SAFE
Safety Augmentation for Flight Experiments

Bachelorarbeit

Zur Erlangung des akademischen Grades Bachelor of Engineering (B. Eng.)

Braunschweig, 10. Juli 2023

von
Sinan Ferdinand Kohmanns
Matrikelnummer: 1426457
Hochschule Hannover HsH

Erster Prüfer:	Prof. Dr. -Ing. Alexander Vendl
Zweite Prüferin:	Dipl. -Ing. Christina Pätzold
Fachlicher Betreuer:	B. Eng. (Hons) Matthew James Bruce

HOCHSCHULE HANNOVER
UNIVERSITY OF APPLIED SCIENCES AND ARTS

DLR

Kohmanns, Sinan Ferdinand:
SAFE - Safety Augmentation
for Flight Experiments
Bachelor Thesis,
Hochschule Hannover, 2023.

"To design a flying machine is nothing. To build one is something.
But to fly is everything."
- Ferdinand Ferber
with dedication to Otto Lilienthal

Kurzfassung

Die Entwicklung der Luftfahrt hat dazu geführt, dass Flugreisen zu einem unverzichtbaren Bestandteil des modernen Lebens geworden sind. Die globalen Entwicklungen des Klimawandels und die schwindenden Ölreserven machen die Luftfahrforschung unverzichtbar, um Lösungen für eine nachhaltige und effiziente Nutzung von Flugzeugen als Transportmittel zu finden. Aufgrund der gravierenden Auswirkungen, die ein Flugzeugabsturz oder Unfall auf Menschenleben haben kann, hat die Flugsicherheit höchste Priorität und muss in jedem Flugbetrieb erhalten werden. Die erheblichen Verbesserungen in der Flugsicherheit seit den Anfängen der Luftfahrt sind auf die Einführung zahlreicher Sicherheitssysteme, technologischer Fortschritte und ein gesteigertes Bewusstsein aller Beteiligten im Hinblick auf die Flugsicherheit zurückzuführen. Dennoch werden aufgrund der hohen Komplexität des "Systems Luftfahrt" immer gewisse Restrisiken für die Flugsicherheit bestehen. Für die Erkennung und Minderung dieser Risiken spielen Flight Data Monitoring (FDM)-Systeme eine entscheidende Rolle. Das Hauptziel eines FDM-Systems besteht darin, Anomalien, Sicherheitsrisiken und andere Situationen zu erkennen, die eine Gefahr für die Flugsicherheit darstellen. Dadurch können wertvolle Sicherheitsinformationen gewonnen werden, als Basis für Abhilfemaßnahmen zur Erhöhung des Sicherheitsniveaus im operativen Betrieb. Die vorliegende Arbeit konzentriert sich auf die Entwicklung, Implementierung und Validierung eines FDM-Systems, angepasst an die einzigartigen Risiken und Gefahren des Forschungsflugbetriebes des Deutschen Zentrums für Luft- und Raumfahrt (DLR). Die Arbeit beginnt mit der Einbettung der Bedeutung von FDM im Safety Management, behandelt die gesetzlichen Anforderungen an die Implementierung von FDM und stellt das "Schweizer-Käse Modell" von Dr. James Reason als Erklärung für den Zielansatz eines FDM-Systems vor. Anschließend werden die Prinzipien und Elemente eines FDM-Systems beschrieben, gefolgt von einer Studie, die Risiken und Gefahren spezifisch für Special Operators im Allgemeinen und den Forschungsflugbetrieb des DLR identifiziert. Diese Studie zeigt, dass unter bestimmten Umständen das Risiko für Controlled Flight Into Terrain (CFIT)- und Mid-Air Collision (MAC)-Ereignisse im Experimentalflugbetrieb im Vergleich zum kommerziellen Linienflugbetrieb leicht erhöht ist. Um diesen Risiken zu begegnen, wird ein Proof of Concept für ein drei Modi umfassendes FDM-Systems präsentiert, welches auf CFIT bezogene Risiken angepasst ist. Anschließend wird die Funktionsweise von Modus 3 präsentiert, welcher für die programmatische Umsetzung ausgewählt wurde. Um das Programm anhand realer Flugdaten zu validieren, wird ein Testflug geplant, durchgeführt und ausgewertet. Bei diesem Testflug wird unter möglichst realen Bedingungen eine Risikosituation erflogen, um demonstrative Daten für das Programm zu gewinnen. Die Auswertung des Testfluges zeigt, dass das entwickelte FDM-System die Risikosituation zuverlässig und präzise erkennt und die herausgegebenen FDM Informationen als Grundlage für Abhilfemaßnahmen geeignet sind. Auf diese Weise trägt das FDM-System zur Verbesserung der Flugsicherheit im experimentellen Flugbetrieb des DLR bei. Das in dieser Arbeit entwickelte System dient als erster Ansatz und als Proof of Concept für den Einsatz eines FDM Systems im DLR Forschungsflugbetrieb und soll in der Zukunft durch weitere Module erweitert werden.

Schlagworte: *Flugsicherheit, Flight Data Monitoring, Flight Operations Quality Assurance, Controlled Flight Into Terrain, Mid-Air Collision, Safety Management System, Flugexperiment, Digitales Geländemodell*

Abstract

The advancement of aviation has made air travel an integral part of modern life. The global developments of climate change and the diminishing oil reserves make aviation research indispensable in finding solutions for sustainable and efficient utilisation of the aircraft as a means of transportation. Due to the serious impact that an aircraft crash or accident can have on human lives, flight safety is the highest priority to be maintained or even enhanced in any aviation operation. The significant improvement in aviation safety since the early days of flight can be attributed to the introduction of numerous safety systems, technological advancements, and an increased awareness among all stakeholders regarding flight safety. However, inherent risks and hazards to flight safety remain due to the highly complex and sophisticated system of aviation. To mitigate these risks, Flight Data Monitoring (FDM) systems play a crucial role. The primary objective of an FDM system is to detect anomalies, safety risks and other situations, which are "out of the ordinary". As a result, valuable safety information can be generated, used for mitigation actions to enhance the level of safety within the operation. This thesis focuses on developing, implementing, and testing an FDM system customised for the unique risks and hazards associated with the experimental flight operation of the German Aerospace Center (DLR). The thesis begins by embedding the significance of FDM within safety management, addressing the legal requirements for FDM implementation, and introducing the Dr. Reasons 'Swiss Cheese Model' as a framework for understanding FDM objectives. The principles and elements of an FDM system are then described, followed by a study that identifies risks and hazards specific to special operations in general and experimental flight operation in the DLR. The study reveals that under certain circumstances, the risk of Controlled Flight Into Terrain (CFIT) and Mid-Air Collision (MAC) events in experimental flight operations is slightly higher compared to commercial airline operations. To address these risks, a proof of concept of an FDM system is presented, focusing on three Modes designed to target CFIT-related risks. The thesis further explains the implementation and functionality of Mode 3, which is selected for programmatic implementation. A flight test is conducted, performing a simulated high-risk scenario to generate real data for the validation of the programs functionality. The results demonstrate that the developed FDM system is suitable, functional, and effective in providing safety information as a foundation for risk mitigation measures. In this way, the FDM system contributes to enhancing flight safety within the DLR experimental flight operation. The system serves as an initial approach and proof of concept, with the intention of continuous expansion and improvement in the future.

Keywords: *Aviation Safety, Flight Data Monitoring, Flight Operations Quality Assurance, Controlled Flight Into Terrain, Mid-Air Collision, Safety Management System, Flight Test, Digital Elevation Model*

Acknowledgements

First and foremost, I would like to express my sincere gratitude to Prof. Alexander Vendl for giving me the opportunity to write this thesis under his academic supervision. I felt well supported and guided by his numerous tips and advices on my writing, as well as his genuine interest in the subject of my thesis. His regular inquiries about my progress and the time he dedicated to me, including the visit to our facility at the DLR in Braunschweig, further confirmed his commitment and dedication as my academic supervisor. I would also like to thank him for the extensive feedback for the reading samples i sent him during the writing process.

Special thanks go to my first supervisor at the DLR, Christina Pätzold, for enabling me to undertake this bachelor thesis and for always supporting me and my ideas. I would also like to express my sincere gratitude to my second supervisor, Matthew James Bruce, for his valuable expertise and his content related advices, as well as his assistance for my technical questions. I appreciate both of you not only being there for me but also standing behind me and supporting me in my endeavors to implement the FDM system and conduct the flight test.

I would like to extend my thanks to Martin von Depka Prondzinski, whose programmatic tips and guidance were of immense help during the implementation of the TERRASAFE program.

I would also like to express my honest appreciation to Anton Dilcher, Malte Kreienfeld, Stefan Seydel, and Jörn Langemann for helping me to put my plans for the flight test with the 'CODE' into practice.

Lastly, I would also like to thank Niels Holger Siegmund, Uwe Göhmann, and Sebastian Soffner for always motivating me in their own "unique" ways which kept me inspired to continue writing.

The same gratitude applies to all my friends and relatives who have consistently motivated and supported me for my work.

Contents

Nomenclature

Abbreviations

ADRS	Aircraft Data Recording System
AGL	Above Ground Level
AMC	Acceptable Means of Compliance
AMSL	Above Mean Sea Level
ARINC 429	Aeronautical Radio Incorporated (ARINC) databus standard for civil aircraft.
ARP	Aircraft Reference Position
ASCB	Avionics Standard Communication Bus
ATC	Air Traffic Control
ATIS	Automatic Terminal Information Service
CVR	Cockpit Voice Recorder
DEM	Digital Elevation Model
DLR	German Aerospace Center (Deutsches Zentrum für Luft- und Raumfahrt e.V.)
EASA	European Aviation Safety Agency
FDAU	Flight Data Acquisition Unit
FDM	Flight Data Monitoring
FDR	Flight Data Recorder
FL	Flightlevel = the altimeter setting related to the ICAO standardatmosphere pressure of 1013,25 hPa.
GASP	Global Aviation Safety Plan
GM	Guidance Material

GS	Groundspeed
ICAO	International Civil Aviation Organisation
IMU	Inertial Measurement Unit
IRH	Inertial Reference Hybrid System
IRS	Inertial Reference System
IRU	Inertial Laser Reference Unit
QAR	Quick Access Recorder
ROD	Rate of Descent or Descent Rate
SMM	ICAO DOC 9859 Safety Management Manual
SPI	Safety Performance Indicator
SRM	Safety Risk Management
TSR	TERRASAFE Report
UTC	Universal Time Coordinated

Definitions

Altitude	Altitude refers to the aircraft height above main sea level (AMSL).
Angle of Attack (AOA)	Angle between the wings longitudinal chord line and the oncoming airflow.
Continuing Airworthiness	All Maintenance activities conducted with the intention to keep the aircraft airworthy.
Ground Proximity Warning System (GPWS)	An airborne system, which monitors ground proximity or possible conflicts of the aircraft with surrounding terrain, based on aircraft position, altitude, climb and descent rates, flight trajectory and an integrated terrain model. If a possible conflict is detected, visual and aural warnings are provided to the involved flight crew.
Hazards	Potential situation or condition within the system or in the environment, which could cause or contribute to an aviation incident or accident [6].

Height	Height refers to the aircraft height above ground level (AGL).
Instrument Flight Rules (IFR)	Procedures and regulations for flight crews to comply when operating an appropriately equipped aircraft under instrumental (non-visual) meteorological conditions. Similarly, large commercial aircraft usually operate under instrument flight rules.
Instrument Landing System (ILS)	Ground-based precision navigation system which emitts two independent radio beams for vertical (Glideslope) and lateral (Localizer) guidance during approach and landing.
Just Culture	Company culture, which aims for a benevolent dealing with inadvertent errors. Encouraging personnel to report on errors, slips and lapses without unemployment worries will foster more reports, leading to increased awareness over the safety situaion within the organisation.
QNH	Current local atmospheric static pressure is adjusted based on temperature and humidity values to correspond to the pressure at mean sea level. QNH is not an abbreviation but a three letter Q-Code, which is historically established.
Risk	(Safety) Risk refers to both the probability and the outcome severity of a potential aviation safety event [6].
Safety Data	Defined series of non-interpreted, safety related facts or values [5]. Foundation for Safety Information.
Safety Information	Processed, analysed and interpreted Safety Data as a foundation for Safety Management decision making [5].
Safety Management	Proactive and practice driven management of procedures and processes for the identification and mitigation of operational risks to ensure aviation safety.

Safety Management System (SMS)	A Systematic top-down framework for the effective management of safety and for the accomodation of all necessary measures, procedures and accountabilities to achieve Safety objectives [5].
Service Providers	Within the context of this thesis, the term 'Service Provider' refers to organisations conducting commercial air transport.
Standard Operating Procedure (SOP)	Standard Operating Procedures within the context of aviation are defined, mandatory processes, describing how certain operational activities or tasks, necessary for a safe operation, have to be performed.
Traffic Collision and Avoidance System (TCAS)	An airborne system which determines seperation between its own and surrounding aircraft, based on vertical and horizontal distance and flight trajectory. If a possible conflict is detected, visual and auditory warnings (Traffic Advisory) or instructional guidances (Resolution Advisory) are provided to all involved flight crews to clear the conflict.
Twin Storage Application and Service Hub (TWINSTASH)	Centralised network for processing and storage of sensor data from experimental flights including digital twins of the experimental aircraft. Facilitated provisioning of the data for scientists.
Visual Flight Rules (VFR)	Procedures and regulations for flight crews, when operating an aircraft under their own navigational responsibility and under visual meteorological conditions. Radio contact with ATC is not mandatory and aircraft seperation is established by flight crews using the 'See and Avoid' principle.

Variables

Δ_{alt}	Spoofing difference: Difference between start altitude and trigger altitude
$\frac{\Delta H_a}{\Delta t_a}$	Actual descent gradient for ROD_a

$\frac{\Delta H_T}{\Delta t_T}$	Threshold gradient for ROD_T
φ	Control volume cone aperture angle
φ_H	Aperture angle horizontal
φ_V	Aperture angle vertical
$alt_{spoofed}$	Spoofed altitude
alt_{trig}	Start altitude for the test series
alt_{trig}	Trigger altitude for the respective ROD threshold
B_{L1}	Control volume cone width *Level 1* threshold
ft_{AGL}	Height AGL in ft
g	Multiple of the gravitational acceleration of the Earth. $1g = 9{,}81\frac{m}{s^2}$
$H(t)$	Height at given time t
L_1	Length between aircraft nose and *Level 1* threshold
$ROD(ft)$	ROD as a function of the height AGL
ROD_a	Actual Rate of Descent line
ROD_{tgt}	Target ROD
ROD_T	Rate of Descent Threshold line
t_e	Time (UTC) at which the trigger event begins
T_{L1}	Projected impact time at *Level 1* threshold
Units	appAppendix **??**
1Hz	1 Hertz = 1 Data Point/s
ft	feet, 1ft = 0,308m
ft/min	feet per minute
NM	Nautical Mile, 1NM = 1,852km

Intentionally left blank

Chapter 1

Introduction

The airplane, as a means of transportation and travel, is practically indispensable in todays life. Although global air travel has increased twentyfold in the past 50 years [2], measured by the number of takeoffs and landings per year, the accident rates for aircraft tell a different story. While between 1962 and 1971, an average of 133 people per one million passengers flown lost their lives in airplane crashes, the average between 2001 and 2013 was only 2 deaths per one million passengers [3]. As the number of passengers and flights have had steadily increased over the past few decades, the entire aviation industry has had to evolve to meet the demands which caused far more complexity throughout all sectors and areas.

The evolution of flight safety can be categorised into four distinct steps according to ICAO Doc 9859 'Safety Management Manual' [5]. Initially, the emphasis was on technical improvements of aircraft, leading to enhanced component reliability and reduced accidents through the identification of component failures and design flaws. This has led to increased technical reliability. From the early 1970s on, attention shifted towards considering the human factor in flight safety, thereby taking into account that humans can contribute to errors and accidents. This resulted in the awareness, that flight safety needed to be approached from an organisational perspective. Organisational culture and company policies have been implemented, focusing on proactive and reactive safety data collection and analysis methodologies, which initially relied on mandatory and voluntary self disclosure by flight crews with regard to operational errors [4]. Finally, the introduction of Safety Management Systems (SMS) as total system approaches allowed a far more comprehensive, systematic and holistic approach to ensure flight safety. In the early 2000s, the ICAO introduced another mandatory safety system into commercial aviation as part of the SMS for the purpose of safety data collection and analysis: Operational Flight Data Monitoring (FDM) [7]. An FDM system is a proactive monitoring system that automatically analyses flight data to identify anomalies, unrecognised risks and hazards to provide contextual information. The ultimate goal is to use this information for the implementation of mitigation measures through which these risks and hazards can be reduced to an acceptable level.

The Facility for Flight Experiments in the German Aerospace Center (in German: DLR Deutsches Zentrum für Luft- und Raumfahrt e.V.) is a provider for scientific research flights. With a total fleet of 10 fixed-wing aircraft and 2 helicopters at two locations, research projects and flight experiments are conducted for internal and external users. At the Oberpfaffenhofen location, the focus is on research "using the aircraft", meaning the aircraft are used as airborne platforms for atmospheric research and Earth observation. At the Braunschweig location, the emphasis is on "research on the

aircraft", specifically conducting scientific projects related to various research areas such as flight physics, flight control and aircraft system engineering, sustainable propulsion systems, cockpit automation, and unmanned flying.

Figure 1.1: DLR experimental research fleet [Credit: DLR Internal Source]

As of June 2023, while FDM systems are mandatory for commercial air transport organisations, they are not yet required for special operators like the DLR. Due to the specific kind of flight performance and flight envelope profiles involved in experimental flight operation, a direct transfer of existing FDM systems from commercial aviation to the DLR is not feasible. Therefore, this thesis focuses on the conceptualisation, development and implementation of an FDM system specifically adapted to the characteristics and requirements of DLR experimental flight operation, with focus on the research aircraft Dornier Do228-101 'D-CODE'.

To establish a theoretical foundation for understanding the role of FDM within the context of safety management, the thesis initially provides the necessary background information. Thereafter, the elements of an FDM system and its impact on detecting and mitigating risks and hazards during flight operations are discussed. Furthermore, the usage of FDM in other special operations is described, alongside an analysis of individual risks and experiences in potentially hazardous situations involving the D-CODE aircraft. Based on this knowledge, a proof of concept is outlined to demonstrate the implementation of an FDM system taking into consideration the specific risks and hazards associated with the flight operation of D-CODE. Subsequently, the methodology and design of the FDM program, which includes three distinct modes, each targeting a specific FDM event are described. From these modes, one is selected for programmatic implementation within the scope of this thesis. The trigger logics and exceedance detection algorithms for this selected mode are then explained in detail. To assess the functionality of the system within this thesis, a real flight test that simulates a hazardous situation shall be designed and performed. The flight test data is then used for evaluation of the FDM program, which is intended to identify and analyse the simulated scenario, so that the systems effectiveness and functionality can be demonstrated.

The developed FDM system serves as an initial approach and proof of concept for implementing such a system in the DLR experimental flight operation. Ultimately, the FDM system developed in this thesis will be continuously expanded and improved with additional modules, thereby contributing to the long-term enhancement of flight safety in the DLR experimental flight operation.

Chapter 2

Theoretical Background

This chapter describes the foundation and knowledge required for the development of Flight Data Monitoring (FDM) algorithms. To begin with, a brief introduction to safety management is given (section 2.1). Thereafter, an overview of the theoretical background of an FDM program as well as practical risks and hazards which can be addressed by an FDM program, are described (section 2.2). Preliminary considerations are then presented (Section 2.3), reflecting the practical conditions and constraints at the DLR under which an FDM program would operate.

2.1 Safety Management - An Integrated Approach towards Improving Aviation Safety

Through safety management service providers in civil aviation aim at proactively mitigating risks and hazards with the ultimate goal of reducing the probability of an aviation incident or accident. Whereas the term *safety measure* refers to a specific barrier or action targeting one or a few hazards, safety management comprises of the application of several means, measures, processes and structures and their interactions within the service providers operation, to maintain and enhance flight safety [5].

Safety management activities performed by aviation service providers extend across all safety related activities regardless of whether these activities are directly or indirectly linked to flight operation. This includes but is not limited to, subjects concerning organisational management, flight crew rostering and other personnel planning, operational procedures and aircraft maintenance. Because of the possibility that hazards and risks could arise, from the relationships between the service provider and subsidiaries or sub-contractors, these activities need to be taken into consideration as well [5]. A systematic top-down framework is required to effectively manage safety and to accomodate all necessary measures, procedures and accountabilities to achieve Safety Management objectives [7], this is referred to as an organisational Safety Management System (SMS). The incorporation of an SMS comes with additional overheads, leading to disadvantages such as increased expenses, more rigid organisational structures and procedures as well as additional bureaucracy. Despite these disadvantages the opportunity costs of disregarding Safety Management principles could indeed be much higher, as the following quote by Easyjet founder Helios Haji-Ioannou eminently proves: "...if you think safety is expensive, try an accident." [8]

2.1.1 Benefits of a Safety Management System

According to ICAO DOC 9859 *Safety Management Manual* (SMM) [5], several benefits come with the incorporation of a SMS. The main aspects are listed below with a short summary:

1. *"Documented, process based approach to assure safety"* (1.1.7.b) - A documented and process based approach ensures transparency and supports understanding of safe operations by the personnel. Additionally, controlled changes of organisational procedures concerning safety improvement are manageable due to the clearly defined baseline perfomance.

2. *"Enhanced early detection of safety hazards"* (1.1.7.d) - Due to the proactive identification of hazards, risks and adverse trends at an early stage, accidents can be prevented through an early identification of contributing factors and the subsequent implementation of corrective actions.

3. *"Safety data-driven decision-making"* (1.1.7.e) - By analysing safety related data, the service provider gathers a wide range of information on which to base strategic and operational decisions. Continuous analysis of the safety related data, highlights areas of greater concern, and can lead to better informed decisions being made in almost real time.

4. *"Evidence that safety is a priority"* (1.1.7.g) - Within the aviation industry, it is desirable to motivate all involved parties to work and behave in accordance with principles of safety. Commitment demonstrated through management policies and company culture has an impact on behavioral patterns of personnel. Being throroughly knowledgable about a specific task and its associated responsibilities reduces the likelihood of errors or faults during the performance. This directly increases safety performance and ultimately the service providers reputation within the aviation community and as percieved by internal and external stakeholders.

5. *"Improved efficiencies"* (1.1.7.i) - Incorporating a Safety Management system not merely exposes safety threats, it moreover can make inefficiencies in existing processes and systems visible, which then can lead to optimisations that reduce operational costs.

6. *"Cost avoidance"* (1.1.7.j) - Risks and hazards, if left undisclosed, can eventually trigger incidents and accidents, which inevitably lead to direct or indirect costs. Direct costs could comprise of: injuries, property damage, equipment repairs and schedule delays. Indirect costs could comprise of: legal action, loss of revenue due to damaged reputation, additional training and increased insurance premiums. By proactively and preveniently identifying and mitigating risks and hazards, the associated costs of their long term effects can be avoided.

2.1.2 Regulatory Background

The International Civil Aviation Organization (ICAO), as a specialized agency of the United Nations, develops authoritative standards and regulations which must be legally implemented by its member states [13]. At the end of the 20th century, the initial version of the Global Aviation Safety Plan (GASP) was introduced by ICAO. The GASP is aimed at aviation authorities of ICAO member states as it provides legal framework for the implementation of effective state safety programs [11]. In 2005, several administrative and industrial representatives gathered to launch the development for a newer conceptual plan for aviation safety. As a result, ICAO revised its GASP with

respect to further harmonised requirements, which then, in 2006, led to the first publishment of the ICAO DOC 9859 Safety Management Manual (SMM) [5]. The SMM encompasses guidelines and framework for the implementation of an SMS. The participants of the ICAO High-Level Safety Conference 2010 have agreed on a resolution to establish a new annex regarding safety management in order to further facilitate implementation of an SMS as well as harmonising the remaining annexes for duplications on this subject [12]. This was the inception for the development of ICAO Annex 19 *Safety Management*, the first edition of which was published in 2013.

Since publishing exact guidance on the implementation of an SMS which addresses every peculiarity of an organisation is practically not suitable, given the many complex and diverse areas and workscope varieties. The framework released by the ICAO therefore merely comprises of more generalised regulations. More specifically, the regulations provide guidance on what needs to be accomplished, but not how to implement the required elements. In the European Union, the European parliament and the council adopt *basic regulations,* which apply to all member states of the European Union and their operating service providers, thereby fulfilling the obligations of the ICAO [14]. *Basic regulations* have a binding character for the service providers and represent the highest level of regulatory material. The *European Aviation Safety Agency* (EASA) is responsible for elaborating the *implementing rules* to provide guidance on how to comply with *basic regulation*s, which are therefore also binding. *Acceptable Means of Compliance (AMC)* and *Guidance Material (GM)* represent the lowest level and are of non-binding character. They provide guidance on means and measures which, when implemented as intended, meet the requirements of the *implementing rule* [17]. Every service provider is obliged to comply to the regulations and meet the mandatory requirements by their own developed means and measures, which will be inspected by competent authority.

As per Annex 19, the following service providers, among others, are obligated to implement an SMS:

1. Approved training organisations which are in accordance with ICAO Annex 1[1] (3.3.2.1.a).
2. Operators of aeroplanes or helicopters conducting commercial air transport in accordance with ICAO Annex 6[2] (3.3.2.1.b).
3. Approved maintenance organisations which provide services to operators engaged in commercial air transport in accordance with ICAO Annex 6 (3.3.2.1.c).

As the DLR is a specialised flight operator for the conduction of flight experiments and therefore not listed as a service provider according to Annex 19, the requirements concerning an implementation of a SMS are not mandatory. However, it is reasonable to voluntarily apply the principles of the regulatory framework regarding SMS and FDM as they provide a good guidance and benefits as listed in section 2.1.1.

2.1.3 Structures of a Safety Management System

Chapter 9 of the ICAO SMM [5] classifies four main components of an SMS which are grouped in Table 2.1.

The four components are briefly explained and summarised below based on Chapter 9 of the ICAO SMM [5].

[1]ICAO Annex 1 *Personal Licensing* contains SARPs for acquisition of licenses for flight crews, ground crews, air traffic controllers etc. [15]

[2]ICAO Annex 6 *Operation of Aircraft* contains SARPs for international air transport operators. [16]

Table 2.1: Components and elements of the ICAO SMS framework [5].

Components	Elements
1. Safety policy and objectives	1.1 Management commitment
	1.2 Safety accountability
	1.3 Appointment of key safety personnel
	1.4 Coordination of emergency response planning
	1.5 SMS documentation
2. Safety risk management	2.1 Hazard identification
	2.2 Safety risk assessment and mitigation
3. Safety assurance	3.1 Safety performance monitoring and measurement
	3.2 The management of change
	3.3 Continuous improvement of the SMS
4. Safety promotion	4.1 Training and education
	4.2 Safety communication

Safety Policy and Objectives

The first component *safety policy and objectives* synopsizes formal elements to facilitate the establishment and the operation of the SMS. These elements include for instance formulating a safety commitment on behalf of the management to verify the creation of an effective Safety Management environment. Furthermore, an Accountable[3] Manager shall be appointed, the scope of work shall be defined and documentation of the associated SMS shall be implemented which includes the procedures, policies and processes of the company in relation to the SMS. In a nutshell, the first component of an SMS should adress the formal administration. In the context of safety management philosophy, it is crucial to underline the non-punitive character of hazard mitigation processes. Since it is the human nature to be susceptible to making mistakes, punitive actions from the management side against individual employees are detrimental for a positive reporting culture within the organisation. Identifying unsafe conditions, to some extent relies on reporting of mistakes from employees. Creating an environment where employees can report inadvertently made mistakes and errors without jeopardising their employment leads to more reports, and therefore more safety relevant information.

Safety Risk Management

The second component *safety risk management* (SRM) rather highlights operational elements. Since this thesis mainly focuses on the implementation of an FDM program into the DLRs experimental flight operation, the element *2.1 Hazard identification* is worth a closer look. *Hazard identification* and *Safety risk assessment and mitigation* are the two elements which build the SRM process. *Hazard identification* as the first step aims towards the implementation of processes, means and procedures to detect safety related occurrences, detrimental conditions and hazards. This can be accomplished through several measures, including but not limited to audits, voluntary and mandatory safety reporting systems or an operational flight data monitoring system, which is discribed in section 2.2. With the obtained information, the ensuing process of SRM shall initiate a systematic approach in assessing the potential impact of the uncovered condition or hazard on flight safety. The resulting mitigation actions are based on the information retrieved and should

[3] *The term 'accountability' refers to obligations which cannot be delegated. The term 'responsibilities' refers to functions and activities which may be delegated.* ([5] p. 9-4)

be appropriate for size and scope of work of the service provider with the ultimate goal of either completely neutralising the risk, or reducing it to an acceptable level.

Safety Assurance

Safety assurance concentrates on monitoring the effectiveness of the SMS, its underlying processes and the operational environment with regard to possible deviations or adverse trends. *Safety performance monitoring and measurement* as the first element essentially relies on measuring the extent to which the previously established safety objectives and safety performance indicators (SPIs) are achieved. Furthermore, adverse trends, induced from previously made changes can be detected. Alteration of already established procedures, technology, operating environment, key personnel or regulatory requirements, among others, inevitably entails new risks. By utilising the *management of change* element, it is necessary to anticipate and subsequently mitigate these new risks to ensure an acceptable level of safety. The last element, *continuous improvement of the SMS*, involves constantly assessing and enhancing its effectiveness through iterative improvement methods, taking into account the information obtained from the *safety performance monitoring and measurement.*

Safety Promotion

Safety Promotion consists of *training and education* and *safety communication.* Whereas *training and education* means safety training program appropriate to maintain and enhance personnel competency regarding their SMS responsibilities and tasks, *safety communication* implies disseminating information on SMS objectives and procedures to all relevant personnel. According to ICAO SMM [5], safety communication includes but is not limited to:

1. *"Ensure that staff is fully aware of the SMS" (9.6.5.1.a).*
2. *"Convey safety critical information" (9.6.5.1.b).*
3. *"Raise awareness of new safety risk controls and corrective actions" (9.6.5.1.c).*
4. *"Provide information on new or amended safety procedures" (9.6.5.1.d).*

2.2 Operational Flight Data Monitoring

Since safety management is largely driven by practical, safety data based decision making, high emphasise has to be given on the acquisition of reliable and accurate information on risks and hazards [20]. As described in section 2.1.3, one approach towards obtaining safety information is by implementing an operational Flight Data Monitoring (FDM) system.

FDM systems are operating in basically every commercial airline and many other service providers due to their regulatory environment. Broken down to its essentials, the FDM works very similarly to the flight data recorder system (FDR). The FDR is in use in aviation since the 1960s and forms, together with the cockpit voice recorder (CVR) the flight recorder, often referred to as the "black box"[4]. FDM and FDR monitor more or less the same systems and sensors, usually covering data

[4]Flight recorders are actually painted in bright orange to facilitate the identification and recovery in case of an accident.

from cockpit displays, aircraft systems, engines and flight control inputs [20]. However, there are key differences between them. The FDR saves recorded data for a certain time and overwrites the preceding dataset in a constant loop, whereas FDM aims to store the data for further use. Moreover, an FDR is generally used, after an accident or incident has happened as a reactive approach, whereas FDM pursues a different approach: It is used to proactively accumulate and process safety relevant data to indicate abnormalities in flight operation. The results and outcomes provide a specific post holder like the safety manager or assigned flight safety specialists with the information needed to identify hazards and adverse safety trends within operation [20]. Once an unaccaptable risk has been identified, either already existing or predicted on the basis of trends, the obtained information is used to implement mitigation measures. Through FDM, those measures should be controlled and validated with regard to their effectiveness [18]. In summary, FDM provides insight into contributing factors and weaknesses in safety barriers that may not have been disclosed earlier, before an accident occurs. The correlation between safety barriers, their weaknesses and the occurrence of accidents as well as the role of FDM in this relationship is colloquially described as the 'Swiss Cheese Model' and is depicted in figure 2.1.

2.2.1 Dr. Reasons Swiss Cheese Model

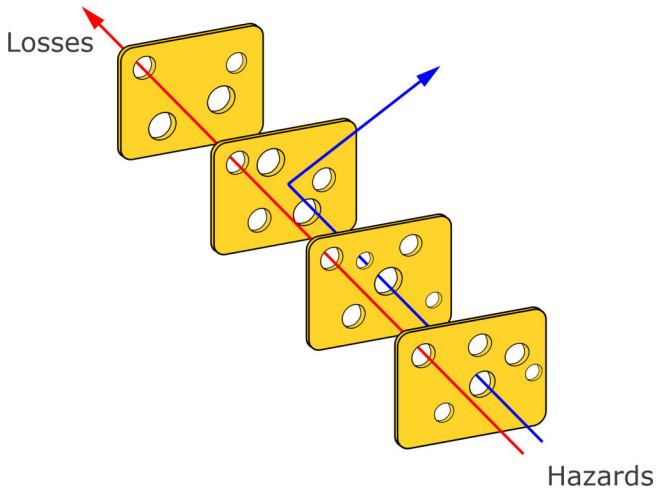

Figure 2.1: Dr. Reasons swiss cheese model.

Dr. James Reasons Swiss Cheese Model is a widely used heuristic explanation of how accidents occur in the context of safety management. In aviation, to prevent accidents or incidents from happening, a multitude of risk mitigation strategies which form safety barriers, are implemented in any safety relevant system. As it is depicted in figure 2.1, these safety barriers are represented as slices, arranged one after the other. Each safety barrier incorporates weaknesses, failures, or imperfections which are portrayed by holes in the slice, comparable to the "eyes" in a slice of an Swiss Cheese. The safety barriers can, depending on the dimension and position of the weaknesses, be breached by hazards which are in figure 2.1 visualised as the red and the blue arrow. A violation of one or a few safety barriers by the hazard may not directly result in an accident or loss, provided, that there is at least one remaining safety barrier which can ultimately mitigate the hazard (indicated by a blue arrow being deflected by a safety barrier). When in specific circumstances, the holes in the safety barriers align, allowing a hazard to breach through

(indicated by a red arrow crossing the safety barriers), the loss becomes unavoidable [19].

The purpose of an FDM program is to search for holes in the slices and to make them visible, so that eventually, these holes could be either downsized or completely closed through effective and non-punitive mitigation processes.

2.2.2 Elements of a Flight Data Monitoring System

The effectiveness and performance of an FDM system is largely determined by the set of flight parameters, availability and its data quality [22], measured by for instance accuracy, sampling rate and consistency of the dataset. Service providers should develop their FDM with regard to their own operational specifications, taking into account factors such as fleet composition, fleet size, route network or business model and hereby selecting flight parameters, appropriate to cover their own safety demands.

This section provides baseline components which have to be established for an FDM System to operate. It is important to note, that in this section, a rather general oversight on the elements of an FDM is given. The application of these principles on the operational specification of the DLR is desribed in section 2.3.

Safety Data Acquisition

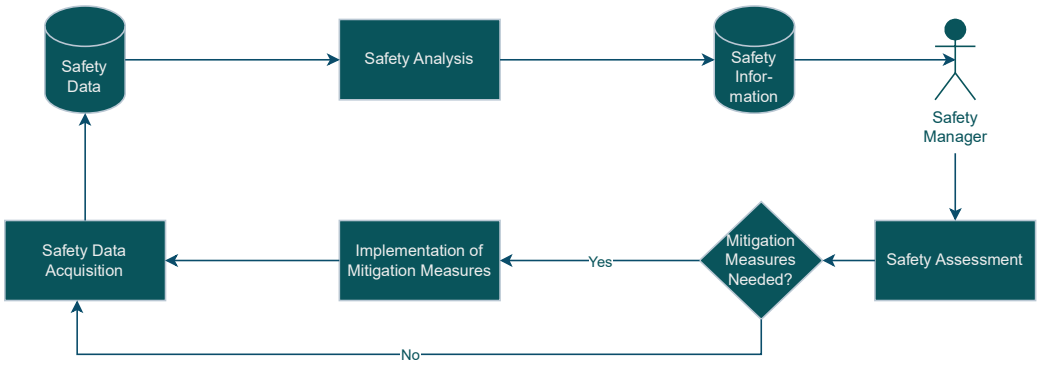

Figure 2.2: FDM-Loop process.

Safety data acquisition comprises of processes and systems to *capture* the required flight parameters and means to *transfer* the data from the aircraft to the ground-based processing system (a set of computer programs) with the safety analysis system [18]. Recording safety data can be accomplished via onboard sources, including, but not limited to digital data-busses, such as Avionics Standard Communication Busses (ASCB) and Aircraft Data Recording Systems (ADRS). Another way of accessing safety data can be accomplished through a Flight Data Acquisition Unit (FDAU). The FDAU is a system which collects numerous analog, digital or discrete signals from aircraft systems and components. If necessary, the data is sampled, digitalised and eventually redirected to the Flight Data Recorder (FDR) or to the Quick Access Recorder (QAR) [23]. The QAR, is a system, which captures and records thousands of flight parameters with different resolutions and accuracies [22] on tapes, optical discs, memory cards or other easily removable recording media. The safety data accumulated with the QAR has to be manually transferred to the processing station, either during regularly scheduled maintenance visits, or when a defined time has elapsed. Nowadays, QAR systems with secure wireless data transmission capabilities are becoming more

common, allowing a safer, more direct and more protected transmission to the safety analysis system [21, 24].

Once securely transferred to the ground-based processing system, the raw data has to be downsampled, erroneous data needs to be fixed and data which is redundant or not beneficial for *safety analysis* has to be filtered, to prevent wasting storage and processing capacity. Furthermore, the raw binary data has to be converted to scaled engineering units and undergo several checks for low quality data [21] or sensor noise, which inevitably accompanies every measurement up to a certain extent. This ensures that the *safety analysis* and resulting mitigation actions are based on reliable and valid data.

Safety Analysis

After the safety data has been transferred from the aircraft and passed through the filtering and downsampling processes, the *safety analysis* and its underlying mechanisms are applied to ultimately turn safety data into safety information. *Exceedance or event detection* builds the foundation of the *safety analysis* element of an FDM System. The methodology of *exceedance or event detection* is based on algorithms, which analyse the safety data for deviations from flight manual limits, Standard Operating Procedures (SOP) [18] or established standards of good airmanship[5]. Common practice is, to establish a set of core events, reflecting each operators main interests or risks [21]. Although operational differences vary between service providers, there are main areas of interest, which are substantially common to all operators. EASA defines four high-priority risk categories of aviation safety occurrences. FDM Systems of the service providers primarily have to monitor events and operational safety issues which could potentially cause these occurrences [25, 26]. The occurrence categories are:

1. RE - Runway Excursion
2. MAC - Mid-Air Collision
3. CFIT - Controlled Flight into Terrain
4. LOC-I - Loss of Control in-Flight

Good examples for events or indicators to be captured by *exceedance or event detection* include, but are not limited to (related occurrence category in squared parantheses): High speed rejected take-off [RE], a resolution advisory from the traffic collision avoidance system (TCAS) [MAC], a terrain warning from the ground proximity warning system (GPWS) [CFIT], excessive roll attitude or rate [LOC-I]. Detection algorithms are basically composed of the trigger logic itself, the indicative circumstances and interdependencies to be detected by the program and the indication of severity of what is detected [26]. The methodology of the trigger logic as such could be realised through simple “redline value” breaching detections. On the other hand it could be constituted through sophisticated and dynamic triggering algorithms which take into account certain triggering conditions and different sets of flight parameters, predicated upon individual situations [18, 26]. It is a reasonable technique to define certain trigger levels for a severity classification of the safety event. This differentiation enables a better assessment and provides deeper insights into the trigger event which improves the determination of its cause or possible consequences. Since the primary focus

[5]Good Airmanship is an adage for a set of favourable behavioural traits of ’Airmen’, for instance a good situational awareness, good judgemental abilities and flying skills. ’Airman’ in the terms of aviation refers to someone, who is piloting an aircraft.

of this thesis is to establish a basic approach to implementing an FDM system, the methodology conveyed in section 2.3 is subject to the *exceedance or event detection* element.

Once the foundation for the *safety analysis* element of the FDM system has been set with the *exceedance or event detection*, further awareness of adverse trends and tendencies before trigger levels are reached, can be provided through *routine data measurements*. Collecting data from all flights, not merely limited to the ones, generating trigger events allows the analysis of adverse cues, emerging trends and tendencies in the long term, and hence promotes the anticipation of arising risks and hazards in the subsequent FDM stage [21]. This allows an impression to be gained of how close to the limits the operation is. Additional elements of the *safety analysis* are the accumulation of *incident investigation data* as well as *continued airworthiness investigation data*. The former element comprises of data for the support of investigations and follow up in the aftermath of incidents, whereas the latter element contains useful data to be utilised for assisting the continuing airworthiness function [18, 21].

Safety Assessment and Mitigation

This stage of the FDM system encompasses the utilisation of the safety information, obtained from the *safety analysis*. Outcomes of *exceedance or event detection* and *routine data measurements* should be anonymised, thereby protecting the identity of the flight crew and realising the non-punitive element of the safety culture. Moreover, the outcomes are usually statistically evaluated, taking into consideration factors such as flights flown per aircraft or total flight time to generate rate and trend information [18]. Exceedances and deviations, detected by the program, are embedded into other contextual information of the particular flight to investigate roots, conditions and background of the situation. Unsolved occurrences from the *Safety Analysis* are referred to a safety representative for further analysis, which may include review of the raw data and discussion with the flight crew [22]. This enables a trustworthy and unbiased communication and therefore promotes unveiling occurence causations, without detracting from Just Culture principles. Such discussions can yield valuable feedback, on procedures which which unintentionally compromise flight safety due to detrimental side effects. This feedback can lead to revisions in company SOPs and manuals, as well as adjustments in air traffic control, navigational, and airport operating procedures. From the other point of view, the assigned safety representative can give advice or recommendations for appropriate action to the respective flight crew, which could include additional and constructive training on managing the particular situation. It is of eminent importance, that non punitive mitigation actions are applied, since giving penalties or even fire employees on inadvertent mistakes, bars the path to an effective SMS [21, 18]. After the causes and contributing factors of exceedances, adverse trends and occurrences have been thorougly identified and investigated, appropriate corrective actions and mitigation processes have to be developed and eventually implemented. The effectiveness of mitigation actions must be evaluated, necessitating thorough follow-up monitoring of their results and consequences on operation in an iterative process [21]. Besides that, it is important to regularly review for cues of emergence of unintentionally created problems due to the mitigation actions. This "FDM-Loop Process" is depicted in figure 2.2.

2.2.3 FDM Application in other Special Operations: Flight Inspection

Navigational facilities in aviation, for instance Instrument Landing Systems (ILS), radio beacons or radar systems constantly have to be calibrated and adjusted to ensure correct indication in

the navigational equipment of aircraft. Measurement flights are conducted by flight inspection companies where the inspecting aircraft frequently performs aerodrome traffic circuits with low approaches and go-arounds as well as circling the respective beacon or system at low height. Unlike commercial transport (airline) operations, these flight operations are characterised as specialised flight operations[6] with regard to their flight profile. Consequently, they are not mandated to adhere to compulsory FDM implementation regulations. However, for the evaluation and analysis of risks and hazards, inherent to the DLR flight operation, safety events of other special operations are worth consideration.

High Rates of Descent During Flight Inspection

G. Marino revealed in his paper in the IFIS 2014 proceedings [27], how FDM contributed to the mitigation of a risk, which very likely could have contributed to an accident. Once, a mission was flown where the approach path monitor of an airport had to be inspected. The approach path monitor is a system which generates an alarm inside the airports tower if an aircraft descended or is predicted to descent below a certain altitude limit. In order to check the systems functionality, the flight inspection mission requires a descent below the altitude limit, with a descent rate, sufficiently high to trigger an alarm in the air traffic control (ATC) tower. Prior to this mission, ATC had inadvertently disarmed the warning system. In order to trigger the alarm, the flight crew initiated very high rates of descent, of up to $6000\frac{ft}{min}$ in $400ft$ above ground level (AGL). By comparison, the rate of descent triggering limit of the GPWS in $400ft$ is $1500\frac{ft}{min}$ [28] and the typical rate of descent of a Boeing 737 descending on a standard 3° ILS Glideslope is between $700\frac{ft}{min}$ and $750\frac{ft}{min}$. While the flight crew was unaware of the fact that the warning system had been disabled, it was attempted to trigger the alarm by unceasingly increasing the decent rate. In the post flight analysis, the FDM information contributed to corrective action, where the crews were retrained that high rates of descent are unnecessary to activate the alarm and lower rates of descent are appropriate and should be targeted to reduce the risk of an accident [27]. Operating an aircraft in an altitude close to the ground inevitably entails the risk of a CFIT incident. Due to the limited margin, which is precious for the execution of any correction maneuvers, the consequences of any inattentiveness by the flight crew can be severe. Mistakes or incautious handling can result in errors which may ultimately lead to a ground collision. The adage “speed is life, altitude is insurance”, which has been taught to student pilots for generations, highlights the significance of ensuring appropriate flying performance, especially in low altitude operations.

Challenges and Current Situation Associated with the Implementation of an FDM System for a Flight Inspection Provider

Based on an interview with a flight safety representative from a flight inspection company [31], the following section demonstates the difficulties, a flight inspection provider could face when implementing an FDM system into their operation.

The operation of flight inspection can be devided into two characteristics. In the first case, these are positioning flights, where the flight crew relocates the aircraft from its homebase to the airport where the inspection misson is to be conducted. This is characterised with an ordinary flight environment, which is comparable to airline flight operation. In the second case, the flight environment

[6]Specialised Operation according to EASA addresses any flight operation other than commercial air transport. Besides experimental flight test operation and flight inspection, special operation comprises of for instance: Agricultural-, surveying-, construction-, powerline and pipeline check operation.

faces further risks and hazards for instance due to low altitude flights, operation against normal traffic flow, conflicts with other traffic[27] and a high cockpit workload.

Inspection missions for the calibration of ILS need to be conducted in low height in landing gear up and flaps up configuration. In practice, for an appropriate calibration of the glideslope antenna, the runway threshold needs to be approached in a height as low as $50ft$ AGL. This kind of flying involves a high workload for the flight crew, where a constant scan of the barometric altimeter is not feasible. In fact, the pilot flying has to concentrate on maintaining a speed, high enough for the aircraft to fly safely. Additionally, the pilot flying constantly judges the height of the aircraft above ground by solely looking out of the windshield, thereby assessing the aircrafts attitude through peripheral vision against the horizon. The higher the airspeed of an aircraft is, the more sensitive the flight controls are to steering inputs. Given the low height of the particular inspection flights, risks of inadvertant ground collisions (CFIT) due to incautious flight control inputs or misjudgements jeopardise flight safety. A good solution, where an FDM system could come into use is by setting a trigger limit at a height of $30ft$. Whenever a flight crew inadvertantly or intentionally descends below this threshold, the FDM system captures the event. After detection, the particular event can be assessed and corrective action, such as additional training or educational instructions can be given.

Another case in which an FDM system could be advantageous is for flights in mountainous terrain. Flight inspection missions are occasionally carried out at aerodromes, which are surrounded by high mountains, for instance Innsbruck airport in Austria or Sion airport in Switzerland. As all larger airports, they have certain departure and approach procedures which give guidance to aircraft, departing and approaching the airport under instrument flight rules (IFR). These departure and approach routes provide valuable information on how to manoeuvre the aircraft safely around the mountains without endangering the flight through conflicts with the surrounding terrain. Visual flight in these regions can potentially trigger GPWS nuisance alerts, detrimental for the concentration of the flight crew. To prevent the latter, flight crews often tend to disarm the GPWS so that the constant aural and visual alerts would not distract the crew from aircraft operation[7]. To detect unsafe situations, for instance an excessive approach to rapidly uprising terrain, it is beneficial to implement an FDM system.

2.3 Preparing for Implementation: Essential Background Information and Proof of Concept for the FDM program

This section provides basic information necessary for the appropriate implementation of an FDM system for the DLR experimental flight operation. First, the specific risks and hazards associated with typical flight experiments, conducted with the Dornier Do228-101 experimental aircraft registered as 'D-CODE' (hereinafter referred to as D-CODE) are described. Thereafter, the data acquisition system of this aircraft and the structure of the Twin Storage Application and Service Hub (TwinSTASH), where the safety data is obtained, are described. Finally, a proof of concept for an initial realisation of an FDM system tailored to the particular operational risks and hazards of the D-CODE is formulated.

[7]Since the flight crews perform briefings with emphasis on terrain obstacles prior to such flights, disarming the GPWS is compared to the constant distracting alerts, the "lesser of two evils".

2.3.1 Risks, Hazards and Peculiarities of the Experimental Flight Operation with the Dornier Do228-101 'D-CODE'

The type of flights in an experimental flight operation cannot easily be divided into the six flight phases of taxi, takeoff, climb, cruise, descent and landing, as is the case, for instance in conventional commercial air transport operations. In fact, there are irregular flight phases, depending on the specific characteristics of the flight program and the experimental mission, including but not limited to several low approaches and traffic circuits, low altitude flights, circling flights, flights at the limits of the flight envelope. A general particularity of experimental flight operations, not merely limited to the operation of the DLR is the fact that flight crews sustain low flight times. Staying current in flying practice and continuous training is essential in aviation, since airplanes are complex machines with numerous systems and unique features that pilots must stay aware of. Flight crews with less flight practice may be more susceptible to reduced situational awareness, as a greater extent of mental capacity is needed for the performance of routine flying tasks. Because of distinctive characteristics of each aircraft type, flight crews with type ratings on more than one type, are potentially susceptible for mistakes and errors in operation. Different aircraft types have different limitations, properties and performances, which are not interchangably applicable. Thus, under certain circumstances, operating errors and mistakes can occur. However, as these risks are more general in nature and can not be attributed to specific operational events of the DLR, they are not subject to this thesis. It is important to note, that flight experiments and consequently the associated risks are not merely limited to those, described herein. Nevertheless, the subsequently described types of experimental flights and the risks inherent thereto are generally applicable to the type of operation normally conducted with the D-CODE and hence within the focus of this thesis. The subsequent section is derived from an interview, conducted with an experimental test pilot who has experience flying the D-CODE aircraft [32].

To begin with, the D-CODE is used to conduct validation and testing of different approach procedures for landings at airports. These procedures vary in their characteristics, ranging from standard 3° approaches to steep approaches, curved approaches or circling approaches. As described in section 2.2.3, operating in low altitude involves limited margins for corrective actions, making steep approaches more prone to CFIT incidents. During certain missions, which require steep approaches, it is intended to capture the ILS 3° glideslope from above. As per common practice, the ILS glideslope is usually captured from below in a height of $3000ft$ above the touchdown zone and in a distance of approximately 9 Nautical Miles (NM) or $16.7km$ in front of the runway. By performing this technique, the risk of gaining excessive airspeed during a steep descent by converting potential energy (altitude) into kinetic energy (speed) can be averted. A secondary effect of capturing the glideslope from above is that ILS antennas inevitably emit erroneous glideslope signals with much steeper descent angles. These "false glideslopes" occur every 6° above the actual glideslope [30]. For most airports a standardised 3° glideslope is established, whereas angles of up to 3.5° are still considered to be routine[8] [33]. In these cases, false glideslope angles of 9°, 15° etc. are emitted by the ILS antenna. Capturing such a false glideslope can lead to a much steeper approach as intended, with very high rates of descent. This circumstance, together with the fact that the aircraft is situated in low altitude, entails the risk of a CFIT incident. Flying such approaches for experimental purposes is frequently performed in assistance with the onboard experimental autoflight system (autopilot) of the D-CODE. In these missions, scientists

[8] Only a small number of airports have approach angles which are significantly steeper than 3°. This is mostly the case at airports where the surrounding terrain necessitates steeper angles or noise abatement procedures are compulsory, for instance at London City airport with an approach angle of 5.5° [33] .

implement and program the experimental autoflight system with required navigational data. The aircraft performs the associated approaches autonomously with the flight crew merely acting as safety pilots, monitoring the systems and flight parameters. As no technical system is invulnerable to malfunctions and glitches, there may be situations where the autoflight system does not stop the descent in the planned altitude, abpruptly changes the aircrafts pitch attitude, increases the rate of descent or operates in any other unpredictable way. Although the pilots will take over and abort the approach to reassure flight safety, these situations still bear a significant risk for ground collision (CFIT).

Other experimental flight missions involve conducting measurement flights for noise and pollutants. This requires the performance of multiple consecutive traffic circuits with low approaches and passes at a height of at least 50ft above the runway, where the ground based measurement system is installed. In order to obtain a broad assortment of experimental data, the low approaches need to be performed in different high lift device and landing gear configuations. The configurations can vary between Gear Up / Flaps Up, or Gear Down / Flaps Full configuration, different airspeeds, power settings and angles of attack. However, these operations entail similar risks and hazards to those desribed in section 2.2.3 and are therefore susceptible to CFIT incidents.

Another risk, inherent to the experimental flight operation of the D-CODE is that the aircraft often operates under visual flight rules (VFR) in airspaces where radio contact with ATC is not mandatory. While ATC generally provides information about conflicting traffic, flight crews are ultimately responsible for ensuring their own seperation and avoiding a collision when operating under VFR. In some cases, aircraft which are not equipped with a transponder[9] cannot be identified by the controller. As a consequence, the flight crews cannot be warned about a potential conflict. During high workload phases of experimental flights, proper and thorough outside checks for other aircraft, are not always feasible which poses risks of mid-air collisions (MAC).

Based on the risks and hazards described in this section and section 2.2.3, a three-mode approach is planned for the FDM program. Each mode is intended to address one particular CFIT risk or hazard inherent to the flight operational activities presented in this thesis. In the following, the three modes and the specific situations they aim to monitor will be defined. Further details regarding these modes can be found in chapter 3, as they will be subjected to their respective algorithms.

Mode 1 is intended to generate an alert whenever the aircraft is approaching steeply ascending terrain, which could potentially lead to a collision if the aircraft maintains its current flight path. With this *Mode* the risk of a collision with mountainous terrain should be addressed.

Mode 2 is intended to address the risk of a ground collision during low altitude flight, such as during low approaches and low passes. It is designed to trigger an alert when the aircraft approaches the ground at dangerously low levels in situations where a full stop landing or touch and go is not intended. Instead, when the aircraft descends below a specific threshold altitude during horizontal low-altitude flight, the algorithms should detect and capture this event.

Mode 3 is intended to issue an alert during descent when the aircraft is at a low altitude close to ground. The program should trigger, whenever the aircrafts rate of descent exceeds certain limits. The closer the aircraft approaches the ground, the smaller is the margin which remains for the flight crew to correct a high rate of descent to ultimately avert an impact. Consequently, the

[9] A transponder is an electronic onboard device, which transmits registration, position, altitude and other information to ATC radar systems.

trigger limits should be gradually adjusted for each altitude level with smaller margins, in lower heights.

2.3.2 Dornier Do228-101 'D-CODE' Data Acquisition System and the TwinSTASH

Barometric measurement data, such as airspeed, altitude readings, and baromentric vertical speed data from the D-CODE is obtained from the basic avionics system. Inertial measurement system based data is obtained from the inertial laser reference unit (IRU). The measurement data is transmitted to the measurement system via the ARINC 429 data bus standard.

Figure 2.3: Dornier DO228-101 D-CODE. [Credit: DLR Internal Source]

The ARINC 429 data bus standard defines the standard for data transmission between avionic systems in aviation. Each transmission message in ARINC 429 consists of a 32-bit long word. The actual frame, which contains the flight data, is made up of a 12-bit long word, with 6 bits allocated as dispositional buffers which are used when the message exceeds the intended length. The remaining bit frames include additional metadata such as the mathematical sign or the parameter label. The measurement system utilises the ARINC 429 standard to interpret the signal. The ARINC 429 standard includes a classification that assigns specific labels to the parameters, indicating the appropriate unit and conversion factor for each. By referencing the label of the parameter, the measurement system obtains the necessary information for decoding and converting the value. The parameter classification is stored within the basic measurement system. Subsequently, the value is assigned the correct unit and conversion factor, enabling it to be converted into a meaningful engineering unit. After processing in the measurement system, the measurement data is packaged into ethernet signal packets and dispatched to the quick access recorder (QAR), where it is then captured on a compact flash memory card.

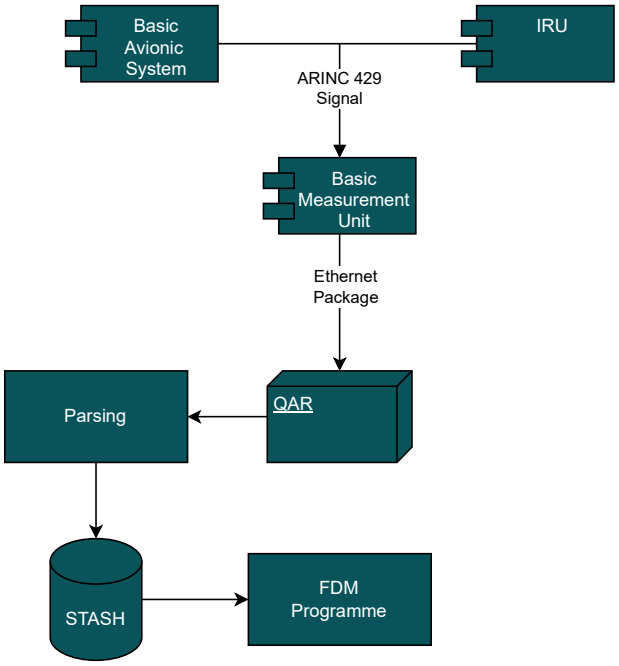

Figure 2.4: Data acquisition process.

The dataset captured on the compact flash memory card is transferred to the DLR network, where it undergoes a parsing process. Subsequently, the dataset is imported into the TwinSTASH, which serves as the centralised database for experimental flight data of the DLR flight operation. This database facilitates convenient access to experimental flight data for scientists. The data is accessible through a Python client and can thereby be directly imported into the FDM program. The ultimate goal is to integrate the FDM program as part of the SAFE module into the TwinSTASH. Whenever a new flight is uploaded to the TwinSTASH, the FDM program runs a check using its algorithms to identify any detrimental or hazardous situations and conditions. The programs outcomes and the safety information are then displayed in the SAFE module for further investigation.

2.3.3 Proof of Concept: Terrain Based Safety Assessment for Flight Envelope - TERRASAFE

Based on the risks and hazards, detailed in section 2.3.1, an FDM program for *exceedance and event detection* is to be developed with the ultimate purpose of safety information acquisition. The FDM program should address the three operative CFIT related risks and hazards, which are described in section 2.3.1. In order to adequately cover these three risks, a three-mode approach is adopted, each targeting a specific risk. These three modes are subject to a parent process through which the outputs and information of the individual modes are conjoined and stored in a database for further usage. A top-down approach is selected for the development of the modes themselves. First, the intended outputs of the modes have to be defined in order to create a basis on which the algorithms and a pre-selection of suitable safety data can be carried out. Then the triggering algorithms have to be developed. In order for the algorithms to perform their assigned tasks, the appropriate flight data parameters have to be pre-selected. Finally, once the algorithms have been established, the right type of flight data from the D-CODE has to be determined in terms of its characteristics, accuracy and stability to meet the requirements of the program. After the

program has processed, a brief report should be dispatched. This report will describe potential trigger events and present the necessary safety information, providing the required data for safety assessment and the derivation of mitigation strategies. In the following chapter, the three *Modes* and their adaption to identify the risks and hazards as mentioned above are presented. Higher emphasis is given to *Mode 3,* as it represents the examplary implementation of the FDM system in this thesis.

Chapter 3

TERRASAFE Program: Conception and Methodology

This chapter describes the conception and methodological realisation of the TERRASAFE program. TERRASAFE, an acronym for **Terra**in Based **S**afety **A**ssessment for **F**light **E**nvelope, emphasises the systems applicability for the risk and hazard detection associated with CFIT events. Development and implementation of a comprehensive FDM program can be challenging, even for a simplified system. Given the complexity and extent of implementing all three modes, this thesis encompasses theoretical algorithm development for all three modes, but with practical implementation concentrated on *Mode 3*. The flowcharts of the remaining *Mode 1* and *Mode 2* can be found in the appendix to this thesis. Section 3.1 provides preliminary considerations for the realisation of the proof of concept for the TERRASAFE FDM program for all three modes, as they are presented in section 2.3.3. The methodological realisation of the *Mode 3* algorithm and its subprocesses is described in section 3.2.

3.1 Preliminary Considerations for the Realisation of the TERRASAFE Proof of Concept

In this section, the realisation of the proof of concept for the TERRASAFE program is presented. A top-down approach for the conception is selected, beginning with the determination of the programs outputs. Thereafter, the performance of the processing algorithms is described. Finally, the required input data parameters for the particular algorithms are described and assessed for appropriateness.

3.1.1 Outputs - What should the program provide?

On the output side, Mode 1 should provide both vertical and horizontal distances to the nearest terrain point in the vicinity of the aircraft when the terrain object permeates certain distance limits from the aircraft. Additionally, contextual information that could be provided includes the heading of the aircraft, its airspeed, altitude, and the geospatial position of the conflict situation.

For Mode 2, the output information provided should include the lowest height above the surface of the earth during the event, the descent rate, airspeed, and geospatial position.

For *Mode 3*, the geospatial position, altitude at exceedance, height AGL of exceedance, the elevation of the terrain below, the actual descent rate that resulted in an exceedance as well as the threshold descent rate for contextual information should be provided.

For *Mode 3*, the following information should be provided: the geospatial position, altitude at the time of exceedance, height AGL at the time of exceedance, the elevation of the terrain below, the actual descent rate that resulted in the exceedance, and the threshold descent rate.

The output information of all events should at least comprise of occurrence time, geospatial position, altitude during the event and descent rate. Exceedances and events should be devided into graduation thresholds or trigger levels. Dividing the event into certain levels enables better classification of severity. A reasonable approach is the classification into three trigger or severity levels.

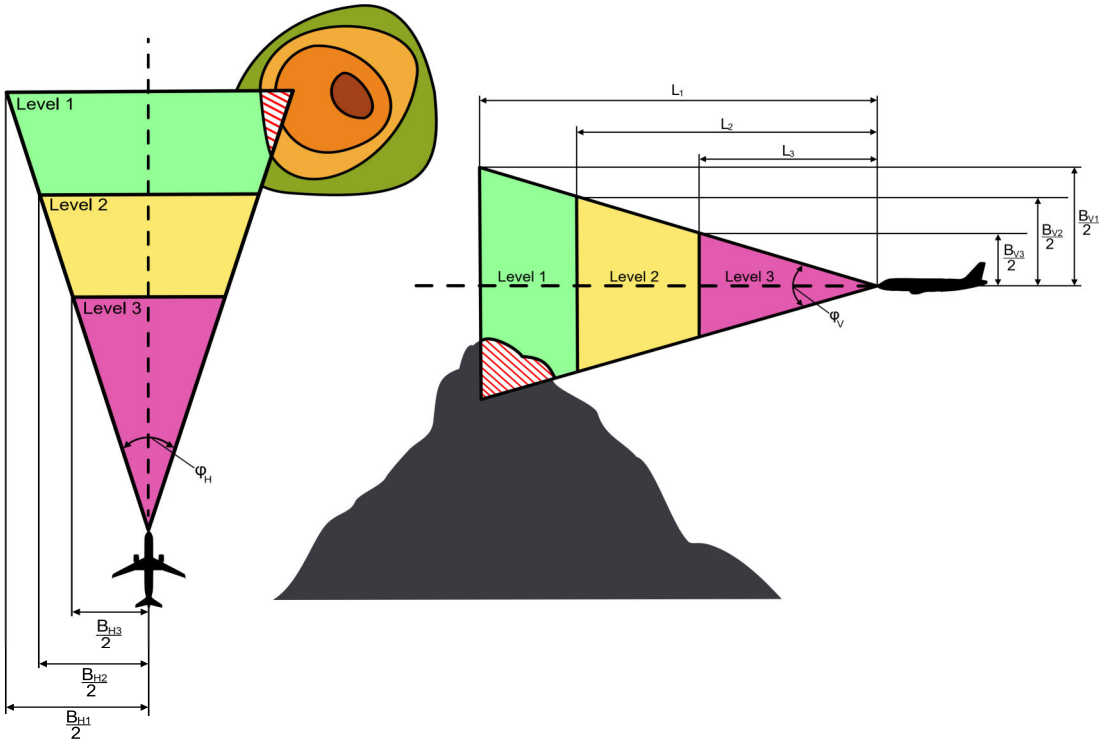

Figure 3.1: *Mode 1* control volume.

3.1.2 Processing - How should the trigger logics and algorithms perform?

Erroneous or low quality data can lead to inappropriate conclusions and detrimental decision making in the post flight analysis. Thus, attention has to be paid that algorithms are designed in such a way that data quality degradation is avoided and the risk of producing erroneous data is minimised. Further, the programs results have to be reproducible. Each of the three modes has its own algorithm and is embedded in an overall process. The overall process is intended to consolidate the outputs from each mode into a centralised database. Input flight data has to be referenced and adjusted in order to be compatible. Moreover, as the sample rate of the aircrafts data acquisition system is typically higher than necessary for the algorithms, a downsampling process of parameters and corresponding timestamps is required to prevent the program from having to

manage excessive data volumes and, leading to poor runtimes. A digital elevation model (DEM) has to be read in, providing the terrain data. The algorithms for each mode use geospatial and altitude data to concisely determine the position of the aircraft and locate it within the terrain model. The appropriate trigger values have to be determined in an iterative process, thereby ensuring the applicability and suitability for the program.

For *Mode 1*, a virtual control volume cone needs to be spanned in front of the aircraft. With a triangular shaped surface in lateral and horizontal dimension, the control volume has a certain length, width and height as well as aperture angle. Detection algorithms of the program are intended to repeatedly compare the control volume and terrain data. If a terrain object penetrates the control volume, the program alerts and saves the relevant parameters for contexual analysis. In order to provide different severity or trigger levels, the control volume accomodates three thresholds in dependency of the distance to the aircrafts reference position (ARP). As it is depicted in figure 3.1, *Level 1* is the frontmost threshold of the control volume and is intended to represent the lowest severity categorisation. *Level 2* in the middle represents an intermediate severity categorisation. Whenever the aircraft approaches terrain close enough so that *Level 3* as the rearmost threshold is penetrated, the highest trigger level is prompted. It is important to emphasise that, in the context of this thesis, the severity classification of the specific event detection algorithms is arranged in an ascending order. While trigger *Level 1* indicates a minor transgression of the thresholds, *Level 3* indicates the most serious breach[1]. The horizontal length expansion of the control volume is intended to be a direct function of the aircrafts groundspeed (GS), as it sufficiently represents the approximation rate of the aircraft towards terrain. This way, the length of the control volume can be extrapolated with the time. This definition allows for the time until impact to be kept constant, regardless of the speed of the aircraft.The functional correlation between length and speed of the cone can be established by the equation of uniform motion:

$$L_1 = GS \cdot T_{L1}$$

with L_1 being the length between ARP and *Level 1* threshold, GS the Groundspeed and T_{L1} = projected impact time at threshold level.

The width extention of the control volume as an isosceles triangle is dependent on the length l as well as the aperture angle φ. Since lateral direction changes of the aircraft are more frequent and faster to perform than vertical ones, the aperture angle for the horizontal part φ_H of the control volume should be selected larger than for the vertical aperture angle φ_V in order to cover a wider area horizontally with regard to the terrain detection. By assuming that each timestamp of the parameters represents a snapshot of the flight, acceleration influences can be neglected. In the following, three trigger level lenghts and widths according to the time values are calculated for a representative timestamp, to provide an examplary illustration of realistical control volume cone dimensions. In order to calculate the control volume length, the time until penetration for each trigger level zone as well as vertical and horizontal aperture angles have to be evaluated and defined. As an initial definition for the impact time, *Level 1* will be penetrated when the aircraft is 60 seconds (T_{L1}) away from impact, *Level 2* will be penetrated within 45 seconds (T_{L2}) and *Level 3* will be penetrated when the aircraft would impact the terrain object with 30 seconds left (T_{L3}). As an initial definition for the aperture angles, consider the horizontal aperture angle $\varphi_H$with 30°

[1]To provide better distinction, the different trigger levels are visualised by green, yellow and red colour. Despite the similiarity to traffic lights, the colours are not meant to be interpreted as green being “good” or yellow as “acceptable” etc. Instead, the colours are used to differentiate the severity of the breach with green representing the least severe and red the most severe.

and the vertical aperture angle $\varphi_V$with 10°. The groundspeed as velocity value is in this example given with GS = 140kts. It is essential to note that the trigger level time values and aperture angles provided here, need to be iteratively reassessed and evaluated regarding appropriateness in practice. The width of the control volume cone threshold can be determined by applying the tangent function as the width size is being represented by twice the length of the opposite cathetus. Since the length of the adjacent cathetus is known, the width of the control volume cone both horizontally and vertically can be determined by the following formula, which is also applicable for the other trigger level cones, but with their corresponding lengths and widths:

$$B_{L1} = 2 \cdot tan\left(\frac{\varphi}{2}\right) \cdot L_1$$

where B_{L1} is the cone width of *Level 1* threshold, and φ the cone aperture angle.

Table 3.1 provides examplary values for control volume cone length and width of the 3 different trigger levels based on both formulae and examplary values described above. The dimension values are seen with the ARP as the coordinate origin. For the modeling of the control volume, it is necessary to calculate the coordinate points around the control volume based on the distance values originating from the ARP. To minimise the effects of wind and influences of crab angles of the aircraft, the longitudinal direction of the control volume is aligned with the aircrafts track above ground instead of magnetic heading. This allows the program to superimpose the terrain accurately based on the data from the DEM.

Table 3.1: Initial control volume dimensions.

Trigger Level	Impact Time [s]	Length [m]	Width Horizontal [m]	Width Vertical [m]
Level 1	60	4321	2315	756
Level 2	45	3241	1737	567
Level 3	30	2160	1158	203

Mode 2 is intended to identify descents below a specific threshold height as limit during horizontal flight in an altitude close to the ground, which is visualised in figure 3.2. The threshold height is a constant value above ground, which is established regardless of the actual elevation of the terrain. The program is intended to obtain the current topographic terrain elevation underneath the aircrafts position. Furthermore, the program needs to constantly calculate the height of the aircraft AGL by subtracting the the terrain elevation from the altitude of the aircraft. It is essential to ensure, that both the aircrafts altitude and terrain elevation are measured in relation to the same reference level. As it is common practice in aviation to measure the altitude of an aircraft above mean sea level (AMSL), the program uses the same reference level (mean sea level) to measure both aircraft altitude and terrain height in order to establish comparability. The detection algorithms determine, whether the aircraft has descended below the threshold height. In order to provide a categorisation of the occurence regarding severity, the space beneath the threshold height is divided into three severity levels.

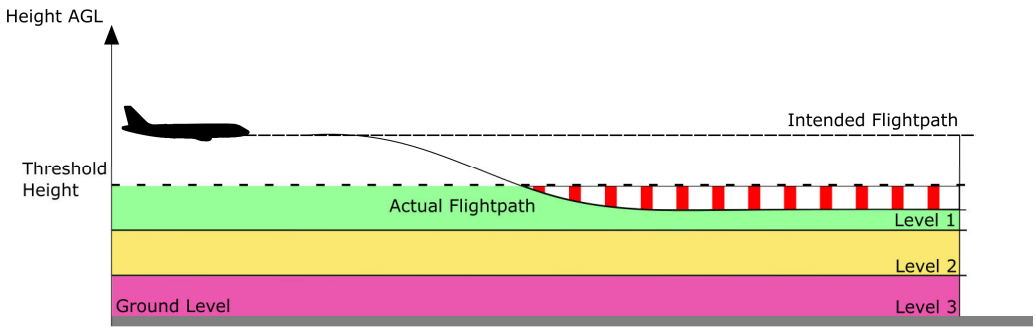

Figure 3.2: *Mode 2* low-level flight detection.

As depicted in figure 3.2, each coloured area beneath a dividing line represents a particular severity level whereby the threshold height itself embodies the threshold to *Level 1*. Whenever the aircraft descends below the threshold height, the program should identify the highest level breached and save the corresponding trigger level for each event. If the aircraft intentionally performs a normal landing or a touch-and-go landing, any alert triggered is to be considered a nuisance alert, since descending below the threshold height is operationally required in these scenarios. In order to avoid nuisance alerts and to differentiate between intended landings and low approaches or low level flights, an algorithm is needed to monitor these events. As of April 2023, the DLR Facility for Flight Experiments - Flight Test Instrumentation Group works on developing and integrating a landing detection module into the SAFE program. This will enable effective identification of intended landings and can be used to supress nuisance alerts.

Mode 3 is intended to identify situations in which the aircraft is descending with a high rate of descent (ROD) in an altitude close to the ground. As described in section 2.3.3, steep approaches in low altitude entail a significant risk of CFIT incidents. First, a specific threshold altitude must be established below which the flight altitude can be defined as "close to the ground". This threshold altitude is called Rad Alt Max, which stands for maximum radio altitude. Radio altitude in aviation is the reading, provided by radio altimeters, which are altimeters measuring the aircrafts current height above earths surface by emitting radio waves, which are reflected by the ground [42]. Second, trigger values for the ROD are established in dependence of the aircrafts height. The lower the height of the aircraft, the lower the trigger value for the ROD, due to decreased safety margins. The algorithm monitors the aircrafts ROD and constantly compares the actual ROD with the ROD trigger limit corresponding to any given height of the aircraft. The program should issue an alert, whenever the aircraft descends with a ROD which exceeds the trigger value corresponding to its current height. Unlike *Mode 1* and *Mode 2*, *Mode 3* is not designed to provide distinctive trigger levels. This is because dividing the threshold breach into severity levels would not yield any additional valuable information. In figure 3.3, a descend of an aircraft with the actual ROD (ROD_a) with the descent gradient $\frac{\Delta H_a}{\Delta t_a}$ is depicted. The ROD threshold line (ROD_T) shows the maximum ROD gradient $\frac{\Delta H_T}{\Delta t_T}$ for the height $(H(t))$[2]. The time of exceedance (t_e) is defined as the accurate UTC time, at which the aircraft exceeds the ROD threshold and the trigger event ultimately occurs and is highlighted in figure 3.3 with the vertical red dash, labeled with 'alert'. The algorithms begin to trigger at the exact moment, when the actual ROD of the aircraft exceeds the threshold ROD corresponding to its current altitude $H(t)$.

[2]Emphasise has to be given on the fact that the situation, depicted in figure 3.3 solely shows the gradient for one specific height. Gradients for lower heights need to be more flat due to restricted height margin and vice versa.

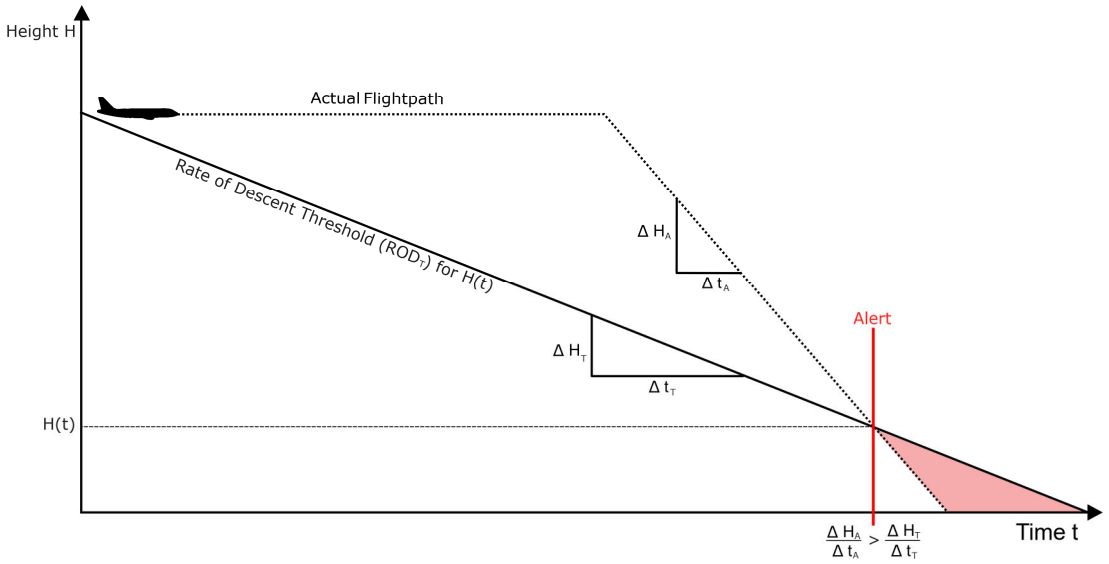

Figure 3.3: *Mode 3* excessive rate of descent (ROD) detection at height H(t).

3.1.3 Inputs - What Flight Data, Sensor Parameters and Elevation Data are appropriate?

On one hand, the relevant flight parameters are needed as safety data for the algorithms to monitor. On the other hand, terrain data needs to be implemented to provide information on elevation for the modes. This can be accomplished by implementing a Digital Elevation Model (DEM). A DEM is a digital geodetic raster model representing the surface of the earth. Further information on the DEM is described in section 3.5. From the aircraft side the following parameters are needed for the algorithms to work properly:

1. altitude data
2. vertical velocity data (ROD)
3. geospatial latitude
4. geospatial longitude
5. track and heading data

From the D-CODE, these parameters can be obtained from three sources, first the air data computer, second the inertial reference system (IRS) and third the inertial reference hybrid system (IRH). Not all parameters are provided by each source. The air data computer does not supply geospatial position data. Table 3.2 shows a qualitative comparison between parameter sources from D-CODE. Note, that data from the global navigation satellite system is not retrieveable from the core flight data measurement system of D-CODE . However to facilitate comparability, the characteristics are nonetheless described in Table 3.2.

For *Mode 1* to detect approximation to rapidly uprising terrain, the altitude of the aircraft as well as its track is needed. Furthermore, geospatial position data (Latitude and Longitude) is required to localise and identify mountains based on the DEM. For *Mode 2* and *Mode 3*, from the aircraft side, altitude data as well as geospatial position data is needed for the algorithms to calculate the

Table 3.2: Data availability by sources [36].

Source/Criteria	Accuracy	Short Term Stability	Long Term Stability
Air Data Computer / Barometric Altitude Data	Adjustment and calibration errors as well as non compensateable temperature and humidity influences may decrease accuracy.	Slightly delayed readings due to mechanical inertia and inner friction (hysteresis) of the instrument.	Reading is based on real time outside parameters, therefore no deviation.
Inertial Reference System	High offset due to potentially erroneous initial position.	High, due to very precise accelerometers and turn rate sensors.	Long term position deviation due to gyroscopic drifting
Global Navigation Satellite System	Very high, due to dual frequency GPS recievers	Low, due to high signal noise.	Very high
Inertial Reference Hybrid System	High	High	High

aircrafts height above ground level, as described previously. *Mode 3* additionally requires vertical velocity data for the ROD limit exceedance interrogation.

Altitude and vertical speed parameters can either be obtained as barometric parameters from the air data computer, or from both inertial reference systems. For the decision which data source is more suitable for the FDM application, the principle functionality of the sources should first be considered. Barometric altimeters for aviation purposes have basically the same operating principle as barometers and measure atmospheric static pressure through static ports[3]. As the aircraft climbs, the static pressure decreases logarithmically. A rule of thumb that every student pilot is taught is, that the atmospheric static pressure halves every $5.500m$. The static pressure reduction is measured by the altimeter and directly translated into an altitude reading by the altimeters internal mechanisms. The static pressure and hence the altitude is always measured relative to a specific reference level. Because atmospheric pressure constantly changes, altimeters have to be adjusted to the current static pressure to prevent inaccurate altitude readings. In aviation, mean sea level is the default reference for altitude and elevation readings. Therefore, pilots adjust the altimeter to the current local air pressure, but calibrated to correspond to the pressure downscaled to mean sea level. This altimeter pressure setting is designated as 'QNH' and can be obtained from ATC, Aerodrome Terminal Information System (ATIS), an automated weather and aerodrome information report, or from meteorological charts. The accuracy and reliability of altitude information from the air data computer is contingent upon the correct QNH being set. Hence, incorrect QNH settings can potentially result in erroneous data. Temperature and other scalar factors, such as air humidity can also affect altitude readings, but cannot be compensated for. As a consequence, the use of the air data computer as data source for altitude is inappropriate.

When considering the two inertial reference systems, the decision on which source is appropriate, depends on the specific characteristics of each system. The basic operating principle of an IRS is based on the deduction of positional and horizontal and vertical translation information from the measurement of acceleration and turning rates based on an established initial fix point. An IRS

[3]Static ports are small holes located at specific positions on the sides of the aircrafts fuselage, perpendicular to the main airflow of the flying aircraft. The exact placement of these ports depends on the design and aerodynamic characteristics of the airframe.

consists of an inertial measurement unit (IMU), which includes three acceleration rate sensors and three turn rate sensors. The IMU is rigidly connected to the aircraft and aligned with the aircrafts axes. To avoid erroneous measurements caused by gravitational influence on the acceleration rate sensors, the IMU "strapped down" to the aircraft to maintain a constant position related to the aircrafts axes. As the aircraft turns, the IMU computes the aircrafts attitude in space based on angles for the longitudinal, vertical, and lateral axes relative to the horizon, using the turn rate sensor data. The acceleration data is then used to calculate flight parameters for instance airspeed, groundspeed and positional data such as latitude, longitude and altitude, as well as vertical velocity data. This is accomplished by integrating the acceleration data over the attitude data [36]. However, IRS are subject to certain systematic errors. Turning rate sensors are constructively realised as gyroscopes [36]. Since gyroscopes are subject to drifting effects, small uncertainties and measurement deviations are propagated into larger errors through the integration. As a consequence, position, horizontal and vertical translation data errors progressively increase with time. In order to mitigate these effects, a hybrid inertial reference system consitutes the third source of flight parameters. In the IRH, the errors due to gyroscopic drift effects are compensated by constant GPS position updates, which are taken into account during calculation. The resulting long term accuracy as well as the indifference againt altimeter setting errors makes the IRH the preferable data source for the FDM program.

3.2 Methodology and Exceedance Detection Algorithms of Mode 3

In this section, the methodology and algorithms of TERRASAFE *Mode 3* are described. First, the overall flowchart depicting the algorithm is presented to provide a general overview. The *Mode 3* algorithm is divided into three segments, each dedicated to accomplishing specific functions contributing to the algorithms purpose. Further details regarding these three segments are then explained in detail. Since this thesis specifically concentrates on the realisation and implementation of *Mode 3* only, detailed flowcharts of *Mode 1* and *Mode 2*, along with their corresponding subprocesses, can be found in the appendix to this thesis.

The first segment of the *Mode 3* algorithm is the *Read and Downsample* segment, followed by the *processing* segment, and finally the *output and storage* segment. The algorithm is implemented as a the proof of concept, utilising a top-down approach. In the flowchart, rectangular boxes represent process steps, diamond-shaped boxes depict yes-or-no interrogations, and rhomboid shapes indicate sources or storage facilities of data. The algorithm is structured in such a way that it can be easily established with regard to programming in the subsequent steps of implementation. Overall, emphasis is placed on avoiding excessive functions, loops, or self-referencing steps. This simplified approach reduces the susceptibility to errors and the propagation and amplification of errors in the process. As outlined in section 3.1, *Mode 3* aims to identify and capture high rates of descent in altitudes close to the Earths surface. The complete flowchart of TERRASAFE *Mode 3* is depicted in figure 3.4. This thesis focuses on providing a practical realisation of the TERRASAFE program. The flowcharts in this thesis depict the methodological algorithms and program logic, while any software source code is described in the appendix to this thesis.

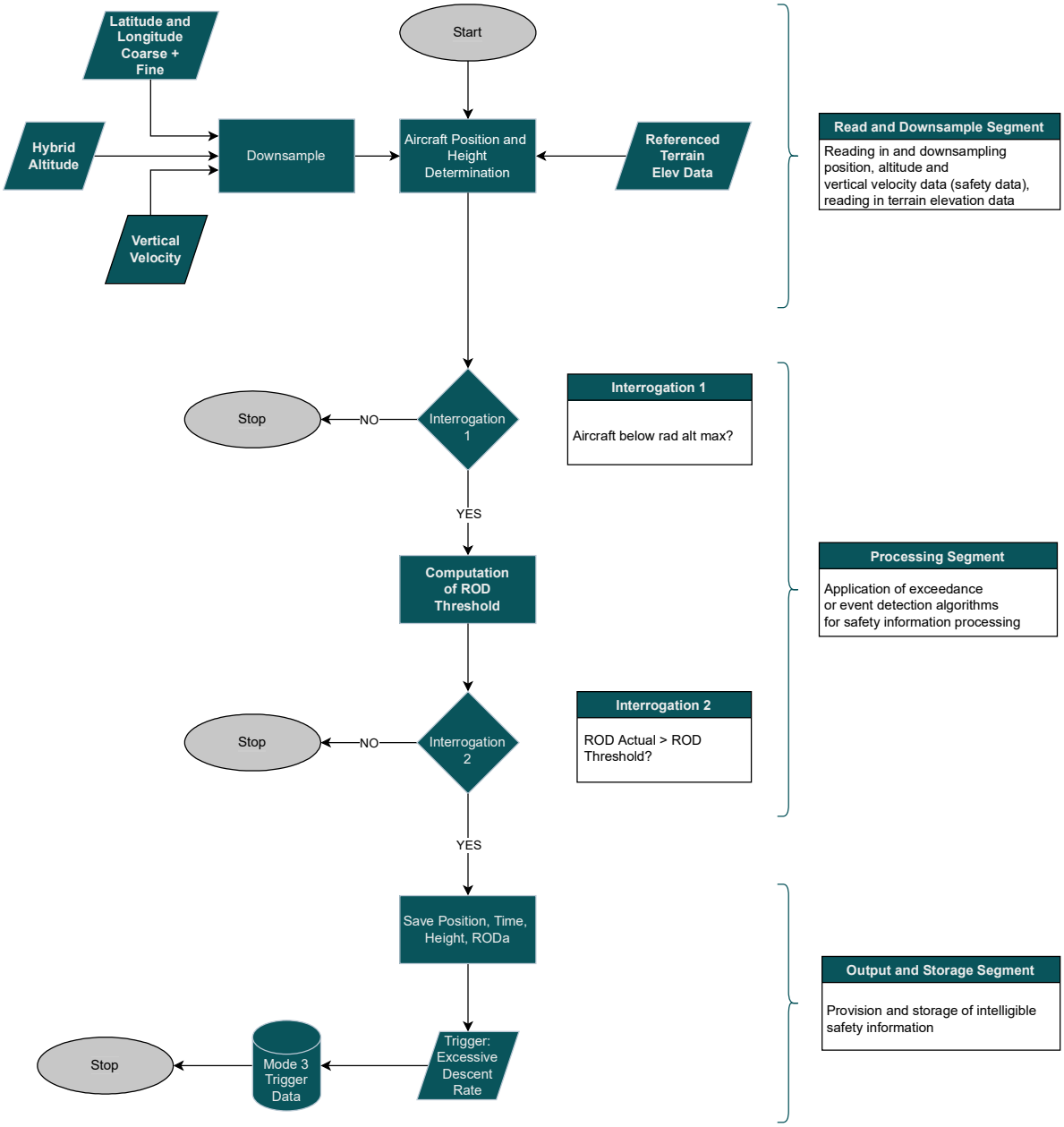

Figure 3.4: Overall flowchart *Mode 3*.

3.2.1 Read and Downsample Segment

The *Read and Downsample* segment encompasses functions which access the required data and necessary parameters and load them into the program initially. This process partly resembles the *safety data acquisition* element of an FDM program, as described in section 2.2.2. *Safety data acquisition* comprises of capturing, collecting and storing relevant safety data from the flights, transmitting them to the ground based processing station and applying filtering and downsampling processes to prepare the data for the *safety analysis*. Due to the nature of the DLR experimental flight operation, aiming to acquire scientific data from the conduction of experimental flights, no attention needs to be paid to capturing and transmitting safety data from the aircraft to the processing

station. The necessary sensors for recording and storing the relevant safety data parameters are already installed and perform as flight test instruments. As explained in section 2.3.2, the raw flight experimental data captured by the aircrafts flight test instrumentation is saved as hexadecimal bytes, which are then parsed into engineering units prior to being imported to the TwinSTASH. As of May 2023, the DLR Facility for Flight Experiments - Flight Test Instrumentation Group works on the implementation of a sensor health monitoring system, in order to provide flawless and reliable high quality data. This system is designed to identify erroneous data or inaccurate readings from flight test instruments and sensors by applying statistical and metrological principles. This ensures sufficient data quality and accuracy, while relieving this task from the TERRASAFE program. The entry segment of the algorithms focuses solely on retrieving the necessary safety data from the TwinSTASH into the program. Additionally, the safety data is to be downsampled to a reasonable sample rate to avoid excessive program runtime.

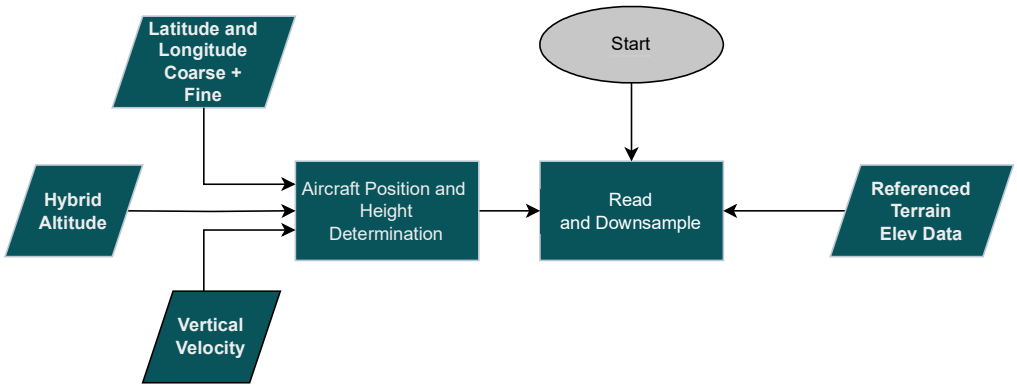

Figure 3.5: *Mode 3 Read and Downsample* segment.

The *Read and Downsample* segment is depicted in figure 3.5. A start sequence initiates the algorithm. From the left side, safety data from the TwinSTASH is retrieved and imported into the program. The necessary data comprises of latitude and longitude data for the position determination, hybrid altitude for the computation of the height AGL and vertical velocity for the rate of descent comparison. First, the safety data is to be downsampled. The sample rate of the core measurement system of D-CODE ranges between $2Hz$ and $25Hz$, depending on the specific parameter. A reasonable sampling time, which meets the programs requirements regarding accuracy and timeliness is $1Hz$ or 1 value each second (timestamp). It is essential to downsample all parameters to the same sample rate and ensure that the values maintain a relative correlation with each other in terms of time. This approach guarantees, that the downsampling process maintains accuracy by sustaining the temporal relationship among the parameters. This process is represented as the *Downsample* rectangle in figure 3.5. As described in section 3.1.3, the preferable data source for the program is the inertial reference hybrid system. Table 3.3 presents a list of parameters and their corresponding labels, which are essential for *Mode 3* and utilised within the program. As described in table 3.3, it is important to note, that the geospatial position data is derived from two distinct parameters, as specified in the ARINC 429 databus standard. Each transmission message in ARINC 429 consists of a 32-bit word. The actual frame, which holds the flight data, is composed of a 12-bit word, with 6 bits allocated as dispositional buffers which are utilised, whenever the message exceeds the intended length. The remaining bit frames include further meta information such as the mathematical sign or the parameter label. The geospatial position, which is designated in the decimal degree system, can contain up to 15 decimal digits.

Table 3.3: Preferable parameters and their labels.

Parameter	Label
Latitude	IRH_LAT
Latitude Fine	IRH_LATFINE
Longitude	IRH_LONG
Longitude Fine	IRH_LONGFINE
Altitude	IRH_ALT
Vertical Velocity	IRH_VERTVEL

As described in section 2.3.2, in each ARINC 429 word, up to 18 bits are reserved for the actual data information. However, converting the geospatial position data into bit numbering would require 27 binary digits, which cannot be accommodated within a single ARINC 429 word. As a result, the latitude and longitude information is sliced into two distinctive parameters: IRH_LAT and IRH_LONG accommodate the coarse values, whereas IRH_LATFINE and IRH_LONGFINE accommodate the fine values. The correct geospatial position can be computed simply by adding the fine value to the coarse value, thereby obtaining the aircrafts precise geospatial position.

When considering the aircrafts height AGL, the elevation of the earths surface AMSL needs to be subtracted from the aircrafts altitude AMSL at any given timestamp. To perform this calculation, a DEM is required, providing earth surface elevation information corresponding to the position of the aircraft. The necessary data of the earths surface for the DEM is generated by using air- or spaceborne high resolution optoelectronic devices such as laser imaging detection and ranging (LIDAR) or interferometric synthetic aperture radar (InSAR) [37]. The acquired data is provided as a raster image file, where the surface is divided into distinct tiles with specific length and width dimensions. The tile dimensions depend on the spatial resolution of the DEM file, which can range from a few metres for military applications up to several hundred metres. A resolution of $25m$ can be considered sufficiently precise for the determination of the elevation information beneath the aircrafts position, as it corresponds to approximately one and a half times the wingspan and length of the D-CODE. It is of emanent importance for the height calculation to ensure that both the aircrafts altitude and DEM elevation data are referenced to the same level, which is preferably MSL.

In the TERRASAFE program the EU-DEM 1.1 elevation dataset with a spatial resolution of $25m$ is utilised. The EU-DEM 1.1 covers the entire European continent and neighboring countries to a certain extent. It is a combined model, which incorporates datasets from the shuttle radar topography mission (SRTM), advanced spaceborne thermal emission and reflection radiometer (ASTER) mission as well as Soviet topographic maps. Figure 3.6 visualises the correlation between the DEM, its corresponding reference level and figure of the earth. As it is widely known, the geometric figure of the Earth is not a perfect sphere but rather a unique ellipsoidal irregular geoid. The reference ellipsoid model describes the figure of the earth as an idealised mathematical model. In reality, due to density fluctuations, gravitational forces deform the earth so that its planetary figure rather resembles a potato shaped object, than a smooth ellipsoidal model [39, 43]. The geoid is a physical model that approximates the Earths actual shape as accurately as possible. The height deviation of the geoid from the ellipsoid is known as the geoid undulation [45]. The MSL is in a state of gravitational equilibrium and can be considered of as extending beneath the continents, thereby closely approximating the shape of the geoid [44]. The vertical geodetic reference datum of the EU-DEM 1.1 is the European Vertical Reference Frame EVRS2000 [40, 41]. EVRS2000, as the vertical datum, is referenced to mean sea level. The mean sea level itself is estimated and averaged on different tide levels of the respective sea. Due to possible differences between the actual sea

surface and the geoid model, there may be deviations between the height reference datum and the actual mean sea level. However, since these differences typically range within one metre, they have a relatively small impact on the elevation data [37, 43].

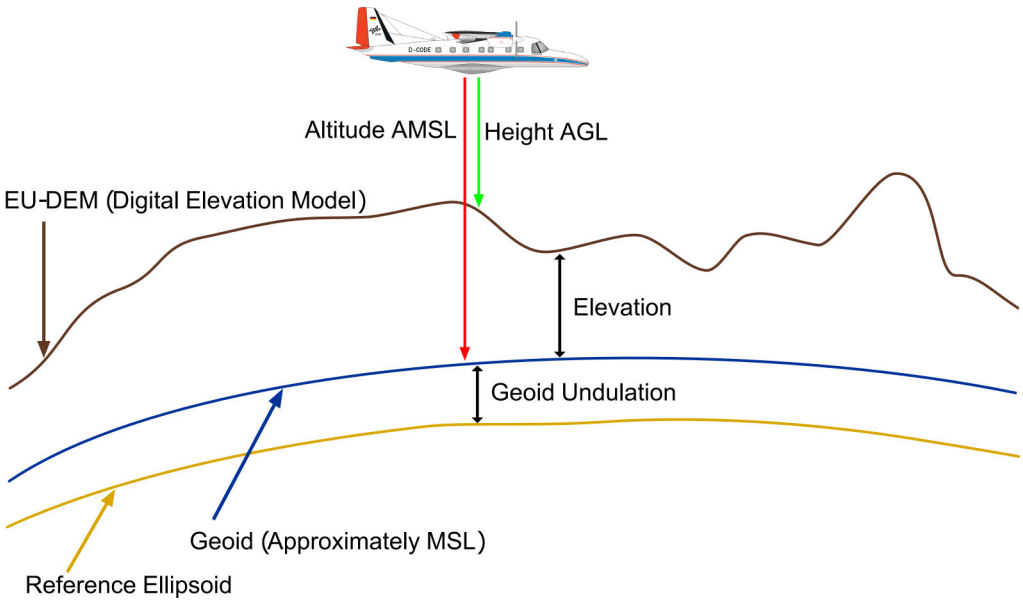

Figure 3.6: Geodetic Earth model. [Licence D-CODE SVG: DLR (CC BY-NC-ND 3.0)]

Consequently, the potential implications on the elevation information provided by the DEM and the resulting inaccuracies in the height calculation, which is based on the elevation information from the DEM, are negligible. Thus, the elevation data derived from the EU-DEM provides a satisfactory foundation for obtaining elevation data referenced to mean sea level. The elevation data for the TERRASAFE program is obtained from the EU-DEM 25m model, which is accessible through a public API provided by the website opentopodata.org [38]. When using the EU-DEM model from opentopodata.org, it is important to mention that by default, each 25m x 25m tile is assigned a specific terrain elevation, which can result in an inconsistent height profile and jumps in elevation. To prevent these jumps, the provider interpolates the elevations between the tiles. The respective elevation values are stored precisely in the middle of the tiles ($\frac{L}{2}$ and $\frac{B}{2}$). Due to the relatively high resolution of the tiles in the used DEM (resolution 25m), the deviations caused by the extrapolation from the real terrain elevations are mostly negligible and allow for a good approximation of the actual relief characteristics. As described in section 3.1.3, the altitude value of IRH_ALT is contingent upon the QNH setting, which is also referenced to mean sea level. Therefore, the height of the aircraft AGL can be appropriately determined by subtracting the DEM model elevation from the aircrafts IRH_ALT altitude.

In the *Read and Downsample* segment, the necessary elevation data acquired from the DEM is read in from the right side, as it is depicted in figure 3.5. The position determination of the aircraft by adding the fine position values to the coarse position values as well as the height determination by subtracting the elevation data AMSL from the aircrafts altitude AMSL is performed in the *Aircraft Position and Height Determination* process. In the flowchart, this process is depicted as the middle rectangle. After the necessary datasets from both the aircraft and the DEM have been acquired, downsampled and position and height has been determined, the safety data is to be routed to the *Processing* segment.

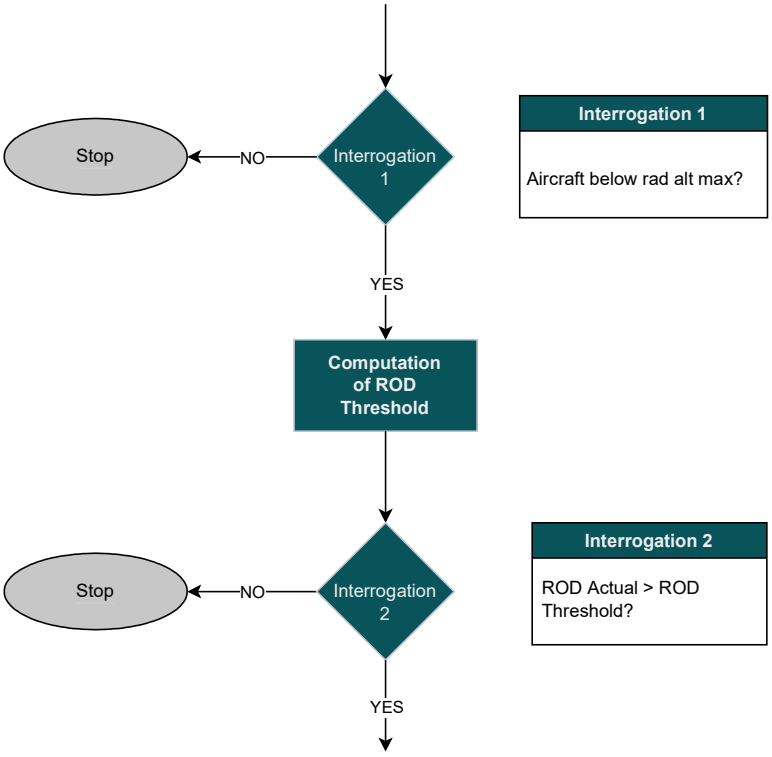

Figure 3.7: *Mode 3 Processing* segment.

3.2.2 Processing Segment

The *Processing* segment consists of the actual trigger detection algorithm, which relies on the data provided by the *Read and Downsample* segment. It encompasses two interrogative sequences and a computation sequence. It is important to note that the algorithms in the processing segment, are always applied for a single timestamp. This means that the program iteratively loops through the dataset and applies the interrogation for each timestamp. The interrogation sequences are designed as simple 'yes-or-no' requests. As described in section 3.1.2, the program should only trigger whenever the aircraft is in close proximity to the surface of the earth or in other words, below Rad Alt Max. An initial value for Rad Alt Max, which serves as the threshold height is $3500ft$ AGL. This value can be adjusted subsequently, when operational experience shows evidence, that another value for Rad Alt Max is more suitable. The triggering algorithms are applied to the safety data, when the aircraft is below or at this height. The first sequence, *Interrogation 1*, serves this purpose by comparing the aircrafts height at a given timestamp with the Rad Alt Max value. If the aircrafts height is above Rad Alt Max, then the triggering algorithms are not to be applied to the dataset for that timestamp, as per program definition. In this case, the program stops for this timestamp and proceeds with the data for the next timestamp. When the aircrafts height is at or below Rad Alt Max, the program continues with the subsequent processes.

After the *Interrogation 1* sequence, the *Computation of ROD Threshold* process is applied. As described in section 3.1.2, each height has its particularly assigned ROD threshold. The ROD threshold values, adopted in the TERRASAFE program are based on the threshold values from the GPWS Mode 1 envelope. Since GPWS serves a similar purpose as the TERRASAFE *Mode 3*, it is reasonable to adopt comparable or similar threshold values or exceedance limits. Figure 3.8 illustrates the excessive descent rate envelope for the GPWS system. The ROD thresholds in *Mode*

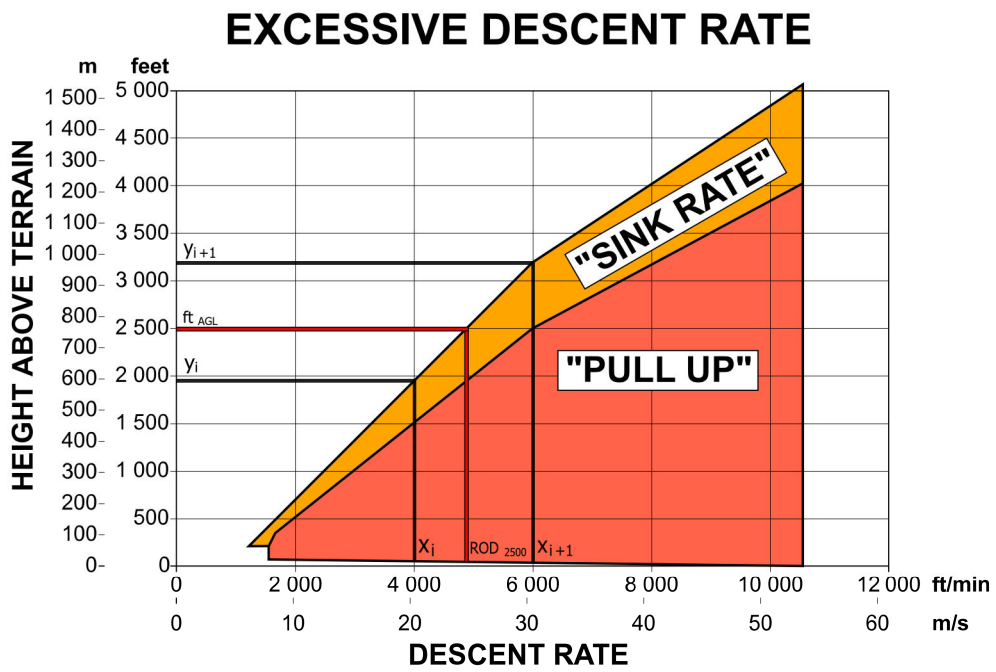

Figure 3.8: GPWS excessive descent rate diagrammeme [46].

3 are derived from the lower part of the graph, covering the yellow area, which indicates “Sink Rate” [4]. The GPWS "Sink Rate" graph consists of two gradients, with the upper part (starting from 3200ft AGL) being shallower. In TERRASAFE *Mode 3*, the threshold values are obtained only from the steeper part of the curve for program simplification.

In order to achieve relatively accurate threshold values for *Mode 3*, a linear interpolation is performed based on values from the GPWS excessive descent rate diagrammeme. The Newtonian interpolation method [47] is selected for the linear interpolation between two uniquely readable points, retrieved from the diagrammeme, with:

$$f(x) = y_i + \frac{y_{i+1} - y_i}{x_{i+1} - x_i} \cdot (x - x_i) \text{ with } x \in [x_i, x_{i+1}]$$

In figure 3.8, the descent rate as the dependent value is unfortunately plotted on the x-axis, while the height AGL as the independent value is plotted on the y-axis. However, the interpolation formula aims to calculate a function of the x-value, which should be the descent rate, the dependent value. To address this, the axes can be interchanged due to the proportional relation between both values, meaning the x-values become the y-values and vice versa.

This allows for an adjusted formula which relates the calculation of the descent rate $[ROD(ft)]$ for a given height AGL $[ft_{AGL}]$:

$$ROD(ft) = x_i + \frac{x_{i+1} - x_i}{y_{i+1} - y_i} \cdot (ft_{AGL} - y_i)$$

where $ROD(ft)$ is the ROD as a function of the height AGL and ft_{AGL} is the height AGL with feet as its unit.

[4] “Sink Rate" is the aural GPWS alert for an excessive descent rate, while "Pull Up" represents a second severity level of an excessive descent rate. In TERRASAFE Mode 3, only one severity level is implemented, disregarding the "Pull Up" graph.

Table 3.4: Approximate data point readings for the interpolation.

	y	x
i	1930	4000
i+1	3200	6000

Table 3.4 provides approximate reference point readings for the linear interpolation. Using the reference point readings from table 3.4, the corresponding ROD can be calculated for each height AGL. It follows an exemplary calculation of the ROD threshold for a height of $2500ft$ AGL:

$$ROD(2500) = 4000\frac{ft}{min} + \frac{6000-4000}{3200-1930} \cdot (2500 - 1930)\frac{ft}{min} = 4897,638\frac{ft}{min} \approx 4898\frac{ft}{min}$$

For the *Computation of the ROD Threshold* section, the algorithm should perform the calculation of the associated ROD value using this formula, with the height AGL determined in the *Read and Downsample* segment as the input value. The resulting value from the formula will be rounded to the nearest whole number by virtue of simplification, while still maintaining sufficient precision for the programs purpose.

Once the ROD Threshold has been computed, the second interrogation sequence comes into action. Similar to *Interrogation 1, Interrogation 2* is a simple yes-or-no interrogation. This sequence compares the actual ROD with the computed ROD threshold. If the actual ROD is below the ROD threshold, the program stops for this particular data point and proceeds to the processing of the next data point. However, if the actual ROD equals or exceeds the ROD threshold, the program records this event and forwards the associated information to initiate the third and final algorithm segment, the *Output and Storage* segment. In this segment, the actual trigger warning is generated based on the results and findings from the *Processing* segment.

3.2.3 Output and Storage Segment

The *Output and Storage* segment involves a process which saves the essential safety information related to the specific trigger event. Besides that, it comprises of generating a trigger report or briefing and storing it in the SAFE database, which is intended to be a component of the TwinSTASH. The input data for this segment is the information on a particular ROD exceedance, retrieved from the *Processing* segment. In order to provide useful safety information, supporting the subsequent contextual evaluation and assessment of the trigger event, additional data and information need to be collected. Accordingly, the algorithm captures the following sensor data for each trigger event timestamp as supporting information:

1. position of event (Latitude, Longitude)
2. time of event
3. height AGL during event
4. actual ROD
5. ROD threshold for the height

Whenever need for additional supplemental information emerges during the ongoing operation of the program, the required sensor data can be easily appended to the program and retrospectively

included in the report. The generated safety information, in the form of a report (represented by the rhomboidal shape in the flowchart of figure 3.9), is then stored in the database (represented by the cylinder). Finally, a stop sequence concludes the program.

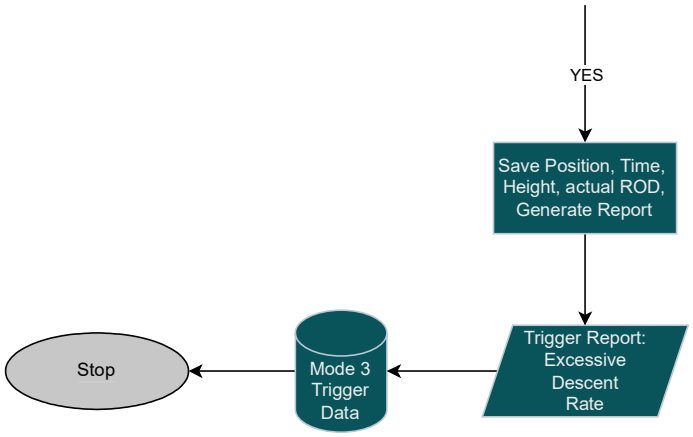

Figure 3.9: *Mode 3 Output and Storage* segment.

When it comes to the representation of the safety information, a clear and concise scheme is selected to foster understandability and prevent misinterpretation of the safety information. Table 3.5 presents a potential array of essential safety information for the trigger report, which will be named according to the name of the program TERRASAFE report (TSR).

Time [UTC]	Latitude [DD]	Longitude [DD]	Height AGL $[ft]$	Altitude $[ft]$	Elevation $[ft]$	Actual ROD $[\frac{ft}{min}]$	Threshold ROD $[\frac{ft}{min}]$

Table 3.5: Safety information report scheme.

The methodology and functionality of TERRASAFE *Mode 3* presented in this section is evaluated and assessed regarding its effectivity and operability in chapter 4. The source code of the programmatical implementation of the *Mode 3* algorithms and exceedance detection can be found in the appendix to this thesis.

Chapter 4

Flight Test Evaluation of TERRASAFE *Mode 3*

In this chapter, the TERRASAFE program is assessed regarding its applicability and operability. A flight test was conducted to demonstrate that the TERRASAFE *Mode 3* operates effectively under real conditions and provides reliable data. In order to obtain the safety data for the evaluation of the TERRASAFE program, the performance of a real flight test was prioritised instead of simulating the flight test with generated data. Only a real flight test is able to portray the true sensor behavior, aircraft behavior, and the actual structure of the data. Furthermore, the flight test was intended to test not only the algorithms of the program but also the functionality of the data acquisition process from the aircraft via the TwinSTASH and into the TERRASAFE program. Because of these advantages, a real flight test was the preferred option. Section 4.1 describes the development and planning of the flight test, section 4.2 describes the conduction and the results of the flight test, performed with the Dornier DO228-101 D-CODE. Subsequently, in section 4.3 the spoofing mechanisms, required for the adjustment of the flight test data for the program are described, and finally the programs results are analysed.

4.1 Test Design and Conduction Planning

This section describes the design approach and planning of the flight test to verify performance of the TERRASAFE *Mode 3* program. Initially, the objective of the flight test is defined to provide guidance and establish a clear goal. Thereafter, the test performance is planned, determining the required descent rates at different altitudes that the system should detect. Additionally, special safety related considerations regarding improvements of the flight test are addressed.

4.1.1 Test Objective

The objective of the flight test is to gather evidence that the TERRASAFE *Mode 3* algorithms perform successfully and that the triggering mechanisms reliably detect exceedances. To accomplish this, the flight test intentionally involves achieving descent rates with D-CODE, that exceed the projected descent rate thresholds. This deliberate approach aims to provide validated data in the most realistic, yet safest way possible, for the TERRASAFE program to analyse and process.

4.1.2 Initial Test Design and Test Procedure

As described in section 3.1.2, each height reading is assigned a specific ROD threshold due to the interrelation between height AGL and ROD gradient. In order to successfully trigger the program, two certain conditions have to be defined, as outlined in the following list. These conditions are derived from the program methodology described in section 3.2.2.

1. The test must be conducted below Rad Alt Max, which is according to the initial program definition $3500ft$.
2. The threshold value for the ROD must be exceeded in relation to the corresponding height AGL.

In order to achieve a statistically significant test result, the test should contain at least 5 serials or repetitions. Additionally, the serials should encompass different descent rate exceedances in different heights to ensure that a broad range of events is covered. One potential issue is that it is practically impossible to determine the precise height AGL during the flight. However, it is important to note that the flight has taken place in northern German airspace. Given the relatively flat terrain and absence of significant elevation changes or leaps, the lack of precise terrain elevation information did not entail a significant problem. The vertical speed indicator display, necessary for the flight crew to precisely measure the aircrafts ROD is divided into a $100\frac{ft}{min}$ scaling by default. To further ensure that the required ROD is actually achieved for the algorithms to be triggered, the calculated planned ROD for the flight test is rounded up to the nearest $100ft$. Table 4.1 shows the targeted ROD and their corresponding heights AGL according to the linear interpolation from the GPWS envelope provided in section 3.2.2.

Table 4.1: Nominal target ROD and corresponding heights AGL.

Test Serial	Target Height AGL $[ft]$	Target ROD $[\frac{ft}{min}]$
1	3000	5700
2	2500	4900
3	2000	4100
4	1500	3300
5	1000	3000

For the flight test it was initially intended to commence the testing with the higher ROD and then consecutively proceed to the smaller ROD in lower heights AGL. This would support an efficient flight test conduction. Figure 4.1 depicts the planned test conduction with different target ROD in the corresponding heights AGL. As TERRASAFE *Mode 3* is an FDM system, the primary purpose of the flight test is to generate experimental data captured by the core measurement system for post flight processing. The acquired experimental data is subsequently imported into the DLR systems (TwinSTASH). Afterwards, the flight data is retrieved and processed by the program as intended for normal operation.

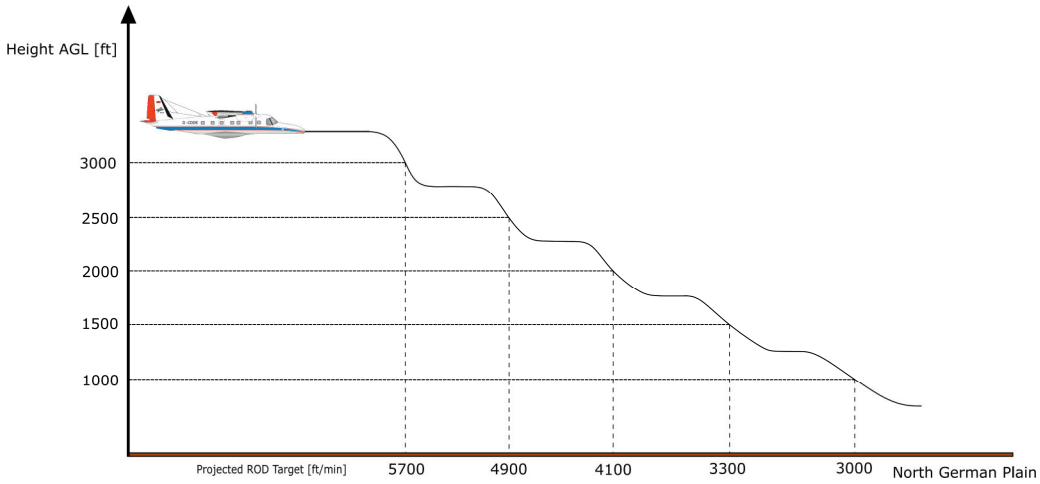

Figure 4.1: Planned flight test conduction with D-CODE.

As per flight test operations manual for the DLR flight experiments, the preparation of a flight test card, tailored to the particular flight test is mandatory. Consequently, a flight test card with the necessary information for the flight crew was developed, including but not limited to: aircraft weight and balance and configuration information, relevant limits, required weather and ATC information, safety considerations as well as the test procedure. The full test card can be found in the appendix to this thesis.

4.1.3 Safety Considerations

At this point, it should be emphasised that flight safety is of unconditional importance during the flight test. For these reasons, the initially planned flight test technique had to be revised in order to incorporate larger safety margins for the flight. Therefore, the approach of performing the flights with their actual descent rates at the corresponding heights was abandoned. Considering that the aircraft descended at a projected rate of $5700\frac{ft}{min}$ at a height of $3000ft$ AGL for instance, the time until ground impact, assuming the descent rate remains unchanged, would be less than one minute. This is a reasonably short time margin for recovery maneuvers of the aircraft and for simultaneously handling the workload on behalf of the flight crew, which accumulates during a test flight. In addition to that, flying at such high descent rates entails several other risks. These risks can be related to exceeding the limits of the aircraft, such as exceeding the maximum operational speed. Another risk is a damage to the engines as a result of overspeeding and overtorquing them due to the oncoming airflow, driving the propeller like a windmill. Furthermore, there is a risk of exceeding the load factor limits by recovery maneuvers, which demand excessive stress for the aircrafts structural capabilities. On top of that, since flying such high ROD in low heights AGL is neither regularly trained nor incorporated into normal flight operations, flight crews generally have less experience in handling such maneuvers. Furthermore, it should be noted that such a flight test, aiming to achieve comparably high descent rates, has not yet been conducted in the DLR experimental flight operations.

As a result, an alternative approach was chosen for conducting the flight test. For the start altitude of each test series Flightlevel (FL) 95 was selected. 'Flightlevel' represents the altimeter setting related to the ICAO standard atmospheric pressure of $1013{,}25hPa$, which means in this case that FL

95 is 9.500ft above the 1013,25hPa reference level[1]. Above a certain altitude (transition altitude), flight crews are required to change their altimeter setting to 'standard' instead of referencing it to the mean sea level (QNH-Setting). In upper airspace, it is crucial to ensure that aircraft use the same altimeter setting, thereby establishing comparable altimeter readings between the different aircraft for proper altitude separation. The exact altitude AMSL (QNH-altitude) becomes less important when flying in the upper airspace while cruising. The transition altitude in Germany is typically at 5000ft.

After a descent has been conducted and the target ROD has successfully been achieved, the flightcrew is required to climb to FL95 again, where the subsequent test series should start, to reassure the appropriate altitude margin. To mitigate the risks associated with very high RODs, the flight test had to be conducted with reduced target descent rates. The new planned target ROD are calculated by dividing the actual ROD by 2 and rounding up to the next 100$\frac{ft}{min}$. Furthermore, to familiarise the flight crew with the flying technique for higher descent rates and ensure a cautious and safe test conduction, the flight tests were to be performed with lower ROD and progressively increasing the descent rate with each test series. Table 4.2 provides the final projected target descent rates, determined based on the considerations described above.

Table 4.2: Final target ROD and start altitudes.

Test Serial	Start Height AGL [ft]	Target ROD [$\frac{ft}{min}$]
1	FL95	1500
2	FL95	1700
3	FL95	2100
4	FL95	2500
5	FL95	2900

The emphasis on safety as the highest priority in conducting the flight test series cannot be overstated at this point. The alteration of the test series is fully justified by ensuring the highest possible level of safety during the flight tests. Despite these alterations, it is ensured that reliable and conclusive experimental data is still be generated for the verification of *Mode 3* under realistic operating conditions. However, the alteration of the flight test parameters requires increased post-processing efforts and necessitates further adjustments to the input safety data without modifying the trigger algorithms. At this juncture, it should be underlined, that the actual TERRASAFE *Mode 3* algorithms are not intended to be modified in order to process the altered flight test parameters. Instead, a separate logic needs to be be developed to process the input safety data, thereby simulating the flight being conducted with the originally suitable, unaltered flight test parameters. This logic is specifically designed for the unique case of the flight test for the program verification. It is not integrated into the algorithms themselves, as it deviates from the original *Mode 3* purpose. The adjustment logic is described in section 4.3. Note that, in order to ensure a safe and comprehensive test conduction with the D-CODE, other safety related considerations were implemented into the test design. However, as these safety considerations are not directly related to the content of this thesis but rather pertain to the operational aspects of flight testing, they are not presented within this thesis. The complete test card, including all safety considerations, can be found in the appendix to this thesis.

[1]The nomenclature for distinguishing between different altimeter settings is as follows: As described in section 3.1.3, 'Altimeter QNH' represents the altitude with a full digit reading (e.g. Altitude 4000ft). 'Altimeter Standard' indicates a Flightlevel setting referenced to the 1013,25hPa pressure level, where the last two digits of the altitude reading are omitted (e.g. FL350, representing an altitude of 35.000ft above the 1013,25hPa pressure level).

4.2 Performance and Results of the Flight Test

The flight test was successfully conducted as planned, and the projected trigger descent rates were achieved, with the core measurement system recording the safety data. All five projected test series were completed successfully. As an ad-hoc addition to the flight test within the scope of the objective of the flight test, the flight test crew decided to determine the maximum stable descent rate for the D-CODE aircraft without exceeding operational limits such as the airspeed. This unplanned test series represents an additional data point for the program, which can be processed and utilised in the post-processing.

As described in section 4.1.2, the relevant flight parameters are captured and recorded by the basic measurement system of the aircraft. However, since no technical system is entirely resistant against malfunctions, certain flight test parameters were manually noted on the test card during the test. This approach offers two specific benefits: Firstly, it serves as a backup measurement, providing at least data to some extent in case of a core measurement system malfunction or when erroneous data is delivered thereof. If the core measurement system had failed or provided erroneous data, the handwritten notes on the test card would serve as manually recorded safety data. In this way, the program algorithms can still process real flight data, albeit with the slight disadvantage, that the data was manually inserted rather than retrieved directly from the aircraft and the TwinSTASH. Secondly, the notes on the test card provide valuable information for reassessing the acquired flight test data and evaluating their reasonableness. The data written on the test card includes:

1. actual altitude (start)
2. event button counter (start)
3. maximum stable ROD
4. actual altitude (end)
5. elapsed time of descent
6. event button counter (end)
7. starttime of test series (UTC time)

During the flight test, the test procedure required the flight crew to verbally communicate the necessary parameters at predefined flight situations and moments. These parameters were then recorded on a test card by the flight test crew. Prior to each series start, the flight crew pressed the event button and noted the corresponding counter number. Although the event button is not directly related to the test progress and its results, it serves as a convenient feature for highlighting specific events within the measurement data, which is particularly useful during test flights lasting several hours and including several test series. Once the event button was pressed, the test series would begin, and the flight crew would initiate the descent. Simultaneously, the stopwatch was started to measure the elapsed time of the descent. Since the start altitude remained constant at FL95, this parameter could be noted before each test series. Once the target ROD was achieved and stabilised, the flight crew would announce the exact stable descent rate reading, which was also noted. After maintaining the target ROD for a few seconds, the descent rate would be reduced, and the descent would be recovered. At the start of the recovery, the corresponding altitude reading was announced and recorded. The stopwatch was then stopped.

132.650
7241
8°C 0°C

TEST CARD OPEN START ALTITUDE – REDUCED ROD

Test	Altitude Start Planned (ft)	Target ROD (ft/min)	Altitude Start Actual	Event Button Counter (Start)	Maximum Stable ROD (ft/min)	Altitude End (ft)	Elapsed Time of Descent (s)	Event Button Counter (End)	Time of Start: (Current Time UTC)	OAT at Altitude Start/ Altitude End
1	00	1500	00	002	1500 5800	00	52	003	10/15 50	10/16 45
2	00	1700	00	004	1200 170	00	53	005	10/18 35	10/19 45
3	00	2100	00	006	2100 165	00	44		10/21 57	10/22 55
4	00	2500	00	007	2500 190	00	51		10/24 43	10/25 35
5	00	2900	00	008	15%TQ 180	00	43		10/27 21	10/28 10

-7° Pitch
+18°

TEST CARD OPEN START ALTITUDE – REDUCED ROD

Test	Altitude Start Planned (ft)	Target ROD (ft/min)	Altitude Start Actual	Event Button Counter (Start)	Maximum Stable ROD (ft/min)	Altitude End (ft)	Elapsed Time of Descent (s)	Event Button Counter (End)	Time of Start: (Current Time UTC)	OAT at Altitude Start/ Altitude End
1	00	1500	00	009	3500 130	00	102	010	10/30 22	10/31 28
2	00	1700	00		-10	00			/	/
3	00	2100	00			00			/	/
4	00	2500	00			00			/	/
5	00	2900	00			00			/	/

6 Vno-10 FI

-10° +20° Pitch

Figure 4.2: Test card for the *Mode 3* flight test.

This approach allowed for manual calculation of the descent rates in case of a malfunction of the basic measurement unit, which then would manually be imported into the program. Furthermore, the event button was pressed to mark the end of the test series, to facilitate the identification of the events end during post-processing. The original data and notes are depicted in figure 4.2. The additionally performed test series for the determination of the highest safely flown ROD is depicted in the lower table, which is intentionally printed on the test card as an empty backup table.

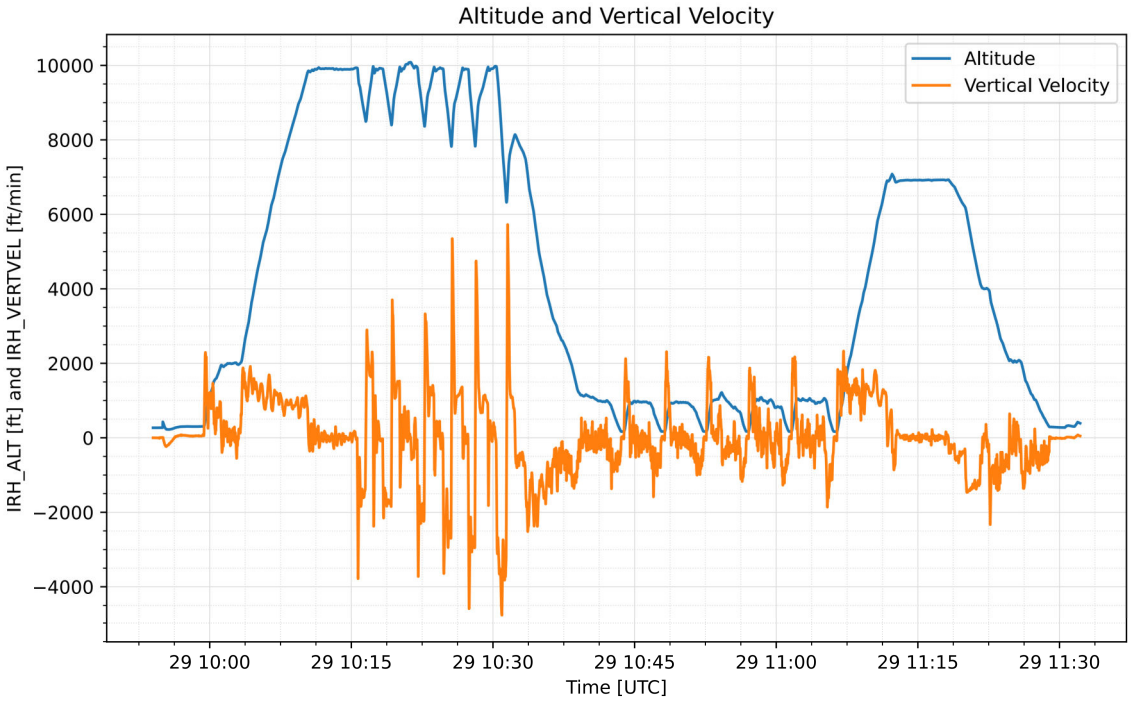

Figure 4.3: IRH_ALT and IRH_VERTVEL flight test data series.

Figure 4.3 shows the IRH_ALT and IRH_VERTVEL data series captured during the test flight. These series were obtained directly from the TwinSTASH and recorded by the basic measurement unit of the D-CODE. When observing the progression of the IRH_ALT curve, it can be noted that after the initial climb to the start altitude and a short cruise, the flight test started with its first series at 10:15 UTC. In the diagrammeme, this is characterised by consecutive and frequent altitude decreases and increases. The flight test concluded with the last series at 10:31 UTC. Comparing this with the test card in Figure 4.2, a temporal relation between the flight test data series and the handwritten notes becomes evident, verifying the accuracy and reliability of the data provided by the basic measurement unit.

When observing the progression of the IRH_VERTVEL curve with regard to its negative values (indicating descent or negative vertical velocity), the graph displays a significant volatility and a certain pattern. The pattern is characterised by a peak, which is subsequently reduced to a relatively stable value. In contrast, the test card indicates a consistent ROD, suggesting a rather stable descent pattern. This can be attributed to the practical difficulty of immediately achieving a stable intended ROD during flight. It is more likely that the target ROD is attained by initially overshooting and subsequently readjusting the ROD until the stable target value is achieved. The precise ROD value during an exceedance is mostly irrelevant to the programs dectection algorithms. What is actually significant for the programs algorithms to work with, is whether the threshold ROD has been exceeded, which is why the fluctuations in ROD can be disregarded. Considering

that the ROD has constantly remained above the respective threshold ROD for the specific test series, it is reasonable to expect the program to capture the exceedances, even if the ROD values may not precisely corresponds to the target ROD.

When analysing the altitude curve of the flight, there is an offset observed between the IRH_ALT reading and the start altitude. Shortly prior to the start of the first test series, it is evident that the altitude reading in figure 4.3 is slightly below $10.000ft$. According to the test planning, the start altitude is set with FL 95, from which results an offset. The FL95 reading is obtained from the barometric altimeter of the D-CODE aircraft. The flight crew determines the start altitude and other relevant altitudes using the barometric altimeter. However, due to the barometric altimeter being set to 'Standard' (Flightlevel), a small offset between the IRH_ALT data values and the handwritten notes on the test card is noticeable as well. When neglecting the minor fluctuations in the start altitude caused by aircraft operation and control, the offset between the defined start altitude in FL95 and the IRH_ALT sourced altitude is approximately $460ft$.

To provide an explanation, at an altitude of $3.000m$ ($9.842ft$), where the flight test started, with an outside air temperature of $0°C$ (as noted on the test card appended to this thesis), the literature value for the barometric altitude step $10{,}8\frac{m}{hPa}$ [43]. The QNH during the test flight was $1029hPa$, resulting in a pressure difference of $15{,}75hPa$ between the QNH and the standard barometric pressure ($1013{,}25hPa$). Therefore, the altitude offset between the QNH setting with mean sea level as the reference and the standard setting is calculated as $15,75hPa \cdot 10,8\frac{m}{hPa} = 170,1m$ or $170,1m \cdot 3,28\frac{ft}{m} = 557,928ft$. This $558ft$ discrepancy is slightly higher than the 460ft offset obtained from the measurement data. This can be explained by the barometric altimeter calibration. The barometric altimeter is calibrated based on the temperature decrease with altitude according to the ICAO standard atmosphere. When the actual temperature decrease in the atmosphere deviates from the standard atmospheric definition, a discrepancy occurs between the altimeter reading and the actual altitude. The precise difference can be determined by comparing the temperature progression with altitude using a Stüve diagrammeme[2]. However, since this approach neither contributes to the accuracy of the flight data nor is relevant to this thesis, it is not further discussed.

4.3 Processing and Analysis of the Safety Data

In this section, the logical framework utilised to adjust the flight test data, aiming to ensure adherence to the *Mode 3* detection envelope, is described. As explained in section 4.1.3, applying the *Mode 3* algorithms directly to the raw and unprocessed safety data from the flight test would not activate the exceedance triggers. To ensure the highest possible level of safety for the flight test, the selected start heights AGL were intentionally set higher, to allow a higher altitude margin. Additionally, the flown ROD values remain outside of the ROD threshold envelope. Consequently, a spoofing process needs to be implemented, simulating the flight test as if it were conducted at lower heights with the necessary ROD. Thereafter, the results from the safety data analysis are discussed.

4.3.1 Spoofing Process of the Safety Data

For the spoofing process, a procedure comprising of four steps is applied. The spoofing process is applied to the altitude readings from the IRH_ALT parameter, as well as the ROD readings

[2]The Stüve diagrammeme is a thermodynamic chart in meteorology, in which the temperature, dew point and atmospheric pressure curve is plotted in dependence of the altitude.

from the IRH_VERTVEL parameter. Both parameters are significant for the program to process, which is why the spoofing procedure is applied to both. Other parameters, such as the geospatial position are not affected by the safety considerations of the flight test, which is why they are not taken into account for the spoofing process. Note that this process is intended to be applied solely to the measurement data and parameters of the flight test, subject to this thesis and is in no direct relation to the usage of the program in normal operation. The ultimate aim of this procedure is to appropriately downscale the actual altitude readings of the test series, in order to allow the exceedance algorithms to trigger. This new downscaled value for the altitude is named 'spoofed altitude' ($alt_{spoofed}$) and builds, along with the adjusted ROD values the foundational dataset, which is processed in the *Mode 3* program for the analysis of the flight test. In addition to that, the IRH_VERTVEL values have to be doubled, so that they align with the initially projected target ROD.

Step 1:

For the first step, the measurement data of the flight test is divided into the six individual test series with a certain start and end time. Since every ROD threshold within a test series is allocated an altitude within the exceedance threshold envelope, this step is crucial for accurately spoofing all actual altitude values down to the spoofed altitude for the exceedance detection during the descent. Each test series start moment is set shortly prior to the descent initiation and concludes shortly after its completion. The climb phase, as well as the cruise phase between every descent phase is not intended to be monitored by the program and is therefore excluded from the analysis. Consequently, the actual altitudes of a time period of approximately one minute, varying depending on the specific test series, need to be spoofed. In total, six test series were conducted, requiring the subsequent processes to be repeated six times, but each time with their particular ROD and spoofing factor specific to that test series.

Step 2:

This step aims to calculate the trigger altitude (alt_{trig}) in which the initially planned target ROD (ROD_{tgt}) is exceeded for every respective test series. As described in section 4.1.2, each test series is assigned a target ROD which was achieved during the flight test. Since the ROD threshold within the exceedance envelope is dependent on the height, it is necessary to calculate the appropriate heights, corresponding to the target ROD in this step. This calculation is necessary to simulate that the flight test was conducted with the initially planned target ROD at their respective altitudes. The appropriate trigger altitudes for each test series are calculated using the linear interpolation equation provided in section 3.2.2, but with the altitude as the unknown variable:

$$alt_{trig} = \frac{1270}{2000} \cdot (2 \cdot ROD_{tgt} - 4000) + 1930$$

In order to provide a better distinction from the initially presented equation, the variables are named as follows: ROD_{tgt} is the target ROD, flown in the flight test and alt_{trig} is the trigger altitude of the exceedance envelope for the target ROD. The coefficient 2 to the ROD_{tgt} variable is originated in the fact that the initially planned target ROD, provided in table 4.1 were divided by two for the conduction of the flight test because of the safety considerations. At this point, it is noteworthy to mention, that altitude and height AGL are not interchangeable, unless the flight is conducted directly above water. The test flight took place in the northern German plain, where

the terrain elevation has minimal variations and is mostly flat. The elevation in the flight test area ranges from $50ft$ to $250ft$, which is a relatively small range. Given the relatively flat landscape in the flight test area, the difference between altitude and height AGL is negligible. Once the trigger altitude as a constant value for each test series is calculated, the next step can be initiated.

Step 3:

In this step, the spoofing difference for the altitude values (Δ_{alt}) is calculated. Since every series has the same start altitude (alt_{start}) but different trigger altitudes due to the different target ROD, applying a single downscaling subtrahend to all series would produce erroneous spoofed altitude readings. The spoofing difference changes for each series, thereby scaling down the respective altitude values within a series to the correct value. The respective spoofing difference for the downgrading of all other actual altitude values within one test series is calculated based on the first values of the respective series. Subsequently, the difference between the trigger altitude and the start altitude is subtracted from each specific actual altitude value recorded by the data acquisition system of the D-CODE within the defined time limits from Step 1. Through this subtraction operation, all altitude values within a test series are linearly scaled down by the same ratio. This prevents distortion of the altitude values and maintains comparability.

$$alt_{spoofed} = alt_{actual} - \Delta_{alt}$$

and

$$\Delta_{alt} = alt_{start} - alt_{trig}$$

For example, in the first test series a comparatively small target ROD was flown, which implies a low trigger altitude. A low trigger altitude entails a larger subtrahend , Consequently, all other altitudes from this test series must be reduced by the same ratio in order to maintain the comparability and consistency of the measurement series. The altitude values in the last test series are generally reduced less in comparison to the start altitude of FL95 than in the previous test series with low ROD. During the flight test, the altimeter setting remains unchanged, which establishes the same reference level for both the start altitude and the spoofed altitudes and therefore ensures compatibility between each other. The IRH_ALT values are, as described in section 3.2.1, referenced to mean sea level, which by default also remains unchanged. This establishes intercomparability and allows the application of the barometrically determined spoofing difference on the IRH_ALT values, which is subject to step 4.

Step 4:

In this step of the adjustment procedure, the respective spoofing factor is applied to each test series actual altitude values. Table 4.3 provides the calculated values for the trigger altitude, determined with the equation provided in Step 2 and the spoofing difference.

Table 4.3: Trigger altitudes, spoofing differences and spoofed target ROD for the test series based on the start altitude of FL95.

Series	Trigger Altitude $[ft]$	Spoofing Difference $[ft]$	Spoofed Target ROD $[\frac{ft}{min}]$
1	1295	8205	3000
2	1549	7951	3400
3	2057	7443	4200
4	2565	6935	5000
5	3073	6427	5800
6	3835	5665	7000

These spoofing differences are now applied to each individual actual altitude value from each test series by subtracting the spoofing differences from all actual altitude values. The calculated spoofed altitude values are programmatically stored in a list, which is then transferred to the TERRASAFE program. Through this four-step process, the excessively high altitude values could be scaled down to an appropriate and correct altitude range for each respective test series. This allowed simulating for the TERRASAFE program that the descent flights were performed at critical altitudes, relevant to the exceedance detection algorithms.

4.3.2 Flight Test Safety Analysis

In this section, the analysis of the results from the TERRASAFE *Mode 3* algorithms, applied on the spoofed flight test data is provided. Based on the experimental design, the intended target ROD, projected altitudes, and the spoofing procedure, it was expected that the TERRASAFE program would detect the exceedances qualitatively and quantitatively at the correct times.

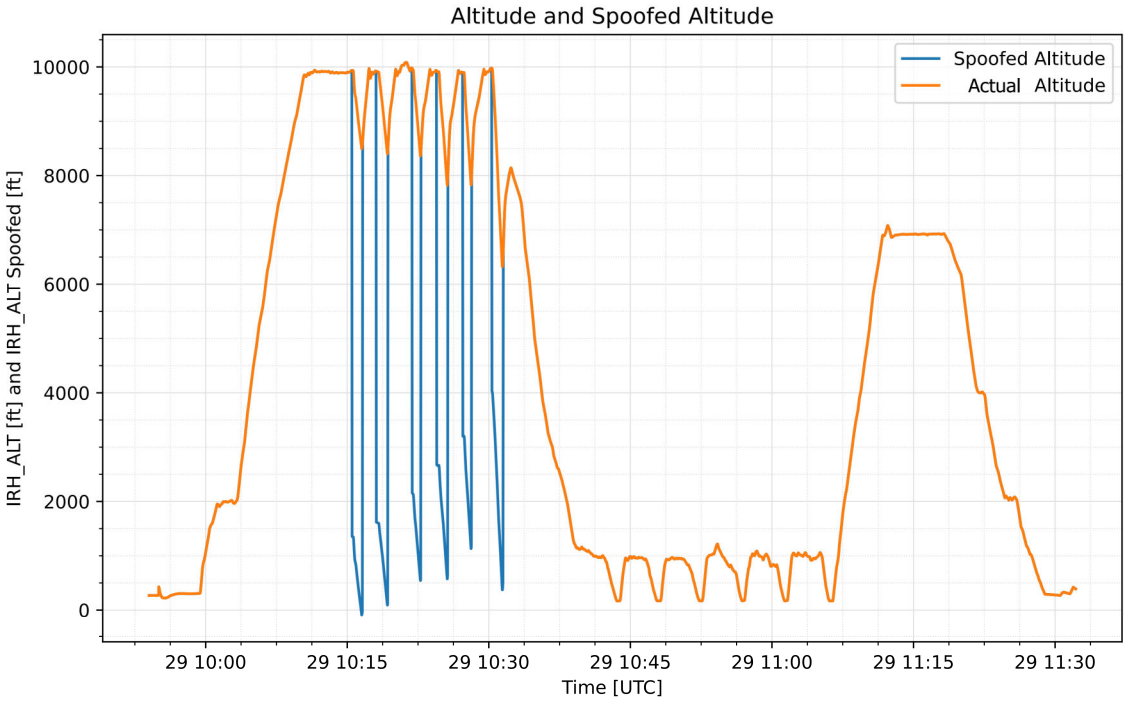

Figure 4.4: IRH_ALT values and spoofed altitude values.

Figure 4.4 shows the diagrammeme of the entire test flights IRH_ALT curve (actual altitude - orange curve). In the time frame from 10:15 UTC to 10:35 UTC, the second curve displays

the spoofed flight trajectory (spoofed altitude - blue curve). The sudden, continuous, but non differentiable altitude jumps can be clearly seen just before the start and after the completion of each test series. Additionally, from the diagrammeme, it is evident that with each progressing test series, the altitude range in which the descent was carried out increases. Furthermore, it is apparent that with each subsequent test series, the steepness of the descent increases. Consequently, as a first approximation, it can be qualitatively confirmed that the spoofing procedure worked as intended for the flight data. The values were not distorted or altered from the spoofing procedure, and the approach for determining the new spoofed altitude values is traceable, clear and comprehensible. When regarding the blue spoofed altitude curve, immediately after each test series completion, the altitude suddenly increases to its actual altitude value again. This again shows, that the spoofing mechanisms were only applied to the descent phase, and that the remainder of the flight data is not detrimentally affected by the spoofing procedure.

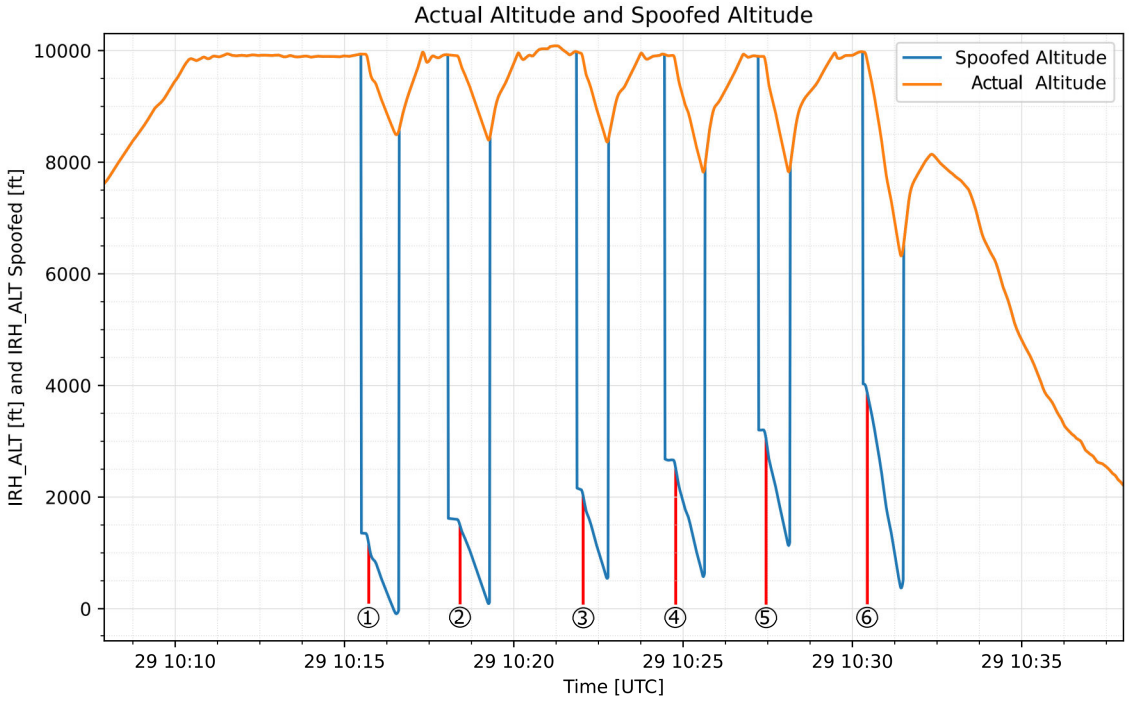

Figure 4.5: Expected trigger positions

Figure 4.5 shows the altitude profile of the flight test. The test period is enlarged to ensure better readability, as the remaining flight profile is irrelevant to the test results. After initiating the descent, a short time of a few seconds, required for the aircraft to establish the target ROD, is expected before the ROD exceedance occurs. Figure 4.5 indicates the expected time of the exceedance and is labeled with a letter corresponding to the test series. The expected results from the test series (labeled with ascending figures from 1 to 6) are provided below in table 4.4.

Clearly visible in all test series is that once the descent was initiated, the target ROD was rapidly achieved and subsequently maintained relatively stable. In the first test series, it is evident that the altitude at which the descent was ended and recovered is below 0ft. This leads to the following conclusion regarding the experimental design and underlying safety considerations: As described in section 4.1.3, the last test series of the flight experiment should initially be conducted at a flight level that allows reaching the target ROD of $3000\frac{ft}{min}$ at an altitude of $1000ft$. Under the assumption that the flight experiment would have been conducted at the initially planned altitude,

a collision with the ground would have occurred, given that the originally projected target ROD was maintained for the same time period. To avoid a ground collision, the test series would have had to be aborted early, or the ROD could not have been maintained stable, long enough to achieve a sufficiently long and meaningful measurement period. Similar observations can be made in the second test series, where the descent would have ended just slightly above the ground. This proves that the decision to conduct the experiment at a much higher start altitude and with half of the originally planned target ROD was reasonably correct. The expected start times of the exceedances were graphically determined by considering a time from initiation of the descent until the target ROD has been achieved of 5-10 seconds, depending on the particular target ROD. The expected end times of the exceedances were determined by adding the descent time, retrieved from the flight test card (figure 4.2) to the start time. Accordingly, to ascertain the programs accuracy, the detection of exceedance times as written in the TERRASAFE report (TSR) should have a margin of approximately ± 30 seconds, thereby taking into account reading errors from the diagrammeme. The higher the target ROD, the longer the time until it is achieved due to the inertia and drag of the aircraft. Once the sink rate was reached shortly after initiating the descent, it was maintained constant and stable, and the descent was only then recovered, after the sink rate had been maintained stable for several seconds.

Taking into account the experimental considerations and the logic of the program, the first trigger event should thus also be issued shortly after initiating the descent, and then continued to be issued for every additional second in which the aircraft remains outside the exceedance threshold envelope. During the flight test, the initiation of the descent was relatively rapid, leading to a reduced load factor of below $1g$, but still above $0{,}5g$. That is why, the indentation of the curve of the spoofed altitude shortly after the test series start appears relatively sudden.

Table 4.4: Expected trigger values provided by the program for test series 1,2 and 3.

Test Series	Start of Exceedance [UTC]	End of Exceedance [UTC]	Altitude of Exceedance $[ft]$	ROD Threshold $[\frac{ft}{min}]$
1	10:15:30	10:16:22	1295	3000
2	10:18:00	10:18:53	1549	3400
3	10:22:00	10:22:44	2057	4200
4	10:24:30	10:25:21	2565	5000
5	10:27:30	10:28:13	3073	5800
6	10:30:30	10:31:32	3835	7000

As described in section 3.2.1, the programs algorithms check the flight data on a second-by-second basis for each timestamp. This means that from the first second in which the ROD threshold was exceeded during descent for its respective altitude, a trigger event with the associated contextual data, as described in section 3.2.3, is issued for each additional second until the sink rate is reduced back into the acceptable range and the steep descent has ended. Although this is not very intuitive for the practical use of the program, since a large number of data points and trigger events are issued at once, it is advantageous for the analysis and evaluation of the program within this thesis. A second-by-second presentation of the individual trigger events allows for a more precise examination of when and at what altitudes the ROD exceedance occurred, as well as providing the associated ROD threshold for a better comparison. In the future operation of the program, it is planned to make the programs frontend more intuitive and user friendly, by displaying grouped individual trigger events supplemented with statistical values, a graphical display with highlighted markings of the individual trigger events (comparable to the graphical highlighting in figure 4.5),

and even a map showing the flight path and geospatial positions of where the trigger events occurred. However, within the scope of this thesis, the focus is on the functionality and evaluation of the program regarding the successful detection of exceedances by the algorithms, which is why the implementation of a user friendly frontend is not further pursued.

Subsequently an excerpt of the TERRASAFE report (TSR), generated by the program is analysed to evaluate the plausibility and accuracy of the results obtained for the first test series. The presentation and verification of all six trigger events in the TSR regarding their correctness and accuracy would exceed the scope of this thesis. Hence, the functionality of the program is solely demonstrated on trigger event 1 from test series 1. However, table 4.4 provides all expected values for each of the six test series, allowing the remaining trigger events to be traced in the full TSR in the appendix to this thesis. Due to the programs output of safety information for each timestamp within each trigger event, the report is quite extensive. To enhance readability and to highlight the most relevant information while avoiding unnecessary details, only the most essential timestamps are presented, sufficiently enough to demonstrate and prove the operability of the program. Thus, the following excerpt from the TSR comprises of three sections of test series 1. Each consisting of a set of five consecutive timestamps. These sections condense and present sufficient information to verify on one hand the expected times of the trigger event, on the other hand the correct and accurate trigger values from table 4.4. The following sections are covered:

1. The initial five timestamps of the first trigger event assigned to test series 1, as the temporal relationship to the threshold ROD exceedance and the programs detection is being examined.
2. Five timestamps from a middle section of the test series, where the flight crew maintained a stable ROD, to verify the programs consistent detection of exceedances.
3. Finally, the last five timestamps of the trigger event for test series 1, to demonstrate the observed reduction in ROD and to verify the timing of the trigger events conclusion.

These three sections of the first trigger event, which is associated to test series 1, are depicted in figure 4.6.

When considering the first five timestamps, the following observations can be made: The acceptable time frame within the first exceedance should occur, according to table 4.4, is at 10:15:30 UTC with a 30-second deviation due to inaccuracies in reading from the measurement graph. The first timestamp of the trigger event, which is the first second of the flight in which the TERRASAFE logics and algorithms detected a ROD exceedance, is at 10:15:40 UTC. This confirms that the program is able of timely and accurately detecting exceedances. When verifying the accuracy of the detected values, the following can be concluded: The actual altitude at which the program initiates the trigger is at $1309ft$. The expected altitude at which the program should trigger was calculated to be $1295ft$. It is important to mention that the altitudes provided by the program are spoofed altitude values and are therefore subject to calculatory uncertainties. Nevertheless, $1309ft$ compared to the calculated value of $1295ft$ is still well within the acceptable margin, with just 1,08% deviation. This demonstrates the accuracy of the program in detecting the right exceedance altitudes. Similarly, when regarding the threshold ROD calculated along the algorithms provided in section 3.2.2, it becomes evident, that the program is relatively accurate in calculating the threshold ROD. The ROD threshold was expected to be $3000\frac{ft}{min}$ and was calculated by the program as $3022\frac{ft}{min}$. Here again, the percentage deviation falls within a good range, with only a 0,73% difference from the expected value. At this point, it should be noted that the ROD threshold

Trigger Event Test Series 1

	Time (UTC)	Latitude (DD)	Longitude (DD)	Height AGL (ft)	Altitude (ft)	Elevation (ft)	Actual ROD (ft/min)	Threshold ROD (ft/min)
Timestamps 1-5	2023-05-29 10:15:40	52.734904	11.207946	1188.7	1309.1	120.4	-4026.0	3022.2
	2023-05-29 10:15:41	52.735271	11.209120	1143.9	1267.2	123.3	-5678.0	2956.3
	2023-05-29 10:15:42	52.735666	11.210390	1105.7	1215.9	110.1	-7036.0	2875.4
	2023-05-29 10:15:43	52.736032	11.211567	1038.8	1151.6	112.9	-7566.0	2774.2
	2023-05-29 10:15:44	52.736432	11.212852	974.3	1090.6	116.3	-6830.0	2678.1
Timestamps 24-28	2023-05-29 10:16:09	52.746049	11.242562	337.0	451.7	114.8	-2862.0	1672.0
	2023-05-29 10:16:10	52.746477	11.243778	313.6	427.1	113.5	-3030.0	1633.3
	2023-05-29 10:16:11	52.746875	11.244904	285.1	402.5	117.4	-3020.0	1594.5
	2023-05-29 10:16:12	52.747310	11.246126	255.7	376.2	120.5	-3016.0	1553.1
	2023-05-29 10:16:13	52.747715	11.247256	227.1	351.6	124.5	-3098.0	1514.4
Timestamps 35-39	2023-05-29 10:16:20	52.750799	11.255593	28.4	163.5	135.0	-3196.0	1218.1
	2023-05-29 10:16:21	52.751237	11.256734	8.5	137.7	129.2	-3192.0	1177.5
	2023-05-29 10:16:22	52.751716	11.257970	-16.3	110.4	126.6	-3066.0	1134.4
	2023-05-29 10:16:23	52.752201	11.259206	-39.4	85.2	124.7	-2944.0	1094.9
	2023-05-29 10:16:24	52.752652	11.260346	-64.5	61.7	126.3	-2910.0	1057.9

Figure 4.6: Trigger Event Test Series 1

calculation is based on the actual altitude of the aircraft, which is why a relatively accurate value for the ROD threshold can be expected due to the application of a single formula, and the deviation from the previously projected threshold ROD value falls within the error tolerance range of the trigger altitude value.

When examining the timestamps 24-28, it becomes evident that the actual ROD value fluctuates around the target ROD of $3000\frac{ft}{min}$. These fluctuations can be attributed to the challenges of consistently maintaining a precise and constant ROD for several seconds, regarding the operational handling of the aircraft. It is worth noting that a deviation of $\pm$100-200$\frac{ft}{min}$ is still within an acceptable range and demonstrates the competent flying abilities of the flight crew. Nevertheless, the actual ROD is consistently kept above the ROD threshold, which is also identified by the program, issueing the respective timestamps in the TSR. Thus, the program has been validated in terms of accurately identifying a continuous exceedance situation. If the sink rate were to be reduced for a second or less, and the actual ROD value falls below the threshold ROD value for the respective altitudes, no exceedance trigger would be listed in the report for those timestamps. The program would consider this specific situation as "acceptable," as it was designed to do. This confirms the long term accuracy and functional reliability of the program.

Finally, for the last timestamps of the particular trigger event, timestamps 35-39, the expected end time of the exceedance is at 10:16:22 UTC. The last trigger of the event occurs at 10:16:24 UTC. This confirms that the temporal duration of the trigger event, identified by the TERRASAFE *Mode 3* program algorithms aligns with the actual simulated trigger event during the flight test, and the program consistently recognises the end of a risk situation or of an FDM event.

Thus, the suitability of the program regarding precise and sharp, as well as accurate and reliable detection of a hazardous situation has been demonstrated. The results proved that the implementation of the FDM system into the flight operation is going to have a huge improvement to flight safety.

Chapter 5

Conclusion and Outlook

5.1 Conclusion

Aircraft and their operation involve a complex interplay of various human and technical factors. Although aviation has become much safer today with technical improvements, the implementation of regulations as well as increased awareness of safety issues, there are still inherent hazards and risks that cannot be completely eliminated. Detecting, anticipating, or inferring hazards and risks is crucial in their mitigation. This is precisely where the Flight Data Monitoring (FDM) system developed in this thesis comes into play. Its primary purpose is to uncover previously unseen things and make them visible. The objective of this thesis was to develop, implement and test an FDM system, customised to the individual Controlled Flight Into Terrain (CFIT) related risks and hazards of the DLR experimental flight operation. Motivation for this was to develop a system, which further enhances the flight safety within operation by revealing undetected safety threats, providing valuable safety information as a basis of mitigation measures and serving as a de-briefing tool for pilots and flight test engineers to assess potential safety issues of flight experiments.

First, the significance of FDM was embedded within the framework of safety management. Subsequently, the legal foundation, objectives, as well as principles and elements of an FDM system were addressed. Following that, a study which aimed to work out potential hazards and risks concerning special operations in general and experimental flight operations in the DLR facility of flight experiments was conducted. The study revealed that particularly in the profile flown in experimental flight operations, an increased risk of CFIT and Mid-Air Collision (MAC) related occurrences exists. The CFIT occurrence category was specifically chosen to be addressed by the programs exceedance detection algorithms due to its significant potential for accidents and associated risks. As the complexity and sophistication of FDM systems mirrors the intricate interplay of risk factors affecting flight safety, designing a fully developed FDM system, adressing all potential risks and hazards in the flight operation is not expedient for this thesis. Therefore, to serve as a basis for the FDM system customised to the DLR, an approach involving the design and conception of three *Modes* was chosen, each of which adressing one particular CFIT related risk. Finally in the theoretical section, a proof of concept for the implementation of the FDM system, customised to the identified hazards and risks related to CFIT occurrences, was presented.

Subsequently, the three *Modes* addressed in the proof of concept for specific CFIT situations were discussed and explained in more detail. Firstly, the output data that the *Modes* of the program should generate were defined. Based on that, the processing mechanisms and exceedance detection

logics were shown through which the intended outputs should be achieved. Then, the appropriate parameters and input data that should lead to the desired results were discussed.

Within this thesis, *Mode 3* was selected to be programmatically realised and implemented. For this purpose, the algorithms and program logics of *Mode 3* were described in more detail using flowcharts and diagrammes.

To validate the program, a flight test was planned and conducted, where the aircraft simulated a high-risk situation by simulating descents with high rates of descent (ROD) at low altitude. The program was expected to detect these hazardous situations by analysing and processing the measurement data obtained from the D-CODE aircraft. Initially, the flight test objective and planning were described, as well as safety related considerations and modifications to the flight test. Since a real flight of the projected exceedance detection parameters in itself entails a significant safety risk for the flight and the crew, the flight test was slightly modified to ensure the highest possible safety. The flight test with its modified flight envelope fell as a consequence outside the critical parameters, and the program would not detect any exceedances. Therefore, the measurement data had to be spoofed in the post flight analysis before being imported into the program, to simulate the flight test results being within the critical envelope. The spoofing mechanisms and logics were also explained to establish a coherent connection between flight test results and program results. Finally, the results of the program analysis were presented and explained in the context of the flight test. This demonstrated and proved, that the logics, algorithms, and functionalities conceived in this thesis have led to a suitable, functional, and tested system for DLR experimental flight operations.

5.2 “The Cockpit Spy” - What is the Influence of an FDM System on Safety Culture?

Is there any truth to how Petter Hornfeld titled FDM in his YouTube video [4]? Aircraft Cockpits remain some kind of black box and tracking mistakes slips and lapses made by pilots, up to a certain extent relies on mandatory and voluntary reporting procedures. Flight trackers like Flightradar24 and ADSB-Exchange on the one hand make certain parameters of flight information accessible to the public and thus also to operational flight safety departments, but yet have limited access to all flight data and potential exceedances. Given that a mistake or an error has occured, unless an aircraft is involved in an incident or accident, requiring the Flight Data Recorder to be analysed, and the flight crew does not adhere to mandatory and voluntary reporting, the mistake remains undisclosed. An implemented FDM system would reveal the error, since it monitors all flights for exceedances and anomalies, regardless of whether an accident or incident has been reported or not. The question of whether an FDM system is like a kind of spy in the cockpit cannot be answered definitively and depends on various perspectives. Primarily, FDM is a system designed to enhance flight safety. In the context of a safety management system, it is important that the different safety means do not operate as separate and independent systems. Instead, a safety management system aims to connect and combine these systems and safety devices, allowing for a mutual identification and improvement of weaknesses and flaws. This enables a holistic approach to be applied in order to enhance flight safety. Within a safety management system, the FDM can serve as a valuable tool by providing contextual and critical information, qualitative and quantitative data regarding specific ocurrences and unsafe situations. Along with the voluntary and mandatory reporting system, where flight crews disclose information on occurrences and unsafe situations, additional pieces can

be added to the puzzle, which ultimately forms a comprehensive picture of the occurrence. Given that, appropriate mitigation actions can be performed, so that the concerning risks and hazards can be effectively ameliorated or even neutralised.

A crucial concept in terms of safety management is operational just culture. Just culture describes how operators handle errors made by employees. It is inherent in human nature to make unintentional mistakes. Factors such as experience, training, and other cognitive characteristics of individuals play a role on that. Even the most experienced captains for example, occasionally make mistakes. A company that adheres to the principles of just culture reacts to errors as an opportunity to investigate their background and causes. Sometimes, contradictory procedures, processes or instructions, as well as inadequate training, can contribute to errors. Even if the flight crew makes an unintentional mistake, a just culture does not involve punitive reactions and retaliatory behavior by the superiors or managers. Unless the error originates in gross negligence or intentional actions, further training or education is likely to be ordered for the respective flight crew as a mitigation measure. That is why FDM is a crucial tool in the risk and hazard indentification and mitigation process of an operator. The implementation of an effective FDM system is also connected to the introduction of extensive procedures for a confidential and responsible handling of the generated data. This highly sensitive data, if handled negatively by the safety management department, can indeed have a detrimental effect on flight safety instead of a positive. A very strict and punitive error culture in the company may result in flight crews not addressing anomalies, errors and hazards, even if they are not to blame, due to fear of negative consequences. Another consequence could be that flight crews in such operations may tend to fly “after the FDM-profile” so that exceedances are avoided on the cost of disregarding standard operating procedures [22]. In conclusion, a strict and punitive error culture with regard to FDM could entail that holes in the cheese slices are not detected, which in extreme cases, when the cheese slices align consecutively, can lead to an accident and loss of life. It is therefore crucial to foster a culture that encourages a well disposed usage of the FDM system, open communication and reporting of mistakes, errors and hazards to prevent such unfortunate outcomes.

The perspective on whether an FDM system is perceived as a spy in the cockpit or a valuable safety system, is closely tied to how an operator employs the system within the framework of just culture and how strongly the corporate culture is aligned with just culture principles. Under the premise of just culture, operational FDM systems should not be seen as a spy, constantly checking and controlling the pilots, but rather an effective system in reviewing the safety of the operation, thereby contributing to a safer operation in aviation.

5.3 Outlook

Based on the information obtained from the interviews described in section 2.3.1, in addition to the risks and hazards related to CFIT, there is another occurrence category which could be addressed by the FDM system: MAC. The D-CODE is primarily involved in operation and flight tests under VFR conditions, relying on the ’see and avoid’ principle. Most of the flights take place in airspace class ’E’ where no mandatory air traffic control surveillance is required and other VFR air traffic participants also rely on the "see and avoid" principle. Therefore, another potential application of the FDM system could be a traffic event detection system. Additionally, the FDM program can be expanded to include modules that cover other risks and hazards from different occurrence categories, such as runway excursions or loss of control in-flight.

The FDM algorithms and logics in this thesis have been designed in a way to be interchangably applicable to a wide range of fixed-wing aircraft types, and even helicopters including within the DLR experimental flight operation. Minor adjustments of the program code may be required to ensure appropriateness of parameters, sensors, and data for each individual aircraft. Additionally, considering the variations in performance and flight characteristics among the different experimental aircraft in the DLR, it is important to customise the trigger and exceedance thresholds to align with each aircrafts unique flight envelope and profile. The exceedance detection algorithms, in their current form, do not require any major modifications as they are designed to be universally applicable. These algorithms can be implemented without any adjustments, as they are capable of detecting exceedances across different aircraft types. This approach ensures optimal functionality and effectiveness of the FDM system for each individual aircraft.

It should be noted that all exceedance threshold values, also the ones provided in this thesis are in to be revised in normal operation through an interative process, requiring a feedback and revision loop for the appropriateness and suitability of the values. Every FDM system needs to be adjusted to the operators individual needs and safety objectives. Above all, the potential applications, advancements and the sophistication of an FDM system are limitless. In the future, the FDM system will be further expanded in its range of applications to adress various other safety risks and hazards. As it evolves within the framework of DLR SAFE module, the system will continuously be improved, thereby contributing to enhance safety and efficiency within the DLR experimental flight operation.

Bibliography

[1] EASA European Aviation Safety Agency, *EASp Annex A Status Report 2014*, European Aviation Safety Plan, Final Issue (2014).

[2] ICAO International Civil Aviation Organisation, *Effects of Novel Coronavirus (COVID-19) on Civil Aviation: Economic Impact Analysis*, (Published April, 27 2023). Retrieved from: https://www.icao.int/sustainability/Documents/COVID-19/ICAO_Coronavirus_Econ_Impact.pdf.

[3] J. Freed, S. Mayerowitz, *Past decade has been safest for airline passengers*, The Washington Times (Published December 31, 2011). Retrieved from: https://www.washingtontimes.com/news/2011/dec/31/past-decade-has-been-safest-airline-passengers/.

[4] P. Hornfeldt, *The Cockpit spy! Who is always watching?!*, Youtube Video by Mentour Pilot [Accessed June 26, 2023], retrieved from: https://www.youtube.com/watch?v=Vw0rlDs5tgs.

[5] ICAO International Civil Aviation Organisation, *Doc 9859 Safety Management Manual (SMM)*, International Civil Aviation Organisation, Third Edition (Published 2013).

[6] European Operators Flight Data Monitoring Forum (EOFDM) Working Group C, *FLIGHT DATA MONITORING ANALYSIS TECHNIQUES AND PRINCIPLES*, EASA Good Practice Document, initial issue (December 2021).

[7] ICAO International Standards and Recommended Practices, *Annex 19 to the Convention on International Civil Aviation - Safety Management*, International Civil Aviation Organisation, Second Edition (Published July 2016).

[8] The Observer Business, *Planes and boats in train* [Accessed March 27, 2023], The Guardian. Retrieved from: https://www.theguardian.com/business/2000/aug/27/transportintheuk.theobserver.

[9] M. Butter, *Event-based Risk Quantification in Flight Data Analysis*, (published doctoral dissertation), Technical University of Munich, Department of Mechanical Engineering, 2018.

[10] A. Pelsser, *Annex 19 - Safety Management, The Postal History of ICAO* [Accessed February 15, 2023]. Retrieved from https://applications.icao.int/postalhistory/annex_19_safety_management.htm.

[11] ICAO International Civil Aviation Organisation, *Doc 10004 Global Aviation Safety Plan*, International Civil Aviation Organisation, 2023-2025 (Published 2022).

[12] ICAO International Civil Aviation Organisation, *High-Level Safety Conference 2010 - Report* [Accessed February 22, 2023]. Retrieved from: https://www.icao.int/Meetings/AMC/HLSC/HLSC%202010%20Report/HLSC.2010.DOC.9335.EN.pdf.

[13] ICAO International Civil Aviation Organisation, *About ICAO* [Accessed February 26, 2023]. Retrieved from: https://www.icao.int/about-icao/Pages/default.aspx.

[14] European Commission, *Regulation (EC) No 216/2008 of the European Parliament and of the Council of 20 February 2008*, Official Journal of the European Union (Published March 19, 2008).

[15] ICAO International Standards and Recommended Practices, *Annex 1 to the Convention on International Civil Aviation - Personnel Licensing*, International Civil Aviation Organisation, Fourteenth Edition (July 2022).

[16] ICAO International Standards and Recommended Practices, *Annex 6 to the Convention on International Civil Aviation - Operation of Aircraft: Part I- International Commercial Air Transport*, International Civil Aviation Organisation, Eleventh Edition (July 2018).

[17] EASA European Aviation Safety Agency, *Acceptable Means of Compliance (AMC) and Alternative Means of Compliance (AltMoC)* [Accessed February 26, 2023], EASA Pro Document Library. Retrieved from: https://www.easa.europa.eu/en/document-library/acceptable-means-compliance-amcs-and-alternative-means-compliance-altmocs.

[18] EASA European Aviation Safety Agency, *Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Annex III Part ORO*, consolidated document containing AMC/GM to Annex Part III (Part-ORO) to Commission Regulation (EU) No 965/2012 on air operations (Published February 2016).

[19] Eurocontrol Experimental Centre, *REVISITING THE « SWISS CHEESE » MODEL OF ACCIDENTS*, Eurocontrol EEC Note No. 13/06 Project Safbuild (Issued October 2006).

[20] A. Stolzer, C. Halford and J. Goglia, *Implementing Safety Management Systems in Aviation*, Ashgate Publishing, Farnham, 2011.

[21] UK Civil Aviation Authority, *CAP 739 - Flight Data Monitoring*, United Kingdom Civil Aviation Authority, Second Edition (Published June 2013).

[22] ICAO International Civil Aviation Organisation, *Doc 10000 Manual on Flight Data Analysis programs (FDAP)*, International Civil Aviation Organisation, First Edition (Published 2014).

[23] Skybrary online library of the ICAO, *Flight Data Acquisition Unit (FDAU)*, [Accessed March 26, 2023]. Retrieved from: https://skybrary.aero/articles/flight-data-acquisition-unit-fdau.

[24] United States General Accounting Office, *Efforts to Implement Flight Operational Quality Assurance programs*, Aviation Safety Report to Congressional Requesters (Published December 1997).

[25] EASA European Aviation Safety Agency, *EASp Annex A Status Report 2014*, European Aviation Safety Plan, Final Issue (2014).

[26] EASA European Authorities Coordination Group on Flight Data Monitoring (EAFDM), *DEVELOPING STANDARDISED FDM-BASED INDICATORS*, Safety Promotion Good Practice Document, Version 2 (December 2016).

[27] G. Marino, *Proactive Flight Safety trough FOQA & ASAP*, International Flight Inspection Symposium Proceedings Report (June, 2014).

[28] ED Decision 2016/013/R Annex II, *ETSO-C151c Terrain Awareness and Warning System (TAWS)*, EASA European Technical Standard Order (Issued August 8, 2016).

[29] EASA European Aviation Safety Agency, *Specialised operations (SPO)* [Accessed March 20, 2023]. Retrieved from: https://www.easa.europa.eu/en/domains/air-operations/specialised-operations-spo.

[30] Safety first, *Lining Up with the Correct Glide Slope*, The Airbus Safety magazine (December 2021). Retrieved from: https://mms-safetyfirst.s3.eu-west-3.amazonaws.com/pdf/safety+first/lining-up-with-the-correct-glide-slope.pdf.

[31] Interview with R. Seeschaaf, Safety Manager and Pilot at Flight Calibration Services, *Challenges and Current Situation Associated with the Implementation of an FDM System for a Flight Inspection Provider*, Braunschweig (March 3, 2023).

[32] Interview with A. Dilcher, Experimental Research Pilot at the DLR, *Risks and Hazards of the DO228-100 D-CODE Experimental Flight Operation,* Braunschweig (April 4, 2023).

[33] UK Civil Aviation Authority, *Form SRG1846 - Steep Approach Approval Compliance Statement and Checklist*, Issue 1 (April 2019).

[34] ATR Training Center, *FLIGHT DATA MONITORING ON ATR AIRCRAFT*, ATR (Published 2016).

[35] S. Woodward, *Circuit transmits ARINC 429 data*, EDN [Accessed May 31, 2023], Retrieved from: https://www.edn.com/circuit-transmits-arinc-429-data/.

[36] J. Wendel, *Integrierte Navigationssysteme*, Oldenbourg Wissenschaftsverlag, München, 2007.

[37] N. Marwaha, E. Duffy, *Tech Everything you need to know about Digital Elevation Models (DEMs), Digital Surface Models (DSMs), and Digital Terrain Models (DTMs)* [Accessed May 23, 2023], Retrieved from: https://up42.com/blog/everything-you-need-to-know-about-digital-elevation-models-dem-digital.

[38] A. J. Nisbet, *Open Topo Data* EU-DEM 25m, Elevation API, Retrieved from: https://api.opentopodata.org/v1/eudem25m?locations=.

[39] W. Fraczek, *Mean Sea Level, GPS and the Geoid*, Esri Applications Prototype Lab [Accessed May 23, 2023], Retrieved from: https://www.esri.com/news/arcuser/0703/geoid1of3.html.

[40] A. Nisbet, *EU-DEM*, Information on Dataset [Accessed May 25, 2023], Retrieved from: https://www.opentopodata.org/datasets/eudem/.

[41] European Petroleum Survey Group Geodesy (EPSG), *EPSG:5129 European Vertical Reference Frame 2000*, Klokan Technologies GmbH, Switzerland [Accessed May 24, 2023], Retrieved from: https://www.epsg.io/5129-datum.

[42] Skybrary online library of the ICAO, *Radio Altimeter*, [Accessed July 8, 2023], retrived from: https://skybrary.aero/articles/radio-altimeter.

[43] W. Augath, J. Ihde, *Definition and Realization of Vertical Reference Systems - The European Solution EVRS/EVRF 2000*, [Accessed May 24, 2023], Retrieved from: https://tu-dresden.de/bu/umwelt/geo/gi/gg/ressourcen/dateien/veroeffentlichungen/ european_solution_evrs.pdf?lang=de.

[44] Propeller Aero, *Geoid vs. Ellipsoid: What's the Difference?* [Accessed May 25, 2023], Retrieved from: https://www.esri.com/news/arcuser/0703/geoid1of3.html.

[45] C. F. Gauss, *Bestimmung des Breitenunterschiedes zwischen den Sternwarten von Göttingen und Altona durch Beobachtungen am Ramsdenschen Zenithsector*, Vandenhoeck und Ruprecht, Göttingen, 1828.

[46] Wikipedia Graphic, *Excessive Descent Rate* [Accessed June 06, 2023], based on FAA Technical Standard Orders (TSO) - TSO-C151d, retrieved from: https://en.wikipedia.org/wiki/Ground_proximity_warning_system#/media/File: FAA_excessive_sink_rate_graph.svg.

[47] J. Engel, *Anwendungsorientierte Mathematik: Von Daten zur Funktion*, Springer Spektrum, Berlin, 2018.

[48] G. Pfeffer, *Luftdruck - Die barometrische Höhenstufe*, [Accessed June 23, 2023], retrieved from: https://www.gerd-pfeffer.de/atm_luftdruck.html.

[49] National Transportation Safety Board NTSB, *Descent Below Visual Glidepath and Impact With Seawall - Asiana Airlines Flight 214*, Accident Report (Published June 2014), retrieved from: https://www.ntsb.gov/investigations/AccidentReports/Reports/AAR1401.pdf.