SafetyBUS p – the first safe fieldbus system

Matthias Brinkmann
Pilz GmbH & Co.
Felix-Wankel-Str. 2
D-73760 Ostfildern

SafetyBUS p

Automation systems of the past few years have been characterised by major changes. Today, PLC has established itself for controlling operative procedures as has decentralisation in the use of conventional field bus systems. A hierarchical structure of operative field buses, which assigns the suitable bus system to the requirements of the respective level, is becoming increasingly important, particularly in larger plants or factories. Therefore the fieldbus spectrum has been expanded by adding a safe bus system. SafetyBUS p is an open bus system for the serial transfer of safety-related data. It is based on the fieldproofed CAN-Bus system.The transfer of bit data is event-driven and also data fields (domains) can be transferred. In the form of telegrams of varying priority the data will be transferred. Telegrams requiring a safe shutdown have the highest priority, while telegrams dealing with configuration and parameter settings have the lowest priority. The central theme is safety, and this is what sets SafetyBUS p apart from other bus systems used in automation technology. Safety is achieved by bringing the outputs to a safe, no-voltage condition in the case of an error. Safety-related networking offers users the same benefits to which they are accustomed from non-safety-related fieldbus systems, such as greater flexibility, reduced wiring and universal diagnostics. The three main aspects of SafetyBUS p are as follows. The decentralisation of the I/O-level, the direct connection of safety-related sensors and actuators and the safety-related coupling of several PSS programmable safety systems. SafetyBUS p enables the user to create a safe network (e.g. of Emergency-Stops, safety gates, ...) using decentralised I/Os or to incorporate safety-related components (e.g. light guards). This is a great benefit to those who are involved in plant and machine engineering, process engineering and the automotive industry. The SafetyBUS p system is approved for category 4 in accordance with EN 954-1 and meets the requirements of AK 6 in accordance with DIN V 19250. This means that its use is guaranteed for safety applications with a defined safe condition for the areas in which these standards are valid. A safe condition is defined as a no-voltage condition. In accordance with valid standards and regulations, SafetyBUS p offers new solutions for configuring networked machines and for modular plants distributed over a wide area.

SafetyBUS p and the CAN data transfer system

The decision to develop SafetyBUS p on the basis of CAN was made primarily because CAN technology is a quick, extremely fault-resistant protocol with multimaster functionality. Because of its high performance, CAN is widely accepted in the area of industrial control and automation. The following points list some of CAN's most im-

free, non-destructive bus access via dominant and recessive bit coding; the 15 bit CRC error management with a max. hamming distance of 6; a permanent synchronisation of the clock generators of individual bus nodes using stuff bits as well as the transmitter obtains acknowledgement that the message has been received by at least one subscriber. This is done by the ACK bit. The SafetyBUS p data communications system has been developed on the basis of non-safety-related CAN, in conjunction with additional fault detection measures. As far as data is concerned, SafetyBUS p is a communications system. It is specified by the layers 7, 2 and 1 of the ISO/OSI-Model. Layer 7 is used by the application (in this case SafetyBUS p) and layers 1 and 2 by the communications medium, i.e. CAN. Data flow is from layer 7 to layer 1. Usable data from Layer 7 continuously receives additional data for telegram checking from the communications side of Layer 7 and subsequent layers. This produces newer, longer telegrams. If data travels in the opposite direction, i.e. from Layer 1 to Layer 7, the length of the telegram will be reduced by the information required within the respective layer for checking purposes. The remainder is passed on to the next highest layer, where the process is repeated. Finally the application receives the actual usable data. The physical structure of SafetyBUS p corresponds therefore to that of the CAN-bus. However, as CAN is not able to detect all data transfer errors, additional fault detection measures are required. These are covered partly in the Application Layer and partly in Network Management. Only these additional measures make CAN-Bus into a failsafe bus, SafetyBUS p. As SafetyBUS p uses CAN as its communications medium, its main features are fixed. The linear bus structure with the advantage that the system can remain fully functional even if a subscriber should fail. The multimaster principle that each bus subscriber has the opportunity to actively place data on the bus. The event-driven data transfer which guarantees that the bus is only used when necessary. The bitwise arbitration where each emitter checks whether the signal it send is actually present on the bus.

SafetyBUS p Basics

As SafetyBUS p uses CAN as its communications medium, its main features are fixed. The following points are specific to SafetyBUS p. Each bus configuration has exactly one Management Device. The MD performs management functions and is not involved in the transport of usable data. The functions are the setting of the transmission rate; the configuration of the bus subscribers; the cyclical connection test (life monitoring) for all bus subscribers; the starting of I/O-Groups; the navigation of the bus errror stack containing all the faults registered via the bus system and the preparation of diagnostic information. The Logic Device is an “intelligent” function device for processing data (on the PSS this function is performed by the user program).The functions of the LD are the establishment of a connection with allocated I/ODs during the configuration phase; the cyclical connection test (life monitoring) for all allocated I/Ods; the reading of the inputs of all allocated I/ODs (LD is slave), the writing of the outputs of all allocated I/ODs and the processing of the user program. The Server Devices (I/OD) are bus subscribers which have input and output data but are not involved in logic information processing. Each I/OD independently carries out test and monitoring functions. I/O’s are self monitoring and have their own error stack. An I/OD can also be located within an LD. This is then referred to as a virtual I/OD. Virtual I/ODs enable data to be exchanged from LD to LD. A SafetyBUS p - PSS (**P**rogrammable **S**afety **S**ystem) can have all the device units named above. Devices such as valve terminals, light guards, PSS SB DI8O8 only have the I/OD part. The forming of I/O-Groups is another topic.

BUS p is that, if an error occurs within an I/O-Group, only the affected I/O-Group will be shut down. A maximum of 32 I/O-Groups (0-31) can be formed; each I/O-Group must be assigned to an LD. If an I/O-Group contains several LDs you will have to define a Master-LD. The MD will only issue a start command to I/O-Groups that are complete and error-free. I/OD inputs and outputs should only be assigned to the LD that needs the data for processing. This can increase the availability of a plant considerably. If a bus subscriber within an I/O-Group fails, only subscribers belonging to that particular I/O-Group need to be shut down safely. The access to SafetyBUS p data is controlled through access rights, which are established when SafetyBUS p is programmed. Certain SafetyBUS p functions can only be acessed via the MD. These are: the bus configuration, the maintenance, the reading of all the device error stacks, the reading of the manufacturer's ID of each individual bus subscriber and the reading of the configuration list. A Master-LD is permitted to read the I/OD inputs and write to the I/OD outputs within all its allocated I/O-Groups. The Master-LD therefore has also read/write access to all I/ODs in the I/O-Groups allocated to it. Cross-connection between Master-LDs is not permitted. This means that two Master-LDs, on which the virtual I/ODs are activated, cannot have read/write access to the virtual I/OD on the other. When a Master-LD is configured in an I/O-Group, all other LDs are automatically given Slave status. These Slave-LD has read only access to all I/ODs in its I/O-Group.

SafetyBUS p Functionality

Extensive fault detection measures are required in order to use CAN as a transport medium for safety-related data. The telegram structure of SafetyBUS p and the way in which it is handled guarantees that the following errors will be safely detected: The Loss, Repetition, Insertion, Corruption or Delay of data will be detected. But not all fault detection measures for the above errors have to be used on all telegrams. If an error occurs, the affected I/O-Group will be stopped, or will be prevented from even starting. One general measure for safeguarding the transfer of telegrams is to include the target address. This means that each recipient is able to detect whether or not the message is intended for it. Telegrams with a different address will not be processed. To detect a data loss, the receiver will send an acknowledgement telegram to confirm that it has received the message. If the acknowledgement telegram fails to materialise, it can be assumed that the telegram has been lost en route. These acknowledgement telegrams are generally monitored for time. The detecting of repetition and insertion in the case of event-driven telegrams, will be solved by including an event counter. The counter status on the issued telegram is compared with the counter status received in the acknowledgement telegram. This means that response telegrams can clearly be assigned. In the case of connection test telegrams, a key code is incorporated into the telegram instead of the event counter. The rest of the procedure is identical to that of the event counter. As well as safeguarding the transfer of telegrams, the security of the transferred data must also be guaranteed. In this case the procedure used is one that is common with serial data transfer, the CR-Check. The RC check character is 16 bits wide. The entering of timeout periods when programming the bus system enables dynamic monitoring of communication. The Cycle Timeout is used to monitor telegrams within the connection test (life monitoring). The Event Timeout is used to check whether bit data has been acknowledged in time by the recipient. The Domain Timeout monitors the transfer of data fields.

Telegram structure/types

SafetyBUS p telegrams are a maximum of 8 bytes in length and mainly consist of a header for the telegram type ID, target address, bytes of usable data and the CRC-check sum. Telegrams are prioritised using an 11 bit SafetyBUS p identifier. Telegrams which have “1” as the first bit in the identifier are not evaluated by SafetyBUS p. The identifier contains 8 message priorities and the send address. The SafetyBUS p identifier and telegram are a component part of CAN-Standard-Frame.

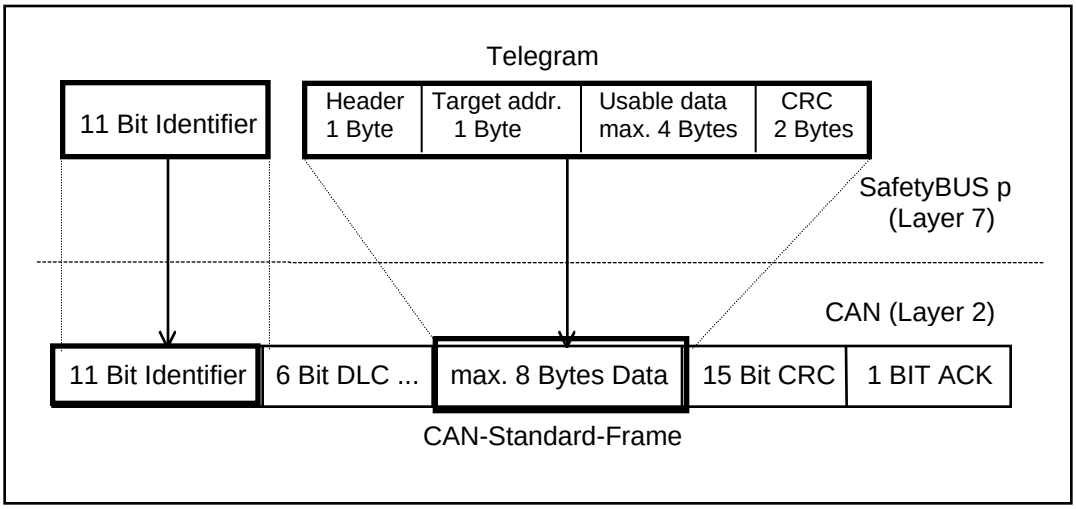
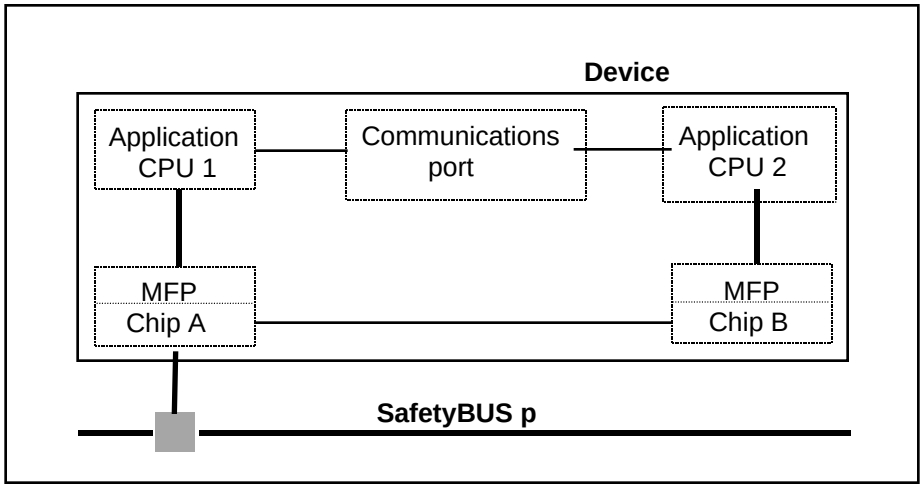


Fig.: SafetyBUS p telegrams within the CAN-Standard-Frame

Creating SafetyBUS p devices using the I/OD chip set

The I/OD chip set from Pilz GmbH & Co. (certified by BG EM III / HZ) enables safety component manufacturers to generate their own products as SafetyBUS p-compatible Servers. The chip set consists of Chip A and Chip B, and is used to create a connection to SafetyBUS p that has both redundancy and diversity. The connection to the application (“external device manufacturer”) is made via a multifunctional port (MFP). It is the responsibility of the user / device manufacturer to ensure that the MFP is operated safely. The chip set ensures that the user’s usable data is safely embedded in a SafetyBUS p telegram. It also guarantees that the usable data destined for the device is extracted safely from a SafetyBUS p telegram. The chip set is designed to meet the requirements of category 4 in accordance with DIN EN 954-1/3.97 and AK 6 in accordance with DIN VDE 19250/5.94. But also the following essential requirements must be in place before implementing a SafetyBUS p Server. The manufacturer’s ID and device data to identify the device. Each device on SafetyBUS p must correspond to a device profile. And last but not least the device must have passed a conformity test.



(Hardware structure for the device when implementing the I/OD chip set.)

The MFP port is a universal interface for the safe connection of the I/OD chip set with the application's processors.

Prognosis

The decentralisation of operative control systems is fact. Definition of the safety-orientated bus system also creates the prerequisite for enabling the functional safety capabilities to profit from the far-reaching benefits of decentralisation. Alongside the openness of a bus system which is only of theoretic value on some field buses, a club brings manufacturers and users together for the purpose of further development and standardisation. Thanks to the certified chip set and the development of directly interfaced field devices, a great deal will become more simple. In future not only the individual safety controllers interconnect reliable (instead of today's hard wired I/O connection), but protection devices such as safety beam gates or press safety valves will be integrated directly in the bus network. On the other hand for economic reasons simple safety functions like the emergency shutdown push-button switch or safety door switch will still be connected to the safe bus system via reliable decentral I/O modules.