HYBRID DATA BUS FOR REAL TIME APPLICATIONS IN AN AIRCRAFT CABIN

P. Klose
AIRBUS Operations GmbH
D-21614 Buxtehude, Germany

Abstract

In the context of LuFo IV a hybrid communication protocol basing on TDMA is developed. The protocol enables the integration of real time communication and standard IP services on the same network. In today's AIRBUS aircrafts all cabin management functions are controlled and monitored by the CIDS. CIDS uses a proprietary real time protocol which provides excellent digital audio transmission but has no provisions for integration of IP services. The new hybrid protocol combines both, CIDS and IP services on the same physical medium without any interference. A time domain segregation of both protocol parts assures that IP data can not disturb the safety critical data of CIDS. At the same time broadband IP services can be provided for non safety critical applications.

1. MOTIVATION

The aircraft cabin becomes more and more important for the competition among airlines since this is the aircraft part that is perceived by the passenger. Essential elements supporting the attractiveness of the cabin are layout flexibility for an easy adaptation to customer demands and high integrated system functionality. Achieving those goals require a fully interconnected cabin. The data communication between the cabin devices and functions show various requirements on the network architecture and communication protocol. The protocol has to ensure a reliable real time communication between safety critical functions as well as a broadband data exchange for multi media applications. At the same time the protocol shall support flexibility regarding cabin layout changes, integration of new functions and support of new evolving technologies during aircraft life. The answer to these challenges can be a hybrid data bus as presented in this paper.

2. HYBRID DATA BUS

The hybrid data bus shall be suitable to replace the current backbone bus of today's cabin intercommunication data system (CIDS), which is the cabin management system of all AIRBUS aircrafts. Further functions to the CIDS backbone shall be added by enabling parallel IP (Internet Protocol) data communication on the same physical line.

The current CIDS protocol is a proprietary real time communication protocol that uses the physical layer of the standard 10 MBit/s Ethernet similar 10Base-T, IEEE 802.3 clause 14 [1]. Compared to the 10Base-T standard the CIDS backbone network is a real bus even when using twisted pair wiring. For the hybrid network not only the protocol changes but also the physical layer and network topology changes due to the used 100 MBit/s communication link.

Main components of CIDS are a server called Director (DIR) which communicates with the Decoder Encoder Units (DEU) via the different backbone lines called top-line and middle line, depending on the functionality of the end devices connected to the respective line. The DEU is a network node which distributes the received data to the end devices and sends the collected data back to the DIR, refer to figure 1.

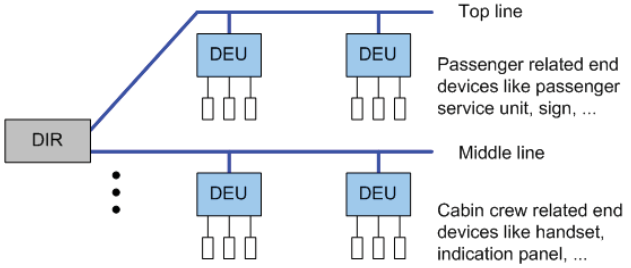

FIGURE 1. Principle of today's CIDS

The timing of the whole CIDS data communication is derived from the requirements on the audio functionality, e.g. a sample rate of 32 kHz for the top line. Keeping those features in mind, the requirements for a new hybrid backbone can be elaborated.

2.1. Requirements and Concept

The requirements of a future hybrid protocol are mainly defined by the today's top and middle line protocols:

- All functions of today's protocol shall be maintained, e.g. timing and deterministic behaviour of the network.
- The frame rate on the hybrid backbone shall be kept at 32 kHz to be compliant with the CIDS audio functionality.
- It shall be possible to transmit IP data in both directions between director, DEU and end-units, respectively.

- This IP communication shall be possible additional to the existing real time communication.
- The transmission of IP data must not influence the real time data transmission.
- The transmission of IP data shall be transparent for the IP based end units, i.e. all higher layer protocols shall be supported.

The basic concept of the hybrid data bus is to put the data from the director, which is transmitted with 10 MBit/s full duplex, onto a 100 MBit/s full duplex communication network. This provides 90% unused bandwidth on the backbone as a first estimation. The unused bandwidth can now be used for additional data transmission, e.g. for non real time data using standard IP and higher layer protocols.

The hybrid protocol is TDMA (time division multiple access) based for keeping the real time constraints. In each time slot a hybrid frame, composed of a real time part and an IP part is sent on the backbone. The time slots have the same size as today's CIDS protocol. The composition and de-composition of the hybrid frame is handled by a multiplexer and de-multiplexer respectively, as depicted in figure 2.

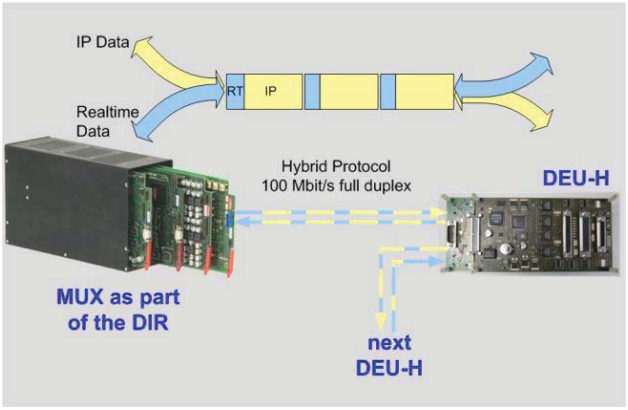

FIGURE 2. Concept of hybrid protocol

The multiplexer and the de-multiplexer are functional blocks, which are integrated in all backbone nodes in the same manner since the communication is bi-directional. As a first approach the multiplexer / de-multiplexer block, just called MUX, can be built as a standalone unit to combine the data streams of the director with the data streams from a standard IP server (e.g. standard PC). All end devices are connected to the backbone via the DEU-H (DEU of the type "hybrid").

The separation of the IP and the real time (RT) data as well as the strict adherence to the time slots is controlled by programmable hardware circuits (FPGA). This ensures the strict segregation of both data worlds (RT for safety critical data and IP data for non critical information). Only if both types of data can not impact on each other a certification of the hybrid network for systems which are classified as DAL-C [2] (design assurance level C) or higher can be achieved.

2.2. System Architecture

The system architecture can be split up into three parts:

- Network topology, describing the physical layer of the hybrid network.
- Collision avoidance, describing the methodology for a collision free data transmission.
- Data frame composition, describing the hybrid frame composition out of RT and IP data streams and the subsequent de-composition at the receiver.

2.2.1. Network Topology

The change of the data rate from 10 MBit/s to 100 MBit/s implies also a change of the network topology. A bus topology with a tapping of the line for each network node is no longer possible for the higher data rate. The physical layer of the used 100 Base-T Ethernet standard defines only point to point connections. The normal network topology for 100 Base-T would be a star architecture with a central switch interconnecting all nodes of one segment. This architecture would show two drawbacks. One central switch would be a single point of failure and thus reducing the reliability of the whole system. The spatial distribution of the DEU in the aircraft cabin shows a line structure from the forward to the aft section of the fuselage. A star architecture from the DIR, which is located in the electronic bay in the aircraft nose, to all DEU in the cabin, would cause high cabling effort, increasing weight and cost compared to today's bus architecture. A bus like topology with point to point connections is a daisy chain. Each node receives all data and forwards it to the next node. A normal daisy chain is prone to failures of preceding nodes. A failing node would cut off all following nodes in the line from the communication. One possible solution is the installation of a fail safe switch at each node.

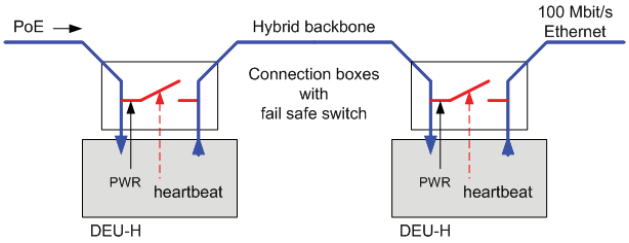

FIGURE 3. Daisy chain with fail safe switch

The function of the fail safe switch is the physical bridging of a failing DEU. The failure can be due a loss of power for the DEU, a DEU hardware failure or a software crash. The fail safe switch has two positions:

- In the normal operating state, it connects the backbone with the connected DEU. This state remains active as long as it is triggered from the DEU through a heartbeat signal.
- In case of loss of the heartbeat signal, the fail safe switch bridges the DEU and connects directly the receive line from the preceding DEU with the transmit line to the next DEU. The loss of heartbeat may be caused by various reasons:
  - Loss of DEU power
  - Serious DEU hardware failure
  - Crash of DEU software

- DEU not installed but installation is prepared

The fail safe switch returns automatically to the normal operating state, when the heartbeat is detected again, e.g. after a reset of the DEU. For covering the “failure” case of a not installed DEU without interrupting the backbone line, the fail safe switch is installed in a separate unit called connection box. This box connects the DEU with the backbone and contains all parts necessary to keep the line operable in case of a DEU failure.

The ideal design of a fail safe switch would be a normally closed switch in unpowered mode. This kind of switch is a classical mechanical relay, which connects the DEU to the backbone only if powered. Unfortunately those mechanical relays have several disadvantages like high weight and large size compared to semiconductor switch elements. The biggest problem however is the reliable high bit rate transmission over the mechanical contacts. As a consequence, the fail safe switch is realised with a standard semiconductor LAN switch IC. Such a device needs to be powered in any case for data transmission. This makes the powering of the fail safe switch to become a critical item of the whole daisy chain. For safety reasons the fail safe switch is powered redundantly via different routes. Normally the fail safe switch is powered from the DEU. This works for normal operating mode of the switch, crash of DEU software and probably for DEU hardware failures (depending on affected hardware parts). The second route for powering the fail safe switch is the backbone itself, using PoE (Power over Ethernet) technology. Power is injected into the backbone from the director to feed the fail safe switch in case of loss of power from the DEU. This could happen if the DEU power is lost, certain DEU hardware failures occur or the DEU is not installed and connected to the connection box. The introduction of a fail safe switch and its redundant powering allows failing of several, even consecutive DEU without loss of the whole backbone line.

2.2.2. Collision Avoidance

The daisy chain topology implies the usage of a shared medium as backbone, like today the bus topology. Connecting several network participants to a shared medium backbone makes data collisions possible if no means for a controlled network access are implemented. At least the collision detection has to be implemented but for the envisaged real time capability collision avoidance is mandatory. Time division multiple access (TDMA) has been selected as method for assuring a collision free communication.

TDMA is a network access method using dedicated, not overlapping time slots for each network participant, during which it is allowed to send its data on the shared medium. TDMA is a kind of time division multiplexing (TDM) technique. The available bandwidth (data per time in this context) is partitioned among the participants by dividing the time into time slots. Each network participant has the full bandwidth available during its assigned time slot but must not send data at any other time. The critical subject for a TDMA network is the common knowledge about the time slots and timing for all network participants. Without such global knowledge individual nodes may violate the network constraints. Two different approaches may be followed for the design of a TDMA network and distribution of its characteristic properties.

The first approach is a time controlled network with independent operating nodes, i.e. each node decides for itself the correct time for accessing the network. In such a network the following information has to be distributed to all nodes:

- Time slot assignment.
- System time.

The drawbacks of such a system are obvious from the above mentioned requirements. Each node has to be configured according to the network time slot design and the clocks have to be synchronised. Depending on the frequency of clock synchronization the stability of each individual clock is essential. Diverging clock would cause violating of timing constraints and thus data collisions on the network.

The second approach is a centrally controlled network in which a master triggers each node to send its data. No clock synchronisation is required and only the master needs to be configured according to the time slot design. This approach is followed for the hybrid data bus.

The DIR operates as network master. The DIR sends data to the DEU in a fixed timing pattern. The DEU are addressed consecutively. Only the addressed DEU sends its data back thereupon. All data from the DIR to any DEU is sent as broadcast to distribute general and individual information in one message frame. The individual data is processed only by the addressed DEU. All data are forwarded to the next DEU, independent of the destination address. The answer from a DEU to the DIR is sent as unicast, i.e. the message is addressed only to one recipient, the DIR. The return messages are also forwarded from one DEU to the next until the DIR is reached. The answer must fit into the assigned time slot to avoid data collision on the back channel. This is handled by the used protocol. Since no direct communication between any two DEU is foreseen, this TDMA design approach assures collision avoidance on the backbone.

2.2.3. Data Frame Composition

The basic idea of the presented system is the transmission of real time and standard IP data on the same physical link. Therefore both types of data are composed to hybrid data frames before sending the data on the network. The hybrid frames can be received only by dedicated devices, the DEU-H. In those devices the hybrid frame is split up again in RT data for standard CIDS equipment and IP data for standard IP equipment, refer to figure 4.

The composition of the hybrid frame is performed in the multiplexer block. The DIR delivers the RT data of fixed length and with a strict timing to the multiplexer block. This timing can be seen as the system clock rate T, at which also the hybrid frames are transmitted. The data rate for the link between multiplexer and DIR is 10 MBit/s. The RT data is put into the hybrid data frames with exactly the same timing as delivered from the DIR but the transmission rate is 100 MBit/s. In parallel the IP data is fed into the multiplexer. The IP data is sent as standard Ethernet frame with variable length from 64 to 1522 Byte

according to the Ethernet standard. The IP data may be buffered in a FIFO (first in first out) memory in case the data is received as burst an can not be transmitted on the hybrid line as fast as received. Due to the designed system clock rate T, a hybrid frame can not carry a whole Ethernet frame of full length. Thus the Ethernet frame has to be fragmented if its length exceeds a certain value. Each hybrid frame comprises exactly one RT frame and one fragment of the Ethernet frame.

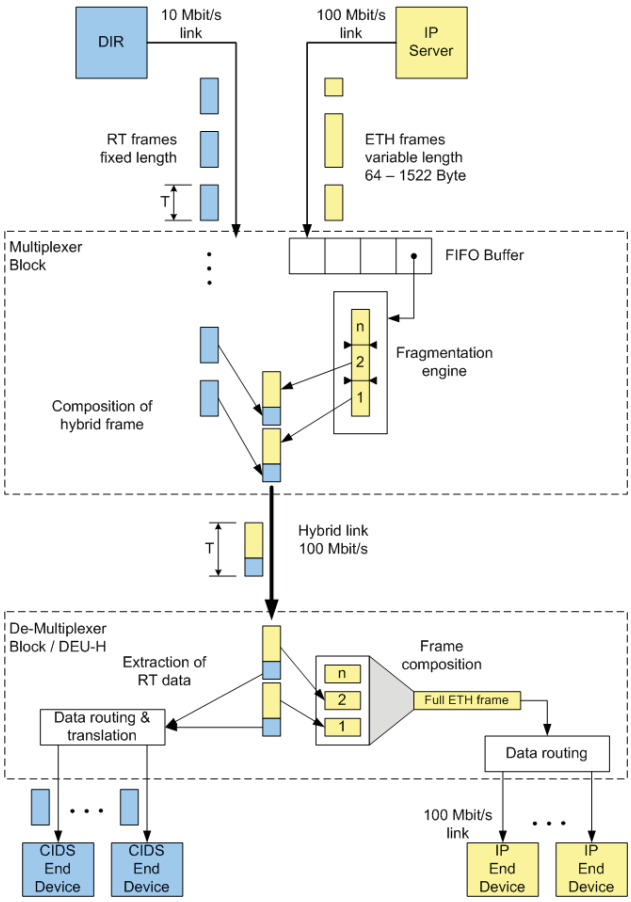

FIGURE 4. Hybrid data frame composition

The receiving network node, in this case a DEU-H, comprises a de-multiplexer block for processing the hybrid frames. This block extracts the RT data from the hybrid frame and passes the data to the standard routing and translation function of a DEU. Here the data may be translated into another protocol, depending on the addressed end device and routes the data to the correct device. The Ethernet fragments are passed to a frame composition function, which restores the original full Ethernet frame and checks for correctness of the frame. This full frame can be understood by any COTS (commercial off-the-shelf) Ethernet compliant device. A routing / switching function passes the data to the addressed IP end device.

Figure 4 shows only one direction of data transmission, from the server to the end devices. The counter direction is set up in the same way but with the multiplexer block in the DEU-H and the de-multiplexer block at the DIR / IP-server.

2.3. Communication Protocol

The hybrid frames are composed of one real time segment and one IP data segment. The segments are separated by a gap, for segment start detection. Therefore a gap is also appended to the IP data segment. Due to the integrated gaps, the hybrid frames can be sent back to back.

A hybrid frame has a length of T=31.25 µs which equals 3125 bit at a bit rate of 100 MBit/s. This time is derived from today's CIDS system timing and audio requirements. As shown in figure 5, the hybrid frame provides 608 bit for RT data and 2216 bit for IP data.

Hybrid Frame (3125 Bit = 31,25 us @ 100 Mbit/s)			
RT-Data	Gap	IP-Data	Gap
608 Bit	150	2216 Bit	151

FIGURE 5, Hybrid data frame

The real time segment, as depicted in figure 6, starts with an Ethernet compliant preamble, followed by a type field. The first two bits of the type field specify whether the following payload shall be interpreted as RT or IP data. For a RT segment the CIDS top line or middle line data frame is copied one to one into the payload. This includes the CIDS destination address and a checksum for safeguarding the transmitted data. The protocol of the TL and ML differ according its structure and content. The option field indicates the line type.

RT-Data				
SYNC	Type		CIDS TL / ML Data	Stuff	
8	1		66,75	0,25	Byte
64	2	6	534	2	Bit
Preamble	Type	Options	Payload	Stuff	

FIGURE 6, Real time segment of hybrid frame

The IP data segment is used to tunnel non real time data from an IP server to an IP end device over the hybrid backbone. As shown in figure 7, the IP segment also starts with a preamble and a type field. In case of an IP segment the options field specifies whether the following payload shall be interpreted as Ethernet frame fragment or configuration protocol format. The configuration protocol format is a future option and not yet specified. The maximum payload of the IP segment is 255 bytes whereas standard Ethernet frames have a length between 64 and 1522 byte. Thus Ethernet frames exceeding 255 bytes have to be fragmented. Since the Ethernet standard does not specify a frame fragmentation, a proprietary fragmentation algorithm is implemented. The algorithm simply cuts the whole Ethernet frame, including source and destination MAC address, type field, optional VLAN tag and checksum into pieces. Each of the IP data segments holds 255 bytes of information coming from the original Ethernet frame. Due to the fragmentation algorithm additional control information is included in each frame as header. The header contains information about number of packets which belong to a single Ethernet frame and the length of the single fragment and the full Ethernet frame. Additionally, the complete fragment and header is secured by a 32 bit checksum and a time stamp.

This information is used at the receiver to validate the sequence and for regeneration of the original Ethernet frame. The source address in the header correspond the to the source address of the RT segment. The source and destination address of the IP end device is coded in the payload. Additional address information is not required since all data to the DEU-H is sent as broadcast and any DEU-H can send its data only to the server/DIR.

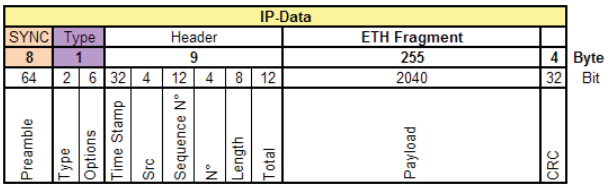

FIGURE 7, IP data segment of hybrid frame

The tunnelling of complete Ethernet frames as fragments between the participants of the hybrid network makes the system transparent for any higher layer protocol.

3. VERIFICATION

For the verification of the hybrid data bus a system has been set up which comprises the following components:

- Original CIDS devices; one director, two passenger service units (PSU), and one handset for passenger announcements connected to the DIR
- Hybrid bus nodes; two DEU-H, one operating as MUX/De-MUX unit for the DIR and IP server, the other operating as DEU-H for the PSU
- One Anritsu data quality analyser MD1230B for Ethernet, serving as IP server and IP end device (data sink) using two of its independent ports

The correct transmission of RT data has been tested by functional tests of CIDS. Therefore it was tested if signs can be switched from the director and a passenger call from the PSU is recognised correctly by the DIR. For assessing the time critical audio functions, passenger announcements have been performed and boarding music was played. The result is that CIDS operates without any difference compared to the original system.

The IP communication has been tested with the data quality analyser by performing automatic throughput tests according RFC2544 [3]. The throughput has been measured for both directions separately (server → end device and end device → server). The test results have been compared with the theoretically expected values.

For the computation of the theoretical values the following characteristic system data apply:

- Ethernet bit rate: 100 MBit/s
- Hybrid frame length: 31.25 µs
- ETH fragment: 255 byte
- Hybrid frames: 32000 per second
- Frames / DEU /s: 2000 (16 DEU per line)

The throughput depends on the frame size of the original Ethernet frame due to its fragmentation, as shown in table 1. The throughput rate depends further on the transmission direction. One DEU can send only each 16th time slot, whereas the server sends its data as broadcast each time slot.

		DEU -> Server		Server -> DEU	
Frame length (byte)	Fragments	Frames/s	Bit/s	Frames/s	Bit/s
64	1	2000,00	1024000	32000,00	16384000
128	1	2000,00	2048000	32000,00	32768000
255	1	2000,00	4080000	32000,00	65280000
256	2	1000,00	2048000	16000,00	32768000
512	3	666,67	2730667	10666,67	43690667
1024	5	400,00	3276800	6400,00	52428800
1280	6	333,33	3413333	5333,33	54613333
1518	6	333,33	4048000	5333,33	64768000

TAB 1, Theoretical throughput rate

The throughput rate has been measured with the RFC2544 test, which is a search test. During the test the analyser tries to find the maximum possible data rate automatically. Therefore a search resolution and accepted loss rate has to be defined. The resolution was set to 0.01% of 100 MBit/s and the loss rate to 0.1%. The measured values and relative deviation between measured and theoretical value are shown in table 2.

		DEU -> Server		Server -> DEU	
Frame length (byte)	Fragments	Bit/s	Deviation	Bit/s	Deviation
64	1	1020928	-0,30%	16380928	-0,02%
128	1	2049024	0,05%	32778240	0,03%
255	1	4080000	0,00%	55404360	-15,13%
256	2	2048000	0,00%	32759808	-0,03%
512	3	2732032	0,05%	43679744	-0,02%
1024	5	3268608	-0,25%	52420608	-0,02%
1280	6	3399680	-0,40%	54599680	-0,02%
1518	6	4043952	-0,10%	64763952	-0,01%

TAB 2, Measured throughput rate

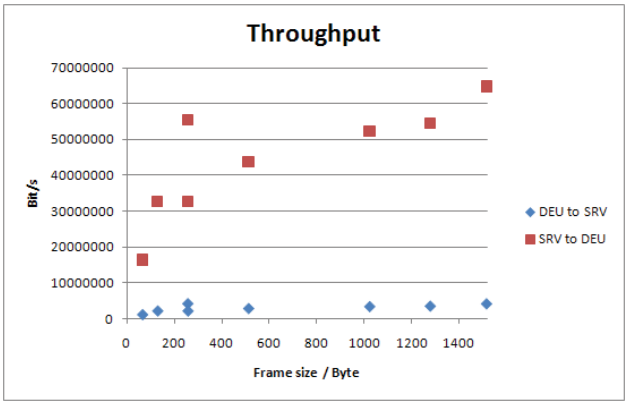

FIGURE 8, Measured throughput rate depending on transmission direction

The effect of frame fragmentation is well shown in figure 8, exemplary for the step from 255 byte to 256 byte. The increase of one byte frame size halves the throughput since the number of fragments to be transmitted doubles. This effect repeats generally for each multiple of 255 byte (not shown in detail due to the selected measurement points).

The test of the real time behaviour and the throughput tests for IP data have been performed in parallel to show the hybrid characteristic of the communication network. The IP data transmission does not influence the real time

communication and vice versa. The measurement results show the successful implementation of the hybrid communication protocol.

4. CONCLUSION

The hybrid data bus combines the advantages of deterministic communication and standardized IP based systems. Real time and non-real time applications do not affect each other. Therefore different kind of services can be provided in parallel on the same network. A typical application could be the distribution of video data from a cabin video monitoring system (standard IP communication) on the same line as used for CIDS (proprietary real time protocol). Another scenario could be an enhanced PSU equipped with a small display which provides additional information, like news or weather data to the passenger. Due to the parallel IP communication no change of the current CIDS protocol or cabin network is necessary. The mentioned examples show the benefits of the hybrid system. Multiple usages of physical lines reduce cabling efforts, which saves weight and costs and enables new services.

The hybrid system is not limited to the presented 100 MBit/s copper network. A future step will be the implementation of the hybrid protocol on a fibre optical network with 1 GBit/s transmission rate. The general principle remains the same.

5. ACKNOWLEDGEMENT

The work on this project is funded by the BMWi (Bundesministerium für Wirtschaft und Technologie) in the context of the LuFo IV project. The project is lead by the pre-development team of AIRBUS Buxtehude. A further partner for the development work is TES Electronic Solutions in Stuttgart, Germany. First investigations have been performed in the context of a diploma thesis by M. Fette [4].

6. ABBREVIATIONS

CIDS	Cabin Intercommunication Data System
COTS	Commercial Off-The-Shelf
DAL	Design Assurance Level
DEU(-H)	Decoder Encoder Unit (of type H)
DIR	Director (CIDS central computer)
ETH	Ethernet
IP	Internet Protocol
LAN	Local Area Network
LuFo	Luftfahrtforschungsprogramm
MAC	Media Access Control
ML	Middle Line (type of CIDS network)
MUX	Multiplexer/De-Multiplexer Unit
PoE	Power over Ethernet
PSU	Passenger Service Unit
RT	Real Time
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TL	Top Line (type of CIDS network)
VLAN	Virtual LAN

7. REFERENCES

[1] IEEE Standard 802.3, “Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specification”, December 2008.

[2] EUROCAE ED-80 / RTCA DO-254, “Design Assurance Guidance for Airborne Electronic Hardware”, April 2000.

[3] S.Bradner and J.McQuaid, “Benchmarking Methodology for Network Interconnect Devices”, IETF RFC2544, March 1999.

[4] M.Fette, “Untersuchung eines hybriden Protokolls für die Übertragung von sicherheitsrelevanten und IP-basierten Daten über einen gemeinsamen Datenbus“, Diplomarbeit TU Hamburg-Harburg / AIRBUS Operations GmbH, January 2009