LINK 2000+ Programme

LINK 2000+
Guidance to Ground Implementers

Cooperative Network Design

EUROCONTROL

EUROPEAN ORGANISATION FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

LINK 2000+
Guidance to Ground
Implementers

LINK 2000+ Programme

Edition	:	**1.1**
Edition Date	:	**09 December 2009**
Status	:	**Released Issue**
Class	:	**LIT**

DOCUMENT IDENTIFICATION SHEET

DOCUMENT DESCRIPTION

Document Title

LINK 2000+ Guidance to Ground Implementers

PROGRAMME REFERENCE INDEX	EDITION :	1.1
LINK 2000+ Programme	EDITION DATE :	09 December 2009

Abstract

This document covers technical aspects of the implementation and use of a number of data link services, derived from the Context Management (CM) and Controller Pilot Data Link Communication (CPDLC) applications, under the LINK 2000+ programme.

Information is compiled from different locations to assist Air Navigation Service Providers (ANSPs) in implementing LINK 2000+ Services (DLIC, ACM, ACL and AMC) by providing guidance on the necessary steps to be followed and by sharing the lessons learned during the Pioneer Phase of the Programme.

Keywords

CONTACT PERSON :	Philippe Sacré	TEL : +352-436061506	DIVISION :	CND

DOCUMENT STATUS AND TYPE

STATUS		CATEGORY		CLASSIFICATION	
Working Draft	☐	Executive Task	☐	General Public	☑
Draft	☐	Specialist Task	☑	CND	☐
Proposed Issue	☐	Lower Layer Task	☐	Restricted	☐
Released Issue	☑				

ELECTRONIC BACKUP

INTERNAL REFERENCE NAME :   LINK 2000+/LIT/Guidance to Ground Implementers

HOST SYSTEM	MEDIA	SOFTWARE(S)
Microsoft Windows	Type : Hard disk	MS Word 2002 SP3
	Media Identification :	

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION	DATE	REASON FOR CHANGE	SECTIONS PAGES AFFECTED
0.1	1 August 2008	Document formatting under template, first internal review copy	All
0.2	24 October 2008	Comments following Internal meeting Input from EEC Brétigny and Maastricht UAC	All
0.3	31 October 2008	Acronym list updated Section 4 enhanced with more details	All
0.4	28 November 2008	Input from Maastricht Input from LINK team review Removed part on timers, AMIC Changed introduction, trimmed reference list	All
0.5	March 2009	Input from NATS, DSNA, LINK team Added tutorial information in Annex 7	All
1.0	March 2009	Re-ordering (section on testing moved) Section 5.3 aligned to airborne document Acronym list aligned to airborne document Sent to LIT as Draft for Comments	All
1.1	Dec. 2009	Released following comment cycle	All

TABLE OF CONTENTS

1. INTRODUCTION

1.1   Background

The implementation of data link is one of the key operational improvements that will alleviate voice channel congestion. It will provide benefits to ATC efficiency, capacity and communications in order to accommodate the expected growth in air traffic demand. The EUROCONTROL LINK 2000+ Programme packages a first set of beneficial and affordable en-route controller pilot data link communication (CPDLC) services for implementation in the European Airspace using the Aeronautical Telecommunication Network and VHF Digital Link Mode 2 (ATN/VDL2).

LINK 2000+ has taken an innovative three-step approach to reap benefits faster than by waiting for the mandatory carriage:

- Pioneer phase,

- Incentives,

- Mandate (Single European Sky Data Link Services Implementing Rule – SES DLS IR)

The Pioneer phase, which started in 2003, provided all parties involved with valuable experience and many important lessons learned.

This document, together with its companion related to airborne aspects, gathers the lessons learned in one place, hopefully offering a good starting point for new Implementers of the LINK 2000+ data link services. It is targeted at a readership comprising ground systems integrators/planners and regulators.

1.2   Scope

This document covers technical aspects of the implementation and use of a number of data link services, derived from the Context Management (CM) and Controller Pilot Data Link Communication (CPDLC) applications, defined by the LINK 2000+ Programme as the LINK Baseline Services, and included in the Implementing Rule for Data Link Services, ref. [2].

Information is compiled from different locations not necessarily easily accessible to the reader (unpublished white papers, emails, etc), in order to assist Air Navigation Service Providers (ANSPs) in implementing LINK 2000+ Services (DLIC, ACM, ACL and AMC) by providing guidance on the necessary steps to be followed and by sharing the lessons learned during the Pioneer Phase of the Programme.

The ultimate objective is to support the use of CPDLC in a harmonised way. If required, appropriate local authorities may promulgate further specific conditions for its use.

1.3   FANS Accommodation

The current version of the document does not address FANS accommodation, given that it is not within the remit of the LINK 2000+ programme, and that each implementer will decide on this independently.

1.4   Document organisation

Section 1 provides an introduction to this guidance document and defines its scope.
Section 2 gives a To Do list for ground implementers and an overview of the basic building blocks of the system.
Section 3 discusses the Data Processing System architecture impact of introducing data link.
Sections 4 and 5 addresses more detailed issues including lessons learned.
Section 6 addresses validation and testing activities support for implementers.
Section 7 addresses performance, safety and security.

A set of annexes includes further details that complement the body of the document.

Annex 7 contains material of **tutorial** nature and additional references.

1.5   Relevant Documents

The documentation supporting the LINK 2000+ programme is extensive, and below is a list of documents which are of immediate relevance given the present scope.

The official list of supporting references for LINK 2000+ is given in [1] and [2].

[1]   DLS IR: Commission Regulation (EC) No 29/2009 of 16 January 2009 laying down requirements on data link services for the Single European Sky

[2]   EUROCONTROL Specification on Data Link Services, V 2.1, 28 January 2009

[3]   LINK 2000+: Network Planning Document (NPD), V. 3.4, 1 May 2007

[4]   LINK 2000+: Generic Requirements for a LINK 2000+ Air/Ground Communications Service Provider (ACSP), V. 1.6, December 2009

[5]   LINK 2000+: ATN Naming and Addressing Plan, V. 1.2, 19 May 2004 ; see also the ATN Addressing Database, v. 1.5 (August 2008)

[6]   LINK 2000+: Guidance to Airborne Implementers, V 1.1, 30 November, 2009

[7]   LINK 2000+: ATC Data Link Guidance for LINK 2000+ Services, V. 5.0, 30 June 2009

[8]   LINK 2000+: Flight Crew Data Link Guidance for LINK 2000+ Services, V. 4.0, 30 June 2009

Note: All reference documents listed above, are available on the LINK 2000+ Programme website – www.eurocontrol.it/link2000

2. DATA LINK IMPLEMENTATION

2.1   Introduction

For background information supporting the contents of this guidance document, a **tutorial introduction** is provided in Annex 7.

2.2   To-do list for ground implementers

Ground Implementers (ANSPs) will need to:
- upgrade Data Processing Systems to enable data link communications and to integrate data link services into controller working positions, see section 3.1,
- upgrade Flight Data Processing System(s) to be compliant with additional requirements directly related to data link services, such as flight plan evolution (including 24-bit ICAO address in field 18), Coordination and Transfer Implementing rule (e.g. new OLDI messages NAN and LOF, section 3.1.5),
- document applicable procedures,
- organise the staffing and train staff in charge of operations, installation and maintenance of systems,
- establish and monitor service level agreements (incl. Quality of Service requirements) with providers of communication services, as appropriate, see section 4.1,
- update Letters of Agreement between adjacent units to reflect the support of data link services,
- implement time-stamping and recording of uplink and downlink ATS data link messages on the ground side in accordance with technical specifications defined in EUROCAE ED 111 Functional specifications for CNS/ATM ground recording, see section 3.2.9,
- verify that their systems supporting data link services comply with the applicable regulatory provisions of the interoperability regulation and of the DLS IR,
- issue as applicable an EC declaration of conformity or suitability for use, or an EC declaration of verification and a technical file containing evidences of compliance with applicable regulatory provisions,
- obtain safety acceptance of data link systems, see section 7.2; when this has been granted by the national authority, the ANSP notifies the provision of ATS supported by data link services to airspace users. The notification should be published in accordance with existing procedures in Aeronautical Information documents (AIC, AIP),
- co-ordinate with the CFMU the necessary changes to the environment database in order to enable IFPS to output warning messages for non-equipped aircraft in the concerned airspace.

2.3   Functional Model

Figure 1 illustrates the overall LINK 2000+ functional model for the provision of data link services using the ICAO ATN. This organises the overall system into three principal domains: the Air Navigation Service Provider (ANSP) domain, the Air-Ground Communications Service

Provider (ACSP) domain and the Aircraft domain. The physical architecture may be different, with functional elements lumped in common physical components.

The ANSP domain includes (among others) the Air Traffic Service Unit (ATSU) Data Processing System, an ATN End System and an ATN ground-ground router. The "**Data Processing System**" is a general term for the technical infrastructure of the Air Traffic Control Centre where data link functionality is to be integrated. This architecture supports typical functions like Surveillance and Flight Data Processing, Operational Display, Data and Voice Communications, etc. The ANSP domain can comprise one or several ATSUs.

The ACSP domain comprises the ground system supporting the air-ground communications network, and air-ground and ground-ground ATN routers operated by the ACSP. For some ground implementers, the ANSP and ACSP domains will be under the same organisation.

The Aircraft domain includes (among others) the Aircraft Avionics System, the ATN End System, an ATN airborne router and the airborne components of the air-ground communications network.

The nomenclature used here is coherent in the LINK 2000+ programme, but can be different in documents from other sources. For instance here we will not use the "Air Traffic Service Provider" (ATSP) term, although it is equivalent to the ANSP for our purposes. ATSU is an acronym also used by Airbus for its avionics architecture, which can lead to confusion. In the latter case we will always use the term "Airbus ATSU".

As illustrated in Figure 1, this document provides guidance related to the ANSP domain and ACSP domain, excluding the controller Human Machine Interface (except for a remark in section 3.2.8), human operators and procedures (see ref. [7]).
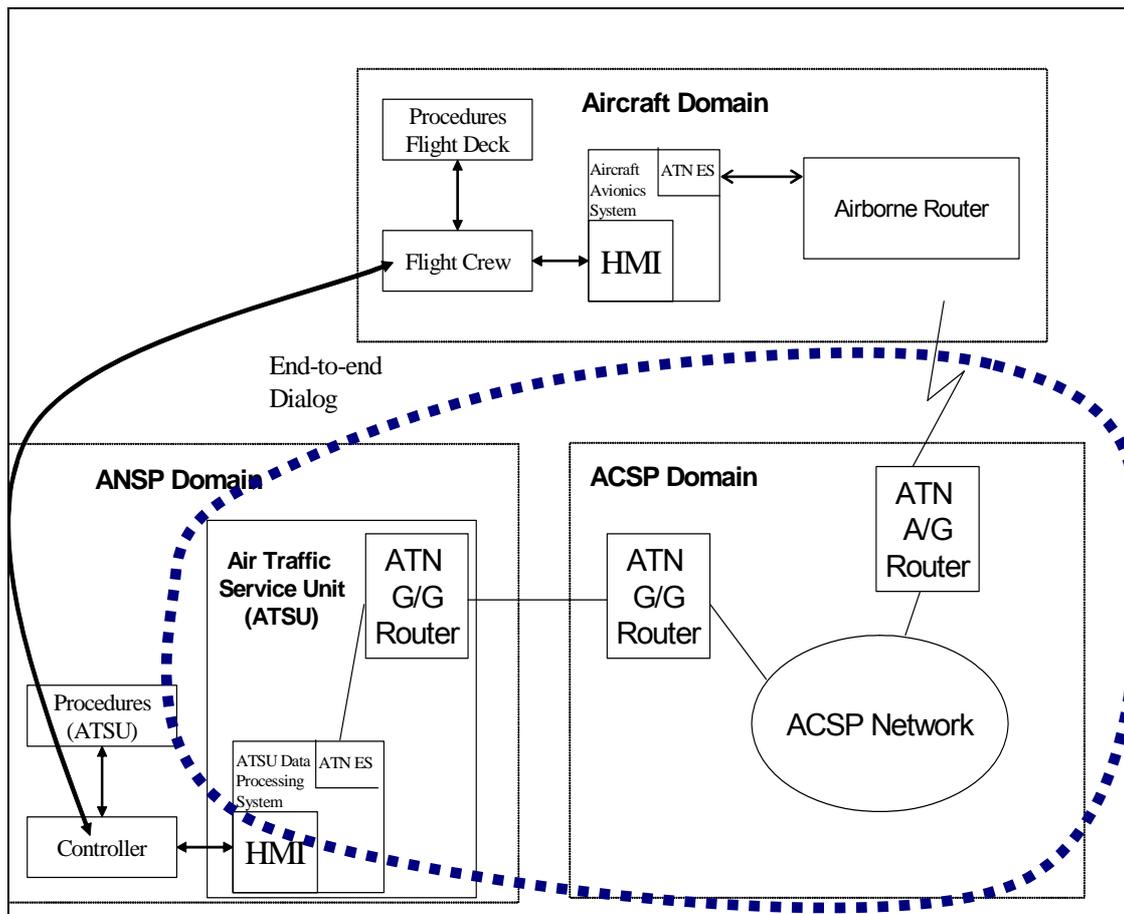
Figure 1- ATN Data Link System Functional Architecture
Scope of this document (bold, dotted)

3. DATA PROCESSING SYSTEMS

3.1 Architectures

One important question faced by Ground Implementers will be how to integrate the new Data Link Communication functionality into their existing Data Processing System (DPS) architecture.

While the latter is specific to each Implementer and no attempt can be made at being both particular and exhaustive, this section gives some broad guidelines as per the main available choices, based on currently known implementations at the time of writing. Subsequent editions of the document may reflect evolutions noticed as LINK 2000+ implementation is under way.

At each ATSU, an ANSP will arguably operate a Flight Data Processing System (FDPS), which may be shared among several ATSUs. The FDPS is part of the overall ATSU Data Processing System. The FDPS may need to be modified in order to support the LINK 2000+ ATS Services and in order to interface to the LINK 2000+ Communications Infrastructure.

When considering the ATN aspects of the FDPS modifications, two questions arise:

- How does the FDPS "plug" into the Communications Infrastructure?

- Where is the end point of the Communications Infrastructure i.e. the ATN End System?

Four possible architectures have been identified, summarised as:

Option 1.   Integrated FDPS and Data Link Services and Communications – *not currently planned*.

Option 2.   Integrated FDPS and Data Link Services, with Remote Data Communications **Front-End.**

See section 3.1.1

Option 3.   FDPS with separate **Data Link Server** (implementing Data link Services and Communications)**.**

See section 3.1.2

Option 4.   FDPS with remote Data Link Server – *not currently planned*.

Ground Implementers will choose the most appropriate architecture given their existing systems and upgrade plans. Two architectures with existing implementations (options 2 and 3) are examined below. There is no planned implementation of options 1 and 4 at the time of writing - this does not mean that the use of these options is discouraged.

3.1.1   Data Communications Front End

Figure 2 is based on the approach used at the pioneer ATSU for LINK 2000+, the Maastricht Upper Area Control Centre (MUAC). The same approach is also used for instance at DFS and NAV-Portugal.

While the data link services (i.e. DLIC, ACL, AMC etc) are implemented in the FDPS, the message formatting and other data communications functions are implemented in a separate Data Link Front End Processor (DL-FEP), which handles the actual communications with aircraft. This system off-loads all communications responsibility from the FDPS and handles all ATN communication protocols: it has no flight data processing function. It formally contains the ATN End System.

In this architecture, the DL-FEP and FDPS together ensure the air ground interoperability in compliance with all data link related standards and have the same functions as listed below in 3.1.2. Among these, specific DL-FEP functions include:
- maintaining a list of flights currently connected,
- carrying out the detection and management of CPDLC errors,
- keeping records of the data link messages and providing them to client systems upon request.
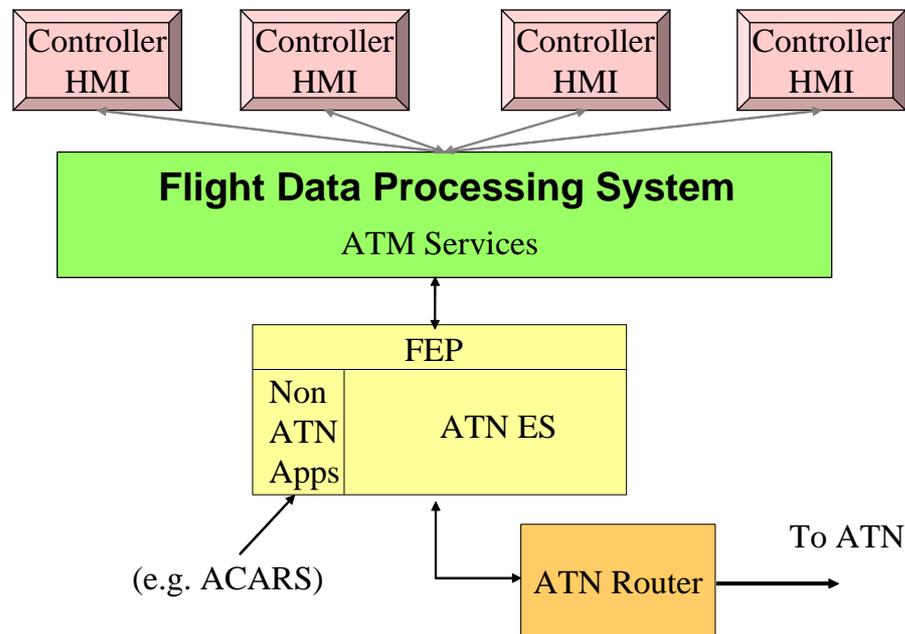
Figure 2 - ANSP Domain – ATSU - Data Link Front End Processor

This approach gives a strong functional separation between the Air Traffic Management (e.g. the creation and interpretation of CPDLC messages) and the data communications aspects. This can be very useful when different software assurance level (SWAL) requirements apply to the different parts of the system, provided that relevant partitioning is used to prevent the propagation of faults occurring in the system.

This also has the advantage that modifications to an existing FDPS can be considerably reduced, and gives the potential for greater flexibility (there is a well defined interface between the data communications subsystem and the FDPS). Hence any change to the data communications subsystem is possible without impact on the FDPS itself.

Other advantages are:
- the system can be made redundant easily and thus offer high reliability and availability,
- the development of the DL-FEP can be performed independently (different contractor) from the FDPS.

In Maastricht the FDPS and Controller Workstations can only handle ATN/CPDLC messages. However, Maastricht UAC also supports communications with FANS-1/A equipped aircraft. This is achieved by the DL-FEP providing a communications gateway and protocol converter between FANS-1/A and ATN/CPDLC.

3.1.2   FDPS with separate Data Link Server
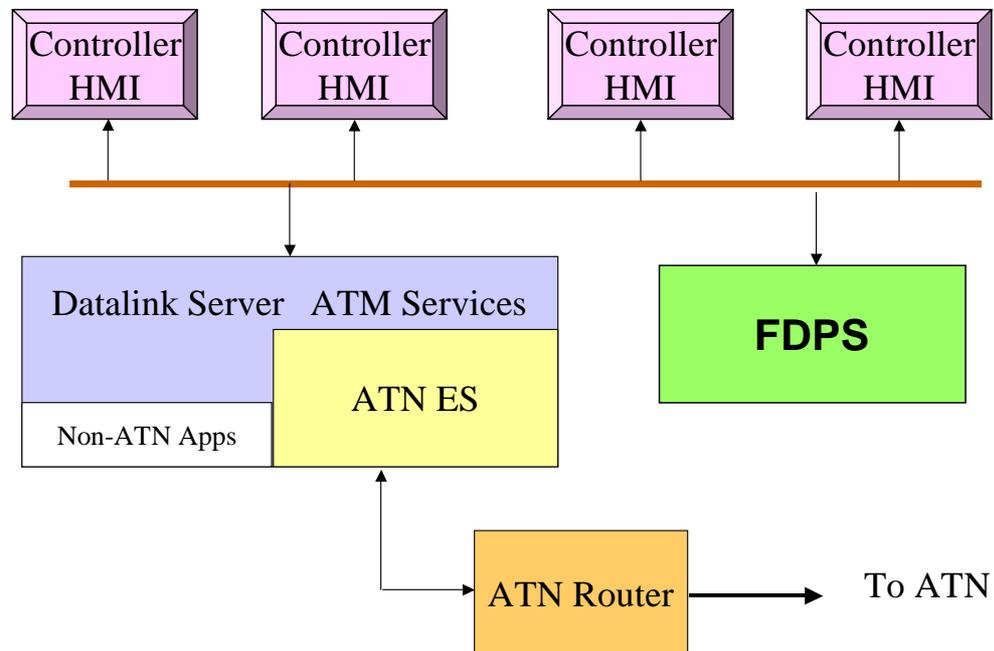
Figure 3 - ANSP Domain – ATSU – Data Link Server

Figure 3 is based on the approach used for instance by the French DSNA (Direction des Services de la Navigation Aérienne). This approach was tested and validated in 2008 by 'EVALINK', a 3 month live trial in Reims ACC, the French control centre next to Maastricht.

This is an alternative approach for minimising changes to the FDPS, placing all data link communications functionality in a separate "Data Link Server" (DL Server), which implements the Data Link Service and ATN End System. The controller HMI is connected to both FDPS and DL Server over a common Local Area Network (LAN).

In this architecture, the DL Server performs all data link functions, while some are part of the FDPS in the architectural option 2. The architecture of the DL Server itself allows to separate data communication management and CPDLC service management.

The DL Server ensures the air ground interoperability in compliance with all data link related standards. In the context of the DLS IR, it:
- manages the DLIC service on the ground side, replying to the CM-Logon, after association of the data link flight with a flight plan (the association can be handled both by the FDPS itself or a dedicated function component of the ATM system),
- manages the CPDLC connection with aircraft according to ATSU configurations and flight plan events,
- maintains a list of flights currently connected,

- manages the CPDLC dialogue list for each aircraft that is connected with CPDLC, according to interoperability requirements,
- carries out the detection and management of CPDLC errors,
- associates the messages concerning CPDLC dialogues with connected aircraft, identified by their flight plans,
- keeps records of the data link messages and provides them to client systems upon request.

This approach offers much the same pros as the previous one, and its main additional advantage is that the DL Server can provide any ATM function with data link communications: for future new services planned in SESAR (Single European Sky ATM Research programme), this architecture will allow interfacing the DL Server with new components which would need to send/receive data by data link.

Another advantage of this solution is about the improvements and evolutions of data link services:

- the compliance of the ATM system to the applicable regulatory provisions is concentrated in the DL Server. Thus, any modification or evolution of ED110, ED120, ED111 and SARPS is allocated only to the DL Server. There is no need to modify the FDPS to maintain/improve data link services,
- future data link services (SESAR) will be added to the DL Server: the impact on the ATM system would thus be limited to specific data to be provided by the FDPS, although this issue needs careful consideration in 4D trajectory management systems of the future.

During the EVALINK experiment, the modularity of such an architecture proved to be an advantage by enabling the provision of CPDLC services without any impact on the existing ATM components (HMI, FDPS).

3.1.3   Summary of Pros/Cons of the two main approaches

	Pros	Cons
Option 2	Data link functions in a separate component. Ease of applying different SWALs to modules. Ease of making the system redundant Front-end processor paradigm common for all communications beyond data link.	FDPS modification to include data link functions.
Option 3	All data link functions in dedicated component (dialog logic, timer management, error management, ATN protocol compliance …). New data link services implementation	More data exchanges on LAN. Potential complexity of

allocated largely to the data link server, with FDPS interface in need of careful consideration. Compliance with standards concentrated in a unique component. Modularity of the ATM architecture allowing to setup experiments in order to validate/evaluate new versions.	definition for the Interface with the FDPS, when the FDPS supports 4D-planning, to guarantee that flight profile change messages are taken into account properly by the FDPS etc

3.1.4   ATN End system function

ATN end systems formally include the complete 7-layer protocol stack hosting the appropriate application(s). They are capable of communicating with other ATN End Systems to provide end-to-end communication services. There exist commercial products embodying this concept.

However, depending on the architecture, the FDPS may also have functions related to data link and the interface between the two needs to be defined.

In architectural option 2, FDPS functions include:
- supporting flight plan association at logon time (the FDPS identifies aircraft via their 7-character aircraft flight Identification (ID), it is the responsibility of the End System to maintain a mapping between these and the ATN addresses). This does not change with the introduction of Protected Mode CPDLC (PM-CPDLC), which has other justifications. See Annex 7 for a review of PM-CPDLC.
- maintaining the operational dialog logic, including:
    - o generation and tracking of message identification and reference numbers, respectively (see Annex 7, section A.7.4.2),
    - o operational timer establishment and tracking.

In architectural option 3, FDPS functions include:
- processing the flight plan association in the CM-Logon process, triggered by the DL Server,
- feeding the DL Server with necessary control and flight plan events
- coordinating with the DL-Server the flight profile change messages so that they are taken into account in a timely manner for FDPS 4D-planning and conflict avoidance.
- coordinating with the DL-Server the display of data link functionality on the HMI (i.e. information on CPDLC availability).

  Note: In EVALINK, these two coordination functions were realised by dedicated components.

3.1.5   Coordination and Transfer

The FDPS also includes the OLDI application, which features two specific messages for CPDLC: the Next Authority Notified (NAN) and Logon Forward (LOF).
The Coordination and Transfer Implementing Rule (COTR IR) (Commission Regulation 1032/2006) has been amended to include these messages: see Commission Regulation

30/2009. OLDI is a EUROCONTROL Specification providing Means of Compliance to the COTR IR.

Note that coordination and transfer processes taking place without OLDI (i.e. if the application is not available for any reason) are described operationally in ref. [7]. The purpose of NAN and LOF is to transfer logon information via ground communication links, preventing aircraft from having to logon to each ground centre as the flight progresses.

3.1.6   Remark

For generality, we henceforth designate the system enabling data link communications under the generic term **"Air Ground Data Link" (AGDL) system**. This obviously corresponds either to the DL-FEP, or the DL Server, in the above architectures.

3.2   Additional aspects

This section includes a number of data processing system related functionalities that are considered useful to ground Implementers and can be implemented on the Front End or Data Link Server component.

3.2.1   Treatment of multiple aircraft logons

This section gives recommendations on desired ground system behaviour when it receives multiple CM Logon Request messages from a given aircraft.

1/ If a CM Logon Request is received while an earlier CM Logon Request from the same aircraft is being processed and the CM Logon Response is outstanding, both CM Logon Requests should be rejected. This is to fulfil ED110B requirement 3.1.1.1: 'There shall be only one CM instantiation on an aircraft connected to a peer CM ground instantiation at the same time'.

Note - An aircraft is uniquely identified by the combination of its ICAO 24-bit address, Aircraft Flight ID, Departure Airport (ADEP), and Destination Airport (ADEST).

2/ If a CM Logon Request is received after a previous CM Logon Response has been uplinked by the ground already, and if it contains the same information as the previous logon, then it should be processed as a normal logon (i.e. generating a CM Logon Response after matching to a flight plan). There should be no change at all in the existing connection, and any existing corresponding CPDLC connection should remain active.

Note: As per ED 110 B, 4.1.4, the CM Logon Request includes the GFD, the long CM TSAP (which includes the 24 bit address), the Aircraft Flight ID, ADEP, ADEST, and application addresses.

3/ If a CM Logon Request is received after a previous CM Logon Response has been uplinked by the ground already, and if it contains different information from the previous CM Logon Request (i.e. any of the field above being different), then the recommended behaviour is the following:
- If the ground system is not able to match the new CM Logon Request information to a flight plan (which may potentially be a revised flight plan), the logon should be rejected and all existing connections with that aircraft should be aborted

- If the ground system is able to match the new CM Logon Request information to a flight plan (which may potentially be a revised flight plan), the logon should be accepted and all existing connections maintained as in case 2/ above.

Note: A CM Logon Request contains some information which is not part of a flight plan. As a result, some CM Logon Request differences may have to be reflected in a revised flight plan, or not, depending on which field is different. For instance, a change in ADEST in the CM Logon Request must correspond to a revised flight plan held by the ground system.

3.2.2   Session Protocol Data Units

As explained, in ref. [7], DLS IR mandate-compliant avionics systems have to be able to support the reception of **any** of the SRF SPDUs, considering the recommendation added in ref. **Error! Reference source not found.**, section B.2.4.3.

However, **ground implementers supporting both mandate and pioneer aircraft are recommended to use E2 in the transition period, in order to accommodate pioneer aircraft not yet fulfilling this requirement before the mandate comes into force**.

3.2.3   Re-establishment of dysfunctional CPDL Connection

There are several circumstances under which a CPDLC connection may become dysfunctional, most notably:

- Failure to receive a CPDLC-start Response
- Delay of downlink CDA Message
- User Abort following Commanded Termination
- User Abort following error condition
- Provider Abort

The initial implementation of CPDLC at UAC Maastricht did not provide for re-establishment of CPDLC after the first attempt. However, the most recent updates to systems at Maastricht now allow for re-establishment of CPDLC following a second valid CM-Logon by the aircraft. Nevertheless, it is noted that re-establishment of CPDLC by this means incurs significant overhead. First, any problem observed at the ground must be conveyed to the aircraft by voice RT. The aircrew must then take steps to initiate again a CM-Logon, which when successful, would then allow CPDLC to be re-established from the ground.

As a general principle, it is recommended that ground systems allow for re-establishment of a lost CPDLC connection, since failure of CPDLC in the circumstances above would contribute to a lack of Availability, compromising compliance with ED-120 performance targets.

The procedure available for re-establishment of CPDLC at UAC Maastricht, requiring a further CM-Logon by the aircrew is considered the most appropriate, and ground implementers are recommended to apply the same procedure.

3.2.4   White, Black and Blocked lists

It can be advantageous to have a means by which access to data link services can be filtered via "white" and "black" / "blocked" lists, respectively. These features have been found useful in MUAC.

- **White list**: the AGDL system can maintain a configurable list of A/C or A/L, respectively characterised by 24-bit ICAO address or Aircraft flight ID prefix (3 letters for the Operating Agency ICAO designator), that are permitted to use the ATN service for CM-Logon Validation.
  Such a white list is arguably useful at the first stages of deployment for a ground centre, up the point where the population of equipped aircraft becomes too large.
- **Black list**: an A/C black list or A/L black list can be used to deny data link service to specific users known not to be compliant or for any reason.
- **Blocked list**: to deal with error or ambiguous conditions where two aircraft try to logon with either the same Aircraft flight ID or the same 24-bit ICAO address, or using such identifications already associated to aircraft currently logged on:
  - A/C blocking due to same Aircraft flight ID ("Aircraft flight ID /Call Sign blocked")
  - A/C blocking due to same 24-bit ICAO address ("peer blocked")

3.2.5   Interfaces

The AGDL System and FDPS have a message passing interface, to exchange information related to CM and CPDLC messages.

For instance in architecture option 2 (see 3.1.1), the FDPS distributes downlink messages to the appropriate Controller Working Position (CWP) and passes uplink messages from the CWP to the AGDL System.

A reliable communications path between the AGDL System and the FDPS can be provided by the industry standard TCP/IP protocol running over Ethernet. TCP is a stream oriented protocol, ensuring ordered message delivery. To facilitate the exchange of messages between the AGDL System and FDPS, an additional protocol is necessary to delimit messages. An example is the use of FMTP (a session layer protocol used to carry OLDI over IP). FMTP[1] is mandated via another Implementing Rule.

3.2.6   Synchronisation

Depending on the selected data processing architecture, a certain level of synchronisation is required between the main systems.

In architecture option 2 (see 3.1.1), control and status messages are used to notify the FDPS and AGDL system about changes to the other system's operational status, respectively, and to reset the systems.

These messages can be used for instance to:

---

[1] The Flight Message Transfer Protocol is a communications stack based on TCP/IPv6. It supports also IPv4. Further guidance material on FMTP is available from EUROCONTROL at the following website http://www.eurocontrol.int/communications/public/standard_page/com_network.html

- notify the FDPS when the AGDL system has re-started and has re-initialised, and vice-versa,
- notify the AGDL system on FDPS restart, to trigger reset and clearing of CM-Logon information and of CPDLC connections.

Annex A.2 contains a list of messages that have been implemented in the Front End architecture at Maastricht UAC, for illustration purposes.

3.2.7   Open Systems, Timing, Supervision

A few additional implementation aspects which have been found useful are listed below:

- Maastricht UAC and DFS have chosen Linux for the operating system used in their new AGDL system. The very large user base of Linux also gives confidence in the reliability of the software and studies have provided the justification for Linux to be used to partition safety related functions from non-safety (administrative) functions[1].

- A unique reference time system is required. Several time distribution systems exist, e.g. Network Time Protocol (NTP), based on a reliable source, e.g. GPS clock.…

- In order to ensure the best availability for data link service provision, a central supervision system can be used. This supervision allows remote monitoring and control of the data link service provision.

- Other optional functions can be implemented on the AGDL system but are given as an example:
    o Message filtering functions,
    o Graphical HMI for the system local monitoring and control,
    o Performance monitoring (LACK time out, message latency, …) and statistics module,
    o Resiliency module,
    o An SNMP agent to allow remote monitoring and control,
    o An AGDL Test system enabling automated test scenarios, comprehensive non-regression testing, and ad hoc tests.

3.2.8   Human Machine Interface

HMI based on paper strips does not lend itself properly to CPDLC implementation, which should rely on <u>HMI based on electronic flight strips</u>.
Other HMI aspects are not in the scope of this document, ref. [7].

3.2.9   Legal Recording

The same legal recording requirements apply to CPDLC message exchanges as to other operational messages handled by the ATSU. These requirements are not to be confused with those of section 3.2.10.

---

[1] A report entitled "Linux Safety Justification Report 2008", V 1.0, 1 July 2008, has been produced by Maastricht UAC on this topic.

3.2.10 Message Logging and Information Exchange – LISAT

It has been recognised that when operational use of CPDLC expands, there will be a need for a repository to collect data obtained in the context of LINK 2000+ operations. This will also act as a single point of information relevant for LINK 2000+ CPDLC operations monitoring. This "Central repository" is named LISAT (LINK 2000+ Statistics Reporting and Analysis Tool), and it is essentially a data base containing the application level data collected from the CPDLC operational use.

The XML format has been chosen for information exchange with this database and should be used by ground implementers. However LISAT also supports ASN.1 Packed Encoded Rule (PER), thus removing the need for ANSPs to develop their own PER/XML converters[1].

It is highly recommended that ANSPs make use of this facility after they start the operational use of CPDLC to ensure proper monitoring of the CPDLC operations at the European level. LISAT can also be provided to ANSPs for local implementation to be used during data link system testing period.

4. COMMUNICATIONS SYSTEMS

The LINK 2000+ communications infrastructure comprises VDL Mode 2 Air/Ground Networks operated by ACSPs, and ground networks (including OLDI connections[2]). ACSPs operate (see Figure 1):

- A network of Air/Ground (A/G) Data Link VHF Ground Stations (VGS) (VDL Mode 2),

- One or more A/G Routers,

- One or more G/G Routers (for interconnection with other ACSPs and with ANSPs)

References [3], [4] and their own references should be consulted in this respect, but specific items of interest are reviewed below.

4.1 Air Ground Communications Service

VDL sub-networks can be operated by Air-Ground Communication Service Providers (ACSPs, i.e. SITA and ARINC in Europe). ANSPs can also choose to provide these services themselves (in partnership with ACSPs), leading to important ATN network design considerations.

The Generic ACSP Requirements document, Ref. [4], provides a reference for use by ANSPs to form the basis of a contract or agreement with an ACSP for the provision of ATN/VDL Mode 2 service in support of the LINK 2000+ programme. It takes into account analysis performed by EUROCONTROL to establish the appropriate requirements together with experience gained during the Pioneer Phase. The document aims to specify the minimum requirements to be satisfied by an ACSP, although ANSPs may add additional

---

[1] The Specification can be obtained from the LINK team www.eurocontrol.int/link2000

[2] OLDI over point-to-point or network links is used for LOF and NAN messages, cf. ante.

requirements or adjust those in this document to reflect local circumstances (such as network architectures). The scope of the evaluation tests defined in annexes of Ref. [4] reflects for completeness the tests required by EUROCONTROL, but may be amended by ANSPs to conform to their local procedures.

4.2   ATN Ground-Ground Router

In order to interoperate with the Air-Ground Communication Service Provider (ACSP) the ANSP operates an ATN Ground-Ground Router.

ATN Ground/Ground routers have interfaces to the physical networks deployed locally. The ATN communication traffic can be encapsulated over these different types of physical networks using Sub-Network Dependent Convergence Functions (SNDCF). The purpose of a Sub-network Dependent Convergence Function (SNDCF) is to provide the connectionless Service assumed by the ATN Internet Protocols over real sub-networks. SNDCFs are defined in the ICAO ATN SARPS for most common types of networks: X.25, IP, Ethernet etc.

X.25 is becoming an obsolete technology, and **use of the IP SNDCF is recommended**.

4.3   Ground Facility Address information

Readers will most likely be familiar with Internet Protocol (IP) addressing schemes. However ATN addresses are based on OSI and readers are invited to consult ref. [5] for detailed information on ATN addressing.

Any new ANSP implementing LINK 2000+ Services should declare their CM application address information: ATN avionics systems need to record the Context Management application addressing information of the Ground ATC Operational Centres involved in the LINK 2000+ programme in order to allow the air crew to perform a first logon with any of the participating centres. LINK 2000+ maintains the Addressing Database for LINK 2000+ document collecting in one place the CM Application addresses of the ATC Operational Centres implementing LINK 2000+ Services, ref. [5].

5.   MESSAGE EXCHANGES AND TIMING

This section contains more detailed and specific technical information and lessons learned.

5.1   ATN Priority – CPDLC-start timing

As explained in Annex A.3, CPDLC and CM have different transport connections and different ATN priorities. Given the implementation of these priorities, the CPDLC-Start request/indication might "overtake" the CM-Logon response sent following an aircraft logon. The CPDLC-Start request/indication is therefore received/processed on board while the aircraft is still in the CPDLC inhibited state.

As per Interoperability requirements, the CPDLC-Start request received while the aircraft is in the CPDLC inhibited state, is answered with a CPDLC-Start response rejected with reason conveying a CPDLC concatenated message DM62+DM98: ERROR(2) + "AIRCREW HAS INHIBITED CPDLC".

In order to prevent the above described situation from happening, two solutions can be envisaged:

- **introduce a <u>delay of 30 to 60 seconds between the CM-Logon response and the CPDLC-Start request</u> transmitted by the ground system**
- **retransmission by the ground of the CPDLC-Start request if the CPDLC-Start response has been rejected with reason DM62+DM98 ('AIRCREW HAS INHIBITED CPDLC').**

5.2 CPDLC Recovery Strategy/Mechanism

Failure of a ground ES would have potential to cause considerable operational disruption. Steps are required on the ground to avoid or minimise this disruption and if necessary re-establish normal CPDLC operation as rapidly as possible.

One recommended solution is the implementation on the ground of a Hot-Standby ES that preserves state-table information accurately for all aircraft, and when the main ES suffers a failure it takes over the CPDLC connections/activity. Implementation of a Hot-Standby ES on the ground would not require the ground to re-establish CPDLC CDA connections to the aircraft nor the associations/connections to the NDA, thus avoiding any operational disruption. However, the Hot-Standby approach may not be technically and economically feasible for all ground architectures.

Where the Hot-Standby approach cannot be implemented, use of a Warm-Stand is assumed, that would require the ground to re-establish CPDLC CDA connections to affected aircraft, as well as associations/connections to the NDA. However, re-establishment of the CPDLC CDA connections could give rise to the VDL Storm Effect, arising from a sudden increase in load on the VDL system causing queues of messages at VDL ground stations. Special measure would be needed to avoid this effect, for example, staggering generation of CPDLC-start messages following ES failure on the ground.

In the event of not employing a Hot-Stanby ES and **in order to reduce the operational impact of failure of a single ES and ease the subsequent recovery, it is recommended that the ground implements multiple ESs, with aircraft being distributed between them.**

Furthermore, it is recommended that the ground should implement the following functionality in the event of an ES failure:

- a) **Alert controllers of loss of CPDLC with affected aircraft, prompting them to settle existing open dialogues by voice.**

- b) **Re-allocate affected aircraft to alternative or Standby ESs.**

- c) **Re-establish CPDLC connection to CDA, either by a voice instruction to re-logon, or else by an automatic process. An automated process would need to stagger CPDLC start-requests so as not to exceed a rate pre-configured by the ATC Centre. This pre-configured rate limit should be set taking account of the number of ESs on the ground, together with the local VDL environment, to ensure minimal loss of AVLC connections from the VDL Storm Effect.**

   d) Identify those aircraft affected by the ES failure that are within 10 minutes of crossing the airspace boundary, and re-send the NDA message to those aircraft.

   e) For the aircraft affected by d), send a NAN message from CDA to NDA to prompt the NDA to re-establish CPDLC.

For further details, see Annex A.4.

5.3   TP4 Parameters

The TP4 protocol includes a number of parameters, for which some appropriate settings have been recommended in the EUROCONTROL Specification on DLS (ref. [2]) Table B-6.

We re-emphasize the need to set the TP4 parameters as recommended in the EUROCONTROL above mentioned document.

Nevertheless, during the LINK 2000+ Pioneer phase, it has been noticed that some airborne and ground implementations have not applied the TP4 settings as recommended in the EUROCONTROL Specification on DLS: this is particularly the case for the Window Timer (W).

The Window Timer may be dynamically computed on a per TP4 connection basis. Dynamic computation taking into account the Remote Inactivity Timer (conveyed in TP4 Connect Request/Connect Confirm) is suggested in Doc. 9705 Ed. 2, Table 5.5-1.

However, when such a computation is used, certain erroneous configurations may lead to a period of inactivity on the TP4 connection (TP4 ACK not sent/TP4 ACK not received) when there are no application exchanges. This eventually leads to the expiry of the local TP4 Inactivity Timer and generation of an application provider abort.

In order to improve robustness of the TP4 protocol under such conditions, the following is recommended:

   a) The formula suggested in the Doc. 9705 (Note 5 of Table 5.5-1) suffers most likely from an editorial omission of a subscript, and the 'I' should be interpreted as referring to the Remote Inactivity Time.

   b) In the Doc. 9705 formula, the Window Timer Offset should be set to a value slightly greater than 50% of the Remote Inactivity Time, to ensure that W expires at least twice prior to expiry of the Remote Inactivity Timer.

   c) The value of W resulting from the Doc. 9705 formula should be constrained by a minimum and maximum value of W:

   - **The minimum value ensures robust behaviour if the computation returns a –ve value, and also avoids saturation of the ATN/VDL network in the event that an exceptionally short value of the Remote Inactivity Timer is erroneously configured.**

- **We propose on the ground that the minimum and maximum W values should be locally configurable. This will give flexibility to adapt the system to restore normal behaviour in the event that a non-compliant aircraft system is encountered. For example, by setting the local ground minimum and maximum values to be the same, the Doc 9705 formula can be effectively switched off, and a fixed value of W imposed.**

6. TEST AND VALIDATION

Ground implementers can benefit from services provided by the LINK 2000+ Data link Test Facility located at the EUROCONTROL Experimental Centre (EEC) in Brétigny-sur-Orge near Paris.

The main objective of the LINK 2000+ Test Facility is to support the validation of operational CPDLC services and ATN/VDL Mode 2 infrastructure for both air and ground implementations before they are approved in an ATC operational environment.
The LINK 2000+ Data link Test Facility provides an inter-operability testing platform for the LINK 2000+ baseline and offers:

- Support to Avionics suppliers on CPDLC/ATN/VDL Mode 2 interoperability testing,

- Support to Airlines in training, familiarisation; support to certification,

- Support to ANSP implementations on CPDLC/ATN interoperability testing,

- Support to Air-Ground Communication Service Providers (ACSPs) in testing of LINK 2000+ ATN/VDL Mode 2 Air-Ground and Ground-Ground infrastructure.
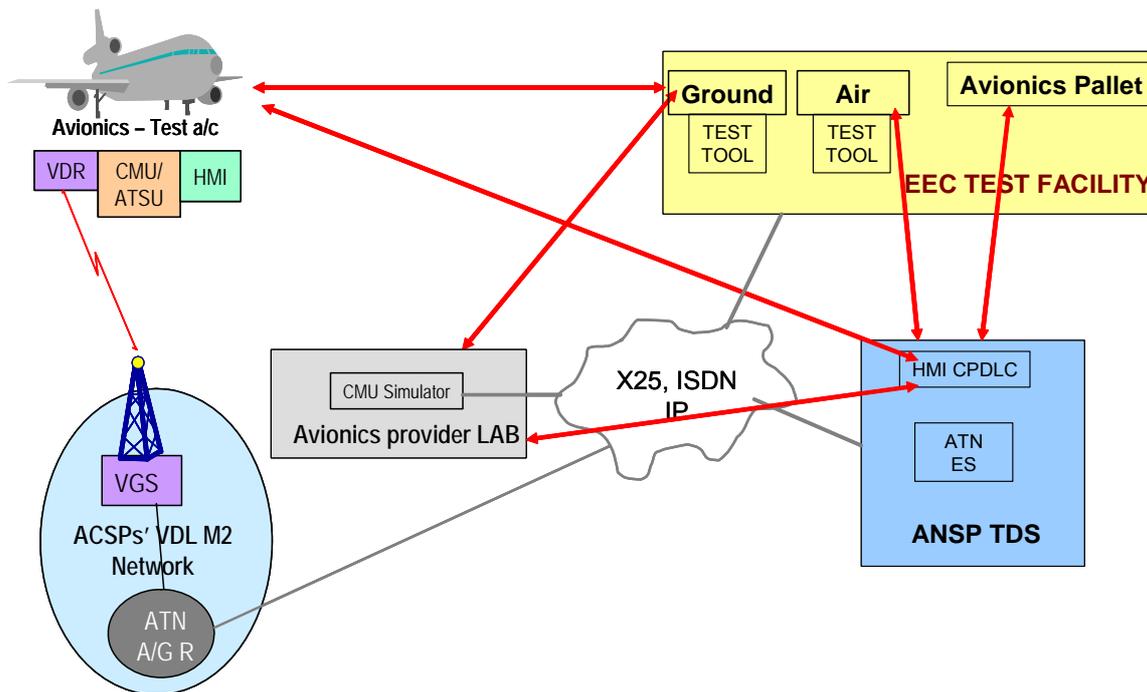
Figure 4 – Test and validation context

Validation activities and Interoperability testing of an ANSP ground implementation may follow the approach described below:

- First, the ANSP defines an Interoperability Test plan at CM/CPDLC level for his ground system. The ANSP may use as a guidance document a Generic CM/CPDLC Interoperability Test Plan document published by EUROCONTROL (see - http://www.eurocontrol.int/link2000/public/standard_page/ansps_validation.html).

  The ground application is first evaluated in a "Lab-to–Lab" configuration against the EEC Facility Air Test Tool (TT):

  o evaluation includes Interoperability testing defined by the ANSP

  o extra test cases can be exercised from the Air Test Tool such as:

    ▪ error test cases: LACK not sent back, invalid Message Identification or Message Reference included in a message, unsupported message sent to the ground implementation,

    ▪ exercise of continuous flow of erroneous messages to test the robustness of the remote ground system (also called "tuning test").

- Second, the ground ANSP application is tested against an Avionics Pallet (real aircraft equipment connected to the Air Ground Test Station - AGTS):

  o this allows the ground application to be tested with realistic round trip delays, with aircraft processing ATN/VDL-M2 handoffs situations as offered by the AGTS,

  o evaluation includes interoperability testing defined by the ANSP.
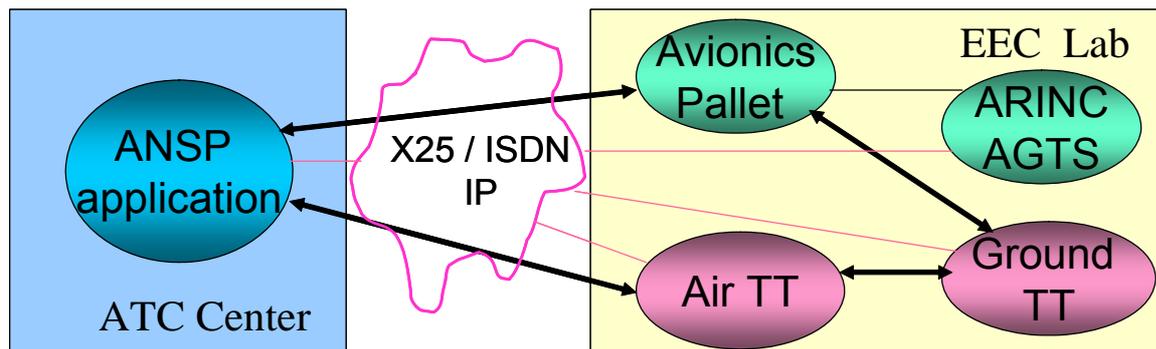
Figure 5 – ANSP Testing Architecture with EEC

7. FURTHER ASPECTS

7.1 Performance requirements

ED120 and its interpretation document, ref. **Error! Reference source not found.** provide safety and performance requirements (SPR).
However, depending on the environment and Safety Case of the local implementer, specific requirements can be more stringent and additional requirements can be added:

▪ Performance requirements (number of messages and aircraft connected per unit of time, CPU/memory maximum load allowed etc…)
▪ Reliability (hardware Mean Time Between Failure)
▪ Availability (time limits on cold/warm restarts)

7.2 Safety

Implementers will have to compile a Safety Case supporting their work. EUROCONTROL has produced a number of documents supporting ANSPs in this work, including a Safety Case Development Manual, but also a "Data Link generic local safety case template" - (see - http://www.eurocontrol.int/link2000/public/site_preferences/display_library_list_public.html).

Annex A.5 provides further details.

7.3 Security

Security has recently seen a growing awareness in Air Traffic Management. Security has many aspects and addressing it has to be balanced against the corresponding costs and operational impacts.
Without being limited to data link communications, the most significant security threats are in general:

• Identity interception: it may be of interest to third parties to establish who is talking to whom. There may be a need in certain organisations to prevent this happening.
• Masquerade: third parties may try to compromise security by pretending to be other known correspondents.

- Replay: third parties may try to repeat a message which they have previously intercepted in the hope of confusing or gaining advantage from the recipient of that message.
- Data interception: where a third party can gain from getting access to the knowledge being conveyed in various messages.
- Manipulation: a third party may change the content of a message to confuse or gain advantage from the recipient.
- Repudiation: where one of the correspondents denies that a communication took place.
- Denial of service: where part or all of a communications service is disrupted intentionally by a third party.
- Mis-routing: third parties to a communication may attempt to divert the communicated information in order to monitor it, change it or destroy it.
- Traffic analysis: third parties to a communication can sometimes derive information about communicating parties by observing the amount, frequency and timing of communication flowing between correspondents even though the nature of the information remains unintelligible.

Deployment of ATC data link results in a general improvement of air safety including a decrease in the overall vulnerability of ATC (Voice and Data) communications to Denial of Service attacks.

There are currently many technical and physical hurdles for an attacker to overcome before a successful masquerade attack could be launched and, even then, surveillance systems and procedures should ensure that such an attack is ultimately fruitless.

Physical Security is relied on to prevent a successful attack based on access to the ground ATN.

Annex A.6 contains more details.

8. CONCLUSION

With the publication of the Data Link Services Implementing Rule in January 2009, implementation is under way and it is hoped that material compiled in this document will be of value to stakeholders concerned by this European Regulation.

Future editions of this document will reflect on-going developments.

ANNEXES

A.1 ANNEX - ACRONYM LIST

This table contains acronyms for the airborne and ground implementers guidance documents.

A/C	Aircraft
A/L	Airline
ACARS	Aircraft Communications Addressing and Reporting System
ACC	Area Control Centre
ACK	Acknowledgement
ACL	ATC Clearances service
ACM	ATC Communications Management service
ACSP	Air-Ground Communications Service Provider
ADS	Automatic Dependent Surveillance
AEEC	Airlines Electronic Engineering Committee
A/G	Air/Ground
AGDL	Air Ground Data Link
AGTS	Air Ground Test Station (at EEC Brétigny)
AIC/P	Aeronautical Information Circular/Publication
AMC	ATC Microphone Check service
AMC	Acceptable Means of Compliance
AMIC	Application Message Integrity Check
ANSP	Air Navigation Service Provider
AOA	ACARS Over AVLC
AOC	Airline Operations Communications / Centre
ASE	Application Service Element
ASN.1	Abstract Syntax Notation 1
ATC	Air Traffic Control
ATM	Air Traffic Management
ATN	Aeronautical Telecommunication Network
ATS	Air Traffic Services
ATSC	Air Traffic Services Communications
ATSP	Air Traffic Services Provider

ATSU	Air Traffic Services Unit
AVLC	Aviation VHF Link Control
BER	ASN.1 Basic Encoding Rules
BIS	Boundary Intermediate System
CDA	Current Data Authority
CFMU	Central Flow Management Unit
CLNP	Connectionless Network Protocol
CM	Context Management
CMU	Communications Management Unit
CNS	Communications, Navigation, Surveillance
COTR	Coordination and Transfer
CPDLC	Controller Pilot Data Link Communication
CWP	Controller Working Position
DCDU	Data Link Control and Display Unit
DL-FEP	Data Link Front End Processor
DLIC	Data Link Initiation Capability service
DLS	Data Link Services
DM	Downlink Message
EATMN	European Air Traffic Management Network
EEC	EUROCONTROL Experimental Centre
ES	End System
ETSO	European Technical Standard Order
EUROCAE	European Organisation for Civil Aviation Equipment
FANS	Future Air Navigation Services
FDPS	Flight Data Processing System
FEP	Front End Processor
FIS	Flight Information Service
FMS/FMC	Flight management System/Computer
FMTP	Flight Message Transfer Protocol
FPL	Flight Plan
G/G	Ground/Ground
GFD	Ground Facility Designator
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSIF	Ground Station Identification Frame

HMI	Human-Machine Interface
ICAO	International Civil Aviation Organisation
ICS	ATN Internet Communications Service
ID	Identification
IDRP	Inter-Domain Routing Protocol
IEC	International Electro technical Commission
IFPS	Initial Flight Plant Processing System
IR	Implementing Rule
IS	Intermediate System
ISO	International Organisation for Standardisation
ITU-T	International Telecommunication Union – Standardisation Sector (formerly CCITT : Comité consultatif international téléphonique et télégraphique)
LACK	Logical Acknowledgement
LAN	Local Area Network
LISAT	LINK 2000+ Statistics Analysis and Reporting Tool
LIT	LINK 2000+ Integration Team
LOF	Logon Forwarding (OLDI Message)
MCDU	Multi-function Control and Display Unit
MMR	Multi Mode Receiver
MOC	Means of Compliance
MsgID	Message Identifier (CPDLC)
MsgRef	Message Reference (CPDLC)
MUAC	EUROCONTROL Maastricht Upper Area Control Centre
NAN	Next Authority Notified (OLDI Message)
NDA	Next Data Authority
NPD	LINK 2000+ Network Planning Document
NSAP	Network Service Access Point
NSEL	Network Selector
NTP	Network Time Protocol
OFG	LINK 2000+ Operational Focus Group
OLDI	On-Line Data Interchange
PDR	Proposed Defect Report (to ICAO Documents)
PDU	Protocol Data Unit
PECT	Peer Entity Contact Table
PER	ASN.1 Packed Encoding Rules

PISC	Pre-Implementation Safety Case
PM-CPDLC	Protected Mode CPDLC
POA	Plain Old ACARS (VDL Mode A)
QoS	Quality of Service
RF	Radio Frequency
SARPs	ICAO Standards and Recommended Practices
SBY	Stand-By, Back-up System
SC	Safety Case
SES	Single European Sky
SESAR	Single European Sky ATM Research
SNDCF	Sub-Network Dependent Convergence Function
SPDR	Specification Defect Report
SPDU	Session Protocol Data Unit
SPR	Safety and Performance Requirements
SQP	Signal Quality Parameter
SRF	Short Refuse
SVC	Switched Virtual Circuit
SWAL	Software Assurance Level
TCP/IP	Transport Control Protocol / Internet Protocol
TDS	Test and Development System
TP4	Transport Protocol Class 4
TP4 CC/CR	TP4 Connect Confirm/Connect Request
TPDU	Transport PDU
TSAP	Transport Service Access Point
TSEL	Transport Selector
TT	Test Tool
ULCS	ATN Upper Layer Communications Service
UM	Uplink Message
UTC	Universal Time Coordinate
VDL	Very High Frequency Digital Link
VDL2	VDL Mode 2
VDR	VHF Data/Digital Radio
VGS	VHF Ground Station
VHF	Very High Frequency
VRB	Voice Read Back

XID	eXchange identification (ID) (frame)
XML	eXtensible Markup Language

A.2 ANNEX – DL FEP MESSAGE SYNCHRONISATION

Hereunder is a list of messages exchanged between the AGDL system and FDPS for CM and CPDLC at MUAC, as well as Control and Status messages, shown to illustrate synchronisation aspects.

CM Message exchange

Message name (example names)	AGDL System to FDPS	FDPS to AGDL SYSTEM	Purpose
CmLogonInd	✓		Conveys a CM-Logon request from an aircraft to the FDPS
CmLogonRsp		✓	Conveys a CM-Logon response from the FDPS to an aircraft.
CmForwardReq		✓	Conveys ground forwarded CM-Logon to the AGDL System. This message is used by the FDPS to forward logon information to the AGDL System which it has received via an OLDI-LOF message from an adjacent ATSU. Requirements and contents of the use of LOF are fully described in the OLDI standard.
CmForwardRsp	✓		Conveys the response to a ground forwarded CM-Logon
CmUpdateReq		✓	Conveys a CM-Update message from the FDPS to an aircraft.
CmContactReq		✓	Conveys a CM-Contact-Request message from the FDPS to an aircraft
CmContactCnf	✓		Conveys a CM-Contact-Response request from an aircraft to the FDPS
CmEndReq	✓	✓	Either results from a CM-End-request received from an aircraft or is a request from the FDPS to end the CM connection. This message is not generated by FDPS, neither by the aircraft because the FDPS shall not apply the 'maintain' option in the Cm-Logon-Response uplink message.

Message (example names)	AGDL SYSTEM to FDPS	FDPS to AGDL SYSTEM	Purpose
CmUAbortReq		✓	Demands abortive end of a CM connection
CmUAbortInd	✓		Notifies FDPS that the airborne CM user has abortively terminated the CM connection.
CmPAbortInd	✓		Notifies FDPS that the CM connection has been lost due to a communications service provider problem.
CmCancelFlightInfo		✓	Used by the FDPS to command the AGDL System to remove any retained CM-Logon information for the identified aircraft.
CmCancelFlightInd	✓		Notifies the FDPS that retained CM-Logon information for the identified aircraft has been autonomously deleted by the AGDL System.

CPDLC message exchange

Message (**example** names)	AGDL SYSTEM to FDPS	FDPS to AGDL SYSTEM	Purpose
CpcStartReq		✓	Sent by the FDPS to the AGDL System to request that a CPDLC connection with the identified aircraft is initiated and optionally contains the first uplink message to be sent to the aircraft. *Note: the ICAO CPDLC protocol also allows an Aircraft to initiate a CPDLC connection. However, this is not supported by the AGDL SYSTEM. Message types have been reserved in order to permit a later extension to support such a function, if required.*
CpcStartCnf	✓		Sent by the AGDL SYSTEM to the FDPS to report the aircraft's response to an FDPS initiated CPDLC-Start.
CpcEndReq		✓	Sent by the FDPS to the AGDL SYSTEM to initiate a termination of the CPDLC connection without data loss
CpcEndCnf	✓		Sent by the AGDL SYSTEM to the FDPS to report the completion of a CPDLC connection termination.
CpcMessageReq		✓	Sent by the FDPS to the AGDL SYSTEM and contains a CPDLC message for uplink to the

Message (**example** names)	AGDL SYSTEM to FDPS	FDPS to AGDL SYSTEM	Purpose
			aircraft.
CpcMessageInd	✓		Sent by the AGDL SYSTEM to the FDPS and contains a CPDLC message received from the aircraft.
CpcUAbortReq		✓	Sent by the FDPS to the AGDL SYSTEM to demand that a CPDLC connection be terminated immediately (with possible data loss).
CpcUAbortInd	✓		Sent by the AGDL SYSTEM to the FDPS to report abortive termination of the CPDLC connection by the aircraft.
CpcPAbortInd	✓		Sent by the AGDL SYSTEM to the FDPS to report abortive termination of the CPDLC connection by the communications service provider.

Control and Status messages

Message	AGDL System to FDPS	FDPS to AGDL System	Purpose
DlFepResetInd	✓		Notifies the FDPS when the AGDL System has restarted and has re-initialised.
DlFepResetCmd		✓	Sent by the FDPS to the AGDL System on FDPS restart to notify it that it should reset and clear down its CM Logon information and terminate any CPDLC connection.

A.3 ANNEX - ATN PRIORITY: CPDLC-START TIMING

This annex gives an overview of the ATC applications priority requirements, which are leading in some specific case to an unfortunate situation where a CPDLC connection cannot be established between an ATC Centre and an avionics Communications Management Unit.
The issue has been observed during some Interoperability testing sessions conducted between EEC Avionics pallet (with both Rockwell Collins and Honeywell CMUs) and Maastricht ground implementation with new FDPS application.
The situation has also been observed when performing Interoperability testing sessions in the context of French EVALINK ground implementation.

Description

- A manual CM-Logon is sent from the aircraft in the CPDLC inhibited state; the CM-Logon request is associated to one TP4 connection.

- The ground answers to the Logon request with a positive CM-Logon response and immediately (within less than 100ms sometimes) generates a CPDLC-Start Request. The ground CPDLC-Start request is associated to a second TP4 connection.

- Due to implementation of ATN priorities, the CPDLC-Start request/indication "overtakes" the CM-Logon response. It is therefore received/processed on board while the aircraft is still in the CPDLC inhibited state.

- As per LINK 2000+ baseline requirement, the CPDLC-Start Request, which is received while CPDLC is still in the inhibited state on the aircraft, is therefore answered with a CPDLC-Start response rejected with reason conveying a CPDLC concatenated message DM62+DM98: ERROR(2) + "AIRCREW HAS INHIBITED CPDLC".

Analysis

The above described situation perfectly illustrates the implementation of ATN SARPs priority requirements. The effect is notably visible in the case described above, due to fact that the critical CM and CPDLC uplink exchanges are sent very close together by the ground systems.

Description of ATN priorities

1- As per ATN SARPs, CPDLC ATC application priority is of higher priority than CM ATC application

2- As per ATN SARPs, CPDLC application traffic is mapped to a higher priority connection at the TP4 layer.

3- Consequently, a TP4 connection of higher priority is then mapped to a higher CLNP priority.

.

4- The corresponding mapping at TP4 and CLNP protocol layers as defined by the SARPs are summarized below:

Application Priority (high to low)	TP4 Priority	CLNP Priority
CPDLC	3	11
CM	6	8

(Priority TP4: Highest 0, Lowest 14 - Priority CLNP: highest 14, Lowest : 0)

5- Both Maastricht Test and Development System (TDS) and the avionics equipment implementation are fully compliant to the above defined priority mapping.

Implementation of CLNP priority

The LINK 2000+ Generic ACSP Requirements Document, ref. [4], mentions that the ACSPs ATN Routers shall follow the SARPs requirements:

- The ACSPs ATN Routers shall enforce CLNP packet priority.

- Higher priority packets shall be forwarded before lower priority packets in the same outgoing queue.

- If an ATN Router discards packets due to congestion then lower priority packets shall be discarded before higher priority packets are discarded.

The SARPs requirements state:

"Note.— In the ATN Internet Layer, an NPDU of a higher priority is given preferred access to resources. During periods of higher network utilisation, higher priority NPDUs may therefore be expected to be more likely to reach their destination (i.e. are less likely to be discarded by a congested router) and to have a lower transit delay (i.e. be more likely to be selected for transmission from an outgoing queue) than are lower priority packets.

5.2.8.4.1 ATN Internet Entities shall maintain their queues of outgoing NPDUs in strict priority order, such that a higher priority NPDU in an outgoing queue will always be selected for transmission in preference to a lower priority NPDU.

Note.— Priority zero is the lowest priority.

5.2.8.4.2 During periods of congestion, or when any other need arises to discard NPDUs currently held by an ATN Internet Entity, lower priority NPDUs shall always be discarded before higher priority NPDUs."

As a result of the implementation of these requirements on the ACSP side, there may arise a situation where some CPDLC PDU overtakes some CM PDU on the ground path of the ACSP ATN infrastructure.

Implementation of ATN Application priority on avionics

Even if the above does not occur, that is CM PDU is delivered before the CPDLC PDU, there may be an additional process on the CMU side that could lead to the same unwanted situation:

- For SARPs compliance, avionics software has been designed so that tasks managing CPDLC application are of higher priority than tasks managing the CM application

- CM application task can be pre-empted by CPDLC application task.

Therefore, even if a CM-Logon response PDU is received on board "slightly" before the CPLDC-Start Indication, we can face a situation where the CPDLC-Start indication process overtakes the CM-Logon response process:

- If the CPDLC-Start indication is processed before the CM-Logon response has been fully processed, i.e., the CMU is still in the CPDLC inhibited state, the CMU rejects the CPDLC connection.

- The CM task continues its processing after the CPDLC task has completed, and this time completes the CM-Logon response event process, which then allows the CMU to move into the "CPDLC ENABLED" state.

- A subsequent CPDLC-Start indication will therefore be accepted.

Conclusion

There is no anomaly detected, the unwanted situation is simply due to implementation of ATN and ATC Application priorities and the critical CM and CPDLC uplink messages sent very close together. The situation is easily reproducible.

The situation can be fixed by:
- Introduction of a delay between the CPDLC-Logon Response and the CPDLC-Start Request transmitted by the ground side, with a value of the delay to be defined (between 30s and 60s). A drawback here is that in case of late logon (aircraft already in the sector), the controller would consider the connection too long to be established (at least 30 seconds between the logon and the connection).

- Possibly, retransmission by the ground of the CPDLC-Start Request if the CPDLC-Start Response has been rejected with reason DM62+DM98 ('AIRCREW HAS INHIBITED CPDLC').

A.4 ANNEX – CPDLC RECOVERY AND VDL STORM

A.4.1 INTRODUCTION

The LINK 2000+ Business Case foresees increased Controller productivity arising from implementation of CPDLC. Accordingly, to realise economic benefit from such implementation, ANSPs will need to design their airspace and procedures under the assumption that CPDLC provides a very high level of availability. Complete loss of critical functionality such as the ground End System (ES) would result in loss of CPDLC to all aircraft connected through it, causing significant operational disruption, and presenting a risk to the realisation of the expected benefits from CPDLC.

This paper discusses operational considerations and technical issues arising from ground ES failure. This case is of particular importance because it has potential to affect CPDLC connections to a large number of aircraft at the same time, raising particular operational and technical challenges.

Throughout this paper, the term ground ES will be used to refer to a component hosting the ATN upper layers (including the TP4 Transport Protocol) associated with the CPDLC application. In the UAC Maastricht architecture, the function is implemented in the Data Link Front End Processor (DL-FEP). However, the principles discussed here are intended to apply generally to ground systems, and not to any single architecture.

In general, failure of a ground ES would be handled by the use of a Standby unit that would take over the functions of the failed unit. Since the ES maintains state tables for each TP4 and CPDLC connection, these state tables would have to be carried over exactly from the failed system to the Standby unit, to avoid disruption to CPDLC. A ground architecture supporting such functionality is referred to as a 'Hot-Standby' system, and is discussed further in Section 2.

In some ground systems, it may not be practicable to employ the 'Hot-Standby' approach, and in such cases a 'Warm-Standby' would most likely be employed, that would take over the functionality of the failed ES, but would not maintain the CPDLC and TP4 state-tables. It would then be necessary to re-establish affected CPDLC connections with every aircraft. This process would impose some delay before restoration of CPDLC, and hence a need for operational procedures to deal with the interruption. The Operational and Technical Considerations are discussed in Section 3 below. In particular, the process of re-establishing CPDLC to a large number of aircraft simultaneously could lead to a surge in demand on the VDL system leading to congestion and substantial additional delay in restoration of CPDLC. Special measures are required to avoid this risk.Measures are discussed that could be employed by the ground system to limit the operational impact, and to re-establish normal CPDLC operation.

Finally, in Section 4, the conclusions are summarised.

A.4.2 HOT-STANDBY GROUND ARCHITECTURE

As discussed previously, the ground ES is a state machine, embracing both TP4 and CPDLC protocols. Therefore to avoid disruption of the CPDLC CDA connections, and NDA associations following ES failure, the CPDLC and TP4 state tables must be transferred with high reliability from the failed ES to the Standby unit.

One technique by which the transfer of state tables could take place would be to maintain a Hot Standby ES with a high bandwidth link to the operational ES, so that the state tables in the Hot Standby unit would mirror exactly those in the operational unit. Such an architecture is often found in high integrity control systems.

This approach would avoid any operational disruption following ES failure. However, it may not be feasible to employ this approach in all ground architectures. Furthermore, there may be substantial cost penalties associated with such 'high availability' systems, particularly if the use of a Hot-Standby was not incorporated into the original ground ES design.

A.4.3 WARM-STANDBY GROUND ARCHITECTURE

In cases where the use of a Hot-Standby ES is not feasible, it must be assumed that the functionality of the failed ground ES would be taken over by one or more Warm-Standby units running alongside the operational unit, but which do not have access to the state tables of the failed unit. Accordingly, the following discussion considers the operational and technical issues associated with re-establishment of both the CPDLC CDA connection as well as the association with the NDA, which would both be required in this case.

A.4.3.1 Operational Considerations

The following principles were adopted as a result of discussion with Controllers of the issues surrounding restoration of CPDLC connections following ground ES failure:

a) OPS should be alerted as soon as possible that CPDLC connections have been lost. For example, in Maastricht, this will be achieved by showing on the Controller Working Position that CPDLC is not available by means of a downward pointing triangle for the concerned aircraft, and in addition the affected dialogues will be placed in an error condition.

b) All open dialogues will need to be settled by voice. The alert in a) above will trigger the controllers to settle open dialogues, and will also give the controllers the choice of postponing transfers that they were just about to initiate.

c) It is considered to be of utmost importance that CPDLC at the CDA (i.e. the unit suffering the failure) becomes available to the controller again as soon as possible.

d) It is considered equally important that CPDLC is available upon first contact to an NDA unit. For example, already today there are certain traffic flows where CPDLC is used extensively after an aircraft first calls on frequency (NSSR, Direct TO). A considerable increase in workload, leading to lost capacity, could be the result if controller/pilot had to co-ordinate proper re-establishment of CPDLC via voice. Technical measures to address this point are considered further in the following section.

e) The process of connection re-establishment should be as transparent as possible for the   controllers.

A.4.3.2 ATN SARPs Requirements

CPDLC SARPs specify a number of provisions that are relevant to recovery of CPDLC in the event of ES failure on the ground. These all relate to the CPDLC User component of the application, and can be found in Section 2.3.7 of SARPs (Ed 2). In summary, these requirements can be stated as:

a) If an aircraft receives a CPDLC-start from either the CDA or NDA, that results in a second CPDLC connection with the given ground system, then the aircraft shall invoke a user-abort on the previous CPDLC connection with that ground system (SARPs 2.3.7.4.1.2.3 refers)

b) If the aircraft invokes or receives a user-abort on the CPDLC connection with the CDA, then in addition to deleting the association with the CDA, the aircraft shall also delete any association with the NDA, and if a CPDLC connection exists to the NDA the aircraft shall invoke a user-abort on that connection also. (SARPs 2.3.7.4.6.2.1 and 2.3.7.6.3.1 refer).

c) If a CPDLC connection with the CDA ceases to exist for any reason other than as a result of a CPDLC-end request, then any existing NDA association shall also cease to exist (SARPs 2.3.7.4.4.2.10 refers).

In other words, if the CPDLC connection with the CDA became dysfunctional due to failure of the ground ES, then the association or CPDLC connection with the NDA would never become operational. Even if the CDA connection was re-established, then it would be necessary to re-establish the association and any CPDLC connection with the NDA as well.

A.4.3.3 Avionics Behaviour

As discussed in SectionA.4.3.1, Operational Considerations place considerable emphasis on enabling an aircraft affected by ground ES failure to be transferred to the NDA with CPDLC operational. This thought has led to discussion as to whether there would be any merit in retaining an NDA association in the avionics, even following loss of CPDLC with the CDA.

However, the results of the computational modelling of the VDL Storm Effect, discussed below, reveal that the benefit of retaining the NDA association within the avionics would be negligible. The NDA connection could not become operational until the current CDA connection had been restored. The restoration of the CDA connection would be likely to suffer significant delay due to the large number of long CPDLC-start messages queued in the VDL system. In contrast, restoration of the NDA association would represent a much smaller burden on the VDL link and occur after the VDL Storm had subsided. Accordingly, there appears to be no justification for a change to the SARPs in this respect.

A.4.3.4 The VDL Storm Effect

A risk has been identified that substantial disruption to the VDL system might be caused by the process of re-establishing CPDLC connections to a large number of aircraft simultaneously. This could arise because VDL Ground Stations do not generally have mutual line-of-sight contact and so when large queues of messages exist at several ground stations, there is a high risk of mutual interference. The effect is made worse because the data-link exchanges to establish CPDLC are much longer than those used to exchange routine messages. This has become known as the VDL Storm Effect.

In order to study this effect, a computational model has been built to explore the sensitivity of the outcome to different design parameters. The computational model assumes a Baseline Scenario that is appropriate to CPDLC Operations in Maastricht under expected LINK 2000+ Mandate Phase conditions, using a single ground ES, and three VDL channels. It takes into account the expected aircraft load and overall deployment of VDL ground stations. It assumes that following failure of a ground ES, approx 26% of aircraft would be sufficiently close to the airspace boundary that re-establishment of the NDA association would be required in addition to the connection to the CDA. It considers variations in the scenario, including the use of multiple ESs, as discussed in Section A.4.3.5 below.

The conclusion of this model is that the VDL Storm Effect is a significant risk, and that technical measures would be required to mitigate the effect. However, caution is required in interpreting the results. First of all, the model has not been subjected to any independent validation. In the event that any safety criticality is attributed to the behaviour of VDL under 'Storm' conditions, then some independent validation of the results must be performed. Furthermore, the model has so far been used only to study specifically a scenario appropriate to Maastricht airspace and operations. It cannot be assumed that identical conclusions can be reached for other airspace.

The technique suggested by the model to mitigate the VDL Storm Effect is that the load of CPDLC start-requests from the CDA to re-establish connections with affected aircraft should be spread over a period of time.

The results of analysis from the computational model can be summarised as follows:

a) In the Baseline Scenario, without measures to mitigate the effect of the VDL Storm following CPDLC recovery, significant disruption of AVLC would be expected. In this scenario, it is predicted that in excess of 25% of AVLC connections would be lost.

b) Spreading the generation of CPDLC-start uplinks by the ATSU could reduce loss of AVLC to negligible levels, at the expense of an increase in the time take to re-establish the CDA and NDA CPDLC connections. In the Baseline Scenario a spreading period of at least 70 seconds would appear to be required. This corresponds to a maximum rate of generating CPDLC-start uplinks to 2.8 aircraft per second, assuming aircraft are randomly distributed to VGSs and channels.

c) The additional effect of uplinking the NDA and re-establishing the NDA connection, once CPDLC had been re-established with the CDA, would appear to be minimal. There are two reasons why the re-establishment of the NDA connection would be less disruptive; firstly it would only be required in those aircraft close to the airspace boundary (26% of the total), and secondly, since the NDA connection could only be established after the CDA connection had become functional, exchanges associated with the NDA would be naturally spread over time. If the NDA connection were not re-established, then the time to achieve the CDA connection would be reduced from 79 seconds in the Baseline Maastricht Scenario to 69 seconds (95%ile in both cases).

d) The deployment of multiple ESs on the ground to limit the number of aircraft affected by a single failure would have a substantially improving effect. If three ESs were to be deployed by Maastricht, only 3% of AVLC connections are predicted to be lost following a single ES failure, with no spreading in place, compared to 25% AVLC loss with only one ES deployed. This could be reduced to a negligible level by introduction of spreading over 20 seconds, which would give rise to a time to re-establish CPDLC with the CDA of just 35 seconds, compared to 79 seconds (95%ile in both cases) with only a single ES.

e) The VDL Storm Effect is sensitive to the number of VGSs within line of sight of a typical aircraft. For example, in a more extreme Maastricht scenario with the number of VGSs in line of sight of the aircraft increased by 50% (the total number of VGSs remaining the same), it would appear to be necessary to increase the spreading period from 70 to 90 seconds to achieve a negligible loss of AVLC. Accordingly in a practical implementation, the spreading function should be configurable, and the optimal configuration should be determined taking into account the local VDL environment.

A.4.3.5 Multiple Ground ESs

An important measure that could be adopted to reduce both the operational and technical impact of ground ES failure would be to distribute the CPDLC connections in an ATC Centre around multiple ESs. In the event of a single ES failure, only a proportion of aircraft would be affected by the failure. If aircraft were randomly allocated to an ES at first contact, then each controller would see only that limited proportion of aircraft lose their CPDLC connection. Furthermore, since the number of affected CPDLC connections requiring re-establishment would be reduced, the resulting VDL load would be diminished by the same extent, thus speeding up recovery. As discussed in Section A.4.3.4 d), the implementation of multiple ESs significantly reduces the degree of spreading of CPDLC-start requests needed to avoid the VDL Storm Effect.

In a multiple ES architecture, such as that outlined here, the CPDLC connections affected by the failure would be re-established either by spare capacity in the remaining ESs, or by a separate 'warm'Standby ES as discussed previously.

A.4.3.6 Re-establishment of CPDLC CDA Connections

With no Hot-Standby ES in place, it would be necessary for the ground to re-establish CPDLC CDA connections with the aircraft and where appropriate to re-establish the NDA associations following ES failure.

Manual CM-logon
The simplest means to re-establish the CPDLC connections to the CDA would be by a voice instruction from the ground to pilots, requesting them to perform another CM-logon. In the absence of such notification from the ground, the aircrew would not normally be aware that the CPDLC connection had failed until 6 minutes after the event. This has the benefit of not requiring additional technical functionality on the ground, and is the approach that will be adopted initially by UAC Maastricht. It should be recognised that the extra VDL load of performing the CM-logon exchanges may cause an additional performance defecit in the VDL system, but the natural delays associated with the manual process would tend to spread the load on the VDL system, mitigating the VDL Storm Effect. Operational procedures to request pilots to re-logon by voice may still need to stagger instructions to individual aircraft. The operational acceptability of this solution is dependent on the number of CPDLC connections affected by the failure (affected by the level of equipped data link traffic). Accordingly it is seen as an initial/transitional measure that (with the increase of data link equipped aircraft) will evolve towards more automation (described below) and/or with implementation of multiple ESs that will reduce the number of CPDLC connection affected by the failure.

Automatic Re-establishment of CPDLC CDA Connections
Alternatively, CPDLC connections with the CDA could be re-established by an automatic process on the ground. This has the benefit of avoiding the controller/pilot workload associated with manual process described above, together with the VDL load associated with the CM-logon, and would ensure that connections were re-established in the minimum possible time. To avoid the VDL Storm Effect, CPDLC start-requests should be staggered, so as not to exceed a rate pre-configured by the ATC Centre. This pre-configured rate limit should be set on the basis of modelling, taking into account the number of ground ESs implemented, together with the local VDL environment, to ensure minimal loss of AVLC connections.

A.4.3.7 Re-establishment of NDA Associations

Following re-establishment of the CDA connections, aircraft affected by the ES failure should be identified that require re-establishment of the association with their NDA. In the case of UAC Maastricht, it is judged that the NDA message should be sent to aircraft within 10 minutes of crossing the airspace boundary. After sending the NDA message, a NAN message should be sent from CDA to NDA to prompt the NDA to re-establish CPDLC.

A.4.4 SUMMARY AND CONCLUSIONS

Failure of a ground ES would have potential to cause considerable operational disruption. Steps are required on the ground to avoid or minimise this disruption and if necessary re-establish normal CPDLC operation as rapidly as possible.

Implementation of a Hot-Standby ES on the ground that preserves state-table information accurately for all aircraft following ground ES failure, would not require the ground to re-establish CPDLC CDA connections to the aircraft nor the associations/connections to the NDA, thus avoiding any operational disruption. However, the Hot-Standby approach may not be technically and economically feasible for all ground architectures.

Where the Hot-Standby approach cannot be implemented, use of a Warm-Stand is assumed, that would require the ground to re-establish CPDLC CDA connections to affected aircraft, as well as associations/connections to the NDA. However, re-establishment of the CPDLC CDA connections could give rise to the VDL Storm Effect, arising from a sudden increase in load on the VDL system causing queues of messages at VDL ground stations. Special measure would be needed to avoid this effect, for example, staggering generation of CPDLC-start messages following ES failure on the ground.

In the event of not employing a Hot-Stanby ES, it is recommended that the ground should implement multiple ESs, with aircraft being distributed between them to reduce the operational impact of failure of a single ES and ease the subsequent recovery.

Furthermore, it is recommended that the ground should implement the following functionality in the event of taking over ES functionality by one or more Warm-Standby ESs:

f) Alert controllers of loss of CPDLC with affected aircraft, prompting them to settle existing open dialogues by voice.

g) Re-allocate affected aircraft to alternative or Standby ESs.

h) Re-establish CPDLC connection to CDA, either by a voice instruction to re-logon, or else by an automatic process. An automated process would need to stagger CPDLC start-requests so as not to exceed a rate pre-configured by the ATC Centre. This pre-configured rate limit should be set taking account of the number of ESs on the ground, together with the local VDL environment, to ensure minimal loss of AVLC connections from the VDL Storm Effect.

i) Identify those aircraft affected by the ES failure that are within 10 minutes of crossing the airspace boundary, and re-send the NDA message to those aircraft.

j) For the aircraft affected by d), send a NAN message from CDA to NDA to prompt the NDA to re-establish CPDLC.

A.5 ANNEX – SAFETY CASE

Implementers will have to compile a Safety Case supporting their work.

A Safety Case (SC) is a matter of ensuring that an institution produces:
- a formal safety assessment to assure itself that its operations are safe,
- a formal document demonstrating the above to a regulatory body. Such a demonstration both meets a legitimate expectation of the end-users and the public and provides a sound basis for regulatory control.

A SC is the entirety of argument and evidence, which substantiate claims for the achievement of acceptable levels of safety. As such the Safety Case is a shortcut to all the documentation (mainly the safety-related documentation) produced or used in the project framework for that aim. It covers rules, regulations, operational & maintenance procedures and manuals, training manuals, verification and validation strategies, design descriptions, safety analyses and results, and whatever is appropriate to substantiate the claims made in the safety argument.

The content of the Safety Case is accumulated incrementally throughout the project lifecycle. During the performance of the Safety Assessment and application of the Safety Assurance process there is a large amount of information to be recorded and managed. A Safety Case is therefore a living suite of documents that should reflect the current state of all the physical, operational and organisational aspects.

The purpose of the Safety Case is to provide all interested parties with justified confidence that the AGDL ground system element is acceptably safe to operate. That implies that the system is acceptably safe on initial entry to service and will remain acceptably safe during ongoing operations.

The Safety Case (SC) provides a framework of safety arguments for the AGDL system and shows how these arguments are supported by evidence from safety assessment, verification and validation activities. The SC will avoid inclusion of a large amount of detail, the majority of the supporting evidence is contained in a series of reports covering the Safety Assessment activities (Functional Hazard Assessment -FHA, Preliminary System Safety Assessment -PSSA, and System Safety Assessment -SSA). These reports, in turn, reference more specific items of evidence such as test reports or training feedbacks.

EUROCAE ED120
The starting point of the Centre AGDL system safety assessment should be the Safety Objectives and Requirements allocated to the ground segment by ED120 from an end-to-end perspective (comprising the aircraft system, the air navigation service provider ANSP provisions, and the operator's provisions to use the data link services).

EUROCONTROL SAM
The EATM ANS Safety Assessment Methodology (SAM), can be applied in conducting the Institutional Safety Assessment (ISA) of the AGDL system. All SAM documents are found at http://www.eurocontrol.int/safety/public/site_preferences/display_library_list_public.html.
The SAM comprises a three-step process:

   i) Functional Hazard Assessment (FHA), which shall be used in determining high level safety objectives and their compliance to the ED 120 guidelines;

ii) Preliminary System Safety Assessment (PSSA) for apportioning these safety objectives across the elements of the Centre AGDL system (equipment, people and procedures), in order to progressively establish safety requirements for all fundamental elements of the design. The safety requirements allocated shall also be traced towards their correspondence in the ED 120 end-to-end safety requirements.

iii) System Safety Assessment (SSA), which shall be applied to the resulting implementation of the design solution. The SSA covers the AGDL ground system Safety Verification with respect to Safety Objectives and Requirements by demonstrating that both safety objectives and requirements are fully met and validated by the Centre and its transfer to operation, operations and maintenance. Moreover, it shall address the system Safety validation with respect to users' expectations.

A local Safety Case template has been produced by EUROCONTROL and is available for supporting implementers in setting up their document – see http://www.eurocontrol.int/link2000/public/site_preferences/display_library_list_public.html.

A.6 ANNEX – SECURITY

Vulnerability Analysis

The current ATC Voice based system is inherently insecure. Only a low level technical capability is needed to jam the channel, listen in to ATC communications or to masquerade as a controller. Prevention against masquerade largely depends on the professional ability of the pilot and controller to recognise an impostor, and safety is assured by several layers of surveillance and conflict alert systems.

The data link system should provide better security than the voice based system if only because it requires greater technical knowledge to monitor data link communications or to masquerade as a pilot or controller. On the other hand, there is nothing in a correctly formed and in-context data link message to betray it as coming from an impostor rather than a genuine pilot or controller.

The first security analysis of the ATN was performed by EUROCONTROL as long ago as 1995. This identified the following threats and vulnerabilities to ATN Security:

● Masquerade of a controller potentially leading to loss of separation due to execution of an invalid clearance.

- ● Masquerade of a pilot leading to confusion (e.g. issuing of a clearance ahead of time).

- ● Modification of uplink messages leading to loss of separation due to execution of an invalid clearance.

- ● Modification of downlink messages leading to confusion (e.g. issuing of a clearance ahead of time).

- ● Denial of Service by jamming or modification or masquerade of routing information.

It should be noted that no threats due to loss of confidentially were identified. In voice based ATC, no attempt is made to keep ATC communications confidential and neither is there any current intent to make data link ATC confidential.

The development of suitable mechanisms to counter these vulnerabilities was delayed whilst institutional issues relating to the export of cryptographic equipment were investigated. These were resolved and the ATN Security Extensions were incorporated into the 3rd edition of the ATN SARPs.

The ATN Security extensions provide:

● Application level integrity verification and authentication of each and every message exchanged.

● Integrity verification and authentication of IDRP routing information exchanged over an air/ground data link.

● A Public Key Infrastructure based on elliptic curve algorithms and using Context Management for the negotiation of session keys.

The possibility of integrating the ATN Security Extensions into PM-CPDLC also exists and should provide for a highly efficient mechanism for authentication of the sender, protecting integrity and protecting against mis-delivery.

Denial of Service attacks based on jamming has to be countered by means to detect the transmitter, and by physical security. These are outside of the scope of the ATN SARPs. However, mitigation of Denial of Service by providing alternative routes via other air/ground technologies is a feature of the ATN Internet, and one of the reasons why the ATN prefers the most complex of the possible mobile routing scenarios i.e. permitting an aircraft to attach to multiple concurrent Air/Ground Networks.

ATN Security and LINK 2000+

No specific technical security mechanisms are proposed for LINK 2000+. Security measures will be limited to aspects such as physical protection, access control (password protection) etc. The justification for this is based on the following consideration of the vulnerabilities discussed above.

Denial of Service Attacks

As with any communications service dependent on the use of free radiating media, the ATN and specifically the VDL Mode 2 data link used by the ATN, is vulnerable to jamming attacks from a high power transmitter operating on the same or adjacent frequencies. Existing Voice Communications are also vulnerable to the same type of attacks.

Jamming of the VDL Mode 2 service itself is not a safety issue. This is because CPDLC Message Loss is countered procedurally by Air Traffic Controllers and Pilots reverting to the use of Voice Communications. The impact of such attacks is on efficiency, as the efficiency gains of CPDLC are lost when the service ceases to be available, resulting in a potential reduction in airspace capacity, and hence delays. The question of how to deal with a significantly increased traffic load when forced to revert to voice is however a safety issue at least for the transition period until the moment flow restrictions are put into place. As a high power transmitter has to be deployed, standard triangulation techniques can be used to rapidly locate the source of the interference and an effective security response organised to remove it. The overall impact of such attacks is thus likely to be minimal and transitory.

As the existing Voice Communications are also vulnerable to the same attacks, deployment of the data link service will increase the safety margin as an attacker will have to jam both services in order to reduce air safety. Currently, they only have to jam the Voice Communications Service. Data link may also require a higher power jamming signal than Voice Communications, as the digital transmissions are robust to relatively high levels of interference and include error correction codes. Aircraft flying at a high enough altitude may also switch automatically to an alternative ground station which, for reasons of relative power levels and physical separation, is not being jammed by the interference signal.

Masquerade Attacks

A successful masquerade attack is serious, as a pilot would not able to tell the difference between a correctly formed but unauthorised clearance and a genuine message from the Current Data Authority. This is why ICAO has specified communications security mechanisms that can demonstrably prevent such attacks from succeeding. However, there are many technical and physical barriers that an attacker must overcome in order to complete a successful attack, which makes it unlikely even without the security extensions.

Specifically, there are two possible routes to such an attack:

1.   Operating an unauthorised VDL Mode 2 Ground Station

2.   Gaining unauthorised access to the ATN Ground Network.

The technical obstacles to successfully completing such an attack include:

a)   Operating a high powered unauthorised transmitter is a very visible activity. The transmitter masts have to be positioned in a visible location on relatively high ground if they are to be effective and the power level must be high enough for the aircraft to select the transmitter as its preferred Ground Station in preference to an authorised transmitter.

b)   Even if the above conditions are met, an aircraft's use of a Ground Station is "sticky" in that it will stay with a preferred ground station until the received power level drops below an acceptable threshold. It is thus non-deterministic as to whether a given aircraft will even use an unauthorised Ground Station. The unauthorised Ground Station will need to be carefully sited on a prime location if it is to be successful. In all probability, such a location will already be occupied by an authorised Ground Station.

c)   An unauthorised Ground Station may attempt to mimic an aircraft's current ground station and hence inject an authorised message that way. However, this is likely to result in a protocol error being detected by the genuine ground station when it receives the VDL2 level response from the aircraft (to an uplink that it had no knowledge of). In turn, this will cause the VDL2 connection to be aborted. The resulting NOCOMM state in the cockpit will force voice completion of the transaction and this will alert the controller to the false message. The result is that such an attack is likely to be detected before a serious outcome is possible.

d)   The communications protocols specified by the ICAO SARPs are based on ISO OSI standards and not industry standard TCP/IP standards. They are also modified from the OSI originals. Access to proven implementations is thus limited, and professional and experienced levels of skill are necessary for deployment, placing a significant skill barrier in the way of an attacker. While industry standard IP Networks can and will be used as part of the ATN, the ATN operates as a VPN, tunnelling its own protocols through the IP Network rendering it inaccessible to other users of the IP Network.

e)   Physical security mechanisms can and will be deployed by Administrations and Service Providers to prevent access to their Ground Networks to unauthorised parties, thus limiting opportunities for this mode of attack.

f)   The connection mode nature of ATN protocols makes it difficult to simply "inject" an authorised message into an established CPDLC dialog between a pilot and a Data Authority.

Communications will have to be observed and the protocols fully understood if a message is to be dynamically constructed that is in sequence and acceptable to a receiver.

g)   Another user can only take over as an Aircraft's Data Authority when nominated as such by the Current Data Authority thus significantly limiting the opportunities for unauthorised communications.

h)   The stream mode compression used over the air/ground data link, while not intended to provide cryptographic levels of confidentially, makes any attempt at observation or modification of a data stream, over the VDL Mode 2 data link, problematic. This is because the compression makes use of dynamically determined entropy codes and references to previous character strings. The dialog has to be observed in its entirety in order to make sense.

i)   Surveillance systems including ground based SSR should detect the results of an unauthorised profile changing message and loss of separation avoided through controller intervention or through an automatic system response.

Modification

Modification is only really an issue in the ground ATN. In theory, a carefully constructed jamming signal could modify a genuine air/ground transmission. However, a very high level of technical skill would be needed and, without advance knowledge of the transmission it would be difficult to predict the correct modification signal. In practice, dynamic issues such as multipath would probably frustrate such an attempt.

Physical level security at both ATC Centre and by Communications Service Providers is relied on to prevent modification s of CPDLC and other messages in the ground ATN.

A.7 ANNEX - DATA LINK COMMUNICATIONS TUTORIAL

A.7.1 Introduction

This data link tutorial gives background information to the LINK 2000+ Ground and Airborne Implementers Guidance Documents.

We have limited the scope to terms and topics encountered in the guidance, recognising that much information is already publicly available. Pointers and references to interesting documents are given at the end of this tutorial. The scope is also limited to data link as implemented in the frame of the LINK 2000+ programme, namely the ICAO version of Controller Pilot Data Link Communication (CPDLC). The FANS 1/A(+) versions of CPDLC are not covered (see [33], [36] for a review).

Reference numbers are local to this tutorial, section A.7.7.

A.7.2 Why data link

Deployment of CPDLC in Europe will provide the following benefits.
- Increasing capacity: in order to cope with forecast traffic increases, many initiatives are on-going, including LINK 2000+. The idea is that Air Traffic Controllers (ATCOs) having to spend less time on voice communication can use part of the saved time to handle more aircraft; it has been proved that increasing capacity in this way is more cost effective than by traditional approach of sectorisation, which suffers from the law of diminishing returns.
- Increasing safety: analog VHF voice communication being limited by a number of technical and human factors, replacing a fraction of these verbal exchanges by an exchange of written messages can eliminate some misunderstandings between ATCOs and flight crew, thus increasing safety. Data link is here understood as a supplement to voice, not a replacement.
- Paving the way for future developments: the SESAR programme relies on improved aeronautical communications enablers, especially on the mobile link with aircraft. Although future data link technologies needed for all SESAR capabilities are in the R&D phase, ATN/VDL2 technology as deployed by LINK 2000+ supports early Implementation Packages of SESAR.

Cost-benefit analyses have been performed and details are in the Justification Material supporting the Single European Sky legislative package mandating LINK 2000+ service deployment as detailed in [21]. An overview of the rule applicability is given below.
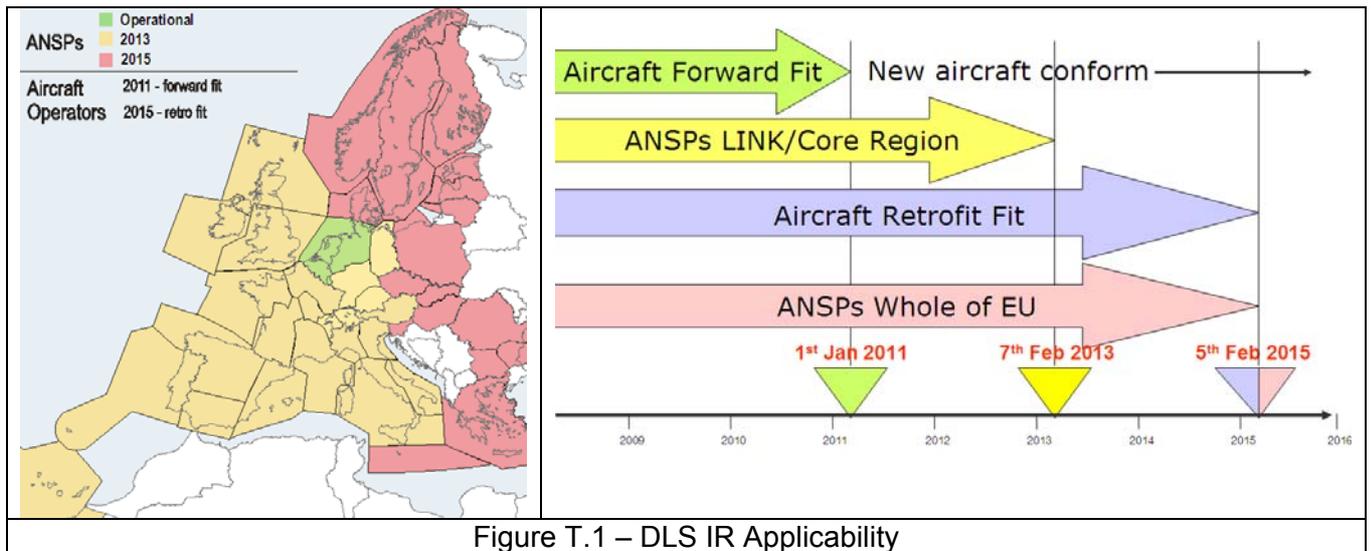
Figure T.1 – DLS IR Applicability

A.7.3 Communication Protocols and ATN

Excellent tutorial and guidance information on the ATN applications and supporting protocols is given in [13]. This section only highlights a number of key concepts.

A.7.3.1 Networking Protocols

ICAO standards for the Aeronautical Telecommunication Network (ATN) specify both the ATM Fixed (Ground-Ground) and Mobile (Air-Ground) **applications**, and the 'ATN Internet', i.e. the underlying **networking technology**.

The ATN internet relies on the Open Systems Interconnection (**OSI**) protocols and conforms to the **OSI seven-layer model and terminology**, fig. T.3. Specifically, each layer provides / receives communication **services** to / from adjacent layers; at each layer as shown on figure T.2, **peer systems** exchange 'protocol data units' (**PDU**) over the network, for instance Session PDUs, Transport PDUs, etc..
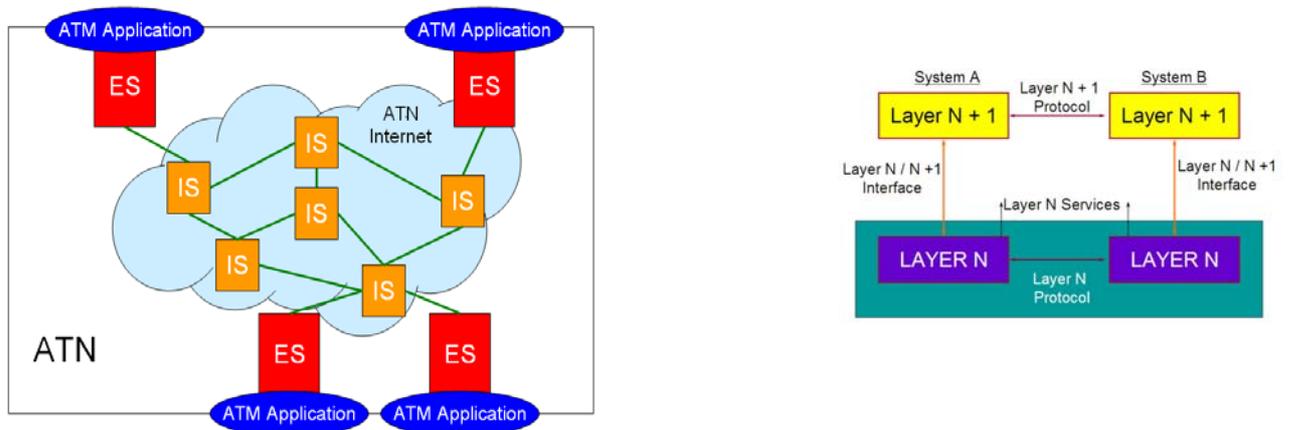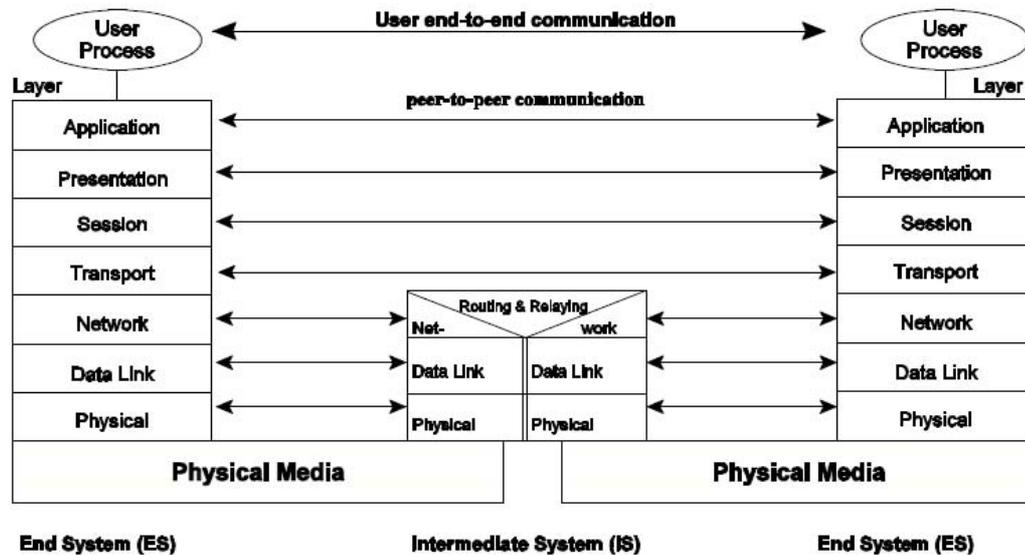

Fig T.2 – ATN overview and OSI layer interaction

Fig T.3 – ATN and the OSI 7-layer model (from ref. [13])

The main infrastructure components of the ATN are the **sub-networks**, the **ATN routers** (**intermediate systems** or **IS**) and the **end systems (ES)**:

- a **sub-network** is as an independent communication network based on a particular communication technology which is used as the physical means of transferring information between ATN systems. A variety of ground-ground as well as air-ground sub-networks provide the possibility of multiple data paths between ATN systems; the sub-network complexity and diversity is hidden by the internetworking communication protocols and "sub-network dependent convergence functions" SNDCF – see below.

- **ATN routers** are responsible for connecting various types of sub-networks together. They route data packets across these sub-networks based on the requested class of service and on the current availability of the network infrastructure (e.g. suitable routes to the destination system); ATN routers are discussed below in more detail.

- **ATN end systems** include a full 7-layer protocol stack to host the appropriate communication services in support of one or more **applications**. ATN end systems are also the interface to automation and/or the human machine interface. The End Systems may run one or several applications, e.g. **Context Management (CM)** and **Controller-Pilot Data Link Communications (CPDLC)**.

A.7.3.2 Routing

ATN connects fixed and mobile users, e.g. aircraft. As an aircraft moves, the path through the network which must be taken to reach that aircraft will change. The ATN supports a dynamic routing process which allows the route information possessed by each router to be updated, both as a result of the movement of the aircraft and as a result of other changes in the network topology due to failures, maintenance activities and so on.

ATN routers comprise the lower 3 layers of the OSI reference model and include, according to their type, the appropriate set of routing protocols. The routers are responsible for forwarding each packet containing the user data via the appropriate path towards its destination, taking into account the particular service requirements encapsulated in the header of the packet. The choice of the appropriate sub-network to be used, when forwarding data packets through the ATN, is based on connectivity, security and quality of service considerations and can be influenced by the application services.

Furthermore ATN routers exchange routing information, i.e. information about available routes, their characteristics, and the end systems reachable via these routes, with other adjacent routers.

ATN Routers can essentially be of three types:
- **air/ground routers** (i.e. ground based but operating over one or more air/ground sub-networks);
- **ground/ground routers** (i.e. ground based and operating over ground/ground sub-networks); and
- **airborne routers** (i.e. aircraft based and operating over air/ground sub-networks).

The main functions of the ATN router are thus to:
- interconnect different sub-network types (e.g. Ethernet LAN and X.25 WAN);
- to forward packets of user data towards their final destination;
- to exchange routing information (i.e. reachability) with adjacent routers and End Systems;
- when operating over air/ground sub-networks - to make efficient use of the limited bandwidth available through use of various techniques such as compression.

At the Network Layer, routers are required to implement the:
- **Connectionless Network Layer Protocol (CLNP),** which is the OSI internetworking protocol and functionally equivalent (but different than) to IP;
- **Inter-Domain Routing Protocol (IDRP)** and the
- **End System to Intermediate System Protocol (ES-IS).**

A.7.3.3 IDRP

IDRP is a routing protocol used to exchange routing information between **Routing Domains** (named 'Autonomous Systems' in the TCP/IP world). In the ATN, each aircraft constitutes a Routing Domain, hence route establishment and maintenance for mobility management in ATN causes the exchange of IDRP Protocol Data Units (**IDRP PDUs**). Details of these processes are out of scope of this document and are given in [5], section IV.3.4.

A.7.3.4 SNDCF

In order to interconnect different types of sub-networks, Routers are required to implement "Sub-network Dependent Convergence Functions" (**SNDCFs**) which essentially map the service offered by the sub-networks in question to that required by the Connectionless network layer service. SNDCFs are defined in the ICAO SARPS and technical manuals for most usual physical networks, including X.25, IP, etc., [2], [6].
In the case of air/ground and airborne routers, the SNDCF for the air/ground sub-network is a special type referred to as the "**Mobile SNDCF**". The mobile SNDCF implements various techniques (e.g. compression) to reduce the amount of data sent over the air/ground link.

A.7.3.5 VDL2 Mobile Sub-network

Several mobile sub-networks have been standardised by ICAO. The choice for LINK 2000+ is VHF Digital Link Mode 2, for the reason that the technology is mature, validated, and already deployed world-wide to support Airline Operations Communications (AOC). The LINK 2000+ Implementing Rule does not preclude the use of other mobile sub-networks for the future.

This tutorial does not discuss the details of the VDL2 technology. The process of network connectivity establishment between air and ground sides, over the VDL2 sub-network, takes place prior to any operational exchange at the application level (see figure T.7). Connectivity maintenance in the presence of mobility, transparently to the applicative user, is ensured by the VDL2 and ATN networking and routing protocols.

In order to understand how this works in details, the reader is encouraged to consult [4] and [5].

VDL2 shares the radio channel using a version of Carrier Sense Multiple Access (**CSMA**). As the number of AOC and ATS users of VDL2 increases, channel utilisation saturates and additional frequencies are needed. How to handle this multi-frequency environment is also out-of-scope of this document. The reader is encouraged to consult refs. [10] and [12] for more details.

A.7.3.6 Transport Protocol

Once a network connection is established between end systems over the internetwork, applications running on the end systems must be able to "identify each other" before data can be exchanged: a transport connection must be established. The overall picture of how applications exchange data over the OSI network is in figure T.4.
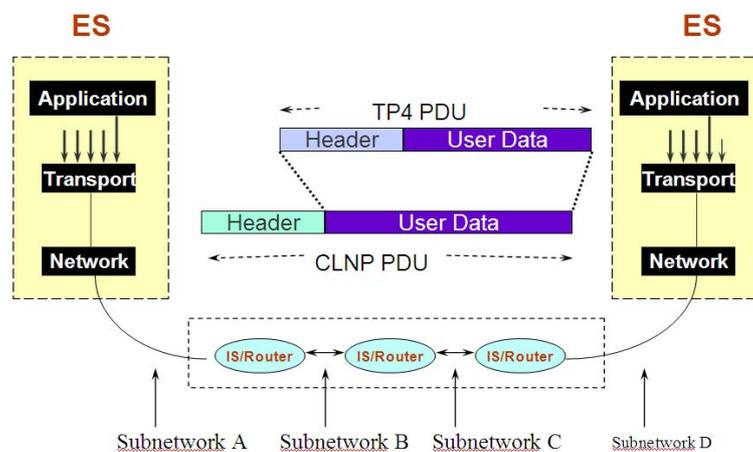

Fig T.4- Transport protocol and encapsulation

In the public internet context this is handled via the familiar concepts to "TCP ports and sockets". In ATN, the transport protocol used is not TCP, but its OSI close relative, the Transport Protocol Class 4 (TP4). Ref. [31] contains an interesting discussion of how TCP/IP and OSI relate (TCP and TP4 in particular, in chapter 12).

In order to establish a transport connection, TP4 uses a "three-way handshake" in combination with a **timer**-based mechanism to ensure connection establishment. Figure T.5 illustrates a typical transport connection establishment procedure.
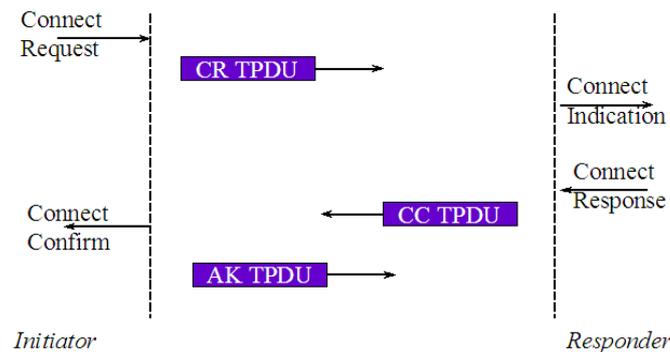
Fig T.5 – Three Way Handshake

A specific user of the transport service passes a 'Connect request' primitive to the transport layer with appropriate parameters for setting up the connection. The transport layer entity then generates a **connection request (CR)** TPDU containing the parameter values and sends it to its peer transport layer entity at the Responder. The Responder's transport entity generates a 'Connect indication' primitive and passes it to its user.

If the responding user accepts the connection establishment request, it generates a 'Connect-response'. The responding transport entity then transmits a **connection confirm** (**CC**) TPDU to the initiating transport entity. Finally the initiating transport entity informs its user that its connection establishment request has been accepted by invoking a 'Connect confirm' primitive.

The initiating transport entity also generates an acknowledgement (AK), or a data, or expedited data TPDU (if there are data to be transferred), and sends it back to the responding transport entity. The connection is considered established only after the responding transport entity has received this acknowledgement or data TPDU.

Much like TCP with which the reader may be familiar, TP4 operates with a number of timers and parameters having different roles. A list of timers is given is ref. [T.31], chapter 12.

In the context of LINK 2000+, the DLS Specification, [14], is the reference.

A.7.3.7 Corresponding TCP/IP protocols

Readers may be more familiar with the TCP/IP than with the OSI protocol suite. Historically, development of the two suites are not independent, and Table 1 summarizes the correspondence .

OSI Protocol	ISO Ref.	OSI Layer	Relatives (*)	Role
CLNP	8473	3	IP	Internetworking
ES-IS	9542	3 - routing	ARP	Discovery
IS-IS	10589	3 - routing	OSPF	Intra domain routing
IDRP	10747	3 - routing	BGP	Inter domain routing
TP4	8073	4	TCP	Transport

Table 1

(*)Internet Protocol, Address Resolution Protocol, Open-Shortest-Path First, Border Gateway Protocol, Transport Control Protocol

A.7.3.8 Addressing

OSI addresses network devices using their hierarchical placement in the network topology: domain, area, and identifier. The hierarchical addressing is used for routing by the longest prefixes. The OSI network service is provided to the transport layer through a conceptual point on the network/transport layer boundary known as the Network Service Access Point (**NSAP**) (sometimes called the "ATN network address" in our context).

When addressing the network layer without being associated with a specific transport entity (e.g. for routing devices), a special network address is used called the **Network Entity Title NET**. A NET is structurally identical to an NSAP but uses a special field in the NSAP (called the NSEL).

ATN is using the OSI CLNP internetworking protocol, and the corresponding addressing scheme. CLNP addresses have a 160-bit (20-byte) hierarchical structure.

Application addresses correspond to **Transport Service Access Points** (TSAP) in ATN, and are exchanged between the air and ground sides during the CM-Logon process as discussed below. TSAP addresses are 21 or 22 byte-long in ATN and correspond to the above NSAP appended with a 1 or 2-byte Transport Selector.

The reference for ATN addressing is [18], section 9.1.4 in particular.

A.7.4 Applications, services, messages

The LINK 2000+ Programme deploys ATN applications and services as given in Table 2. By definition, [19],
- a **data link application** "facilitates specific ATM operational functionalities, using specific data link technology",
- a **data link service** is "a set of ATM related dialogues, both system supported and manual, within a data link application, which have a clearly defined operational goal",
- data link services perform **functions** implemented by an exchange of standardised **messages**.

Application	Service	Examples of Functions/ Messages (*)
Context Management (**CM**)	Data Link Initiation Capability (DLIC)	CM-Logon CM-Contact
Controller Pilot Data Link Communication (**CPDLC**)	ATC Communications Management (ACM)	CPDLC-Start CPDLC-End CPDLC-Message (transfer of data authority e.g. "Next Data Authority ")
	ATC Clearances (ACL)	CPDLC-Message (controller-pilot message exchange, e.g. " Proceed direct to ")
	ATC Microphone Check (AMC)	CPDLC-message (e.g. "Check Stuck Microphone")

Table 2.

(*)details for all messages are given in [14], the operational view is given in [19].

A.7.4.1 Context Management

Context Management (CM) enables an initial contact between the aircraft and the ATC unit that supports data link communications, in order to accurately determine the identity of the aircraft, and to ensure compatibility of aircraft and ground equipage. It is a necessary pre-requisite to any exchange of operational messages between air crew and controllers.

For example, as shown in the table above, DLIC is a service which uses the CM application to provide the necessary information to enable data link communications between ground and aircraft system.

To achieve unambiguous identification of the aircraft executing DLIC, the aircraft sends to the ground a CM-Logon message providing its airframe identification (24-bit ICAO address), aircraft flight ID, departure airport, destination airport, as well as information about available air applications.

Note that CM has several extra functionalities for mobility management, which we do not detail here.

A.7.4.2 CPDLC

Each CPDLC message has the following structure, composed of a message header, and one to five message elements. The message elements are the 'actual' information that is exchanged (e.g. 'Climb to FL290'). The operational usage of such multi-element 'concatenated' messages is the object of discussions in the LINK 2000+ Operational Focus Group, see ref. [19], chapter 11.
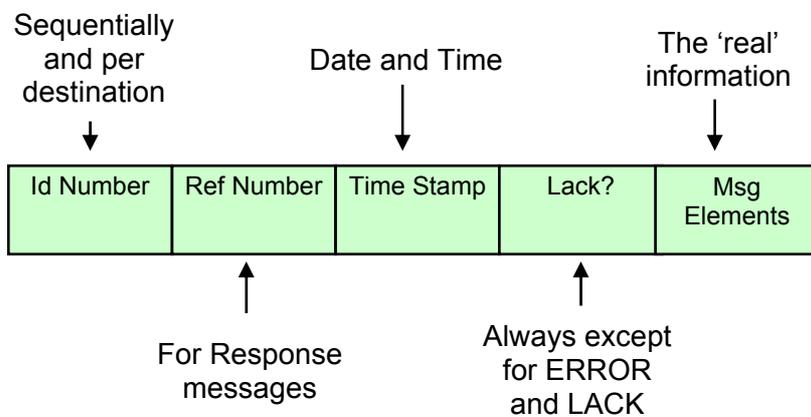

Figure T.6 – CPDLC Message Structure

Field	Description
Message Identification Number (**Msg ID**)	assigned by the sending system sequentially and per destination (a different counter shall be used for each destination).
Message Reference Number (**Msg Ref**)	for response messages only. The message reference number of a response message shall be identical to the message identification number of the received message to which it responds.

Time Stamp	the time the message is dispatched by the originating user. It consists of the date (YYMMDD) and time (HHMMSS).
Logical Acknowledgement Requirement	Indicates whether a logical acknowledgement (**LACK**) is required for the message. The ACL, ACM require a LACK for all messages (except for ERROR and LACK messages).
Message Element 1-5	The Message Elements are the actual information exchanged.

Table 3

A message element itself consists of a message element identifier, data as indicated by the specified message element, and associated message element attributes. This is beyond the scope of this document and details can be found in ref. [T.19].

CPDLC messages are grouped in "**UM**" (uplink message to aircraft) and "**DM**" (downlink to the ground) categories.

Note we should not confuse CM-Contact, which transfers a CPDLC connection to another centre, and the ACM service "Contact [Frequency]", using CPDLC message UM 117.

A.7.4.3 Connection establishment and management

In this section we summarise the connection establishment process because it is important to have in mind the different steps that are taking place. This is a summary and details are given in the bibliography.

Prior to the establishment of a connection between CPDLC applications on the air and ground sides, the sub-network establishment process takes place. This basically works up the communication protocol stack up to layer 3 including routing information updates via IDRP, as briefly mentioned in section 3.
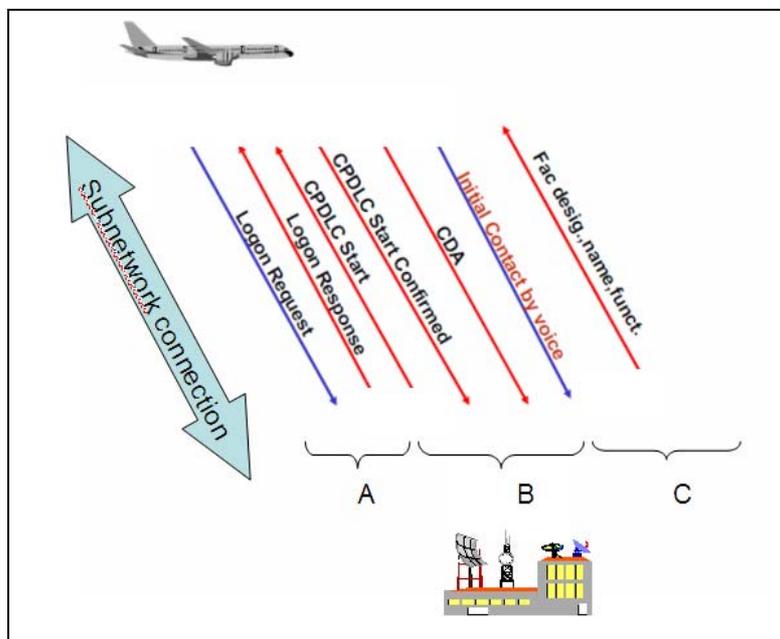

Figure T.7 (adapted from [19])

Once sub-network connectivity is present, the following steps take place towards CPDLC connection enabling (see refs. [18], [19], [21], and [29]):

- Phase A corresponds to the CM-Logon above, where the air and ground sides exchange application information and "recognise each other over the network"; a transport connection is established in support of the CM application in this process.
- Phase B **establishes** the connection between **CPDLC applications**, i.e. it creates a transport connection between the CPDLC applications on the air and ground sides;
- Phase C **enables** it.

A) <u>Logon</u>

In Phase A, the CM-Logon exchange takes place.

The logon is a flight crew initiated activity but does not itself establish a CPDLC connection. How the flight crew is notified of this possibility to perform a logon is implementation dependent and not discussed here.

B) <u>CPDLC establishment</u>:

This process establishes an applicative link over the network: when completed, the systems are ready to transfer data link messages. Unlike logon, CPDLC connection establishment is done automatically system-to-system and does not require human intervention:

- following successful Logon, and prior to entry of the aircraft into the airspace of the concerned Area Control Centre (ACC), the ground system will initiate CPDLC connection through a CPDLC-Start request being sent to the aircraft;
- The aircraft system replies automatically with a CPDLC-Start confirmed message;
- The aircraft system subsequently also sends a Current Data Authority (CDA) message to the ground. CDA is the notification for the receiving ACC that the aircraft is ready to conduct CPDLC with that ACC;
- The flight crew will receive an uplink message confirming the CPLDC connection and also an indication, on the logon page, of the CDA.

From the aircraft perspective, the CPDLC connection is actually enabled at this stage, in that the flight crew can in principle send a CPDLC downlink message. However, until step C) below has taken place, the ground system will reject this message from the air.

C) <u>CPDLC enabling</u>:

- An aircraft must be transferred to, and under the control of, the appropriate ACC before CPDLC is enabled for use. Flight crew shall only initiate CPDLC messages, when CPDLC is enabled.
- The aircraft is under control of the appropriate ACC when:
  a. flight crew have made initial voice contact with the first controller of the ACC providing the service,
  b. a CPDLC message is displayed to the flight crew, indicating the name and function of the current ATC unit. This message is automatically generated by the ground system.

Following this three-step process, operational message exchange can take place. This is perfectly detailed in [19], [20].

A.7.5 Protected Mode CPDLC

This section summarises ref. [24], which must be consulted for further details.

In the pioneer phase of LINK 2000+, it was found that verification of correct delivery of a clearance to the intended aircraft relied upon the correct operation of several functions, and that a failure in any one of them could result in the **mis-delivery and execution of an en-route clearance by an un-intended aircraft**.

Correction of the problem requires the addition of an end-to-end checksum with each CPDLC message that includes the aircraft flight IDentifier and a unique airframe identifier (the ICAO 24-bit Aircraft Address). Verification of this checksum by the aircraft on receipt of a clearance results in an immediate verification of correct delivery that does not rely on the correct operation of any function other than the ground function that generated the checksum. It offers the necessary level of verification.

The version of CPDLC that incorporates the checksum is known as **Protected Mode CPDLC (PM-CPDLC)** and will replace the original "checksum less" version of CPDLC (now known as standard mode CPDLC).

A.7.5.1 The Rationale for PM-CPDLC

Figure T.8 illustrates the process for successful transfer of a clearance from a controller to a pilot.

The process starts with the controller issuing the clearance and identifying the intended aircraft by its Aircraft flight ID. The Flight Data Processing System (FDPS) is now responsible for initiating the transfer of the clearance to the aircraft, but must first determine the ATN network address of that aircraft.

The ATN network address is a fixed property of a given airframe, [18]. However, the Aircraft flight ID is typically a dynamic property assigned to an airframe simply because that aircraft was chosen to fly that particular route at that time. A linkage must thus be established between Aircraft flight ID and airframe. The Context Management (CM) Application provides a means to do this.

| **Figure T.8 - The Delivery of an Uplink Clearance** | **Figure T.9 - The Delivery of an Uplink** |
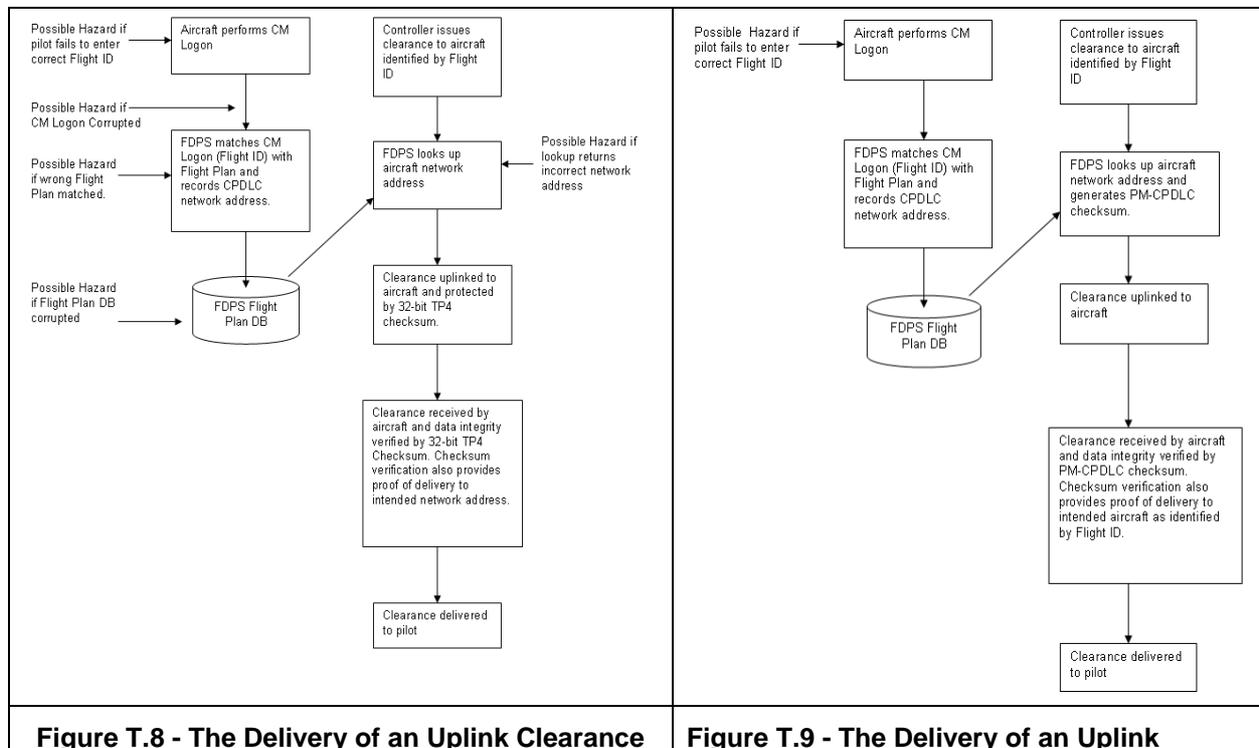
(Standard Mode CPDLC)	**Clearance (PM-CPDLC)**

When an aircraft performs a CM-Logon, it identifies itself by providing its 24-bit ICAO Address, its current Aircraft flight ID, Departure Airport, Destination Airport, and the Transport Addresses that may be used by ground initiated applications, including CPDLC.

The Aircraft flight ID, Departure Airport and Destination Airport can be used to locate the Flight Plan which can then be updated with the airframe identification (24-bit ICAO Address) and the Transport Address (which includes the network address) of each application (e.g. CPDLC).

Using the information learnt from CM, the FDPS can determine the Network Address of an aircraft and use this to determine the destination of a CPDLC transport connection and hence which transport connection to use when up-linking a given message to a selected Flight.

The transport protocol provides a high integrity 32-bit checksum that is computed over the message transferred and a pseudo header including the destination Network Address. This provides verification that data integrity has been maintained and that the message has been delivered to the intended network address. However, for uplink messages, this only provides verification that the message has been delivered to the identified airframe (a Network Address can be viewed as identifying an airframe). It does not include the Aircraft flight ID and hence provides no direct verification of correct delivery to an aircraft identified by Aircraft flight ID.

However, if CPDLC is to ensure that uplink messages are delivered to the intended recipient then it must provide verification that the message has been delivered to the intended Flight as identified by its Aircraft flight ID as well as to the intended airframe. The problem is that in order to assert this, the aircraft has to rely upon the ground system selecting the correct network address for the uplink. It has no way of independently verifying that this was done.

A long dependency chain is present and Figure T.8 indicates where hazards may occur as a result of an error in information handling. If any of these errors occur, then the potential hazard will not be detectable by the aircraft systems.

PM-CPDLC has been developed to provide straightforward verification that:

      a) A CPDLC Message has been delivered to its intended recipient, and

      b) A CPDLC Message has been delivered without loss of content integrity.

In PM-CPDLC, these verifications can both be obtained by successfully validating an **Application Message Integrity Check (AMIC)** that is transferred along with each CPDLC Message. This AMIC is computed over not just the CPDLC Message but additionally over a "pseudo header" that includes, among others, the Aircraft flight ID, 24-bit ICAO address and the Data Authority's Ground Facility Designation.

This is called a "pseudo header" because it is used as a message header only for the purpose of generating the Integrity Check. It is never sent with the message. However, the pseudo header does have to be re-created by the receiver in order to successfully validate a received AMIC. As both ground and airborne systems already know this information, recreation of the pseudo header is not a problem.

The key improvement made by PM-CPDLC is that when the PM-CPDLC checksum is verified, it provides verification that the controller directed the clearance to the aircraft as identified by its Aircraft flight ID and this verification is independent of data handling functions in the ground system (Figure T.9). The importance difference with Figure T.8 is that the checksum is now at the application level and includes the Aircraft flight ID in its scope. This removes the vulnerabilities identified earlier as any error that results in the clearance being mis-directed to the wrong aircraft as the PM-CPDLC checksum will only be successfully verified if the Aircraft flight ID configured into the aircraft's avionics matches the Aircraft flight ID of the aircraft selected by the controller when the clearance was generated.

The only vulnerability left is the pilot failing to enter the correct Aircraft flight ID into the avionics when the flight starts. This could be the result, for example, a late change of aircraft with the pilot failing to re-enter the Aircraft flight ID.

To counter this vulnerability requires a means to independently verify the association between a Aircraft flight ID and an airframe. In order to achieve this, LINK 2000+ has also proposed the mandatory inclusion of the aircraft's 24-bit ICAO aircraft address as part of the filed Flight Plan, ref. [7030].

A.7.5.2 24-bit ICAO address in the flight plan

ICAO Doc 4444 (PANS-ATM) provides the means for including the 24-bit ICAO aircraft address into the flight plan, item 18 starting with the 'CODE/' indicator. However, insertion of this information is optional.

ICAO ANNEX 10 – Aeronautical Telecommunications – Volume III, Part I (Digital Data Communication Systems)–Chapter 3 specifies the requirements for CM and CPDLC.

Parameters used by CM are defined in ICAO Doc 9705, Sub-volume II, Manual of Technical Provisions for the Aeronautical Telecommunication Network (ATN). Aircraft 24-bit ICAO address is one of the mandatory parameters.

During the CM-Logon process, the ATN based data link equipped ATSU (Air Traffic Service Unit) must ensure an unambiguous association in the ground system between a CM-Logon Request from an aircraft and its corresponding flight plan.

For any exchange of CPDLC messages, the ATSU must ensure that the message is sent to the CPDLC network address of the corresponding aircraft.

CM-Logon

Before the establishment of a CPDLC connection between an ATSU and a specific aircraft, it is essential that the ATSUs system selects the corresponding Flight Plan (only flights having a Flight Plan can use CPDLC). This is achieved during the CM-Logon process.

During this process, the ATSU compares the aircraft flight identification, Airport of Departure (ADEP) and Airport of Destination (ADES) received from the aircraft with the aircraft flight identification, ADEP and ADES from the flight plan.

However, the combination of parameters may not always be unique and so it does not guarantee unambiguous association with the corresponding flight plan. Different flights may have same ADEP and ADES, while at the same time aircraft flight identification may be duplicated

In order to meet the required level of safety for integrity degradation, the verification of an additional parameter, available in both Logon Request and flight plan, is required.

<u>CPDLC exchanges</u>

After the establishment of the CPDLC connection, it must be ensured that any subsequent exchange of CPDLC messages occurs with the intended aircraft. The controller will normally send and receive CPDLC messages via the CWP (Control Working Position) Interface. Therefore, the controller will rely on the ATSU systems to ensure correct association between the information displayed for an aircraft and its corresponding CPDLC network address when:

- Sending a CPDLC message to that aircraft;

- Receiving a CPDLC message from that aircraft.

This requirement is achieved through the design of the ATSU systems to ascertain the corresponding aircraft's CPDLC network address. Safety analysis shows that mapping to/from the aircraft's CPDLC network address must be based on a mechanism entailing at least two independent processes to ensure a correct addressing of the CPDLC message.

Moreover, the best practices in mitigating safety hazards in such cases are to use independent sources for the data to be processed. Since the first set of parameters (aircraft flight identification, ADEP and ADES) is not sufficient to achieve the required level of safety to mitigate for the misdirection of CPDLC messages (1 error per 1 000 000 messages) additional parameters are needed for checking.

<u>Conclusion</u>

In addressing the above safety requirements the LINK 2000+ Pre-Implementation Safety Case (PISC) V1.0, [22], strongly recommends the use of a second **independent** parameter set for the FPL association and message distribution processes.

The evaluation of the available elements in both the flight plan and the CM-Logon request led to the conclusion that the most appropriate parameter is the 24-bit ICAO address.

The 24-bit ICAO address is considered **independent** because it is specific to the aircraft and normally not changed. The aircraft address is "hard wired" in the aircraft equipment (e.g. Personality Module) and therefore not subject to either flight crew error input when entering such data in the aircraft equipment nor to some aircraft software memory management error when "reading" it as part of the flight plan data.

It should be added that the verification of the aircraft address also supports the AMIC.

Consequently, the processes for enabling and conducting CPDLC will consist of:

- o During CM-Logon, the comparison of aircraft flight ID, ADEP, ADES and 24-bit ICAO address received from the airborne systems with the same parameters extracted from the corresponding flight plan.

- o Upon successful logon, any subsequent exchange of CPDLC message will entail running of two independent processes, using independent data sources.

The AMIC algorithm is given in doc. 9880, part 1, vol 6

A.7.6 Aircraft Identification

This specific issue merits attention since different terms may be encountered in various documents. We do not discuss the question of whether any terminology is proper. The terms we use in the LIT guidance documents are highlighted in **BOLD**.

Terminology	Note	Example
• Aircraft Flight Identification (**Aircraft Flight ID**) • Flight ID • ICAO Call Sign (*)	• Entered in FMS • Field 7 in ICAO flight plan • 3 letters + up to 4 alpha-numeric characters	BAW1234
Flight number		1234
Aircraft address **24-bit ICAO address**		3C6501 (+)
IATA address IATA Flight ID	Note used in ATC	BA1234
Aircraft Registration number Aircraft Registration Tail Number	Used for FANS 1/A Up to 7 characters (including hyphen)	F-ABCD

(*) The "Call Sign" normally corresponds to the ATC verbal designation, such as "Speedbird 1234" in this example, but the above terminology is sometimes encountered.

(+) a mapping between 24-bit ICAO addresses and aircraft details can be found via the EUROCONTROL PRISME database, although some public Internet sites will provide relevant information as well.

Reference [28] LINK 2000+: Flight Crew Data Link Guidance for LINK 2000+ Services, V. 4.0, 30 June 2009 notes that flight crews should logon using the Aircraft flight ID (ex: SAS593, DLH23) as filed in the ICAO flight plan, field 7 and that they should **not** use the two-letter IATA Flight ID (ex: **SK**593, **LH**23), or insert a leading zero [0] into the Aircraft flight ID (ex: SAS**0**593, LH**00**23), as doing so will result in a failed logon.
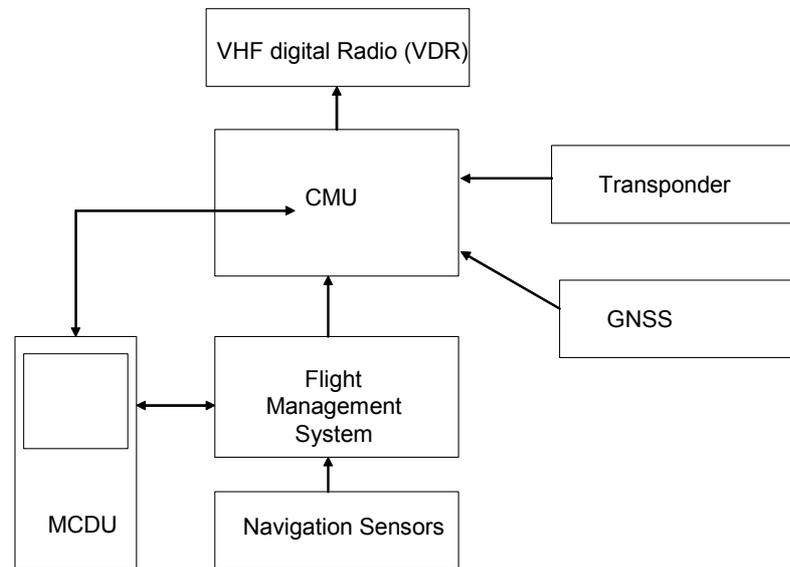
A.7.7 Avionics Architecture

Two main families of avionics architectures can be encountered: federated or integrated[5], and they can be both offered by vendors depending on airframe type.

A basic functional diagram based of a federated architecture is shown below, The figure is generic since units can be physically doubled.

In a federated architecture, the Communications Management Unit (CMU)/Airbus ATSU provides access to all data communications services and hosts the ATN Airborne Router and End System. One of the on-board VHF Digital Radios (VDR) is used for VDL Mode 2.

---

[5] Integrated Modular Architecture (IMA) and Distributed IMA (DIMA)

Figure 2 - Aircraft Implementation - General Avionics Architecture

The Flight Management System (FMS) provides information to the CMU (Flight number, departure airport, arrival airport). The Multi-function Control and Display Unit (MCDU) is used to prepare and receive preformatted messages exchanged with the ground.

> *Note: For the Airbus ATSU, a separate screen, the Data Link Control and Display Unit (DCDU), is used for data link messages exchange.*

All CPDLC messages sent to the ground must be time stamped with an accuracy of better than 1 second. Therefore a Global Navigation Satellite System (GNSS) receiver is generally implemented. At the time of writing the prevalent GNSS in use is the Global Positioning System (GPS). The GPS receiver can be standalone or incorporated in a Multi Mode Receiver (MMR). If the clock of the aircraft is synchronised to the GPS, this will reduce the drift of the clock information. The clock is used to time stamp downlink CPDLC messages, and to verify the transit delay of uplink CPDLC messages.

The transponder may provide the CMU/Airbus ATSU with the 24-bit ICAO address of the aircraft. This information is needed for VDL Mode 2, CM and Protected Mode CPDLC

A.7.8 Documentation

LINK 2000+ official references

The official LINK 2000+ baseline reference list is given in refs. [21] and [22]. It includes ICAO **Doc. 9705, ed 2 + "PDRs listed in ED110B**".

General Bibliography

The bibliography provided below contains information of varying nature, from standards to working papers, tutorials, books, etc, all supporting a reader wishing to obtain more detailed information than given in this tutorial section. Note that web page URL's below were correct at the time of writing but of course may evolve. A reader having difficulty finding a listed reference can contact the LIT Secretary.

ICAO

[9]   ICAO ATN SARPs: Annex 10, Vol. 3, Chapter 3

[10]   ICAO Doc. 9705: Manual of Technical Provisions for the ATN

Doc. 9705, ed. 2 + PDR are available on the ICAO ACP web site at:

http://www.icao.int/anb/panels/acp/index.cfm

[11]   ICAO VDL SARPs: Annex 10, Vol. 3, Chapter 6

[12]   ICAO Doc. 9776, Manual on VDL Mode 2

[13]   ICAO Doc. 9739: Comprehensive ATN Manual – available at
http://www.icao.int/anb/panels/acp/atnp/misc/DOC9739/

[14]   ICAO Doc. 9880, Part 1 - (Chapter 6: AMIC)

Document 9705 ed.3 (which is not equivalent to Doc 9705 ed. 2 + PDR because it contains extra features), is being replaced by Doc. 9880, which is in 'unedited advance version as approved, in principle, by the Secretary Genera' state at the time of writing.

Doc. 9880 Part 1 contains 'air-ground applications' including CM and (PM) CPDLC, and the algorithm for AMIC computation in Chapter 6.

[15]   Doc 7030 amendment for 24-bit
http://www.paris.icao.int/documents_open/subcategory.php?id=68

OTHER STANDARDS OR GUIDANCE

[16]   EUROCAE ED-110B

[17]   EUROCAE ED-120

[18]   ARINC 631-5

[19]   RTCA DO-224 (VDL MASPS) and ED-92 (VDL MOPS)

EUROCONTROL and EUROPEAN COMMISSION

[20] LINK 2000+: the web page contains many references, see
http://www.eurocontrol.int/link2000/public/standard_page/baseline_post_pioneer.ht
ml ; see also http://www.eurocontrol.int/vdl2 for details on VDL mode 2.

[21] DLS IR: Commission Regulation (EC) No 29/2009 of 16 January 2009 laying down
requirements on data link services for the Single European Sky

[22] EUROCONTROL Specification on Data Link Services , V 2.1, 28 January 2009

[23] LINK 2000+: Network Planning Document (NPD), V. 3.4, 1 May 2007

[24] LINK 2000+: Interpretation of EUROCAE ED-120/RTCA DO-290 Performance
Requirements, V. 1.3, 4 May 2007

[25] LINK 2000+: Generic Requirements for a LINK 2000+ Air/Ground Communications
Service Provider (ACSP), V. 1.5, 14 Aug. 2008

[26] LINK 2000+: ATN Naming and Addressing Plan, V. 1.2, 19 May 2004

[27] LINK 2000+: ATC Data Link Guidance for LINK 2000+ Services, V. 5.0, 30 June
2009

[28] LINK 2000+: Flight Crew Data Link Guidance for LINK 2000+ Services, V. 4.0, 30
June 2009

[29] Maastricht AGDL page
http://www.eurocontrol.int/agdl/public/subsite_homepage/homepage.html

[30] LINK 2000+: Pre-Implementation Safety Case,
http://www.eurocontrol.int/link2000/public/standard_page/specific_docs.html#4

[31] EUROCONTROL Safety Assessment Methodology:
http://www.eurocontrol.int/safety/public/site_preferences/display_library_list_public.h
tml#8

ARTICLES, MISCELLANEOUS

[32] PM (high level cover paper): WG-N 5
http://www.icao.int/ANB/PANELS/ACP/WG/N/wgn5/wgn05.html

[33] "FANS-1/A Technical Capabilities", Data Link Steering Group, Second Meeting,
DLSG/2, Working Paper / 2, Paris, Sept. 2005 (see
http://www.paris.icao.int/documents_open_meetings/subcategory.php?id=42)

[34] "LINK 2000+: A European programme for better communication in ATC", DSNA/DTI
Technical Review, December 2005 (see http://www.dsna-dti.aviation-
civile.gouv.fr/actualites/revuesgb/index.html)

[35] "EOLIA: European pre-operational data link applications", DSNA/DTI Technical
Review, December 2000, " http://www.dsna-dti.aviation-
civile.gouv.fr/actualites/revuesgb/revue59gb/59pgarticle1gb/fr59art1gb.html

[36] Airbus Flight Operations Support and Services "Getting to grips with FANS", Issue
III, April 2007

[37] Air Europa, "Data link communications", Private Communication (J. Manzano, J.
Rossello)

BOOKS

[38]   F. Halsall "Data Communications, Computer Networks and Open Systems", 4rd Edition, Addison-Wesley, 1996

[39]   D. Piscitello, A. Chapin "Open Systems Networking – TCP/IP and OSI", Addison-Wesley, 1993

[40]   R. Pužmanovà "Routing and switching", Addison-Wesley, 2002 (section 12.6 covers OSI protocols)

[41]   CISCO "Internetworking Technologies Handbook", 4/e, Cisco Press 2004 (available on-line – chapter 30 covers OSI protocols - http://www.cisco.com/en/US/docs/internetworking/technology/handbook/ito_doc.html)

[42]   O. Dubuisson "ASN.1", available at http://www.oss.com/asn1/dubuisson.html

[43]   J. Larmouth "Understanding OSI", available at http://www.business.salford.ac.uk/legacy/isi/books/osi/osi.html

EUROCONTROL