRU1;                 //! [m/s],
  float navGroundSpdADIRU2;                 //! [m/s],
  float navGroundSpdADIRU3;                 //! [m/s],
  float navLateralLoadFactorADIRU1;         //! [-],
  float navLateralLoadFactorADIRU2;         //! [-],
  float navLateralLoadFactorADIRU3;         //! [-],
  float navLonAccelerationADIRU1;           //! [m/s^2], Body-fixed longitudinal acceleration
  float navLonAccelerationADIRU2;           //! [m/s^2], Body-fixed longitudinal acceleration
  float navLonAccelerationADIRU3;           //! [m/s^2], Body-fixed longitudinal acceleration
  float navPitchAttitudeRateADIRU1;         //! [rad/s], Pitch attitude rate
  float navPitchAttitudeRateADIRU2;         //! [rad/s], Pitch attitude rate
  float navPitchAttitudeRateADIRU3;         //! [rad/s], Pitch attitude rate
  float navRollAttitudeRateADIRU1;          //! [rad/s], Roll attitude rate
  float navRollAttitudeRateADIRU2;          //! [rad/s], Roll attitude rate
  float navRollAttitudeRateADIRU3;          //! [rad/s], Roll attitude rate
  float navTASADIRU1;                       //! [m/s], True Air Speed (TAS)
  float navTASADIRU2;                       //! [m/s], True Air Speed (TAS)
  float navTASADIRU3;                       //! [m/s], True Air Speed (TAS)
  float navTrackAngleADIRU1;                //! [rad], Track angle
  float navTrackAngleADIRU2;                //! [rad], Track angle
  float navTrackAngleADIRU3;                //! [rad], Track angle
  float navVertFlightPathAngleADIRU1;       //! [rad], VFPA
  float navVertFlightPathAngleADIRU2;       //! [rad], VFPA
  float navVertFlightPathAngleADIRU3;       //! [rad], VFPA
  float navVerticalLoadFactorADIRU1;        //! [-],
  float navVerticalLoadFactorADIRU2;        //! [-],
  float navVerticalLoadFactorADIRU3;        //! [-],
  float navYawRateADIRU1;                   //! [rad/s],
  float navYawRateADIRU2;                   //! [rad/s],
  float navYawRateADIRU3;                   //! [rad/s],
  double simCGAlt;                          //! [m], WGS84 altitude of center of gravity (from equations of
                                              motion)
  double simCGLat;                          //! [rad], WGS84 latitude of center of gravity (from equations
                                              of motion)
  double simCGLon;                          //! [rad], WGS84 longitude of center of gravity (from equations
                                              of motion)
  unsigned char simGtsmSpoofingMode;        //! [-], 0: Off,1: Scenario 1, 2: Scenario 2, etc.
  double simPhi;                            //! [rad], Bank angle (from equations of motion)
  double simPitchAcc;                       //! [rad/s^2], Body-fixed pitch acceleration (from equations of
                                              motion)
  double simPsi;                            //! [rad], Heading angle (from equations of motion)
  unsigned char simReset;                   //! [-], 0: Off, 1: Reset (Dispatcher internal)
  double simRollAcc;                        //! [rad/s^2], Body-fixed roll acceleration (from equations of
                                              motion)
  unsigned char simRun;                     //! [-], 0: Off, 1: Running (Dispatcher internal)
  double simTheta;                          //! [rad], Pitch angle (from equations of motion)
  double simTime;                           //! [sec], cst
  double simYawAcc;                         //! [rad/s^2], Body-fixed yaw acceleration (from equations of
                                              motion)
} Ic2Gtsm;
#pragma pack()
#endif   // #ifndef _IC2GTSM_H_
// AVES export End
```

Figure 5-11: IC to GSTM interface definition.

5.4.2 GTSM OUTPUT INTERFACE

The GTSM output interface is defined in the struct Gtsm2Ic given in the file Gtsm2Ic.h, see Figure 5-12.



```
// AVES Variable Database export, 18.9.2017 13:32:50

#ifndef  GTSM2IC H
#define _GTSM2IC_H_

////////////////////////////////////////////////////////////////////////////
// IODefinition: Gtsm2Ic
// IP: 127.0.0.1 Port: 12020 Frequency: 100
////////////////////////////////////////////////////////////////////////////

#define GTSM2IC_IP               "127.0.0.1"
#define GTSM2IC INTERFACE                 "127.0.0.1"
#define GTSM2IC PORT             12020
#define GTSM2IC_FREQU            100
#define GTSM2IC_TTL              0

#pragma pack(1)

typedef struct Gtsm2Ic {
  double navGtsm1IrsAltitude;                 //! [rad], GTSM IRS1 altitude
  double navGtsm1IrsLatitude;                 //! [rad], GTSM IRS1 Latitude
  double navGtsm1IrsLongitude;                //! [rad], GTSM IRS1 Longitude
  double navGtsm2IrsAltitude;                 //! [rad], GTSM IRS2 altitude
  double navGtsm2IrsLatitude;                 //! [rad], GTSM IRS2 Latitude
  double navGtsm2IrsLongitude;                //! [rad], GTSM IRS2 Longitude
  double navGtsm3IrsAltitude;                 //! [rad], GTSM IRS3 altitude
  double navGtsm3IrsLatitude;                 //! [rad], GTSM IRS3 Latitude
  double navGtsm3IrsLongitude;                //! [rad], GTSM IRS3 Longitude
  double navGtsmGpirs1Altitude;               //! [m], GTSM GPIRS 1 Altitude
  double navGtsmGpirs1Latitude;               //! [rad], GPIRS 1 latitude
  double navGtsmGpirs1Longitude;              //! [rad], GPIRS 1 longitude
  double navGtsmGpirs2Altitude;               //! [m], GTSM GPIRS 2 Altitude
  double navGtsmGpirs2Latitude;               //! [rad], GPIRS 2 latitude
  double navGtsmGpirs2Longitude;              //! [rad], GPIRS 2 longitude
  double navGtsmGpirs3Altitude;               //! [m], GTSM GPIRS 3 Altitude
  double navGtsmGpirs3Latitude;               //! [rad], GPIRS 3 latitude
  double navGtsmGpirs3Longitude;              //! [rad], GPIRS 3 longitude
  double navGtsmGps1Altitude;                 //! [m], GPS 1 altitude
  double navGtsmGps1EastWestVelocity;         //! [m/s], GPS 1 east west velocity
  double navGtsmGps1GroundSpd;                //! [m/s], GPS 1 ground speed
  double navGtsmGps1HoriztFom;                //! [m], GPS 1 horizontal FOM
  double navGtsmGps1Latitude;                 //! [rad], GPS 1 latitude
  double navGtsmGps1Longitude;                //! [rad], GPS 1 longitude
  unsigned char navGtsmGps1Mode;              //! [-], GPS 1 mode; 0: Self Test, 1: Initialization, 2: Ac
                                                  quisition; 3: Navigation; 4: Altitude Aiding; 5: Aided;
                                                  6: Diff; 7: Fault
  double navGtsmGps1NorthSouthVelocity;       //! [m/s], GPS 1 north south velocity
  unsigned char navGtsmGps1NumOfSatellites;   //! [-], GPS 1 number of used satellites
  double navGtsmGps1TrueTrack;                //! [rad], GPS 1 true track
  __int32 navGtsmGps1Utc;                     //! [sec], GPS 1 UTC
  double navGtsmGps1VertFom;                  //! [m], GPS 1 vertical FOM
  double navGtsmGps1VertSpd;                  //! [m/s], GPS 1 vertical speed
  double navGtsmGps2Altitude;                 //! [m], GPS 2 altitude
  double navGtsmGps2EastWestVelocity;         //! [m/s], GPS 2 east west velocity
  double navGtsmGps2GroundSpd;                //! [m/s], GPS 2 ground speed
  double navGtsmGps2HorizFom;                 //! [m], GPS 2 horizontal FOM
  double navGtsmGps2Latitude;                 //! [rad], GPS 2 latitude
  double navGtsmGps2Longitude;                //! [rad], GPS 2 longitude
  unsigned char navGtsmGps2Mode;              //! [-], GPS 1 mode; 0: Self Test, 1: Initialization, 2: Ac
                                                  quisition; 3: Navigation; 4: Altitude Aiding; 5: Aided;
                                                  6: Diff; 7: Fault
  double navGtsmGps2NorthSouthVelocity;       //! [m/s], GPS 2 north south velocity
  unsigned char navGtsmGps2NumOfSatellites;   //! [-], GPS 2 number of used satellites
  double navGtsmGps2TrueTrack;                //! [rad], GPS 2 true track
  __int32 navGtsmGps2Utc;                     //! [sec], GPS 2 UTC
  double navGtsmGps2VertFom;                  //! [m], GPS 2 vertical FOM
  double navGtsmGps2VertSpd;                  //! [m/s], GPS 2 vertical speed
} Gtsm2Ic;

#pragma pack()

#endif   // #ifndef _GTSM2IC_H_
// AVES export End
```

Figure 5-12: GSTM to IC interface definition.

6 TEST REPORT AND MITIGATION RECOMMENDATIONS

6.1 INTERNAL PRE-ASSESSMENT

Before airline pilots were invited to perform flight trials in the simulator, the scenarios and the simulator setup was assessed internally by the project partners. Firstly, some interviews with DLR pilots (all active in airline duties as well) were conducted regarding the plausibility of the scenarios and the operational procedures involved. In addition, the functionality of the simulated attacks was tested and assessed in various forms and presented to EASA before the actual flight trials with airline pilots were conducted.

6.2 KEY PERSONAL INVOLVED

In the simulation trials, DLR staff, external airline pilots and one ENAV Air Traffic Controller (ATCO) were involved. DLR staff was responsible for setting up the simulator, performing the relevant briefings, operating the simulator and acting as the Co-Pilot for the individual flight trials. The simulator Co-pilot was holding a PPL-A with several years of experience with test flights or an commercial airplane type rating.

Table 6-1 summarizes the flying experience and the role at the respective airline for the pilots involved in the trials.

In addition to the pilots, an ATCO from ENAV with 17 years of professional experience was involved in the trials.

Pilot's role at airline	Pilot since	Flight hours
Pilot 1, First officer	6 years	4.000
Pilot 2, Captain	22 years	12.000
Pilot 3, First officer	10 years	6.200
Pilot 4, Captain	21 years	14.500
Pilot 5, First officer	8 years	5.900
Pilot 6, First officer	6 years	4.000
Pilot 7, First officer	19 years	10.500
Pilot 8, First officer	4 years	2.700

Table 6-1: Information about the pilots involved.

6.3 TRIALS OVERVIEW

In total, 7 simulator trials were performed. Within those 7 trials, several FMS as well as GNSS receiver attacks were simulated. Table 6-2 shows the staff distribution for the different trials. Notice that in the 6th trial two airline pilots have been involved (instead of one airline pilot + one DLR staff), and for the 7th trial an ATCO has been involved, making these scenarios even more realistic.

It is worth to highlight that the numbering of the trials does not correspond to the pilot numbers in Table 6-1, in order to ensure data privacy for the pilots involved.

During each flight trial, three simulated attacks were conducted. Table 6-3 shows the distribution of the attacks during the individual flight trials.

It is important to remark again that the test subjects were invited to the trials under false pretences in order to obtain unbiased results. As a result, no simulated attack was considered to be cyber-induced. Therefore, the pilots were very interested in the results afterwards and their awareness in cyber-security was increased.

Trial No.	Captain	First Officer	ATC and ATC interface	Date
1	Airline pilot	DLR staff	DLR staff, pseudo ATC	30.01.2018
2	Airline pilot	DLR staff	DLR staff, pseudo ATC	02.02.2018
3	Airline pilot	DLR staff	DLR staff, pseudo ATC	06.02.2018
4	Airline pilot	DLR staff	DLR staff, pseudo ATC	15.02.2018
5	Airline pilot	DLR staff	DLR staff, pseudo ATC	20.03.2018
6	Airline pilot	Airline pilot	DLR staff, pseudo ATC	23.03.2018
7	Airline pilot	DLR staff	ATCO present	04.04.2018

Table 6-2: Staff information during the trials.

Trial No.	Attack 1	Attack 2	Attack 3
1	ACARS W&B update	ACARS Flight Plan Update	Hacked Database (RNP 0.1 Appr)
2	ACARS W&B update	ACARS Flight Plan Update	Hacked Database (RNP 0.1 Appr)
3	ACARS W&B update	DoS attack on FMS 1+2	Hacked Database (RNP 0.1 Appr)
4	ACARS W&B update	DoS attack on FMS 1+2	Hacked Database (RNP 0.1 Appr)
5	ACARS W&B update	GNSS En-Route Spoofing	Hacked Database (RNP 0.1 Appr)
6	ACARS W&B update	GNSS En-Route Spoofing	Hacked Database (RNP 0.1 Appr)
7	ACARS W&B update	GNSS En-Route Spoofing	GNSS Approach Spoofing

Table 6-3: Attack scenarios conducted.

The simulator trials were conducted in DLR's AVES simulator in Braunschweig. The simulator is described in chapter 5. In addition, an ATC interface was used to investigate the impact of a cyber-attack on an Air Traffic Controller (ATCO). Figure 6-1 shows the setup of the controller working position. Figure 6-2 shows the HMI used for the Air Traffic Controller. The solid black part is the sector that is controlled by the ATCO and this is also the space where the GNSS en-route spoofing occurred.

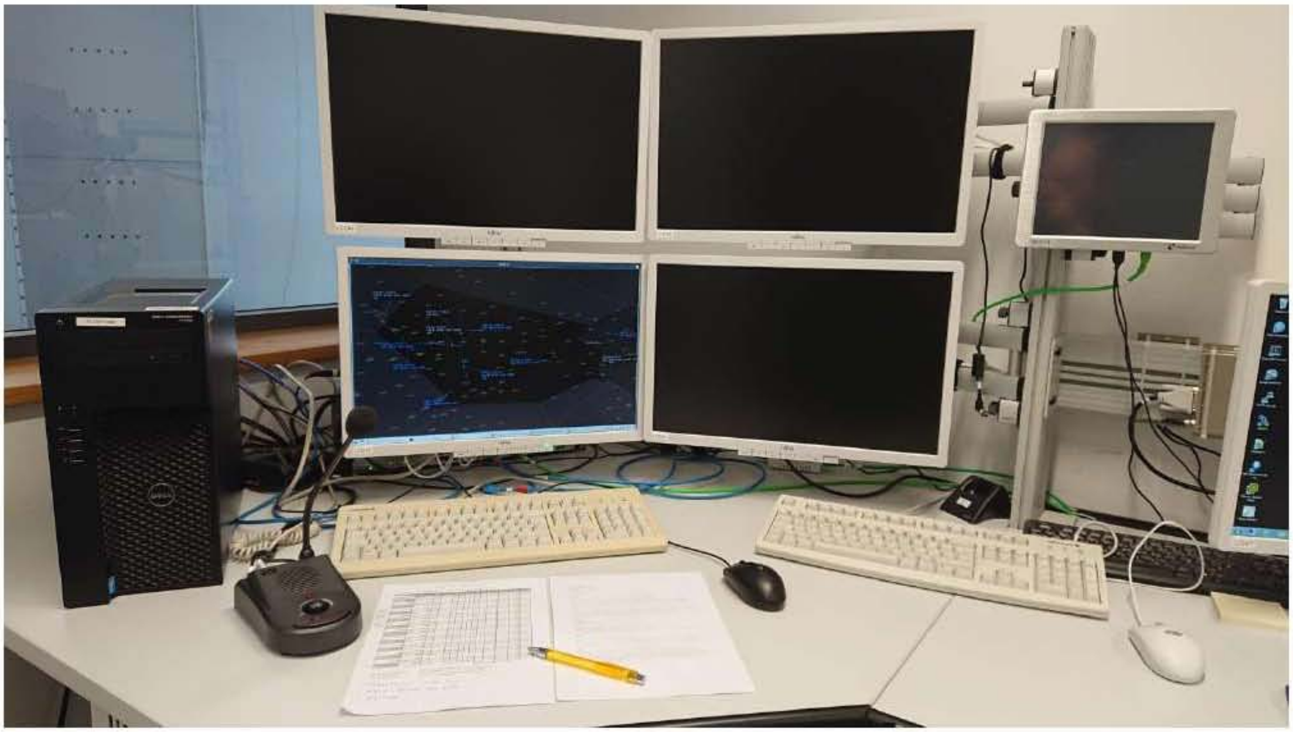


Figure 6-1: Controller working position.

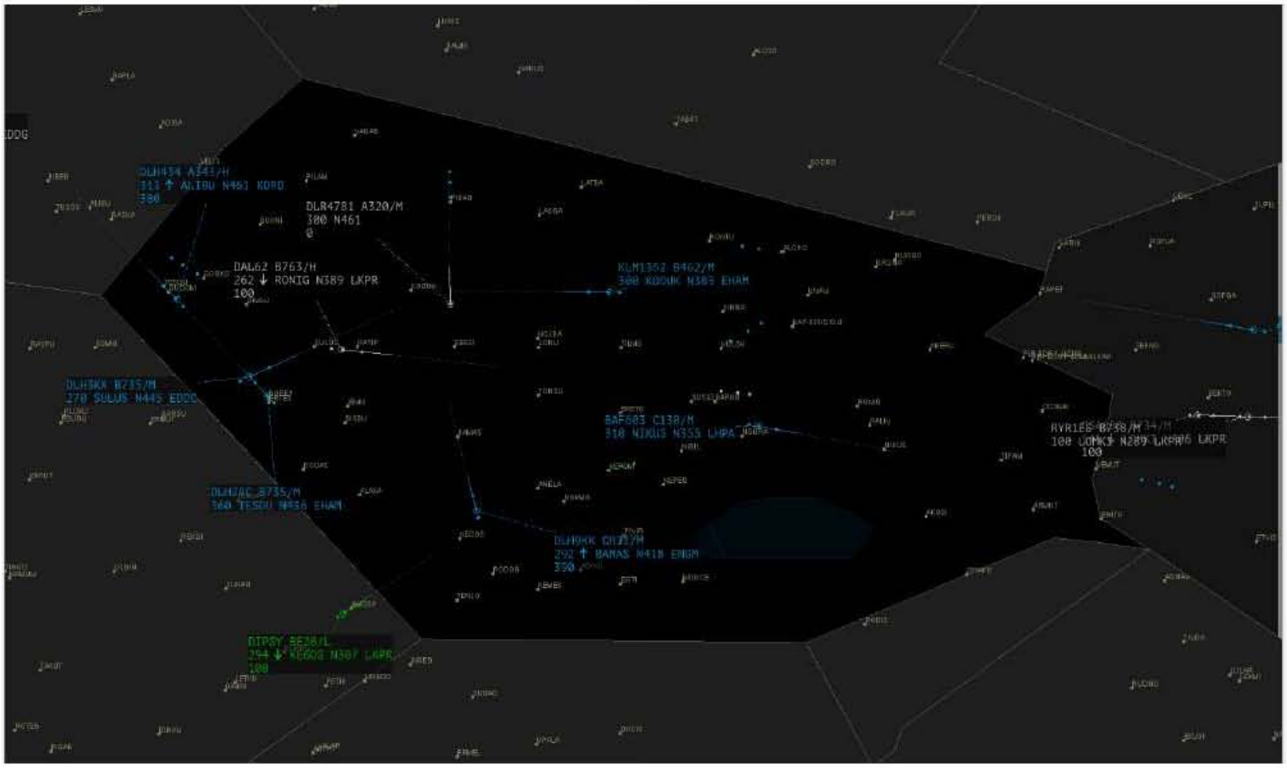


Figure 6-2: HMI for Air Traffic Controller.

6.4 TEST REPORT

In total 7 flight trials were conducted at DLR premises in Braunschweig. Eight airline pilots and one ATCO were involved in the trials. This chapter describes the main outcomes associated to the different trials. It is subdivided into 7 subchapters, one for each performed trial. Each subchapter describes the main outcomes of the associated trial.

It is worth to remark that in the subchapters the term Crew Member (CM) is used in the following way:

- Crew Member 1 (CM1) is the captain, sitting in the left seat. In all the trials CM1 is the Pilot Monitoring (PM), from the beginning to the end of the flight, with an exception in the 6th trial, during which for some time CM1 is the flying pilot. CM1 is always the invited airline pilot;
- Crew Member 1 (CM2) is the first officer, sitting in the right seat. In all the trials CM2 is the Pilot Flying (PF), from the beginning to the end of the flight, with an exception in the 6th trial, during which for some time CM2 is the monitoring pilot. CM2 is always the DLR actor, with the exception of the 6th trial, in which both CM1 and CM2 are invited airline pilots.

6.4.1 TRIAL 1

This scenario run included the following three attack events: ACARS loadsheet update, ACARS flight plan update, and hacked RNP 0.1 data base. Table 6-4 reports the time instants, since the beginning of the associated recorded video, at which the attacks occur, and the roles of the pilots during the attacks; whereas Table 6-5 reports whether the attacks where identified during or after the events. More details concerning the behavior of the crew during each attack and the feedback provided by the crew after the simulation are provided in the following subchapters.

Attack	Time elapsed in video	Roles
ACARS W&B update	08:23	Airline pilot: CM1, monitoring, entering values of loadsheet DLR pilot: CM2, flying
ACARS flight plan update	30:04	Airline pilot: CM1, monitoring, co-ordination with OPS and ATC DLR pilot: CM2, flying
Hacked database (RNP 0.1 approach)	58:30 start of final descent	Airline pilot: CM1, monitoring, cross-checking with chart DLR pilot: CM2, flying

Table 6-4: Time instants at which the attacks occurred in the recorded video and roles of the pilots for trial 1.

Attack	Identified during event	Identified after event
ACARS W&B update	No	Yes, the aircraft rotated too early. But not considered as an attack.
ACARS flight plan update	No	Yes, the update was discarded after contacting ATC, but it was not considered as an attack.
Hacked database (RNP 0.1 approach)	Yes, during the approach the altitude was cross-checked. A go-around was initiated at 4 NM before the runway threshold.	-

Table 6-5: Identification of the cyberattacks of trial 1.

6.4.1.1 ACARS W&B UPDATE

Description of the behavior of the crew:

- CM1 identified the soundness of the values of the new load sheet but also observed huge differences in the trim setting. Nevertheless, the new trim setting was used for the take-off.
- As the aircraft rotated too early during the take-off, CM1 contacted OPS afterwards doubting of the correctness of the new loadsheet.
- As OPS stated that they did not issue another loadsheet, the received loadsheet was assumed to be faulty by CM1

Feedback based on the operating experience of CM1:

- CM1 stated that it is common practice to receive multiple loadsheet updates in daily operations. At some airlines there is a requirement to acknowledge the reception with a digital signature but it is very rare and not always reliable. CM1 was the only airline pilot that made a comment about the digital signature.

6.4.1.2 ACARS FLIGHT PLAN UPDATE

Description of the behavior of the crew:

- CM1 spotted a discrepancy in the new flight plan compared to the old one. As the crew requested a shortcut before, the change was not applicable anymore. However, CM1 made contact with ATC as well as OPS regarding the update. Neither ATC nor OPS knew anything about the update, hence it was disregarded.

Feedback based on the operating experience of CM1:

- CM1 stated that it is rather uncommon that a flight plan update is only communicated via ACARS during flight and not via ATC.
- On the other hand, an update via ACARS on ground is common. Therefore, this would be more dangerous because not all waypoints are checked with ATC before flight.
- There is an operational flight plan number that can be used to check whether the flight plan is valid and intended for the individual aircraft, but this number is not especially protected.
- CM1 was the only one stating the existence of this number in the trials.

6.4.1.3 HACKED DATABASE (RNP 0.1 APPROACH)

Description of the behavior of the crew:

- The approach was briefed according to the chart and the operational checklist.
- CM1 cross-checked the altitude with the charted values during the approach.
- A deviation was observed starting at 6 NM away from the runway threshold.
- At 4 NM a go-around was initiated by CM1 at a safe altitude.
- An ILS approach with landing is conducted afterwards.

Feedback based on the operating experience of CM1:

- CM1 stated that the altitude cross-check is required by the standard operating procedures and must be applied during all RNP approaches. This is trained as well.
- CM1 stated that a digital signature of the database could help to prevent hacking of the database.

6.4.2 TRIAL 2

This scenario run included the following three attack events: ACARS loadsheet update, ACARS flight plan update, and hacked RNP 0.1 data base. Table 6-6 reports the time instants, since the beginning of the associated recorded video, at which the attacks occur, and the roles of the pilots during the attacks; whereas Table 6-7 reports whether the attacks where identified during or after the events. More details concerning the behavior of the crew during each attack and the feedback provided by the crew after the simulation are provided in the following subchapters.

Attack	Time elapsed in video	Roles
ACARS W&B update	4:44	Airline pilot: CM1, monitoring, entering values of loadsheet DLR pilot: CM2, flying
ACARS flight plan update	26:45	Airline pilot: CM1, monitoring, co-ordination with OPS and ATC DLR pilot: CM2, flying
Hacked database (RNP 0.1 approach)	57:00 start of final descent	Airline pilot: CM1, monitoring, cross-checking with chart DLR pilot: CM2, flying

Table 6-6: Time instants at which the attacks occurred in the recorded video and roles of the pilots for trial 2.

Attack	Identified during event	Identified after event
ACARS W&B update	No	Yes, the aircraft rotated too early. But not considered as an attack.
ACARS flight plan update	No	Yes, the update was discarded after contacting ATC but it was not considered as an attack.
Hacked database (RNP 0.1 approach)	Yes, during the approach the altitude was cross-checked. A go-around was initiated.	-

Table 6-7: Identification of the cyberattacks of trial 2.

6.4.2.1 ACARS W&B UPDATE

Description of the behavior of the crew:

- CM1 observed the differences in the trim setting and the center of gravity.
- Nevertheless, the new trim setting was used for the take-off as the values themselves were valid.
- As the aircraft rotated too early during the take-off, CM1 commanded “nose down”.
- After it occurred, the event was not discussed further.

Feedback based on the operating experience of CM1:

- CM1 assessed the scenario as realistic as multiple updates of the loadsheet are common.

- Depending on the ground crew, the load sheet can also contain unintentional errors from time to time. Therefore, it needs to be checked carefully.
- CM1 stated that in reality more care would have been given to the loadsheet.

6.4.2.2 ACARS FLIGHT PLAN UPDATE

Description of the behavior of the crew:

- The crew requested a shortcut as 3 minutes of delay was accumulated during flight.
- CM1 received the flight plan update through the simulated printer.
- CM1 asked the opinion of CM2, but then CM1 decided to coordinate the update with OPS. As OPS did not send the update they did not confirm the update, as a consequence CM1 contacted ATC.
- ATC had no knowledge about the update, hence the update is disregarded.
- CM1 then realized that there was a wrong flight number on the update (by mistake) and informs OPS.
- The aircraft stayed on the intended path all the time.

Feedback based on the operating experience of CM1:

- CM1 confirmed that en-route flight plan updates are always received by ATC.
- CM1 also stated that a flight plan update on ground could be more dangerous as usually only the departure route is confirmed with ATC.

6.4.2.3 HACKED DATABASE (RNP 0.1 APPROACH)

Description of the behavior of the crew:

- The approach was briefed according to the chart and the operational checklist.
- CM1 cross-checked the altitude with the charted values during the approach according to the standard operating procedures.
- A deviation was observed by CM1 during the approach.
- A go-around was initiated by CM1 at a safe altitude well before the minimum descent altitude.
- An ILS approach with landing was conducted afterwards.

Feedback based on the operating experience of CM1:

- CM1 stated that ILS is always preferred since it is a precision approach, therefore it is safer.
- CM1 assessed this attack scenario as the most critical one within the trial.

6.4.3 TRIAL 3

This scenario run included the following three attack events: ACARS loadsheet update, denial of service attack on both FMS during the en-route phase, and hacked RNP 0.1 data base. Table 6-8 reports the time instants, since the beginning of the associated recorded video, at which the attacks occur, and the roles of the pilots during the attacks; whereas Table 6-9 reports whether the attacks where identified during or after the events. More details concerning the behavior of the crew during each attack and the feedback provided by the crew after the simulation are provided in the following subchapters.

Attack	Time elapsed in video	Roles
ACARS W&B update	6:22	Airline pilot: CM1, monitoring, entering values of loadsheet DLR pilot: CM2, flying
DoS attack on FMS 1 + 2	32:35	Airline pilot: CM1, monitoring, co-ordination with ATC DLR pilot: CM2, flying
Hacked database (RNP 0.1 approach)	62:20 start of final descent	Airline pilot: CM1, monitoring, cross-checking with chart DLR pilot: CM2, flying

Table 6-8: Time instants at which the attacks occurred in the recorded video and roles of the pilots for trial 3.

Attack	Identified during event	Identified after event
ACARS W&B update	No	Yes, the aircraft rotated too early. But not considered as an attack
DoS attack on FMS 1 + 2	Yes, but not considered as an attack	Yes, but not considered as an attack
Hacked database (RNP 0.1 approach)	Yes, go-around initiated at approx. 300ft AGL (50ft above minimum descent height)	-

Table 6-9: Identification of the cyberattacks of trial 3.

6.4.3.1 ACARS W&B UPDATE

Description of the behavior of the crew:

- CM1 received the loadsheet update via the simulated printer.
- CM1 read the loadsheet out loud and transferred the new values to the cockpit systems.
- There was no discussion about the new values.
- The aircraft rotated too early and CM2 expressed his astonishment about that.
- There was no discussion afterwards about the event.

Feedback based on the operating experience of CM1:

- CM1 stated that loadsheet updates are common practice and assessed this scenario as very realistic. As the values themselves were in the range of allowed values, no suspicion was raised.
- CM1 stated that unencrypted ACARS transmission is problematic from his point of view.

6.4.3.2 DOS ATTACK ON FMS 1+2

Description of the behavior of the crew:

- The simulated attack was started at waypoint BAMAS.
- The autopilot was disconnected, the MCDU was frozen and no map data was available on the navigation displays.
- CM2 called out "AP and FD disconnect".
- CM1 assessed the state of the aircraft and observed that the aircraft was still manually controllable.
- CM2 stated that the NAV mode was not available either. CM1 then called for ECAM actions, searched for error indication and checked the ECAM status page, which was empty.
- CM1 then informed ATC that the aircraft lost navigation accuracy and asked for RADAR vectors to follow the filed flight plan.
- CM1 then analyzed the impact on the flight and concluded that ILS approaches could still be flown, but not the RNP 0.1 approach.
- When CM1 was contacting ATC regarding an alternate approach, the attack stopped and all systems returned to normal.

Feedback based on the operating experience of CM1:

- CM1 stated that the error was unexpected especially because no ECAM actions was raised and the ECAM status page was empty.
- Based on CM1's opinion, it was crucial to check if the aircraft was still controllable. As a flight based on raw data was possible, the situation was manageable and represented a common scenario in training sessions.

6.4.3.3 HACKED DATABASE (RNP 0.1 APPROACH)

Description of the behavior of the crew:

- CM1 wanted to change the approach to ILS after the DoS attack.
- For the sake of the experiment ATC denied ILS and insisted on RNP 0.1 approach
- The approach was briefed according to the chart and the operational checklist.
- CM1 cross-checked the altitude with the charted values during the approach according to the standard operating procedures.
- CM1 stopped with the cross checks at 3 NM from the runway threshold, after a 100 ft displacement was observed at 4N from runway threshold.
- Go-around initiated at approximatively 300 ft AGL (i.e., 50 ft above minimum descent height).
- A normal ILS approach was conducted afterwards.

Feedback based on the operating experience of CM1:

- CM1 stated that this was the most critical attack during the trial.
- Currently, there is a computer-based training for PBN and there is a lot of confusion regarding the terms and acronyms for PBN based procedures among the pilots.
- CM1 stated that if RNP approaches become more common in the future, the protection of the databases is very important.

6.4.4 TRIAL 4

This scenario run included the following three attacks: ACARS W&B update, DoS attack on FMS 1+2, and hacked database (RNP 0.1 approach). Table 6-10 reports the time instants, since the beginning of the associated recorded video, at which the attacks occur, and the roles of the pilots during the attacks; whereas Table 6-11 reports whether the attacks where identified during or after the events. More details concerning the behavior of the crew during each attack and the feedback provided by the crew after the simulation are provided in the following subchapters.

Attack	Time elapsed in video	Roles
ACARS W&B update	03:53	Airline pilot: CM1, monitoring, reading values of loadsheet DLR pilot: CM2, entering values of the loadsheet
DoS attack on FMS 1 + 2	30:10	Airline pilot: CM1, monitoring, co-ordination with ATC DLR pilot: CM2, flying
Hacked database (RNP 0.1 approach)	56:55 start of final descent	Airline pilot: CM1, monitoring DLR pilot: CM2, flying

Table 6-10: Time instants at which the attacks occurred in the recorded video and roles of the pilots for trial 4.

Attack	Identified during event	Identified after event
ACARS W&B update	No	Yes, but no further inquiry and not considered as an attack.
DoS attack on FMS 1 + 2	Yes, but not considered as an attack.	
Hacked database (RNP 0.1 approach)	No, go around due to nonexistent visual contact at decision altitude.	No

Table 6-11: Identification of the cyberattacks of trial 4.

6.4.4.1 ACARS W&B UPDATE

Description of the behavior of the crew:

- CM1 identified changes in the updated loadsheet and ordered CM2 to enter the updated loadsheet.
- CM2 performed the takeoff as pilot flying and remarked that the aircraft automatically rotated before reaching rotation speed. When, during climb-out, CM2 again remarked the early self-rotation without stick input, CM1 questioned whether they had a mistrim and decided to analyze the event above FL100. This analysis never happened.

Feedback based on the operating experience of CM1:

- CM1 stated that in his airline the W&B must be computed by the crew according to the ramp agent's loadsheet. The use of ACARS is very unusual. Consequently, he was not used to read the printout.
- CM1 stated that in reality he would have questioned the loadsheet update more than what he had. He stated to have the pretended experiment goal of workload measurements during approach in mind, for this reason he did not give much attention to the loadsheet.

6.4.4.2 DOS ATTACK ON FMS 1+2

Description of the behavior of the crew:

- The AP disconnect was noticed by CM1 and CM2 simultaneously. CM1 noticed that also the FDs and the map on ND were not working anymore and activated the FPA/TRK mode (bird) while trying to reengage the AP, which did not work.
- CM1 noticed that both MCDUs were frozen and started analyzing the situation with a FORDEC mnemonic before informing ATC about the event and asking for radar vectors.
- CM1 further checked the ECAM pages and the status of the aircraft, which did not present any abnormality. He thought about a FMGC reset but knowing about the limitations of the simulator he only mentioned the possibility.
- When CM1 wanted to start a discussion about a possible diversion the attack ended and the FMGC functionality, including the AP, was restored. CM1 subsequently reengaged the FDs and AP and returned the aircraft's avionic back to normal. He informed ATC about the recovery and requested a direct to the next waypoint.
- Subsequently, CM1 checked the event back with the Airline Operations Center (AOC).

Feedback based on the operating experience of CM1:

- CM1 reported the FMGC freeze to be realistic. In his airline though, there is no frequency for further support in such a case.

6.4.4.3 HACKED DATABASE (RNP 0.1 APPROACH)

Description of the behavior of the crew:

- CM1 did not perform the altitude/distance check. Therefore, CM2 initiated a go around at the decision altitude due to nonexistent visual runway contact.
- During the go around, based on the cloud base, CM1 decided to take the ILS for the next approach as a conventional system with a lower decision altitude.
- CM1 stated that he forgot about the distance/altitude check because of the rushed approach with the aircraft being too fast and too high during initial approach.

Feedback based on the operating experience of CM1:

- CM1 stated that RNP approaches are seldom flown fully managed. The ones that are flown in CM1's airline are performed using the FPA mode. In this mode the altitude/distance check is mandatory, as the altitude could not be checked otherwise.
- According to CM1 the VDEV and HDEV indication used in the simulator study can create an overreliance about the true aircraft position in terms of the desired path. This may drive the crew to omit the altitude/distance check.

6.4.5 TRIAL 5

This scenario run included the following three attacks: ACARS W&B update, GNSS enroute spoofing, and hacked database (RNP 0.1 approach). Table 6-12 reports the time instants, since the beginning of the associated recorded video, at which the attacks occur, and the roles of the pilots during the attacks; whereas Table 6-13 reports whether the attacks where identified during or after the events. More details concerning the behavior of the crew during each attack and the feedback provided by the crew after the simulation are provided in the following subchapters.

Attack	Time elapsed in video	Roles
ACARS W&B update	04:50	Airline pilot: CM1, monitoring, entering values of loadsheet DLR pilot: CM2, flying
GNSS en-route spoofing	28:50 start of attack 41:07 end of attack	Airline pilot: CM1, monitoring DLR pilot: CM2, flying
Hacked database (RNP 0.1 approach)	57:15 start of final descent	Airline pilot: CM1, monitoring, cross-checking with chart DLR pilot: CM2, flying

Table 6-12 Time instants at which the attacks occurred in the recorded video and roles of the pilots for trial 5.

Attack	Identified during event	Identified after event
ACARS W&B update	No	Yes, update suspected to be erroneous, but not considered as an attack.
GNSS en-route spoofing	Yes, but not considered as an attack.	-
Hacked database (RNP 0.1 approach)	Yes, but not considered as an attack.	

Table 6-13: Identification of the cyberattacks of trial 5.

6.4.5.1 ACARS W&B UPDATE

Description of the behavior of the crew:

- CM1 identified various differences between the initial and updated loadsheet: zero fuel weight, pax, cargo, and trim setting. Despite the identified large deviations, he orderd the data to be entered and checked back the correctness of the entering.
- CM2 performed the takeoff as pilot flying and remarked the aircraft's automatic rotation below the rotation speed. During climb-out CM1 doubted the correctness of the trim setting. He speculated that the aircraft's center of gravity was potentially aft, which would also have fitted the initial loadsheet at startup.

Feedback based on the operating experience of CM1:

- CM1 stated that even if loadsheet amendments are common, such large deviations without further clarifications of the load master are very unusual. In reality, he would have recalculated the trim setting on his EFB.

- CM1 stated that the normal procedure for entering the weight and balance setting is that the pilot flying enters the loadsheet data into the MCDU and sets the trim setting according to the value presented on the MCDU's FUEL PRED page. Thereafter, the pilot monitoring checks the trim wheel setting with the value given on the loadsheet. This generates redundancy due to two different sources of information.
- CM1 reported that in his airline, if an aircraft's trim is critical (at the envelope of the allowed CG range) the crew is not allowed to make last minute changes to the load sheet on their own, but instead they must ask for an updated loadsheet at the AOC or airline's W&B hotline.

6.4.5.2 GNSS ENROUTE SPOOFING

Description of the behavior of the crew:

- The navigation mode changes to GPS PRIMARY LOST and back to GPS PRIMARY are identified a few seconds after their occurrence. CM1 checked the navigation accuracy during the outage, which remained high.
- At first CM1 thought that the manual navaid tuning made by CM2 was the cause for the change in navigation mode, but CM2 clarified that the change happened shortly before he made changes in the MCDU.
- After regaining GPS PRIMARY, CM1 stated that they had encountered a map shift and that the aircraft rolled significantly to reacquire its intended flight path. Based on the aircraft's behavior and the large map shift of 3 NM cross track error, CM1 decided to switch the approach from the planned RNP to a standard ILS approach with radar vectors. The experiment leader noted CM1's doubts and asked him to keep the RNP approach for the sake of the (pretended) experiments, CM1 accepted.

Feedback based on the operating experience of CM1:

- CM1 stated that his airline uses an EFB system in which the aircraft's current position is indicated in the displayed charts for increased situational awareness. According to CM1, the displayed position that is based on the EFB's internal GPS receiver was up to now always reliable and he never experienced any problems with this functionality.

6.4.5.3 HACKED DATABASE (RNP 0.1 APPROACH)

Description of the behavior of the crew:

- During final approach CM1 performed the altitude/distance check as demanded by the Standard Operating Procedure (SOP) and identified the aircraft being too low too early, calling out a go around. Due to the comfortable fuel situation CM1 proposed to retry the RNP approach before changing to the ILS approach. As CM2 insisted on directly changing to the ILS approach, CM1 agreed as he stated that "both pilots need to be comfortable with the situation".

Feedback based on the operating experience of CM1:

- CM1 stated that, in reality, based on the high fuel situation he probably would have tried a second approach on the RNP 0.1, thereby "trying to identify the error encountered during the first approach".

6.4.6 TRIAL 6

This scenario run included the following three attacks: ACARS W&B update, GNSS enroute spoofing, and hacked database (RNP 0.1 approach). The flight was performed by a crew consisting of a captain and a first officer of the same airline, making this scenario even more realistic compared to the standard experiment crew configuration consisting of a real pilot as Pilot Monitoring (PM) and DLR staff as Pilot Flying (PF).
Table 6-14 reports the time instants, since the beginning of the associated recorded video, at which the attacks occur, and the roles of the pilots during the attacks; whereas Table 6-15 reports whether the attacks where identified during or after the events. More details concerning the behavior of the crew during each attack and the feedback provided by the crew after the simulation are provided in the following subchapters.

Attack	Time elapsed in video	Roles
ACARS W&B update	05:30	Airline pilot 1: CM1, monitoring, entering trim setting in MCDU Airline pilot 2: CM2, entering values of loadsheet
GNSS enroute spoofing	35:37 start of the attack 47:54 end of the attack	Airline pilot 1: CM1, monitoring Airline pilot 2: CM2, flying
Hacked database (RNP 0.1 approach)	62:30 start of final descent	Airline pilot 1: CM1, monitoring and flying. Role changed at 64:20. Then monitoring with cross-checking with chart Airline pilot 2: CM2, flying and monitoring. First cross-check with chart. Role changed at 64:20. Then flying

Table 6-14: Time instants at which the attacks occurred in the recorded video and roles of the pilots for trial 6.

Attack	Identified during event	Identified after event
ACARS W&B update	No, although data was doubted.	Yes, but not considered as an attack.
GNSS enroute spoofing	Yes, but not considered as an attack.	
Hacked database (RNP 0.1 approach)	Yes, but not considered as an attack.	

Table 6-15: Identification of the cyberattacks of trial 6.

6.4.6.1 ACARS W&B UPDATE

Description of the behavior of the crew:

- CM1 identified the large trim setting of the difference from -1.6 to +1.6 THS as the result of the ramp agent's misloading of the aircraft, but anyhow accepted the new data. Consequently, the new loadsheet was entered without further confirmation.
- Shortly prior rotation speed, CM2 announced that the aircraft rotated with the sidestick in neutral. CM1 directly assumed that the loadsheet must have been erroneous.

Feedback based on the operating experience of CM1:

- CM1 stated that loadsheet updates are common, but that an update has to be acknowledged to the AOC with a special code that is only known by the captain.
- CM1 stated that in reality he would have not accepted the new loadsheet without further inquiry.

6.4.6.2 GNSS ENROUTE SPOOFING

Description of the behavior of the crew:

- CM1 identified the change in navigation mode to GPS PRIMARY LOST and back to GPS PRIMARY at the moment of their occurrence, combined with a map shift in the ND.
- CM1 assumed an error in the GPS and questioned whether they would be able to fly the planned RNP 0.1 approach. CM1 checked the GPS availability through the MCDU's "predictive GPS" page, which showed that the GPS was predicted to be available.
- CM2 proposed, in the case should the GPS problems return during approach, to continue for "two to three seconds" and see whether GPS functionality returns. He assumed that there probably was a problem with the GPS antennas.
- CM1 checked and discussed the SOP for degraded navigation with CM2 to prepare for a possible degradation, which resulted in questioning the usability of the planned RNP 0.1 approach.
- The crew's doubts were noted by the experiment leader. For the sake of the pretended experiment goals of workload and fatigue measurement during RNP approaches, CM1 and CM2 were asked (and accepted) to hang on to the RNP 0.1 approach.

Feedback based on the operating experience of CM1:

- CM1 and CM2 were used to occasional short outages of the GPS PRIMARY functionality with a few seconds duration.

6.4.6.3 HACKED DATABASE (RNP 0.1 APPROACH)

Description of the behavior of the crew:

- During the early final approach CM2 performed the altitude/distance check as demanded by the SOP and identified the aircraft being below the vertical profile, while CM1 stated that the VDEV indication in the PFD was centered.
- CM2 took over manual control, keeping the VDEV and HDEV indications centered. While CM2 was go around minded, CM1 proposed to at least continue to the minimum before going around. At the minimum CM2 initiated the go around as he had the feeling of being low too early with no visual contact to the runway.
- After the go around on downwind, the crew decided to choose the ILS approach on the same runway.

Feedback based on the operating experience of CM1:

- CM1 and CM2 stated that, if in doubt, they would always prefer an ILS approach over a PBN one.
- From personal experience, CM1 knows the process NAV databases are generated and was surprised that, despite the manual data entering process, the error rate was still low.
- CM2 remembered an incident at his airline where an erroneous antenna height in the EGPWS database generated an EGPWS alert, although being well clear of terrain.

6.4.7 TRIAL 7

This scenario run included the following three attack events: ACARS loadsheet update, GNSS enroute spoofing, and GNSS approach spoofing. In this run an ATCO from ENAV carried on ATC operations. Like the invited pilots, the ATCO was not aware of the cyberattacks. Table 6-16 reports the time instants, since the beginning of the associated recorded video, at which the attacks occur, and the roles of the pilots during the attacks; whereas Table 6-17 reports whether the attacks where identified during or after the events. More details concerning the behavior of the crew during each attack and the feedback provided by the crew after the simulation are provided in the following subchapters.

Attack	Time elapsed in video	Roles
ACARS W&B update	04:17	Airline pilot: CM1, monitoring, checking the values of loadsheet at 07:30 again, refusing the loadsheet at 09:40 DLR pilot: CM2, entering the values of loadsheet, coordinating with OPS
GNSS enroute spoofing	42:56 start of the attack 51:56 end of the attack	Airline pilot: CM1, monitoring, coordinating with ATC DLR pilot: CM2, flying
GNSS approach spoofing	60:24 start of the attack 72:23 end of the attack	Airline pilot: CM1, monitoring, coordination with ATC DLR pilot: CM2, flying

Table 6-16: Time instants at which the attacks occurred in the recorded video and roles of the pilots for trial 7.

Attack	Identified during event	Identified after event
ACARS W&B update	Yes, new setting discarded after consulting AOC, but not considered as an attack.	
GNSS enroute spoofing	Yes, changed to HDG mode with radar vectors, but not considered as an attack.	
GNSS approach spoofing		Yes, attempt to recover approach before initiating go around, but not considered as an attack

Table 6-17: Identification of the cyberattacks of trial 7.

6.4.7.1 ACARS W&B UPDATE

Description of the behavior of the crew:

- CM1 initiated the input of the newly received loadsheet update by CM2 and noticed a large CG shift from 38% to 21% MAC despite the unchanged gross weight.
- CM2 asked CM1 to look for possible position changes in pax or cargo. CM1 then took the initiative to check the loadsheet update by contacting the AOC, despite the fact that the trim setting was still within the green band, as he had noticed.
- When OPS confirmed the values of the original loadsheet, hence CM1 disregards the update and planned to write a flight report about the incident after arriving at the destination airport.

Feedback based on the operating experience of CM1:

- CM1 stated that loadsheet updates are common, although not with such large CG shifts.
- In reality CM1 would have checked the values with the ramp agent and additionally with the airline's weight & balance hotline. Alternatively, he would have done a weight & balance calculation with the EFB.

6.4.7.2 GNSS ENROUTE SPOOFING

Description of the behavior of the crew and of the ATCO:

- CM1 noticed an oscillating flying behavior shortly before the planned flight path was intended to make a turn. Therefore, CM1 decided to switch into heading mode.
- ATC noticed that the aircraft turned several nautical miles in front of the intended turn and informed the crew about their deviation and asked for their reason to deviate. The ATCO later stated that even for a fly-by-waypoint the distance was too far. At that time the crew also had an additional displayed cross track error of 0.6 NM right while being 3-4 NM off course in reality.
- Due to the deviations, CM1 requested radar vectors.
- CM1 identified and announced the change in navigation mode from GPS PRIMARY to GPS PRIMARY LOST and, after the unidentified attack, back to GPS PRIMARY.
- After the aircraft was reestablished on its intended path, while still flying with radar vectors, due to the experienced GPS events CM1 decided for an ILS approach at Hanover, instead of the pre-planned RNP 0.1 approach.
- As the scenario relied on flying the RNP 0.1 approach, CM1's decision was was asked to disregard the experienced GPS difficulties for the sake of performing the RNP approach due to (pretended) experimental reasons. CM1 agreed to perform the RNP approach under these circumstances.
- CM1 requested a direct to ATC to return to NAV mode and received a direct to NORTA.

Feedback based on the operating experience of CM1:

- CM1 knew about the possibility of jammed GPS signals, but did not know about the possibility of GNSS spoofing.
- CM1 stated that the aircraft's GPS PRIMARY function is very reliant. He had only experienced five short term outages in ten years of flying experience.
- After the spoofing attack, CM1 stated to still have "neutral trust" in the aircraft's navigation solution. With the decision for an alternative ILS approach instead of the planned RNP 0.1 approach, he wanted to prevent a go around situation early.

Feedback based on the operating experience of ACTO:

- The ATCO, like the pilots in this study, was invited under false pretenses. His briefing primed him to analyze a "newly developed and improved controller software under operational circumstances". His initial debriefing comments showed that he was not aware of any cybersecurity threats.

- The ATCO had some remarks about the graphical user interface of his workstation. He missed the possibility to measure distances and time between points in space (aircraft, waypoints, and airspaces).
- Inside his controlled sector the ATCO identified unexpected descent clearances he did not clear, which led to separation violations. These violations stemmed from the traffic simulation. During the flight the experiment leader also explained these violations as simulation errors.
- The ATCO stated that just prior to a planned turn (at the waypoint BAMKI) the aircraft's deviation to the planned path was significant. In reality he would accept cross track errors of ½ nm. In the case of larger deviations, he also would inform the crew and ask about the reason of the deviation.
- The ATCO stated that in the upper airspace the aircraft's drift was hard to detect with the provided software as well as it would be in reality, because in upper air space, especially in a FRAIT environment, aircrafts are instructed to fly direct routes instead of point by point. A detection in the lower airspace might be easier.

6.4.7.3 GNSS APPROACH SPOOFING

Description of the behavior of the crew:

- The GNSS spoofing stayed unnoticed until the navigation mode changed to GPS PRIMARY LOST (which also correlates to the end of the attack for this spoofing scenario). The attack ended during the final turn. A few seconds later he FMGC reacquired the correct aircraft position, a cross track error of 0.6 NM on the left was indicated on PFD and ND.
- CM1 decided to continue the approach despite the SOP, demanding to abort the approach in case of GPS PRIMARY LOSS on both FMGCs, as the aircraft "was not yet on final approach".
- Only when FINAL APP mode did not engage CM1 aborted the approach and decided for the ILS approach on runway 27R.

Feedback based on the operating experience of CM1:

- CM1 stated that he wanted to recover the approach although the deviation was greater than 0.1 NM.
- CM1 stated that, compared to ILS approaches, RNP approaches are still rare.
- CM1 also stated that, due to current regulation changes, he had to perform a computer-based training for assuring his knowledge in PBN. This also included RNP approaches.

6.5 SUMMARY OF THE TEST RESULTS

Table 6-18 shows the summary of the results. It can be seen that some attacks had a high detection rate and some had a very low detection rate.

Attack	Detection	Results / comments
ACARS load sheet update	1 out of 7 times	Aircraft rotated before V_r
ACARS flight plan update	2 out of 2 times	Flight plan change rejected, aircraft stayed on course
Hacked database during RNP 0.1 approach	5 out of 6 times	Go-around and missed approach detected during approach, once at the MDA
Denial of service attack FMS	2 out of 2 times	FMS/map functionality lost, aircraft still controllable, help from ATC requested, raw data available
En-route GNSS spoofing	0 out of 3 times	Diverging flight path not detected during event, except from ATC, slightly increased workload after event, reduction of confidence in navigation system
Approach GNSS spoofing	0 out of 1 time	Spoofing not detected during event, after event, due to the cross-track error and the disengagement of auto pilot, approach was discontinued

Table 6-18: Summary of the results of the trials.

6.5.1 ACARS LOAD SHEET UPDATE

In the threat scenario "ACARS load sheet update" a falsified load sheet was handed to the flight crew, emulating the role of an ACARS printer in the cockpit (see Figure 6-3). It was received after the take-off briefing was conducted and all data were entered into the MCDU. The new ACARS load sheet contained a new trim setting 1.6 UP while the aircraft had actually an aft CG. The ACARS load sheet update attack was conducted in every trial. Only in one case the update was rejected by the PM. In all the other cases the new trim setting was used and resulted in a pitch up event prior to Vr. In some cases, the reason was discussed and the simulated airline operations center was contacted. As the new trim setting was in the allowed range, the result was not too critical with this type of simulated aircraft and the workload for the PF was only increased for a few seconds. Still, this unexpected behavior was in occupying some mental capacities of the crew and could led to severe events in rare cases.

Afterwards, the pilots stated that in reality they would have not accepted the update as the trim setting was so far off the first value. In reality they would have contacted the ramp agent or the operations center before accepting the new load sheet.

Figure 6-3: ACARS load sheet update during simulation.

6.5.2 ACARS FLIGHT PLAN UPDATE

For the threat scenario "ACARS flight plan update", like for the loadsheet update, the updated flight plan was handed to the flight crew. Since changes of the flight path in flight must be coordinated with ATC, in the two simulated cases a contact was established with ATC before accepting the new flight plan. As ATC was not aware of the update, the flight was continued as planned. The pilots did not worry about the update afterwards. Still, this unexpected behavior occupied some mental capacities of the crew and could lead to extended voice communication and workload if a number of aircraft are being attacked in one ATC sector. The pilots stated that it would be very unlikely for them to accept an update in flight without coordinating with ATC. However, two pilots stated that an update before take-off could be considered dangerous as this would not necessarily be coordinated with ATC.

6.5.3 DENIAL OF SERVICE ATTACK ON FMS

This attack was simulated twice during the trials. The denial of service attack on the FMS was discovered instantaneously as the auto pilot disconnected and the map and MCDU was not available anymore. This attack led to an increase of the workload for the pilots as well as an increase of the voice communication demand with the ATC. The stress level reduced when it was discovered that the aircraft was still controllable, raw navigation data was available and ATC was able to provide radar vectors. The pilots stated that an FMS failure (even a double FMS failure) was a standard training item for them. Therefore, they were familiar to the situation to a certain degree. When it was established that the aircraft was still controllable, the situation was assessed to be manageable.

6.5.4 EN-ROUTE GNSS SPOOFING

The GNSS en-route spoofing was not discovered during the event except when an actual ATC controller was part of the trial. After the attack, the lateral displacement and the "GPS primary lost" message was discovered. The lateral deviations observed were up to 10 NM in the conducted trials. The final lateral deviation depends on the deviation rate and on the duration of the spoofing attack. Figure 6-4 shows one instance of the observed lateral deviation at the end of the attack. The observed behavior caused some confusion to the flight crew and also resulted in a reduced confidence in the navigation system. Two pilots would have not conducted the RNP approach as briefed after the spoofing. The attack led to slightly increased workload but the attack was only sustained for a few minutes in the trials. As it was not discovered during the trials, a prolonged attack time could have led to large displacements, which in turn could have resulted in severe events, especially in lower altitudes with surrounding terrain.

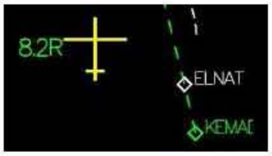


Figure 6-4: Lateral deviation after GNSS spoofing en-route.

6.5.5 APPROACH GNSS SPOOFING

The GNSS spoofing during the approach was not discovered in the single trial in which it was performed. The attack led to a large lateral displacement before the final approach point (see Figure 6-5), as a consequence the approach was discontinued by the pilots. This is a common practice and it only slightly increased the workload of the pilots. Still, as in the en-route case, a prolonged attack time could have resulted in large displacements, which in turn could have led to severe events, especially in lower altitudes with surrounding terrain.

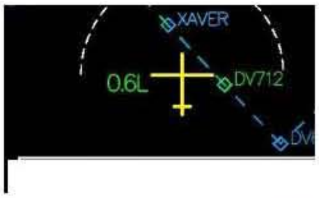


Figure 6-5: Lateral deviation after GNSS spoofing during approach.

6.5.6 HACKED DATABASE DURING RNP 0.1 APPROACH

During the RNP 0.1 approach with the hacked FMS database the diverging flight path was discovered 5 out of 6 times by the PM. In those cases, the PM was cross checking the actual distance/altitude with the approach chart. Instead, in the undetected case the PM did not perform the cross-checks, this resulted in a go-around at the Minimum Descent Altitude (MDA). As a go-around is a common practice, this attack only resulted in a slight increase of the workload for the pilot, but it could lead to a severe capacity decrease at an airport if multiple go-arounds have to be conducted.

6.6 RECOMMENDATIONS FOR THREAT MITIGATION

Based on the results of the tests and on the feedbacks from the involved pilots and ATCO, the following list of recommendations should be considered in order to implement procedures for threat mitigation:

- The altitude / height cross-check during GNSS based approaches is a valuable and important safety net, it should be strictly enforced and considered as a valid safety tool; indeed one test showed that without checking the altitude the wrong flight path was only noticed at the Minimum Decent Altitude, whereas in the other tests the pilot monitoring checked the altitude and was able to identify the deviation from the charted path before the MDA which led to a go-around at a higher altitude.
- The altitude / height of the runway threshold should be displayed explicitly in the FMS in order to be checked in the approach briefing; the tests showed that the coordinates of the runway threshold as well as the height of the threshold could not be checked properly beforehand. It would be beneficial to clearly display the threshold data in the MCDU so that it can be cross-checked before the approach. That would help to identify mistakes at an earlier stage.

- For ACARS updates, a procedure should be considered to ensure the validity of the received information, for example through an authenticated data transmission, or by letting the flight crew respond to or confirm the changes in a secure way. This especially includes updates of the flight plan on the ground; the tests showed that in the simulator environment, the Loadsheet update via ACARS was accepted in 6 out of 7 cases. This means, that there is a lack of control possibilities to validate the correctness of the update. It was also identified that a flight plan update on ground could be a dangerous attack as this is usually not checked and confirmed with ATC.
- The pilots and ATCO should be trained to be aware of the possibility of cyber-attacks and the effects they could have; In general, the pilots did not suspect cyber-attacks behind the malfunctions during the trials. Therefore, the awareness for possible attacks and their impact should be intensified.
- During the en-route segment, an ATC tool for automatically alerting the ATCOs when a significant deviation from the assigned / planned RNP route occurs could be helpful for early cyber-attack detection, especially in busy en-route sectors. Therefore, the intended flight path would have to be shared by the aircraft; the tests showed that the pilots were not able to spot deviations from the intended flight path during sophisticated spoofing attacks. Therefore, a ground-based tool could help to identify those deviations. It would have to be independent from the aircraft's navigation system to ensure resistance to spoofing attacks.
- During GNSS based approaches the ATCOs should focus on monitoring the correct aircraft position, in particular the altitude and lateral displacements with respect to the nominal route. The same comment on a ground-based tool from above applies here.

7 CONCLUSIONS AND FUTURE WORK

7.1 CONCLUSIONS

Within the IACT activity, seven simulation flights were performed with real pilots, emulating several cyberattacks on FMS and GNSS at different flight phases. The pilots were invited to the trials under false pretenses in order to obtain unbiased results.

During each flight trial, three simulated attacks were conducted. No involved pilot associated the experienced effects to a cyberattack. Indeed, the pilots were very interested in the results afterwards and their awareness in cyber-security was increased.

Most of the considered cyberattack were not detected by the crew at the time of the attack. Mis-detected attacks always led to an increase workload of the crew and of the ATCO, but they never resulted in critical situations during the flight exercises. However, the results of the flight exercises are limited to the considered flight route scenario and statistical considerations cannot be derived because of the limited number of tests. In fact, some pilots considered certain attacks as potentially dangerous in real scenarios.

Among the considered attacks, the two attacks that were considered most critical are the “Hacked database” attack and the “GNSS spoofing attack”. The “Hacked database” attack was discovered 5 out of 6 times by the monitoring pilots, thanks to the cross checking of the actual distance/altitude with the approach chart. Instead, in the undetected case the monitoring pilot did not perform the cross-checks, this resulted in a go-around at the minimum descent altitude.

“GNSS spoofing” attacks were performed both during the en-route phase (three times) and during the approach phase (one time). They were never detected at the beginning of the attack, indeed possible temporary losses of the GPS as primary navigation method were disregard as temporary problems, they were not linked to a potential cyberattack. Only in the experiment including an invited ATCO the GNSS spoofing attack has been detected while ongoing, because the ATCO noticed that the aircraft turned several nautical miles in front of the intended turn and informed the crew about their deviation and asked for their reason to deviate. In all the other cases, the effects of the spoofing attacks were discovered only at the end of the attacks, when the system recovered the authentic GNSS position solution and the pilots realized they significantly deviated from the flight route. This suggests that a prolonged attack time could have led to even larger displacements, which in turn could have resulted in severe events, especially in lower altitudes with surrounding terrain. In the single trial with a GNSS spoofing attack on the approach phase the GNSS-based approach was discontinued.

In addition to help in understanding the cyberattacks effects during a flight, test exercises performed with real pilots were also useful to collect the feedback from the pilots, such as the most critical attack scenarios, differences in operations / procedures of different airlines, and recommendations for threat mitigation procedures. The outcomes of the trials show that important mitigation procedures include altitude / height cross-checks, interaction among pilots and ATCO to confirm updates and aircraft positions, and pilots and ATCO awareness of the possibility of cyber-attacks.

Even though much more exercises should be performed to derive statistically significant results and different scenarios should be evaluated to assess the impact of different types of route and attack configurations, the limited number of simulations performed within the IACT activity show the importance for the aircraft industry to investigate the impact of cyberattack on different aircraft systems. In particular, putting the pilots “in the loop”, analyzing their actions during simulated attacks and collecting their feedback afterwards, appears to be the correct path to pursue this investigation.

7.2 FUTURE WORK

IACT project led to very interesting results from several perspectives:

- Formal validation of the ED-202A procedure to airworthiness cybersecurity risk assessment.
- Implementation of a cyber-attack-enabled flight simulator
- Preliminary validation of the full chain through CAT pilots and ATCOs.

For sure, the approach implemented in IACT is right after the "take-off" phase. It can be further improved and applied in several contexts, such as: theoretical study, crew training, standardization activities.

Some interesting ideas worth to be explored in the future are:

- Enhance the statistical confidence of already performed tests:
    - By increasing the number of trials and refining the synthesis of results.
    - By increasing the test cases, to explore a wider range of cases (new flight plans, for instance) that could trigger different critical points.
- Enhance the realism of the simulator:
    - By improving some software implementations
    - By including avionic hardware in the loop, as for instance a COTS avionic receiver.
- Explore from the Electromagnetic perspective the coupling of insider/outsider GNSS spoofing attack with the GNSS antennas via:
    - Finite elements software simulations
    - Laboratory trials in anechoic chambers
    - Real trials in remote regions
- Support EASA in the standardization of the IACT outcomes, to improve training protocols by increasing cybersecurity awareness in the operators and regulators.

END OF DOCUMENT

EASA

European Aviation Safety Agency

European Aviation Safety Agency

Postal address
Postfach 10 12 53
50452 Cologne
Germany

Visiting address
Ottoplatz 1
50679 Cologne
Germany

Tel.	+49 221 89990 - 000
Fax	+49 221 89990 - 999
Mail	info@easa.europa.eu
Web	www.easa.europa.eu