Smoke Detectors interfaced by a safety critical aircraft based CAN-Bus Network

Ralph Knueppel, Christian Schmid, Airbus Deutschland GmbH, Bremen, Germany

Classic architectures of aircraft systems contain equipments using interfaces with digital, analogue or discrete signals. The electrical network to interface the equipments varies between the applications. Some equipment requires a dedicated power supply and provides information on an analogue current loop, while others use proprietary digital busses or discrete I/Os for information exchange.

CAN initially was developed for use in the automotive industry, but is nowadays being used in an increasing number of applications. One of these areas is aviation, where CAN in the past 5 years has grown from being an exotic newcomer to an established and widely accepted solution. Within the Fire Protection System on an Airbus, smoke detectors are installed in various areas overall in the pressurized zones of the aircraft like lavatories, equipment bays and cargo compartments. As the CAN bus defines only layers 1 and 2 of the OSI communication model, additional higher layer features are necessary to achieve the level of operational assurance required for a safety critical application, namely fire protection on an aircraft.

This paper is particularly focused on the development of a safety critical CAN bus network with strict configuration control of smoke detectors in the scope of an aircraft application. International airworthiness authorities in 2003 approved the application in the frame of the Airbus A318 Type certification.

1 Introduction

The objective of the new Smoke Detection System was to replace the proprietary current modulated supply and communication loop with an open, non-proprietary bus standard. The overall system reliability and performance was to match or surpass the existing architecture while keeping development and purchasing costs at a comparative level.

The latter was feasible by reusing the existing smoke detector core, and fitting it with an altered communication and power interface (see figures 1 and 2).

The communication medium had to meet a number of requirements for eligibility in a safety-critical application:

- Advanced data integrity, and error detection features
- Deterministic behavior
- Operability in challenging EMC environments
- High degree of flexibility in choice of network size and topology

Considering the 30-year design life of a modern passenger aircraft, the long-term availability of electronic components was scrutinized in order to minimize the risk of equipment redesign resulting from component obsolescence throughout the life cycle of the aircraft.

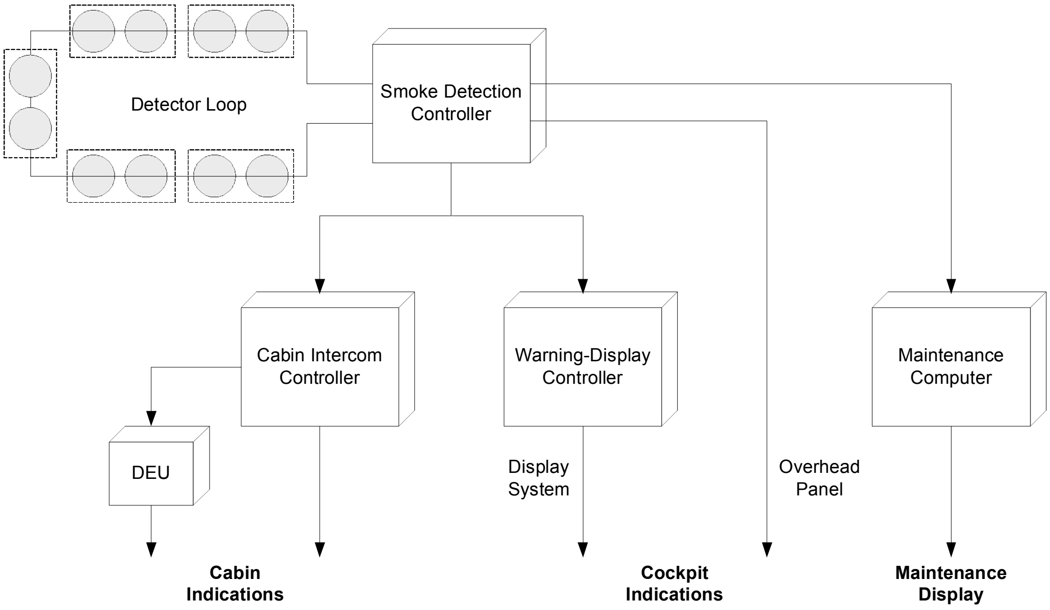

Figure 1: Smoke Detection System using proprietary detector supply & communication loop

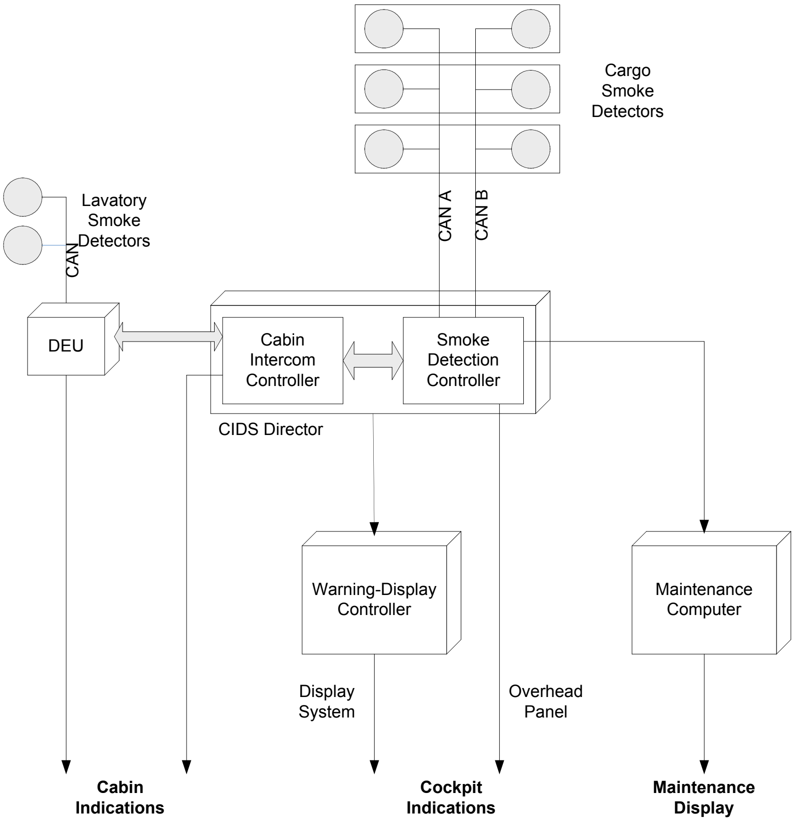

Figure 2: Smoke Detection System using an open standard CAN bus to interface detectors

The CAN bus was deemed the most suitable communication medium capable of fulfilling the above requirements.

2 Protocol

The CAN protocol, as defined in ISO 11898 [1], covers layers 1 and 2 of the OSI communication model. The remaining

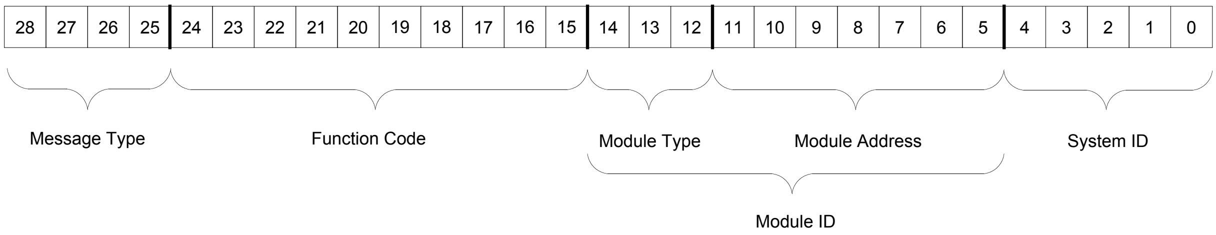

Figure 3: CAN identifier

layers up to layer 7 have to be managed by additional services up to the application. Various standardized higher layer protocols such as CANopen are available and widely used in industrial applications. Instead of selecting a generic high layer protocol, a specific to-type application layer protocol was developed and documented in a System Interface Document [2] in order to ease compliance with RTCA/DO-178 [3] guidelines.

Analysis of the communication needs resulted in the following protocol requirements:

- Every individual smoke detector on the network must be uniquely identifiable
- Messages generated by a smoke detector must contain information about its identity
- Support a Master-Slave communication model

CAN identifier

The 29 bit extended identifier is utilized, and partitioned into the sub fields as shown in figure 3.

Message type

The purpose of the Message Type is to categorize messages according to their overall relative priority and indicate whether the Module ID contains a transmitter or receiver address. Two classes of Message Type, Process Data Object (PDO) and Service Data Object (SDO) are instantiated either as Transmit or Receive objects; T_PDO and R_PDO as well as T_SDO and R_SDO respectively. A Transmit Data Object (T_xDO) denotes the Module ID contains the network address of the transmitter, whereas a Receive Data Object (R_xDO) contains the network address of the intended receiver in the Module ID field.

Function code (bits 24..15)

Every application function is designated a unique Function Code within its respective Message Type. In addition to describing the next level of arbitration priority, the Function Code is used to transport logical data without the use of the actual CAN data fields. In this case the Data Length Code (DLC) is 0, enabling efficient use of data bandwidth, particularly for R_PDOs and R_SDOs which contain mostly status requests directed at smoke detectors and don't carry any further information than the request itself.

Module ID (bits 14..5)

The Module ID field contains the unique network identification of the CAN node. This may also be a broadcast identification when a message is directed at several nodes simultaneously. Two sub fields Module Type and Module Address split the Module ID into equipment classes and their individual addresses. The entire Module Address space may be reused for every Module Type on the network.

System ID (bits 4..0)

The System ID is used to tag the CAN identifier with a unique system identification code. All smoke detectors and other fire protection components are assigned a fixed value.

Data frames

A Data Frame is generated by a transmitter to transfer application data to one, or in the case of a broadcast, several receivers. Within the Data Frame, the Data Field consisting of 1-8 bytes carries the application data. A Data Frame may contain an empty Data Field (DLC = 0). In this case, data is carried through the Function Code alone.

Data byte	MSB	LSB	Description	Format
1	7	5	spare / not used	-
	4	4	Detector Warning	Discrete
	3	3	Prefault threshold exceeded	Discrete
	2	2	Detector standby	Discrete
	1	1	Detector alarm	Discrete
	0	0	Detector failure	Discrete
2	7	0	Trouble shooting data	Binary
3	7	2	spare / not used	-
	1	0	MSB contamination level	Binary
4	7	0	LSB contamination level	Binary
5	7	2	spare / not used	-
	1	0	MSB smoke level	Binary
6	7	0	LSB smoke level	Binary
7	7	2	spare / not used	-
	1	0	MSB temperature	Binary
8	7	0	LSB temperature	Binary

Table 1: Smoke Detector Data Field

A smoke detector's 8-byte status Data Field is as defined in table 1 with the meaning of the data bits in table 2.

3 Network management

It is of utmost importance that the system configuration and availability of resources (smoke detectors) is known to the network master. Lack of configuration control through the network master device would jeopardize safety and disqualify the system. From a safety assessment point of view, the worst case condition is an undetected configuration error leading to an incorrect compartment designation incase of fire; an alarm reported in the aircraft's forward cargo compartment while the real fire occurrence is in the aft cargo compartment and vice versa. Such a case is classified as catastrophic. A catastrophic event is defined as an occurrence leading to total loss of the aircraft and occupants and must be ruled out with a defined level of probability of failure < $1\cdot10^{-9}$. Therefore, various network management mechanisms are necessary to ensure proper system configuration during initialization and normal operation.

Designatio	bit	Meaning
Failure	0	The smoke detector is no longer able to detect smoke or to communicate this information in a reliable manner
Alarm	1	Smoke is detected and confirmed
Standby	2	The smoke detector is able to detect smoke and communicate this information in a reliable manner
Prefault	3	The smoke detector optical cell contamination level has exceeded the internal threshold for triggering a corresponding maintenance message
Warning	4	The CAN TX error counter has exceeded 96

Table 2: Meaning of the status bits

3.1 Power-up configuration control

The normal expected configuration of smoke detectors is fixed in a lookup table within the network master's operational software. At power up or system initialization, the current configuration is compared with the expected through a mechanism called Configuration Check Request. During the Configuration Check Request process, the network master broadcasts the Configuration Check Request as an R_PDO with the broadcast Module ID to all smoke detectors. These in turn reply with T_PDOs containing their individual Module Address, enabling the network master to make a comparison of the received replies with the expected replies, and thereby detecting the following failure cases:

- Incorrect configuration of the network master for the intended installation

- An expected smoke detector has not replied (missing smoke detector on network)
- An unexpected smoke detector has replied (excessive smoke detector on network)

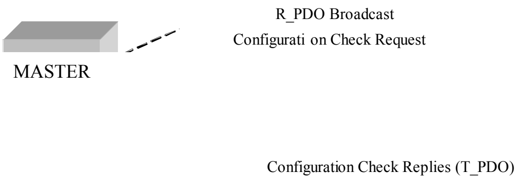
R_PDO Broadcast
Configurati on Check Request
MASTER
Configuration Check Replies (T_PDO)

Figure 4: Normal configuration check request / reply process

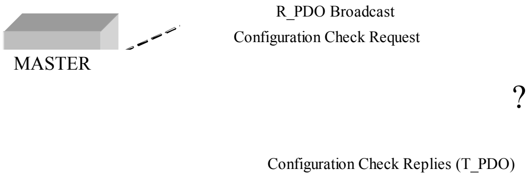
R_PDO Broadcast
Configuration Check Request
MASTER
?
Configuration Check Replies (T_PDO)

Figure 5: Failure of expected smoke detector to reply

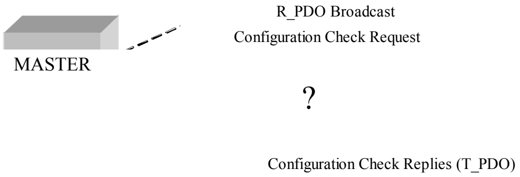
R_PDO Broadcast
Configuration Check Request
MASTER
?
Configuration Check Replies (T_PDO)

Figure 6: Unexpected smoke detector reply

Thus, comparison of the configuration present on the network with the expected configuration, is a prerequisite for determined network behavior.

3.2 Normal polling operation

The CAN bus is operated in Master-Slave mode. The network master cyclically acquires the status of each smoke detector by an explicitly addressed request frame. Not to be confused with CAN remote request frames, the request message is a regular data frame of type R_PDO containing the individual Module ID of the subject smoke detector, and is replied to by a T_PDO data frame containing the Module ID of the replying transmitter.

Each polling request is monitored by a timeout in which the reply is expected. The polling cycle is repeated every 2 seconds.

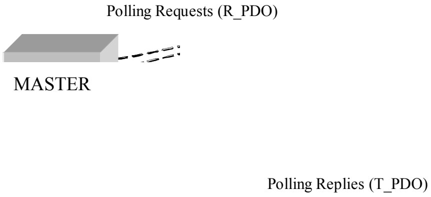

Figure 7: Normal polling operation

3.3 Failure detection / reconfiguration

The response time of the smoke detector is 60ms, including internal processing time and retry mechanisms inherent to CAN. A reply is considered timed out by the network master when not received prior to the following polling cycle; 2 seconds later. An outstanding reply increments a counter C in the network master. The reception of a normal polling reply while the counter is 1 ≤ C < 5 leads to a reset of the counter to 0 and the smoke detector is restored to normal operation. Once the counter reaches 5 outstanding replies (10s), the smoke detector is declared inoperable and is no longer polled, thereby resulting in a reconfiguration of the system. System determinism is ensured through the request-reply time window and the polling cycle:

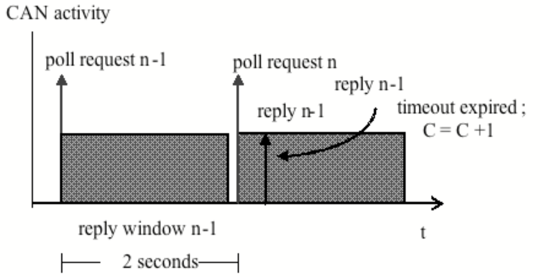

Figure 8: Timeout expired

In summary, the polling process abides by the following rules:

- Only expected smoke detectors are polled
- A smoke detector determined missing during power up is not polled
- A smoke detector is no longer polled following 5 consecutive timeouts
- A smoke detector is no longer polled when declared failed

3.4 Smoke detector monitoring

In addition to the network based configuration and time monitoring, the smoke detector is monitored for proper functional behavior by the network master.

Normally the smoke detector is in the standby condition (bit 2 on data byte 1 is TRUE). In case of alarm, the standby bit becomes false while the alarm condition (bit 1 on data byte 1) is TRUE. These conditions are by definition mutually exclusive and are therefore monitored for proper behavior. If two consecutive polling replies are received with neither the standby nor the alarm bit set to TRUE, or both bits set to TRUE, the smoke detector is declared failed and is no longer polled. In Boolean terms:

$$Failed = (alarm * s\tan dby) + (\overline{alarm} * \overline{s\tan dby})$$

4 Network topology

The smoke detectors are connected with the network in a linear bus topology with stubs departing from a central bus line. Bus termination is accomplished through resistors implemented within the network master at one end of the network, and the last smoke detector at the other end. Each item of equipment is qualified to operate on a CAN bus of length 150m, with 32 nodes connected through 2m long stubs to the main bus line.

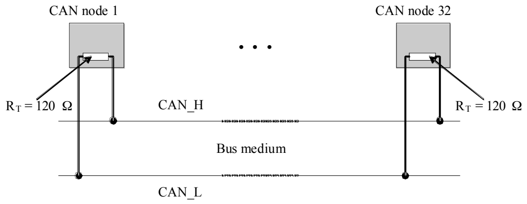

Figure 9: Network topology

Depending on the aircraft compartment being monitored, either a single or dual-redundant bus line is incorporated depending on the reliability requirements and whether the compartment is accessible or not during flight. The dual redundant architecture implies two smoke detectors at each location within a compartment. This is the case for the cargo compartments in the lower deck of the aircraft. Each lavatory, on the other hand, is fitted with a single smoke detector.

5 Development process

The safety-philosophy in aviation defines quantitative safety objectives and assigns acceptable probabilities. The overall probability for a failure with catastrophic consequences must be extremely improbable. This must be demonstrated to the airworthiness authorities for certification. The demonstration is endorsed through a complete, detailed and documented safety analysis, which is one of the integral parts of the software development process.

Guidelines for development of aviation software in the USA are defined in the DO-178B. Since its production by the RTCA, the DO-178B has become a de facto standard. The FAA's Advisory Circular AC20-115B established DO-178B as the accepted means of certifying all new aviation software.

DO178-B is primarily concerned with development processes. As a result, certification to DO178-B requires delivery of multiple supporting documents and records. The quantity of items needed for DO178-B certification, and the amount of information that they must contain, is determined by the level of certification being sought.

The higher the consequences of a potential failure of the software (catastrophic, hazardous-severe, major, minor, or no-effect), the higher the DO178-B certification level. The levels are from A for the highest certification level through B, C, D to E.

This aviation specific development process had to be followed on equipment and on system level.

6 Conclusion

Through clever system design and network management, a CAN bus based safety critical smoke detection system with deterministic behavior, capable of fulfilling the safety and reliability requirements, was developed and approved by airworthiness authorities. The robustness and reliability of CAN in this airborne application is being closely monitored, with some $1,45 \cdot 10^7$ accumulated flight hours (including multiple equipment factor) having been accumulated in the period between mid 2003 and February 2006.

References

[1] ISO11898 AMENDMENT 1 Road vehicles – Interchange of digital information- Controller are network (CAN) for high-speed communication.

[2] Schmid, C., SID 2616DD100 “ATA26 CAN Application Layer Protocol”, Issue 2.

[3] Radio Technical Commission for Aeronautics (RTCA) Washington D.C., RTCA/DO-178B Software Considerations in Airborne Systems and Equipment Certification.