CPDLC in Practice
- A Dissection of the Controller Pilot Data Link Communication Security

CPDLC i praktiken

André Lehto
Isak Sestorp

Supervisor : Andrei Gurtov
Examiner : Marcus Bendtsen
Upphovsrätt

Detta dokument hålls tillgängligt på internet - eller dess framtida ersättare - under 25 år från publiceringsdatum under förutsättning att inga extraordinära omständigheter uppstår. Tillgång till dokumentet innebär tillstånd för var och en att läsa, ladda ner, skriva ut enstaka kopior för enskilt bruk och att använda det oförändrat för ickekomersiell forskning och för undervisning. Överföring av upphovsrätten vid en senare tidpunkt kan inte upphäva detta tillstånd. All annan användning av dokumentet kräver upphovsmannens medgivande. För att garantera äktheten, säkerheten och tillgängligheten finns lösningar av teknisk och administrativ art.

Upphovsmannens ideella rätt innefattar rätt att bli nämnd som upphovsman i den omfattning som god sed kräver vid användning av dokumentet på ovan beskrivna sätt samt skydd mot att dokumentet ändras eller presenteras i sådan form eller i sådant sammanhang som är kränkande för upphovsmannens litterära eller konstnärliga anseende eller egenart.

För ytterligare information om Linköping University Electronic Press se förlagets hemsida http://www.ep.liu.se/.

Copyright

The publishers will keep this document online on the Internet - or its possible replacement - for a period of 25 years starting from the date of publication barring exceptional circumstances.

The online availability of the document implies permanent permission for anyone to read, to download, or to print out single copies for his/her own use and to use it unchanged for non-commercial research and educational purpose. Subsequent transfers of copyright cannot revoke this permission. All other uses of the document are conditional upon the consent of the copyright owner. The publisher has taken technical and administrative measures to assure authenticity, security and accessibility.

According to intellectual property law the author has the right to be mentioned when his/her work is accessed as described above and to be protected against infringement.

For additional information about the Linköping University Electronic Press and its procedures for publication and for assurance of document integrity, please refer to its www home page: http://www.ep.liu.se/.

André Lehto
© Isak Sestorp
Students in the 5 year Information Technology program complete a semester-long software development project during their sixth semester (third year). The project is completed in mid-sized groups, and the students implement a mobile application intended to be used in a multi-actor setting, currently a search and rescue scenario. In parallel they study several topics relevant to the technical and ethical considerations in the project. The project culminates by demonstrating a working product and a written report documenting the results of the practical development process including requirements elicitation. During the final stage of the semester, students create small groups and specialise in one topic, resulting in a bachelor thesis. The current report represents the results obtained during this specialisation work. Hence, the thesis should be viewed as part of a larger body of work required to pass the semester, including the conditions and requirements for a bachelor thesis.
Abstract

Controller-Pilot Data Link Communication, a technology that has been introduced to help offload the congested, previously used voice communication in larger airports, has in recent years started being questioned on its sufficiency in security. As the traffic load in air traffic communication keeps demanding more reliable and secure systems, we will in this thesis look at how widely CPDLC is actually used in practice in Europe. By using the newly introduced technology in software defined radios, we show that it is possible to capture and decode CPDLC messages to readable plain text. We furthermore discuss which type of attacks that could be possible with information retrieved from CPDLC communication.
Acknowledgments

We would like to take this opportunity to express our gratitude and to thank our supervisor, Andrei Gurtov, for his support, and continuous encouragement.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>iii</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>v</td>
</tr>
<tr>
<td>Contents</td>
<td>vi</td>
</tr>
<tr>
<td>List of Figures</td>
<td>vii</td>
</tr>
<tr>
<td>List of Tables</td>
<td>viii</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>3</td>
</tr>
<tr>
<td>1.1 Motivation</td>
<td>3</td>
</tr>
<tr>
<td>1.2 Aim</td>
<td>4</td>
</tr>
<tr>
<td>1.3 Research questions</td>
<td>4</td>
</tr>
<tr>
<td>1.4 Delimitations</td>
<td>4</td>
</tr>
<tr>
<td>1.5 Related work</td>
<td>4</td>
</tr>
<tr>
<td>2 Theory</td>
<td>5</td>
</tr>
<tr>
<td>2.1 Controller–pilot data link communications (CPDLC)</td>
<td>5</td>
</tr>
<tr>
<td>2.2 Procedures</td>
<td>8</td>
</tr>
<tr>
<td>2.3 Aircraft Communications Addressing and Reporting System</td>
<td>15</td>
</tr>
<tr>
<td>2.4 Realtek-Software Defined Radio (RTL-SDR)</td>
<td>15</td>
</tr>
<tr>
<td>3 Method</td>
<td>16</td>
</tr>
<tr>
<td>3.1 Pre-study</td>
<td>16</td>
</tr>
<tr>
<td>3.2 Implementation</td>
<td>16</td>
</tr>
<tr>
<td>3.3 Evaluation</td>
<td>19</td>
</tr>
<tr>
<td>4 Results</td>
<td>20</td>
</tr>
<tr>
<td>4.1 CPDLC elements</td>
<td>20</td>
</tr>
<tr>
<td>4.2 Flight position</td>
<td>23</td>
</tr>
<tr>
<td>5 Discussion</td>
<td>24</td>
</tr>
<tr>
<td>5.1 Method</td>
<td>24</td>
</tr>
<tr>
<td>5.2 Results</td>
<td>24</td>
</tr>
<tr>
<td>6 Conclusions and future work</td>
<td>28</td>
</tr>
<tr>
<td>6.1 Conclusion</td>
<td>28</td>
</tr>
<tr>
<td>6.2 Future work</td>
<td>29</td>
</tr>
<tr>
<td>Bibliography</td>
<td>30</td>
</tr>
<tr>
<td>A Appendix</td>
<td>32</td>
</tr>
</tbody>
</table>
List of Figures

2.1 CPDLC implementation July 2017 (Eurocontrol, 2017) ................................. 6
2.2 CPDLC implementation June 2018 (Eurocontrol, 2018) ............................... 7
2.3 VDL SARPS in the ATN/OSI Organization (ETSI, 2011) ............................... 8
2.4 Example of communication in a CPDLC connection (GOLD, 2013) ............... 9
2.5 Example of an empty flight plan ................................................................. 10
2.6 Connection forwarding (GOLD, 2013) ...................................................... 12
3.1 Picture of the setup used in the tests to capture CPDLC data .......................... 17
4.1 Aircraft details for tracked flight between Stockholm Arlanda (ARN) and Paris ............................ (Flightradar24, 2019) ............................ 20
4.2 ACARS and CPDLC data traffic ................................................................. 21
4.3 Flight path of the tracked flight with time-stamps when messages were sent (Flightradar24, 2019) ............................ 23
List of Tables

2.1 Air-ground data link messages for DLIC (GOLD, 2013) ........................................... 11
2.2 Precedence of responses (GOLD, 2013) ................................................................. 12
2.3 Example of CPDL C dialogue (GOLD, 2013) .......................................................... 13

4.1 Flight details for tracked flight between Stockholm Arlanda (ARN) and Paris Charles de Gaulle (CDG) (Flightradar24, 2019) ......................................................... 21
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACARS</td>
<td>Aircraft Communications Addressing and Reporting System</td>
</tr>
<tr>
<td>ATC</td>
<td>Air Traffic Control</td>
</tr>
<tr>
<td>ATN</td>
<td>Air Traffic Network</td>
</tr>
<tr>
<td>AMIC</td>
<td>Application Message Integrity Check</td>
</tr>
<tr>
<td>ATSU</td>
<td>Air Traffic Services Unit</td>
</tr>
<tr>
<td>CPDLC</td>
<td>Controller-Pilot Data Link Communication</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>CDA</td>
<td>Current Data Authority</td>
</tr>
<tr>
<td>CSMA</td>
<td>Carrier Sense Multiple Access</td>
</tr>
<tr>
<td>DLS</td>
<td>Data Link Service</td>
</tr>
<tr>
<td>DM</td>
<td>Downlink Message</td>
</tr>
<tr>
<td>DLIC</td>
<td>Data Link Initiation Capability</td>
</tr>
<tr>
<td>D8PSK</td>
<td>Eight-Ary Differential Phase Shifting Keying</td>
</tr>
<tr>
<td>FEC</td>
<td>Forward Error Correction</td>
</tr>
<tr>
<td>FL</td>
<td>Flight Level</td>
</tr>
<tr>
<td>GAT</td>
<td>General Air Traffic</td>
</tr>
<tr>
<td>GFD</td>
<td>Ground Facility Designator</td>
</tr>
<tr>
<td>ICAO</td>
<td>International Aviation Organization</td>
</tr>
<tr>
<td>LME</td>
<td>Link Management Entity</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MIN</td>
<td>Message Identification Number</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>MRN</td>
<td>Message Reference Number</td>
</tr>
<tr>
<td>NDA</td>
<td>Next Data Authority</td>
</tr>
<tr>
<td>RTL-SDR</td>
<td>Realtek-Software Defined Radio</td>
</tr>
<tr>
<td>SARPS</td>
<td>Standards and Recommended Practices</td>
</tr>
<tr>
<td>UM</td>
<td>Uplink Message</td>
</tr>
<tr>
<td>UAV</td>
<td>Unmanned Aerial Vehicles</td>
</tr>
<tr>
<td>VHF</td>
<td>Very High Frequency</td>
</tr>
<tr>
<td>VDL2</td>
<td>Very High Frequency Digital Link Mode 2</td>
</tr>
<tr>
<td>CIA</td>
<td>Confidentiality, Integrity, Availability</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Motivation

As the air traffic load and air traffic communication at larger airports keeps expanding, a technology to unburden the traditional Very High Frequency (VHF) voice communication has become necessary. It is estimated that the world-wide aerial traffic will double until 2037, with big European airports handling up to 3000 daily take-offs and landings [1]. Meanwhile, the Unmanned Aerial Vehicles (UAV) is predicted to outnumber traditional air traffic, congesting the airspace and making reliable and secure systems a necessity [17]. To solve the overload in air traffic communication, Controller-Pilot Data Link Communication (CPDLC) was introduced. CPDLC complements VHF radio voice communication by handling non-critical communication and has since its introduction reduced miscommunications and increased communication effectiveness. [9]

In recent years, the question if the security in CPDLC is suitable for its use has arisen. Historically, security has not been a consideration when designing communication systems and was instead built around the procedural measures and vigilance of aircraft crew and air traffic controllers [14]. This demands situational awareness of the anticipated air traffic at any given time, where the security lies in the trust between the Air Traffic Control (ATC) and pilot. ATCs are then relying on pilots to not divert from instructions and pilots trusting the ATC to not give them instructions that will divert them from their intended destination. CPDLC suffers from this type of lack of security, which according to [15] makes CPDLC insecure on a conceptual level.

At the same time, lightweight, easily purchasable hardware such as the software-defined radios has entered the market. This has given common people access to sophisticated radio manipulation tools and taken away the technical advantage that used to protect aviation communication. With the increasing aerial traffic, this has raised the question of whether CPDLC, a system that has not been designed considering security, can withstand the security risks today.
1.2 Aim

The purpose of this thesis is to investigate how secure CPDLC is. This will be determined by looking at how the standard is used, and whether data sent using this technology can be captured using a RTL-SDR dongle, freeware, and open source software. In the thesis this setup is referred to as a RTL-SDR setup. The captured data will be analyzed in an attempt to identify messages and processes in the CPDLC standard that could be used in attacks against the technology.

1.3 Research questions

This thesis will cover the following research questions:

- What kind of sensitive information can be acquired from capturing and decoding CPDLC communication?
- How could this information be utilized in attacks against CPDLC?

1.4 Delimitations

This thesis focuses on demonstrating how secure CPDLC is by proving whether data can be captured using a Realtek-Software Defined Radio (RTL-SDR) of model R820T2 RTL2832U with limited capabilities in terms of range and reception. The tests described in the thesis are proof of concept and are for this reason limited in the number of attempts and locations. Of the two CPDLC implementations ATN-B1 and FANS 1/A, ATN-B1 is looked at in this thesis whereas FANS 1/A has been excluded. This is a deliberate decision, since tests will take place in Sweden, where ATN-B1 is used exclusively. In the thesis, possible attacks that could be performed on CPDLC are proposed but without suggesting how this would be done in reality which would encourage something illegal.

1.5 Related work

The security in the CPDLC standard has been questioned by several researchers and there is some consensus on that the security is insufficient. In [14] Stromheimer accentuates the lack of security in most systems used in aviation communication, CPDLC included. Di Marco et al. investigated the possibility of carrying out injection and manipulation attacks on CPDLC in [8], where they simulated attacks in a controlled environment, using free and open source software. By showing that it is possible to perform attacks on CPDLC, their work demonstrated that the standard is insecure. The insecure state of CPDLC is further investigated by Wernberg in [19]. Wernberg identifies threats, possible attacks and ways of mitigating these. In [4] Gurtov et al. expands on Wernbergs work and discusses how improvements in CPDLC security are constrained by how the standard is put together.
2 Theory

This chapter presents technical information about the CPDLC standard and technologies related to it. It gives an overview of where CPDLC is implemented in Europe and explains the practical aspects of CPDLC communication.

2.1 Controller–pilot data link communications (CPDLC)

The primary means of communication between ATC and aircraft is voice-communication over VHF, which is an analogue technology and is limited to a number of frequencies. Since voice communication always has a risk of misunderstandings, e.g., from pronunciation differences, the high level of usage together with the limited frequency band and necessity of reliable communication led to the introduction of the CPDLC standard. CPDLC is a message-based Air Traffic Network (ATN) between aircraft and Air Traffic Services Unit (ATSU). The aircraft and ATC send predefined messages (e.g., clearances and requests) using terminals, which could be compared to sending SMS with cellphones. As with SMS, CPDLC is primarily used for non-critical communication. Examples also exist where human error has been removed altogether by automating clearance and start-up CPDLC messages. The introduction of CPDLC has reduced traffic on the VHF voice band and has thereby also reduced the miscommunications due to speech misunderstandings. Even though CPDLC is intended to use predefined messages, the terminals have the capability to send messages that are formulated in free text. In addition, CPDLC features accountability by logging messages that are exchanged. [14]
2.1. Controller–pilot data link communications (CPDLC)

Implementation

Most of the airspace in Europe is controlled by the organization Eurocontrol. The international organization has 41 member states, with the majority being European countries. Besides these, there are also several partner organization with which there are agreements about the airspace [2]. These include the European Union Commission which constituted a regulation saying that all air traffic services within the union should support CPDLC by February 7th, 2013 [18]. The guideline for CPDLC usage is to use it for all non-critical communication and to revert to voice when it cannot be used [9].

Figure 2.1 shows the status of implementation in Europe by July 2017. However, we can see a distinct increase just a year later, as seen in Figure 2.2. By February 5th, 2020, supporting CPDLC becomes mandatory for General Air Traffic (GAT) flights above Flight Level (FL) 285, affecting aircraft flying at high altitude [18]. FL is defined as "A surface of constant atmospheric pressure which is related to a specific pressure datum, 1 013.2 hectopascals (hPa), and is separated from other such surfaces by specific pressure intervals." [9] and 285 refers to one such interval.

In both Figure 2.1 and Figure 2.2 it can be seen that CPDLC has been implemented and is fully operational in Sweden. There are two ATSUs for sending and receiving, one located in Malmö and one in Stockholm. Malmö has the ATN address ESMM and Stockholm ESOS [7]. The ATN addresses are used in the CPDLC procedures explained in Section 2.2.

![Figure 2.1: CPDLC implementation July 2017 (Eurocontrol, 2017)](image-url)
2.1. Controller–pilot data link communications (CPDLC)

Very High Frequency (VHF) Digital Link (VDL) Mode 2 (VDL2)

Very High Frequency (VHF) Digital Link (VDL) Mode 2 (VDL2) is an air interface with the means of sending information between ATC and aircraft. The architecture is specified in the Standards and Recommended Practices (SARPS) by the International Civil Aviation Organization (ICAO). It works on frequency 118.00 to 136.975 MHz and a data rate of 31.5 kilobits/sec [4]. VDL2 uses the three lower layers of the OSI model, as seen in Figure 2.3.

- Layer 1 - Physical Layer
- Layer 2 - Data Link Layer
- Layer 3 - Network Layer

The first layer handles the frequency control, bit exchanges and radio modulation. It also eases the data encoding with interleaving and Reed-Solomon coding, also called Forward Error Correction (FEC). The interface uses the modulation technique called Eight-Ary Differential Phase Shifting Keying (D8PSK) with an excess bandwidth filter and a raised cosine filter. The input data is transmitted using the Gray Coding method, in which the data is differentiated by splitting it into groups of 3 bits. It puts the least significant bit first while padding the end of the transmission with zeroes if needed [4]. Since the Gray Coding method only carries the risk of single bit errors, this protects transmitted data from errors caused by noise. Every transmission contains a FEC header and a training sequence to allow for synchronization to be made. With the Reed-Solomon coding, the correction of 1-bit errors is covered but also corrects around 25% of possible 2-bit errors [5].

The data link layers responsibility is primarily transferring data between network entities via services working with frames, such as assembling, dissembling, and synchronization but also choosing radio frequency channels. In this layer, there are three sub-layers: Media Access Control (MAC), Link Management Entity (LME) and Data Link Service (DLS).
2.2. Procedures

This section describes the two key procedures in CPDLC communication, which are logon and handover between ATSUs, as well as how messages are formatted. Figure 2.4 depicts a generic CPDLC communication flow with the procedures explained in this section.

Initial logon request

An initial logon request (CMLogonRequest) is used in multiple instances of CPDLC procedures. The simplest being the aircraft preparing for departure, in which the aircraft remain stationary. Other reasons to make a logon request includes an aircraft in motion, either an aircraft entering an area that supports data link services from an area where no such support exists or by the instruction by ATC in case of a failed data link transfer. To be able to set up a
2.2. Procedures

Figure 2.4: Example of communication in a CPDLC connection (GOLD, 2013)

For an initial logon request (CMLogonRequest) to be made, the flight crew has to enter a four-character identifier code, representing the ATSU to which the logon request is to be sent, including the following information:

- **Aircraft identification** (Item 7 in Figure 2.5) and aircraftFlightIdentification in a CPDLC message, is a group of figures, letters or a combination of them which is the same as the aircraft call sign that is to be used in air-ground communications as well as to identify the aircraft in ground-ground air traffic services communication.

- **Aircraft registration and/or aircraft address** (Item 18, preceded by REG and/or CODE of Figure 2.5) is an identification assigned by the State of Registry to identify different aircraft. It consist of a group of letters, figures or a combination of them. This aircraft address is contained in the cMLongTSAP of a CMLogonRequest. cMLongTSAP is a string of 18 or 19 octets with three being the aircraft address.

- **Departure and destination aerodromes** (Item 13 and 16 of Figure 2.5) is a group of four characters identifying departure and destination airports. In CPDLC format these are airportDeparture and airportDestination.

It is paramount that the flight crew ensure that the information entered into the aircraft system is equivalent to the details in the flight plan of the aircraft. When the logon request is being performed by the flight crew, the logon information is being transmitted to the specified ATSU in a logon request message as seen in Table 2.1 [9]
Logon response

When the ground system receives a logon request it automatically responds with a logon response message as seen in Table 2.1. The message contains whether the logon request was successful or not. A logon request is denied by the ATSU if:

- There is no flight plan for the flight.
- The aircraft registration/address does not match the aircraft registration/address in the logon request message.

The message also contains information about the ATS data link applications that the ATSU supports. [9]

Active and inactive Connection

When discussing CPDLC connections, active and inactive connections are two central concepts. A CPDLC connection is either active or inactive depending on whether it is designated for communication or not. Where an ATSU and an aircraft uses the CPDLC connection to communicate, the connection is referred to as an active connection and the ATSU becomes the Current Data Authority (CDA), i.e. the ground system through which the CPDLC dialogue is authorized to take place. A CPDLC connection that is not used for communicating is referred to as an inactive connection and the ATSU is then referred to as Next Data Authority (NDA). [9]
### Table 2.1: Air-ground data link messages for DLIC (GOLD, 2013)

<table>
<thead>
<tr>
<th>Generic Message Name</th>
<th>Purpose</th>
<th>ATN B1 Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Air-ground logon procedure</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logon request</td>
<td>Used to confirm the identity of the aircraft and its data link capabilities, as well as notifying the ATSU about the flight crew’s intention to use data link services.</td>
<td>CM_LOGON_REQUEST</td>
</tr>
<tr>
<td>Logon Response</td>
<td>A reply to the aircraft containing the status of its logon request.</td>
<td>CM_LOGON_RESPONSE</td>
</tr>
<tr>
<td><strong>Air-ground address forwarding procedure</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact Request</td>
<td>To instruct the aircraft to send a logon request to the specified ATSU.</td>
<td>CM_CONTACT_REQUEST</td>
</tr>
<tr>
<td>Contact Complete</td>
<td>To provide the initiating ATSU with the status of the logon request sent to the specified ATSU.</td>
<td>CM_CONTACT_RESPONSE</td>
</tr>
</tbody>
</table>

### Establishing Connection

After an ATSU has successfully correlated an aircraft with an associated flight plan and the aircraft is logged on, a CPDLC connection can be established. An active CPDLC connection can be established if there is no existing connection to an aircraft whereas an inactive connection can be established if there is a previous connection. This is illustrated in Figure 2.4 before the first Exchange of CPDLC messages.

How a CPDLC connection is established depends on whether there is a connection or not, in other words, if an active or inactive CPDLC connection is to be established. To establish an active or inactive CPDLC connection, an ATSU sends a connection request to the aircraft. The recipient aircraft can then establish an active or inactive CPDLC connection by setting the requested connection as active or inactive. For an inactive CPDLC connection, an aircraft also verifies that the sender ATSU is specified as NDA. Lastly, an aircraft responds with a CPDLC connection confirmation. An aircraft also has the possibility to reject a CPDLC connection by sending a connection reject message. [9]

### Address forwarding

When an aircraft is leaving an area that the ATSU controls, the ATSU can forward the air-ground address and instruct the aircraft to initiate a logon request to another ATSU. This is done automatically by the ATSU, without the involvement of the flight crew. The CDA usually initiates the forwarding to permit a downstream or adjacent ATSU to establish an inactive CPDLC connection. The forwarding is done by sending a contact request message. When received, the aircraft automatically sends a logon request to the next ATSU using the address specified in the contact request message. If the forwarding is successful, the initiating ATSU also receives a contact complete message. The forwarding procedure can, if functionality allows, also be done between two ATSUs. The information sent in this case is the same as within air-ground address forwarding. [9]

### Transferring connection

Since aircraft are not stationary and VDL2 has a limited transmission range, CPDLC connections need to be transferred between ATSUs. In Figure 2.4 this process is illustrated, begin-
2.2. Procedures

Figure 2.6: Connection forwarding (GOLD, 2013)

ning after the first Exchange of CPDLC messages. This is managed by the ATSUs to ensure that the ATSU with control over an aircraft has an active connection. By transferring an active CPDLC connection, control is transferred between ATSUs, as seen in Figure 2.6. A transfer is initiated by the CDA which sends a NDA message containing the identity of the ATSU that is to be transferred to. The CDA then initiates address forwarding with the ATSU that the aircraft is transferring to. When the aircraft is in the proximity of the ATSU it is transferring to, the CDA sends a CPDLC termination request terminating the active CPDLC connection to the aircraft. A termination request containing a CONTACT or MONITOR message element is replied to with a WILCO (Will Comply) message element to terminate a connection. The passive connection to the next ATSU is then changed to active and that ATSU becomes CDA.

Table 2.2: Precedence of responses (GOLD, 2013)

<table>
<thead>
<tr>
<th>Response type</th>
<th>Precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>W/U</td>
<td>1</td>
</tr>
<tr>
<td>A/N</td>
<td>2</td>
</tr>
<tr>
<td>R</td>
<td>3</td>
</tr>
<tr>
<td>Y</td>
<td>4</td>
</tr>
<tr>
<td>N</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 2.2: Precedence of responses (GOLD, 2013)

<table>
<thead>
<tr>
<th>CPDLC uplink messages</th>
<th>Response type</th>
<th>Precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>W/U</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>A/N</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Y</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CPDLC downlink messages</th>
<th>Response type</th>
<th>Precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>N</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

Message format

The messages sent in a CPDLC connection follow a specified format and consist of a number of message elements for message types, identification, responses, and ordering. The number of message elements are ranging from one to five, making it either a single or multi-element. Each message element is composed of a number of attributes. Currently, a type identifier
attribute and a response attribute is used but urgency and alert attributes also exist. The uplink and downlink message elements are prefixed as UM and DM respectively, followed by a number. The combinations are standardized and have predetermined meanings.

CPDLC messages also contain a response attribute that specifies if a response is required. In UM this attribute furthermore specifies what type of response that is required. Multi-element CPDLC messages can have multiple response types but are limited to a single response. The type of response is determined by precedence of response types Table 2.2 with higher giving priority.

Table 2.3: Example of CPDLC dialogue (GOLD, 2013)

<table>
<thead>
<tr>
<th>CPDLC message</th>
<th>MIN</th>
<th>MRN</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DM 6 REQUEST FL350</strong></td>
<td>8</td>
<td>0</td>
<td>MIN 8 is assigned for this message, the downlink request has not yet been responded to, hence the request is still open.</td>
</tr>
<tr>
<td><strong>UM 1 STANDBY</strong></td>
<td>12</td>
<td>8</td>
<td>The ground system assigns MIN 12 to the uplink. Since it is a response to previous downlink request, MRN is assigned 8 (MIN of the downlink request). UM 1 is not a closing message since it gives a standby, hence the downlink request is still open.</td>
</tr>
<tr>
<td><strong>UM 20 CLIMB TO FL350</strong></td>
<td>13</td>
<td>8</td>
<td>The ground system assigns MIN 13 to the uplink (increment by one from the previous uplink message). Since this is a response to the previous downlink request, the MRN is again assigned 8 (MIN of the downlink request).</td>
</tr>
<tr>
<td><strong>UM 129 REPORT MAINTAINING [level]</strong></td>
<td>13</td>
<td>8</td>
<td>The ground system assigns MIN 13 to the uplink (increment by one from the previous uplink message). Since this is a response to the previous downlink request, the MRN is again assigned 8 (MIN of the downlink request).</td>
</tr>
<tr>
<td><strong>DM 0 WILCO</strong></td>
<td>9</td>
<td>13</td>
<td>The aircraft system assigns MIN 9 to the downlink (increment by one from the previous downlink message). Since this is a response to the previous uplink request the MRN is assigned 13 (MIN of the uplink request). DM 0 is also a closure message, so the status of the uplink message is closed.</td>
</tr>
<tr>
<td><strong>DM 37 MAINTAINING FL350</strong></td>
<td>10</td>
<td></td>
<td>The aircraft system assigns MIN 10 to the downlink (increment by one from the previous downlink message). There is no MRN assignment since the associated uplink message is already closed by DM 0 in the previous response. This message does not require a response from the ground system.</td>
</tr>
</tbody>
</table>
2.2. Procedures

CPDLC uses two identification numbers and dialogues to relate CPDLC messages. Every UM and DM is assigned a Message Identification Number (MIN) that is used to identify individual CPDLC messages. The number is an integer within 0-63 that is incremented independently for up- and downlink messages. CPDLC messages related to each other are grouped into dialogues where messages are referenced in responses using Message Reference Numbers (MRN). In a dialogue, MRN of a response is the same as the MIN of the message it responds to. An example of this can be found in Table 2.3.

A CPDLC message is open if it requires but has not yet received a response. When a response has been received or no response is required the CPDLC message is closed. A CPDLC dialogue that has an open message is also open. In other cases than this, a dialogue is closed.

Security

CPDLC data is not encrypted but still not completely unprotected. In the current implementation of CPDLC, referred to as protected mode, a 32-bit Cyclic Redundancy Check (CRC) called Application Message Integrity Check (AMIC) is used to ensure the integrity of the messages. [16]

Cyclic Redundancy Check (CRC)

CRC checks integrity by using checksums that are calculated by sending and receiving nodes using a predetermined algorithm. The sending node calculates it using known values and adds it to the data that is sent. Since the checksum does not change the data it is added to, it is said to add redundancy. The receiving node then performs a check, where the received checksum is compared to a checksum it has calculated, using known values. If the received checksum and the one calculated by the receiving node are equal, the same parameters have been used in the calculations and the message data is unchanged. [11]

Application Message Integrity Check (AMIC)

AMIC, used in CPDLC protected mode, uses CRC to verify message delivery. This verifies that messages are sent to the correct recipient and sent by the intended sender. The locally known values used to calculate the AMIC checksums are a 24-bit ICAO address, Aircraft Flight ID and Ground Facility Designator (GFD). [12]

Attacks

The lack of security measures in CPDLC leaves it at risk of attacks exploiting the system. In [4] Gurtov et al. describes six types of attacks that CPDLC could be exposed to, briefly explained in the bullet points below:

- **Eavesdropping** is listening in on communication without being authorized to do so. Hardware to receive a signal and software to decode data are the only things required to eavesdrop and this type of attack is therefore regarded as very simple. There are no direct effects besides broken confidentiality caused by eavesdropping. Sensitive information could be extracted and be used to carry out more complex attacks.

- **Jamming** denies a user correct service. By filling a channel with noise the channel’s capacity is reduced and data sent to a receiver becomes incomprehensible.

- **Flooding** also denies a user correct service but does it by “flooding” a receiver with data. This overfills the user’s receiving queue and makes it unable for the user to timely handle incoming traffic.
• *Injection* is where unauthorized data is sent. The data is sent by an unauthorized source and injected into the network where it is delivered.

• *Masquerading* is impersonating an authorized user to gain privileges. Conducting a full conversation is possible if the masque remains undetected.

### 2.3 Aircraft Communications Addressing and Reporting System

*Aircraft Communication Addressing and Reporting System (ACARS)* is a digital data link system developed in the 1970s, used to send short and simple messages in communication to and from aircraft. The system has a known lack of security and uses a standardized solution and is as of now an available standard. [19]

### 2.4 Realtek-Software Defined Radio (RTL-SDR)

Realtek-Software Defined Radio, or RTL-SDR, is an affordable USB dongle that can be used as a computer-based radio scanner for receiving live radio signals in your area without the involvement of internet connection.

The software-defined radio technology is a solution to replace conventional hardware used in radio by building a software-based radio system with functional modules such as modulation, demodulation, signal generation, coding and link layer protocols. Since the technology changes an initial hardware problem into a software one, the architecture is highly adjustable and re-programmable. [13]
In this chapter, we will describe the method created and used to capture CPDLC data. The requisites for the method are explained and lastly, the method is evaluated.

3.1 Pre-study

Some key findings in the pre-study were frequencies used to transmit CPDLC data, software to decode it and where CPDLC is implemented. This formed the foundation of the research of the practical implementation of CPDLC. In this research, we found how CPDLC data can be captured using a RTL-SDR setup. An explanation of the implementation, containing the software used to decode CPDLC data can be found in Section 3.2. Since the decoder found able to decode CPDLC required Linux, a lightweight Linux operating system for ChromeOS named Crouton was installed on a Chromebook. This gave a lightweight solution that was sufficient to do the tasks necessary without expensive additional hardware.

When software necessary to capture and decode CPDLC data had been set up and information about which frequencies CPDLC uses on VDL2 had been gathered, we tested that it worked as intended. By going to the local airport (Linköping City Airport) we could verify that the setup could receive airplane data when in the proximity of approximately one kilometer of an airport. We did, however, learn that CPDLC is not used at smaller airports, such as Linköping City Airport. Subsequently, it was concluded that CPDLC is used at Arlanda, and the tests capturing CPDLC data was conducted there. This is explained in further detail in Section 3.2 about the implementation of the method.

3.2 Implementation

In our experiments, a setup consisting of a RTL-SDR dongle of model R820T2 RTL2832U, an antenna and a Chromebook running Crouton was used, as can be seen in Figure 3.1. As described in Section 2.4, a RTL-SDR is a light-weight, software-based radio solution with functional modules that can be used to receiving live radio signals. In our experiment, we used the community-created software dumpvdl2, created by Tomasz Lemiech. dumpvdl2 is a lightweight decoder that decodes VDL2 data sent on the VHF radio-band. It has originally been used to capture ACARS messages in applications such as PlanePlotter but has in recent time started supporting decoding of the CPDLC protocol.
3.2. Implementation

Installation and configuration

The installation of dumpvdl2 was done on the Crouton Linux extension for ChromeOS following the README file from Tomasz Lemiech GitHub project [6]. The necessary dependencies for dumpvdl2 are the following:

- gcc
- make
- cmake
- pkg-config
- git
- glib2
- libacars

Dependencies such as gcc, are already included in linux OS by standard, but some has to be added manually. We add required dependencies for cmake and pkg-config using:

```bash
$ sudo apt-get install build-essential cmake git libglib2.0-dev pkg-config
```

Another necessary dependency is libacars, which also has to be manually installed. We can do this by cloning the project from GitHub, compile and build it:
3.2. Implementation

When all dependencies have been installed, we go on to install dumpvdl2 by cloning the project from GitHub and configuring the build using:

$ cd
$ git clone https://github.com/szpajder/dumpvdl2.git
$ cd dumpvdl2
$ mkdir build
$ cd build
$ cmake ../

After making the configuration, the process will display a message with a short configuration summary using:

-- dumpvdl2 configuration summary:
-- - SDR drivers:
-- - librtlsdr: requested: ON enabled: TRUE
-- - mirisdr: requested: ON enabled: TRUE
-- - sdrplay: requested: ON enabled: FALSE
-- - soapysdr: requested: ON enabled: TRUE
-- - Other options:
-- - Etsy StatsD: requested: ON enabled: FALSE
-- Configuring done

After the configuration is complete, we can compile and install the program using:

$ make
$ sudo make install

The last install-command will install a binary named dumpvdl2 in the default directory, /usr/local/bin on Linux. By using the following command we can display a list of available command line options.

$ /usr/local/bin/dumpvdl2 --help
3.3 Evaluation

Usage

The tests using dumpvd2 was, as described in Section 3.1, conducted at Stockholm Arlanda Airport. The antenna was placed within a kilometer of the ATC and dumpvd2 was started, collecting and decoding radio traffic on frequencies 136,725, 136,975, 136,955, 136,775 and 136,975 MHz. The test lasted one hour, divided in 10-minute intervals, and the decoded data was saved into text-files as plain text using the command:

```bash
$ dumpvd2 --rtlsdr 0 --output-file <'name of output-file'>
--raw-frames --gain 48 136725000 136975000 136955000 136775000 136975000
```

3.3 Evaluation

The method we have presented should, given the prescribed requisites, successfully capture and decode CPDLC. The software used in our tests are publically available and easily accessible, which promotes the replicability of our tests. Since the results of our tests would classify as qualitative, the length of the test could have been shorter, but the intention was to have enough data collected to be able to continue our work without having to redo the test.
This chapter presents the results achieved from investigating the usage of CPDLC and from the tests to capture CPDLC data.

4.1 CPDLC elements

The results obtained from the tests made at Stockholm Arlanda Airport are presented in Appendix A. In total one hour of traffic was captured corresponding to logs with over 65 thousand lines of data. In Figure 4.2 we present a comparison of the number of ACARS and CPDLC messages sent during the tests. The output logs are therefore a selection from the tests, exemplifying sequences relevant to the aim of this thesis. The logs present the CPDLC messages that could be filtered out between a ground station and aircraft with addresses 119AAA and 47BB0A respectively. The logs also show that the Aircraft Identification is SAS571, which correlates with the scheduled flight between Stockholm Arlanda Airport (ARN) and Paris Charles de Gaulle Airport (CDG) [3]. In Figure 4.1 and Table 4.1 details for the tracked flight are presented.

Figure 4.1: Aircraft details for tracked flight between Stockholm Arlanda (ARN) and Paris Charles de Gaulle (CDG) (Flightradar24, 2019)
4.1. CPDLC elements

Table 4.1: Flight details for tracked flight between Stockholm Arlanda (ARN) and Paris Charles de Gaulle (CDG) (Flightradar24, 2019)

<table>
<thead>
<tr>
<th>Date</th>
<th>From</th>
<th>To</th>
<th>Flight ID</th>
<th>Departure</th>
<th>Arrival</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 5th 2019</td>
<td>Stockholm (ARN)</td>
<td>Paris (CDG)</td>
<td>SK571</td>
<td>09:00 UTC</td>
<td>11:17 UTC</td>
</tr>
</tbody>
</table>

Figure 4.2: ACARS and CPDLC data traffic

The logs in Appendix A.1 contain elements used in CPDLC processes that have been explained in Chapter 2. Which parts of the logs that correspond to certain elements in CPDLC processes will be presented in this Section. The analysis of the found messages can be found in Chapter 5.

Logon

Lines 1-95 in Appendix A.1 show how a logon sequence of a CPDLC connection is established. The CMLogonRequest made by the aircraft can be seen on lines 11-35. It is evident that this is a logon request since it contains the information required for an initial logon request, as explained in Section 2.1. In the message, we can see that the field aircraftFlightIdentification correlates with the mandatory request parameter Aircraft identification. In the same way can aRS, which is the Aircraft address, be found in the log (line 27). Lastly, the parameter Departure and Destination aerodromes can be found under fields airportDeparture and airportDestination (line 33-34). This is further verified by the filtered and reformatted version of the message (line 36-47) which is generated by the decoding software.

The request is replied to with CMLogonResponse. This is however followed by an exact replica of the CMLogonResponse. The reason for this double transmission of the response is unknown but could be a re-transmission, a consequence of transmission data loss.

Message format

These two (three, counting the re-transmission of the response) messages complete the logon, and all remaining messages following these will be CPDLC messages, following a certain
format. Every message will contain two fields, header, and messageData. header contains, as the name suggests, fields with the information about the message. It holds the following fields:

- messageIdNumber and messageRefNumber: correlates with MIN and MRN respectively, as explained in Section 2.2.
- dateTime: gives the exact date and time of when the message was sent (given in the UTC-timezone).
- logicalAck: tells the recipient of the message if a logical acknowledgement is required.

messageData contains the actual message, and can either be a standard UM/DM message (as described in Section 2.2) or free text.

Establishing a connection

The first downlink message, identified by having identification number 0 (line 97-136), is sent by the aircraft to establish a CPDLC connection. Since there is no current connection the aircraft wants to establish an active connection. The message data of the message is dM99, which correlates to the command CURRENT DATA AUTHORITY. We can also see that the message specifies that a logical acknowledgement is required. This is the request sent by the aircraft to establish the CPDLC connection. The following uplink message (line 140-181) contains the logical acknowledgement that is requested. The message has message id 1 but more importantly, we can see that the message reference is 0 which shows that the acknowledgement is an answer to the previous message asking to establish a CPDLC connection. The ATC unit then follows this up with another message (line 185-226), with message-id 2, that has the message data UM183, which correlates to the command FREE TEXT and contains information about itself. From this, we can in plain-text read that the current ATC unit has the data-link address ESOS, which is address to Stockholm Arlanda Airport ATC unit.

Connection transfer

Directly following the logon and establishing a connection, the CDA initiates a connection transfer by sending a message (line 230-270) containing message data UM160, which correlates to NEXT DATA AUTHORITY. It also contains the data-link address for the NDA ESMM, which is the address to Malmö Airport ATC unit. The aircraft responds to this, as well as the previous message sent by the CDA with two logical acknowledgements. The CDA then proceeds by initiating termination of the connection by sending a message (line 364-413) containing UM117, correlating to the command CONTACT. The message also contains information about the NDA as well as the frequency on which to make the request.

The aircraft replies to this message with an acknowledgement to confirm that the message has been received and proceeds by sending a response to the request. The response (line 464-505) contains message data DM0, which correlates to the command WILCO, telling the CDA that the CONTACT request has been acknowledged. This response also confirms the termination of the current connection to the CDA that the request was initiating.

Following the termination of the connection, the aircraft is once again sending out a message (line 509-548) containing the message data DM99, asking for the CDA. The (new) CDA responds with a logical acknowledgement to confirm that the request has been received and that the connection has been established. It then replies with a message (line 597-638) containing the message data UM183 (FREE TEXT). The message data also contains information about itself, which now shows that the ATC unit has the data-link address ESMM (Malmö).
4.2 Flight position

Instructions

Once the new connection has been established the new CDA sends a message (line 689-754) with the message data containing UM74, which correlates to the command PROCEED DIRECT TO, followed by the reference point DEMIR and coordinates given in latitude and longitude. The message is acknowledged by the aircraft but no response to the request could be captured.

4.2 Flight position

Using data from Flightradar24 [3], that was imported into Google Earth, Figure 4.3 was created. This shows the part of the flight route between Stockholm Arlanda and Linköping Airport, where the messages in the CPDLC procedures in Section 4.1 were sent. The time-stamps in the figure are those closest to when the messages in the identified procedures were sent. By comparing these time-stamps with those in the logs in Appendix A.1 the approximate locations of the aircraft can be determined.

The first time-stamp in the figure shows that the logon procedure took place shortly after take-off, whilst the aircraft was still in close proximity to Arlanda Airport. Around the time when flight control was handed over, the aircraft was about midway between Arlanda and Strängnäs. Finally, the instruction containing directions to the aircraft, was sent when the aircraft was in proximity of Linköping Airport.

Figure 4.3: Flight path of the tracked flight with time-stamps when messages were sent (Flightradar24, 2019)
5 Discussion

In this Chapter we will discuss the method and the results from the tests. The discussion of the method can be found in Section 5.1 and the results are discussed in Section 5.2.

5.1 Method

In the method used, traffic was captured in intervals of 10 minutes and repeated six times. The reasoning behind this was to make the recorded logs smaller and more manageable. Another reason was that we were unsure of how rapidly the amount of data would add up in the test and came to the conclusion that 10-minute intervals was the best approach. This made it possible for us to continuously check the logs while capturing more data. The disadvantage of this approach was that we got discontinuation between the intervals where messages might have been lost. In hindsight, the tests could have been recorded in a single file, which would have removed the risk of losing messages in the downtime of the test.

Since a third-party application was used to capture and decode the data, there is an uncertainty in validity of the results. In addition, the decoder that was used seems to be the only open-source application that is available for SDRs as of now, which deny us the opportunity to compare the results with another method.

In terms of replicability, the tests performed are easily repeated. The hardware used is cheap and easily acquired and the software open-source and available online. The only limitation in replicability of the tests is the necessity of being in proximity of an airport that supports CPDLC.

5.2 Results

In this section we will discuss our results in terms of what the usage of CPDLC is like and the security of the standard by looking at its CIA (confidentiality, integrity and availability). This is then used to discuss attacks on CPDLC.
5.2. Results

CPDLC usage

Even though there was legislation saying that all air traffic services within the European Union should use CPDLC by 2013, not all member nations have currently implemented it. It is however apparent that the implementation of this is progressing, looking at the increase in implementation made in several countries from 2017 to 2018. This also coincides with the use of CPDLC becoming mandatory for GAT flights above FL 285 by 2020. In Sweden, where the tests for this thesis were conducted, CPDLC is fully operational but only broadcasted from Stockholm and Malmö. The immediate switch from Stockholm to Malmö by the aircraft analyzed in Chapter 4 indicate that these stations together provide the entire country with CPDLC coverage. It would therefore also be reasonable to say that the same applies to other countries where CPDLC is implemented.

CIA in CPDLC

By looking at the implementation of security in CPDLC, we can discuss weaknesses in the system in perspective of confidentiality, integrity and availability (CIA).

- **Confidentiality:** Since CPDLC does not utilize encryption of data, messages that are sent are unprotected. AMIC offers protection against noise but does not prevent data from being captured, decoded and read. This leaves information exchanged in CPDLC open to anyone with equipment to capture and decode CPDLC data. As presented in Chapter 2 CPDLC processes contains several instances of sensitive information that could be considered confidential. In this case, the classification of what information is confidential and not depends on how the data can be used. Information that can be used to gain access to a data link between an aircraft and ATC creates a gateway where attacks with more severe consequences could be performed. Data with that kind of information could therefore be classified as confidential. In spite of confidential CPDLC data not being protected, real-life attacks exploiting this have not been recorded. This argues that the data does not have to be protected but does not imply that the standard is secure in terms of confidentiality.

- **Integrity:** CPDLC does to some extent provide protection towards the integrity of its data, with the implementation of CRC technology in AMIC. However, the technology only corrects errors upon delivery of the information and secures the communication against noise. There is currently no way of ensuring the authenticity nor integrity of a message, and information manipulation can go unnoticed if done properly. Instead, the validation of a message lies in the human vigilance, which could easily be surpassed if the information appears legitimate. For information to be considered false, it would therefore have to be in clear contradiction to the message’s original intention.

- **Availability:** In the event of an attack with the aim at causing damage on availability, such as jamming or flooding, there are no defense mechanisms implemented in CPDLC. Depending on the objective of the attack, the severity can vary. An attack targeting a single aircraft would be less severe than one targeting a ground station. A comparison to this could be made to attacks directed towards client and servers, where the consequences of attacks against clients usually are less severe than attacks against servers. Since the knowledge of how procedures within the aeronautical community are handled are transparent, the attack can be made more sophisticated by focusing the attack on certain weak spots of the procedures such as logon and termination of a connection.
5.2. Results

Attacks

The CPDLC elements we identified in Chapter 4 contains information that can be considered sensitive by affecting the confidentiality, integrity and availability of CPDLC and ultimately be used in attacks. If the attacks described in Section 2 are possible to perform on CPDLC and if so, how feasible they are.

- **Eavesdropping**: The results prove that it is possible to eavesdrop on CPDLC communication, given the right conditions. With the RTL-SDR setup and requisites described in Chapter 3, we captured CPDLC data at Stockholm Arlanda Airport. This demonstrated that CPDLC data can be captured using readily available hardware and software at a location accessible to the general public.

  We cannot make any real claim on how the implementation at Stockholm Arlanda airport relates to Malmö or airports in other European countries, but we can argue that they would follow a similar implementation. The fact that CPDLC is a standard implicates that how it is implemented should be the same or at least similar in different geographic regions, which further implicates that eavesdropping should be possible with the same type of RTL-SDR setup and requisites that we used in our tests. This gives an indication of the difficulty level of eavesdropping on CPDLC. As we managed to find all information required and create a functional RTL-SDR setup, with some trial and error, this can be considered moderately difficult. Since eavesdropping on CPDLC communication does not affect the communication, the consequences of this are modest and could be said to be in proportion to the difficulty of doing so. If information extracted from CPDLC by eavesdropping is combined it could however be used in attacks with more severe consequences.

- **Jamming/flooding**: In the results, we can see that certain CPDLC messages require logical acknowledgements as a response to verify that the request has been received. By jamming or flooding the communication medium, these types of responses could be interrupted causing the communication to slow down, which would counteract the intention of why CPDLC was introduced and has been implemented. Especially severe damage could be caused if the attack were to be directed towards a ground station rather than an aircraft, since blocking out communication from the ground station would impair communication to multiple rather than a single aircraft. If such an attack would be carried out in an airspace with high air traffic, the consequences could rise to be bigger than just an inconvenience. As CPDLC is a necessity to manage traffic loads today, it is questionable whether there is capacity in other aeronautical communication systems to handle the load.

- **Masquerading/Injection**: With CPDLC lacking encryption and with AMIC as its only implementation of security, the possibility of attacks as sophisticated as masquerading and injection increase significantly. As AMIC is a type of CRC, a hashing defense mechanism based on certain predetermined parameters, it is possible to compute the AMIC. The fact that we in our results see that we can find most of the parameters used in the AMIC algorithm as plain text, greatly increases the chance of a successful attack. If an attacker wanted to pose as a participant in the CPDLC communication, all that would be required would be to send a message requesting a logical acknowledgement. If the message is received and accepted by the recipient, and a logical acknowledgement was to be received by the attacker, the attacker would know that the AMIC sequence had been found. From here, the attacker could continue posing as either participant of the communication, possibly causing severe damage by giving false instructions. Even though this attack in theory is possible, the security lies in the vigilance of the participants of the communication. Any instruction with evil intent would realistically be detected if it deviates to much from the original plan. With that said, since actually
posing as either participant in the communication being feasible, an attack not deviating much from the original plan, hence not being detected, could still cause potential damage.
6 Conclusions and future work

6.1 Conclusion

The introduction of CPDLC, made to reduce the traffic load on VHF, has led to improvements in communication effectiveness. However, this has not come without complications. Prior to CPDLC, large airports using were congested due to the high usage of voice communication, something that CPDLC has relieved and made more reliable by minimizing misunderstandings and automating parts of the communication. As the results presented in this thesis show, the CPDLC standard lacks sufficient security measures to protect the data that is being sent over VDL2. The logon process and AMIC provide CPDLC with the means to verify the origin and integrity of data but does not protect the standard from external influence. Currently, CPDLC is implemented in most of the European Union and to be fully operational by the first quarter of 2020. Usage will, however, only be mandatory for GAT flight above FL 285.

By successfully capturing and decoding CPDLC data, we have proven that it is possible to eavesdrop on CPDLC. The data that we have captured and interpreted into the results, presented in Chapter 4, contains CPDLC elements with sensitive information that could be utilized to carry out attacks with severe consequences to air traffic. The consequences of these attacks would be especially noticeable at larger airports, that rely on CPDLC to handle the high communication traffic loads, but also to air traffic in general. If a jamming or flooding attack would target CPDLC, the communication might have to revert to voice, which could be speculated whether large airports are capable of handling today. If the function used to calculate hashes in AMIC is discovered, data could be injected into CPDLC communication. Masquerading, by infiltrating the logon process of CPDLC, could enable an attacker to gain ATC privileges to for example send instructions to aircraft. The attacks that have been described target each and every of confidentiality, integrity and availability in the CIA triad, arguing that CPDLC as of today is not secure.
6.2 Future work

Despite CPDLC being used widely today and is expected to increase in the years to come, there is relatively little research about the technology. This report has merely scratched the surface of what can be done within CPDLC and leaves room for future work. The price and availability of an aircraft CPDLC unit could be explored for simulating attacks in a closed environment. This would also include looking into hardware and software to transmit CPDLC data. As of now, software that captures and decode communication data is emerging. However, software to encode and send such data is yet to be seen.

The technology can also be approached with an ethical viewpoint, with communication secrecy laws and integrity laws such as GDPR in mind. With the introduction of software-defined radio, the availability of capturing sensitive radio communication has greatly increased. Is it however legal and ethically right to capture and use this data without permission?

Investigating the more technical aspects of CPDLC could provide further insights into what kind of attacks that could be performed. E.g. looking at the throughput of the Medium Access Control could be of interest when designing malicious software that focuses on subduing the availability of communication using CPDLC.


Appendix

A.1 CPDLC logs

[2019-04-05 11:04:37 CEST] [136.725] [0.1/-50.5 dBFS] [50.6 dB] [-1.0 ppm]

47BB0A (Aircraft, Airborne) -> 119AAA (Ground station): Command

1b ff 00 18 28 f6 00 00 10 0a f0 ef f0 80 08 04 1b df fa 43 e8 02 00 20
10 42 b1 b0 30 10 20 ac 6c 06 0a 7b d8 28 00 28 1a b1 34 a7 06 9b 56 ec
50 54 d0 54 c0 28 f7 61 40 00 05 34 14 14 20 00 00 10 10 01 60 02 0a 9a
0a 98 05 1e ec 28 00 00 a6 82 82 84 00 00 02 2d 16 9d 38 33 23 50 8e

AVLC type: I sseq: 5 rseq: 2 poll: 0

X.25 Data: grp: 11 chan: 255 sseq: 0 rseq: 0 more: 0

CLNP PDU, compressed header:

COTP Data:

cmLogonRequest: CMLogonRequest ::= {
  aircraftFlightIdentification: SAS571
  cMLongTsAP: LongTsap ::= {
    rDP: 41 53 41 53 00
    shortTsap: ShortTsap ::= {
      aRS: 47 BB 0A
      locSysNselTsel: 00 00 53 41 41 42 00 00 01 16
    }
  }
}

groundInitiatedApplications: GroundInitiatedApplications ::= {
  AEQualifierVersionAddress ::= {
    aeQualifier: 22
    apVersion: 1
    apAddress: longTsap: LongTsap ::= {
      rDP: 41 53 41 53 00
      shortTsap: ShortTsap ::= {
        aRS: 47 BB 0A
        locSysNselTsel: 00 00 53 41 41 42 00 00 01 16
      }
    }
  }
  airportDeparture: ESSA
  airportDestination: LFPG
}
A.1. CPDL logs

ATN Context Management - Logon Request:
Flight ID: SAS571
Long TSAP: 41 53 41 53 00 47 bb 0a 00 00 53 41 41 42 00 00 01 01
"ASAS.G....SAAB...."

Ground-initiated applications:
Application Entity Qualifier: 22
Version number: 1
AP Address:
Long TSAP: 41 53 41 53 00 47 bb 0a 00 00 53 41 41 42 00 00 01 16
"ASAS.G....SAAB...."
Departure airport: ESSA
Destination airport: LFPG

[2019-04-05 11:04:38 CEST] [136.725] [-28.3/-50.9 dBFS] [22.7 dB] [-0.4 ppm]
119AAA (Ground station, On ground) -> 47BB0A (Aircraft): Command
1b ff 22 38 5e c0 00 c4 eb 0a f0 00 32 80 08 04 1d 75 93 af e2 02 10 01 04
2b 1b 03 01 20 84 3c 08 00 b0 00
AVLC type: I sseq: 3 rseq: 6 poll: 0
X.25 Data: grp: 11 chan: 255 sseq: 1 rseq: 1 more: 0
CLNP PDU, compressed header:
COTP Data:
cmLogonResponse: CMLogonResponse ::= {
  groundOnlyInitiatedApplications: GroundOnlyInitiatedApplications ::= {
    AEQualifierVersion ::= {
      aeQualifier: 22
      apVersion: 1
    }
  }
}

ATN Context Management - Logon Response:
Ground-only-initiated applications:
Application Entity Qualifier: 22
Version number: 1

[2019-04-05 11:04:40 CEST] [136.725] [-28.7/-51.0 dBFS] [22.3 dB] [-0.4 ppm]
119AAA (Ground station, On ground) -> 47BB0A (Aircraft): Command
1b ff 22 38 5e c0 00 c4 eb 0a f0 00 32 80 08 04 1d 75 93 af e2 02 10 01 04
2b 1b 03 01 20 84 3c 08 00 b0 00
AVLC type: I sseq: 3 rseq: 6 poll: 0
X.25 Data: grp: 11 chan: 255 sseq: 1 rseq: 1 more: 0
CLNP PDU, compressed header:
COTP Data:
cmLogonResponse: CMLogonResponse ::= {
  groundOnlyInitiatedApplications: GroundOnlyInitiatedApplications ::= {
    AEQualifierVersion ::= {
      aeQualifier: 22
      apVersion: 1
    }
  }
}

ATN Context Management - Logon Response:
Ground-only-initiated applications:
Application Entity Qualifier: 22
Version number: 1

[2019-04-05 11:04:50 CEST] [136.725] [-28.7/-51.0 dBFS] [22.3 dB] [-0.4 ppm]
47BB0A (Aircraft, Airborne) -> 119AAA (Ground station): Command
A.1. CPDLC logs

```
1b ff c8 1b 28 f6 41 00 14 0d f0 f4 c9 80 00 00 00 08 04 69 9b 03 a4 00
a6 c6 4d 90 0b 99 12 25 c0 63 20 87 a1 c4 1e

AVLC type: I sseq: 1 rseq: 0 poll: 0
CLNP PDU, compressed header:
COTP Data:
```

```
ATCDownlinkMessage ::= {
  header: ATCMessageHeader ::= {
    messageIdNumber: 0
    dateTime: DateTimeGroup ::= {
      date: Date ::= {
        year: 2019
        month: 4
        day: 5
      } timehhmmss: Timehhmmss ::= {
        hoursminutes: Time ::= {
          hours: 9
          minutes: 4
        } seconds: 46
      } } logicalAck: 0
  } messageData: ATCDownlinkMessageData ::= {
    elementIds: ATCDownlinkMsgElementIdSequence ::= {
      dM99NULL: <present>
    } }
}

CPDLC Downlink Message:
Header:
Msg ID: 0
Timestamp: 2019-04-05 09:04:46
Logical ACK: required
Message data:
CURRENT DATA AUTHORITY

[2019-04-05 11:04:51 CEST] [136.725] [-27.6/-51.3 dBFS] [23.8 dB] [-0.3 ppm]
119AAA (Ground station, On ground) -> 47BB0A (Aircraft): Command
1b ff ae 3b 5e c0 41 c4 f0 0d f0 00 33 80 00 00 08 04 24 7c 8d e1 00 a7
AVLC type: I sseq: 1 rseq: 2 poll: 0
X.25 Data: grp: 11 chan: 255 sseq: 7 rseq: 5 more: 0
CLNP PDU, compressed header:
COTP Data:
```

```
ATCUplinkMessage ::= {
  header: ATCMessageHeader ::= {
    messageIdNumber: 1
    messageRefNumber: 0
    dateTime: DateTimeGroup ::= {
      date: Date ::= {
        year: 2019
        month: 4
        day: 5
      } timehhmmss: Timehhmmss ::= {
        hoursminutes: Time ::= {
          hours: 9
          minutes: 4
        } }
    } }
```

A.1. CPDLC logs

    } } } } }
    seconds: 48 } } logicalAck: 1
    } } messageData: ATCUplinkMessageData ::= {
      elementIds: ATCUplinkMsgElementIdSequence ::= {
        uM227NULL: <present>
      } } }
CPDLC Uplink Message:
    Header:
      Msg ID: 1
      Msg Ref: 0
      Timestamp: 2019-04-05 09:04:48
      Logical ACK: notRequired
      Message data:
        LOGICAL ACKNOWLEDGMENT
        - - - - - -
        [2019-04-05 11:04:52 CEST] [136.725] [-27.7/-50.9 dBFS] [23.2 dB] [-0.2 ppm]
        119AAA (Ground station, On ground) -> 478BB0A (Aircraft): Command
        1b ff c0 3b 5e c0 41 c4 f1 0d f0 00 33 80 00 00 01 08 04 38 9a 7d 5b 00 a8
        17 a3 30 27 68 45 cc 89 13 00 2d c8 e1 d5 a5 4a 2c ea 88 20 d4 86 82 ac e9
        35 10 45 a7 3e 9a ca 75 e2 c4 8b 39 64 39 f3 a5 52 9f 30 81 e6 f7 98 50
        AVLc type: I sseq: 2 rseq: 3 poll: 0
        X.25 Data: grp: 11 chan: 255 sseq: 0 rseq: 6 more: 0
        CLNP PDU, compressed header:
        CTP Data:
        ATCUplinkMessage ::= {
          header: ATCMessageHeader ::= {
            messageIdNumber: 2
            dateTime: DateTimeGroup ::= {
              date: Date ::= {
                year: 2019
                month: 4
                day: 5
              }
              timehhmmss: Timehhmmss ::= {
                hoursminutes: Time ::= {
                  hours: 9
                  minutes: 4
                }
              }
              seconds: 48
            }
            logicalAck: 0
          } } messageData: ATCUplinkMessageData ::= {
            elementIds: ATCUplinkMsgElementIdSequence ::= {
              uM183FreeText: CURRENT ATC UNIT ESOS, SWEDEN, CONTROL
            } } }
CPDLC Uplink Message:
    Header:
      Msg ID: 2
      Timestamp: 2019-04-05 09:04:48
      Logical ACK: required
      Message data:
A.1. CPDLC logs

Current ATC unit ESOS, Sweden, Control

- - - - - -

[2019-04-05 11:04:52 CEST] [136.725] [-28.0/-50.7 dBFS] [22.7 dB] [-0.2 ppm]

119AAA (Ground station, on ground) -> 47BB0A (Aircraft): Command

08 e3 2a e8 65 cc 89 13 10 28 22 2d 39 b3 48 0e a8 55 f0 80

AVLC type: I sseq: 3 rseq: 3 poll: 0

X.25 Data: grp: 11 chan: 255 sseq: 1 rseq: 6 more: 0

CLNP PDU, compressed header:

COTP Data:

ATC Uplink Message ::= {
    header: ATCMMessageHeader ::= {
        messageIdNumber: 3
        dateTime: DateTimeGroup ::= {
            date: Date ::= {
                year: 2019
                month: 4
                day: 5
            }
            timehhmmss: Timehhmmss ::= {
                hoursminutes: Time ::= {
                    hours: 9
                    minutes: 4
                }
                seconds: 49
            }
        }
        logicalAck: 0
    }
    messageData: ATC Uplink Message Data ::= {
        elementIds: ATC Uplink Message Element Id Sequence ::= {
            uM160Facility: facilityDesignation: ESMM
        }
    }
}

CPDLC Uplink Message:

Header:

Msg ID: 3
Timestamp: 2019-04-05 09:04:49
Logical ACK: required
Message data:

NEXT DATA AUTHORITY [facility]
Facility designation: ESMM

- - - - - -

[2019-04-05 11:04:53 CEST] [136.725] [0.3/-50.7 dBFS] [51.0 dB] [-1.2 ppm]

47BB0A (Aircraft, Airborne) -> 119AAA (Ground station): Command

a7 26 4f 30 42 2e 64 48 99 41 90 80 6f 59 55 fc

AVLC type: I sseq: 4 rseq: 4 poll: 0

X.25 Data: grp: 11 chan: 255 sseq: 7 rseq: 2 more: 0

CLNP PDU, compressed header:

COTP Data:

ATC Downlink Message ::= {
    header: ATCMMessageHeader ::= {
        messageIdNumber: 1
        messageRefNumber: 2
        dateTime: DateTimeGroup ::= {
            date: Date ::= {
        }
    }
}

36
CPDLC Downlink Message:

Header:
- Msg ID: 1
- Msg Ref: 2
- Timestamp: 2019-04-05 09:04:50
- Logical ACK: notRequired

Message data:
- LOGICAL ACKNOWLEDGMENT

[2019-04-05 11:04:53 CEST] [136.725] [-0.0/-51.1 dBFS] [51.0 dB] [-1.3 ppm]
47BB0A (Aircraft, Airborne) -> 119AAA (Ground station): Command
1b ff 40 1b 28 f6 41 00 18 0d f0 f4 c9 80 00 00 02 08 04 24 d3 db 3c 00 a7
26 4f 30 83 2e 64 48 99 41 90 83 78 b3 17 34
AVLC type: I sseq: 5 rseq: 4 poll: 0
X.25 Data: grp: 11 chan: 255 sseq: 0 rseq: 2 more: 0
CLNP PDU, compressed header:
COTP Data:

ATCDownlinkMessage ::= {
  header: ATCMessageHeader ::= {
    messageIdNumber: 2
    messageRefNumber: 3
    dateTime: DateTimeGroup ::= {
      date: Date ::= {
        year: 2019
        month: 4
        day: 5
      }
      timehhmmss: Timehhmmss ::= {
        hoursminutes: Time ::= {
          hours: 9
          minutes: 4
        }
        seconds: 50
      }
    }
    logicalAck: 1
  }
  messageData: ATCDownlinkMessageData ::= {
    elementIds: ATCDownlinkMsgElementIdSequence ::= {
      dM100NULL: <present>
    }
  }
}
A.1. CPDLC logs

CPDLC Downlink Message:

Header:

Msg ID: 2
Msg Ref: 3
Timestamp: 2019-04-05 09:04:50
Logical ACK: notRequired
Message data:

LOGICAL ACKNOWLEDGMENT

- - - - - -

[2019-04-05 11:07:03 CEST] [136.725] [-27.4/-50.9 dBFS] [23.5 dB] [-0.3 ppm]

119AAA (Ground station, On ground) -> 47BB0A (Aircraft): Command

0f a2 60 05 01 ae 66 02 61 10 b9 91 23 80 03 ac 45 a7 36 69 d3 af 16 24 59
c7 6f b0 81 52 ae 63 9c

AVLC type: I sseq: 7 rseq: 0 poll: 0
X.25 Data: grp: 11 chan: 255 sseq: 5 rseq: 3 more: 0

CLNP PDU, compressed header:

COTP Data:

ATCUplinkMessage ::= {
  header: ATCMMessageHeader ::= {
    messageIdNumber: 4
    date: DateTimeGroup ::= {
      date: Date ::= {
        year: 2019
        month: 4
        day: 5
      }
      time: TimeGroup ::= {
        hoursminutes: Time ::= {
          hours: 9
          minutes: 7
        }
        seconds: 0
      }
    }
    logicalAck: 0
  }
  messageData: ATCUplinkMessageData ::= {
    unitNameFrequency: UnitNameFrequency ::= {
      unitName: UnitName ::= {
        facilityDesignation: ESMM
        facilityName: SWEDEN
        facilityFunction: 7
      }
      frequency: frequencyvhf: 26652
    }
  }
}

CPDLC Uplink Message:

Header:

Msg ID: 4
Timestamp: 2019-04-05 09:07:00
Logical ACK: required
Message data:

CONTACT [unitname] [frequency]
Unit name: ESMM, SWEDEN, control
VHF: 133.260 MHz
A.1. CPDL logs

[2019-04-05 11:07:04 CEST] [136.725] [-23.4/-51.0 dBFS] [27.6 dB] [-1.6 ppm]

47BB0A (Aircraft, Airborne) -> 119AAA (Ground station): Command
1b ff c6 1b 28 f6 41 00 1b 0f 60 f4 c9 00 00 00 04 00 03 08 04 02 5f 59 46
0d f0 f4 c9 80 00 00 03 08 04 00 36 5c dc 00 a7 26 4f 30 c4 2e 64 48 e0 c1
90 82 9e 97 fc c0
AVLC type: I sseq: 0 rseq: 0 poll: 0

X.25 Data: grp: 11 chan: 255 sseq: 3 rseq: 6 more: 0
CLNP PDU, compressed header:
COTP Data Acknowledgement:
COTP Data:
ATCDownlinkMessage ::= {
  header: ATCMessageHeader ::= {
    messageIdNumber: 3
    messageRefNumber: 4
    dateTime: DateTimeGroup ::= {
      date: Date ::= {
        year: 2019
        month: 4
        day: 5
      }
      timehhmmss: Timehhmmss ::= {
        hoursminutes: Time ::= {
          hours: 9
          minutes: 7
        }
        seconds: 1
      }
    }
    logicalAck: 1
  }
  messageData: ATCDownlinkMessageData ::= {
    elementIds: ATCDownlinkMsgElementIdSequence ::= {
      dM100NULL: <present>
    }
  }
}

CPDLC Downlink Message:
Header:
  Msg ID: 3
  Msg Ref: 4
  Timestamp: 2019-04-05 09:07:01
  Logical ACK: notRequired
Message data:
LOGICAL ACKNOWLEDGMENT

[2019-04-05 11:07:11 CEST] [136.725] [-23.1/-51.1 dBFS] [28.0 dB] [-1.7 ppm]

47BB0A (Aircraft, Airborne) -> 119AAA (Ground station): Command
1b ff e8 1b 28 f6 41 00 1c 0d f0 f4 c9 80 00 00 04 08 04 aa f4 4b f2 00 28
08 d3 60 04 e4 c9 e6 20 85 cc 89 1c 78 00 10 74 3c 7b 77 00
AVLC type: I sseq: 1 rseq: 1 poll: 0
X.25 Data: grp: 11 chan: 255 sseq: 4 rseq: 7 more: 0
CLNP PDU, compressed header:
COTP Data:
ATCDownlinkMessage ::= {
  header: ATCMessageHeader ::= {
    messageIdNumber: 4
    messageRefNumber: 4
    dateTime: DateTimeGroup ::= {

39
A.1. CPDLC logs

```plaintext
477    date: Date ::= {
478        year: 2019
479        month: 4
480        day: 5
481    }
482    timehhmmss: Timehhmmss ::= {
483        hoursminutes: Time ::= {
484            hours: 9
485            minutes: 7
486        }
487        seconds: 7
488    }
489    logicalAck: 1
490  }
491  }
492  messageData: ATCDownlinkMessageData ::= {
493      elementIds: ATCDownlinkMsgElementIdSequence ::= {
494          dM0NULL: <present>
495      }
496  }
497  }
498  CPDLC Downlink Message:
499  Header:
500      Msg ID: 4
501      Msg Ref: 4
502      Timestamp: 2019-04-05 09:07:07
503      Logical ACK: notRequired
504  Message data:
505      WILCO
506  - - - - - -
507  [2019-04-05 11:07:39 CEST] [136.725] [-25.0/-50.9 dBFS] [25.9 dB] [-1.5 ppm]
508  47BB0A (Aircraft, Airborne) -> 119AAA (Ground station): Command
509  1b ff 8e 1b 28 f6 42 00 1f 0d f0 eb 3f 80 00 00 00 08 04 ce de 46 3c 00 a6
510  c6 4d 90 0b 99 12 3c 60 63 20 91 05 cf 07
511  AVLC type: I sseq: 4 rseq: 6 poll: 0
512  X.25 Data: grp: 11 chan: 255 sseq: 7 rseq: 4 more: 0
513  CLNP PDU, compressed header:
514  COTP Data:
515    ATCDownlinkMessage ::= {
516      header: ATCMessagesHeader ::= {
517        messageIdNumber: 0
518        dateTime: DateTimeGroup ::= {
519            date: Date ::= {
520                year: 2019
521                month: 4
522                day: 5
523            }
524            timehhmmss: Timehhmmss ::= {
525                hoursminutes: Time ::= {
526                    hours: 9
527                    minutes: 7
528                }
529            }
530        }
531        logicalAck: 0
532      }
533  messageData: ATCDownlinkMessageData ::= {
534      elementIds: ATCDownlinkMsgElementIdSequence ::= {
535          dM0NULL: <present>
536      }
537  }
538  }
539  }
```
A.1. CPDLC logs

540 }  
541 }  
542 CPDLC Downlink Message:  
543 Header:  
544 Msg ID: 0  
545 Timestamp: 2019-04-05 09:07:35  
546 Logical ACK: required  
547 Message data:  
548 CURRENT DATA AUTHORITY  
549  
550 [2019-04-05 11:07:40 CEST] [136.725] [-27.3/-50.6 dBFS] [23.3 dB] [-0.3 ppm]  
551 119AAA (Ground station, On ground) -> 47BB0A (Aircraft): Command  
552  
553 AVLC type: I sseq: 7 rseq: 5 poll: 0  
554 X.25 Data: grp: 11 chan: 255 sseq: 5 rseq: 0 more: 0  
555 CLNP PDU, compressed header:  
556 COTP Data:  
557 ATCUplinkMessage ::= {  
558   header: ATCMessageHeader ::= {  
559     messageIdNumber: 1  
560     messageRefNumber: 0  
561     dateTime: DateTimeGroup ::= {  
562       date: Date ::= {  
563         year: 2019  
564         month: 4  
565         day: 5  
566       }  
567       timehhmmss: Timehhmmss ::= {  
568         hoursminutes: Time ::= {  
569           hours: 9  
570           minutes: 7  
571         }  
572         seconds: 37  
573       }  
574     logicalAck: 1  
575   }  
576   messageData: ATCUplinkMessageData ::= {  
577     elementIds: ATCUplinkMsgElementIdSequence ::= {  
578       uM227NULL: <present>  
579     }  
580   }  
581 }  
582 CPDLC Uplink Message:  
583 Header:  
584 Msg ID: 1  
585 Msg Ref: 0  
586 Timestamp: 2019-04-05 09:07:37  
587 Logical ACK: notRequired  
588 Message data:  
589 LOGICAL ACKNOWLEDGMENT  
590  
591 [2019-04-05 11:07:41 CEST] [136.725] [-27.7/-51.2 dBFS] [23.6 dB] [-0.1 ppm]  
592 119AAA (Ground station, On ground) -> 47BB0A (Aircraft): Command  
593  
594 AVLC type: I sseq: 0 rseq: 6 poll: 0  
595
A.1. CPDLC logs

X.25 Data: grp: 11 chan: 255 sseq: 6 rseq: 1 more: 0

CLNP PDU, compressed header:

COTP Data:

ATCuplinkMessage ::= {
  header: ATCMessageHeader ::= {
    messageIdNumber: 2
    dateTime: DateTimeGroup ::= {
      date: Date ::= {
        year: 2019
        month: 4
        day: 5
      }
      timehhmmss: Timehhmmss ::= {
        hoursminutes: Time ::= {
          hours: 9
          minutes: 7
        }
        seconds: 37
      }
    }
    logicalAck: 0
  }
  messageData: ATCuplinkMessageData ::= {
    elementIds: ATCuplinkMsgElementIdSequence ::= {
      uM183FreeText: CURRENT ATC UNIT ESMM, SWEDEN, CONTROL
    }
  }
}

CPDLC Uplink Message:

Header:
Msg ID: 2
Timestamp: 2019-04-05 09:07:37
Logical ACK: required
Message data:
FREE TEXT
- - - - - -

[2019-04-05 11:07:42 CEST] [136.725] [-25.7/-51.1 dBFS] [25.4 dB] [-1.6 ppm]
47BB0A (Aircraft, Airborne) -> 119AAA (Ground station): Command
1b ff e2 1b 28 f6 42 00 21 0f 60 eb 3f 00 00 02 00 02 08 04 6f d6 cf b4
0d f0 eb 3f 80 00 00 01 08 04 f1 2f da 03 00 a7 26 4f 30 42 42 e4 48 f3 c1
90 81 f0 f1 ad fc
AVLC type: I sseq: 6 rseq: 1 poll: 0

X.25 Data: grp: 11 chan: 255 sseq: 1 rseq: 7 more: 0

CLNP PDU, compressed header:
COTP Data Acknowledgment:
COTP Data:
ATCDownlinkMessage ::= {
  header: ATCMessageHeader ::= {
    messageIdNumber: 1
    messageRefNumber: 2
    dateTime: DateTimeGroup ::= {
      date: Date ::= {
        year: 2019
        month: 4
        day: 5
      }
      timehhmmss: Timehhmmss ::= {
        hoursminutes: Time ::= {
          hours: 9
          minutes: 7
        }
      }
    }
  }
}
A.1. CPDLC logs

```
seconds: 39

{ logicalAck: 1 }

messageData: ATCDownlinkMessageData ::= {
  elementIds: ATCDownlinkMsgElementIdSequence ::= {
    dM100NULL: <present>
  }
}

CPDLC Downlink Message:
Header:
  Msg ID: 1
  Msg Ref: 2
  Timestamp: 2019-04-05 09:07:39
  Logical ACK: notRequired
Message data:
  LOGICAL ACKNOWLEDGMENT
  {[2019-04-05 11:19:22 CEST] [136.725] [-30.9/-51.1 dBFS] [20.2 dB] [-0.2 ppm]
  1b ff c6 3b 5e c0 42 5a 66 0d f0 00 34 80 00 00 02 08 04 0a c6 a9 a5 00 a8
  0c f3 30 12 08 65 cc 89 4d 30 12 86 44 8b 36 4d 2e 6d 91 68 27 32 84 01 fc
  ce 1c 20
  AVLC type: I sseq: 0 rseq: 6 poll: 0
  X.25 Data: grp: 11 chan: 255 sseq: 3 rseq: 6 more: 0
  CLNP PDU, compressed header:
  COTP Data:
ATCUplinkMessage ::= {
  header: ATCMessageHeader ::= {
    messageIdNumber: 3
    dateTime: DateTimeGroup ::= {
      date: Date ::= {
        year: 2019
        month: 4
        day: 5
      }
      timehhmmss: Timehhmmss ::= {
        hoursminutes: Time ::= {
          hours: 9
          minutes: 19
        }
        seconds: 19
      }
    }
    logicalAck: 0
  }
  messageData: ATCUplinkMessageData ::= {
    elementIds: ATCUplinkMsgElementIdSequence ::= {
      uM74Position: fixName: FixName ::= {
        name: DEMIR
        latlon: LatitudeLongitude ::= {
          latitude: Latitude ::= {
            latitudeType: latitudeDMS:
            LatitudeDegreesMinutesSeconds ::= {
              latitudeWholeDegrees: 54
              latlonWholeMinutes: 50
              secondsLatLon: 11
            }
          }
        }
      }
    }
```
A.1. CPDLC logs

latitudeDirection: 0

longitude: Longitude ::= {
longitudetype: longitudeDMS:
LongitudesDegreesMinutesSeconds ::= {
longitudeWholeDegrees: 9
latLonWholeMinutes: 51
secondsLatLon: 10
}
longitudeDirection: 0
}

CPDLC Uplink Message:
Header:
Msg ID: 3
Timestamp: 2019-04-05 09:19:19
Logical ACK: required
Message data:
PROCEED DIRECT TO [position]
Fix: DEMIR
Latitude: 54 50'11" north
Longitude: 009 51'10" east

[2019-04-05 11:19:29 CEST] [136.725] [-30.7/-51.3 dBFS] [20.5 dB] [-0.3 ppm]
119AAA (Ground station, On ground) -> 47BB0A (Aircraft): Command
1b ff 0c 3b 5e c0 42 5a 70 0d f0 00 34 80 00 00 03 08 04 e4 a8 ed c9 00 a7
33 27 90 81 97 32 25 36 81 c6 41 1c 07 f7 90
AVLC type: r sseq: 3 rseq: 0 poll: 0
X.25 Data: grp: 11 chan: 255 sseq: 6 rseq: 0 more: 0
CLNP PDU, compressed header:
COTP Data:
ATCUpplinkMessage ::= {
header: ATCMessageHeader ::= {
messageIdNumber: 4
messageRefNumber: 3
dateTime: DateTimeGroup ::= {
date: Date ::= {
year: 2019
month: 4
day: 5
}
timemmss: Timehhmmss ::= {
hoursminutes: Time ::= {
hours: 9
minutes: 19
}
seconds: 26
}
logicalAck: 1
}
messageData: ATCUpplinkMessageData ::= {
elementIds: ATCUpplinkMsgElementIdSequence ::= {
uM227NULL: <present>
}
}
CPDLC Uplink Message:

Header:

   Msg ID: 4
   Msg Ref: 3
   Timestamp: 2019-04-05 09:19:26
   Logical ACK: notRequired

Message data:

   LOGICAL ACKNOWLEDGMENT

Listing A.1: CPDLC Messages filtered from captured data