NEWS

Contact:

EPSG POWERLINK-OFFICE
Kurfürstenstraße 112
10787 Berlin · Germany
Phone: +49 (0) 30 - 85 08 85 - 29
Fax: +49 (0) 30 - 85 08 85 - 86
info@ethernet-powerlink.org
www.ethernet-powerlink.org

Safe dual drive controller deSDAC 3003 PLC for POWERLINK networks

Control technology specialist dresden elektronik ingenieurtechnik provides the deSDAC 3003 PLC drive controller for POWERLINK networks, which enables safe drive control as well as safety-oriented data processing for digital and analog process peripherals.

Figure: The deSDAC 3003 PLC drive controller features a POWERLINK interface

The unit, which can control two drives, features two-channel redundancy with cross-checking and fulfills the safety requirements of the 61508 (SIL 3) and EN ISO 13849-1 (category 4) standards. It is optionally supplied with an integrated PLC based on the SafeOS operating system from KW Software. This safe PLC operating system allows users to employ complex drive functions and IEC 61131-compliant safety modules implemented according to the PLCopen standard in their application programs. deSDAC 3003 PLC controllers are configured by means of the SAFEPROG engineering tool. The units are capable of controlling highly dynamic positioning drives used in e.g. machine tools, logistics systems or stage machinery. A reliable, comprehensive safety concept is especially important in applications where data transmission errors can endanger the staff. The controller's POWERLINK interface is an ideal base for networks where the safety-oriented POWERLINK Safety protocol ensures SIL 3-compliant data transfer or where the real-time protocol POWERLINK provides high speed and bandwidth for safe components. An integrated HMI panel displays the operating status of peripheral components and application-specific values, thereby facilitating the initial set-up and diagnosis. The system's hardware platform consists of two ARM7-LPC2292 microcontrollers. Users can compile their own applications using C/C++ programming systems.

POWERLINK fieldbus coupler from WAGO

WAGO's IO SYSTEM 750 features robust, POWERLINK compliant couplers for the industry-proven POWERLINK fieldbus system.

continued on page 2 →

NEWS

continued:
POWERLINK fieldbus coupler from WAGO

The coupler supports up to 64 I/O terminals, or even 250 via a bus extension. Its application interface is based on the CANopen communication profile DS 301 (i.e. EN 50325-4). POWERLINK's key benefit is that it is both based on standard Ethernet and meets extreme demands on deterministic performance and cycle times. The protocol is therefore ideally suited for use in applications with hard real-time requirements, but also for reliably transferring large amounts of data within a given span of time. In addition, POWERLINK features a flexible, well-engineered application interface that gives users access to a broad base of existing device and application profiles.
Given its comprehensive range of I/O terminals, WAGO's I/O SYSTEM 750 provides an industry-grade hardware base for POWERLINK.

Figure: Fieldbus coupler I/O system 750 from WAGO

POWERLINK Safety error detection mechanisms

Data transmission errors can never be completely eliminated. However, in industrial applications, where staff and machines are at risk, they must by all means be recognized in time. Safety-oriented protocols must therefore detect all instances of faulty data packets and filter them or put the machine or plant into a safe state if required.

Since the Safety protocol reliably detects all known types of data transmission errors, even unsafe networks can be used for safety-relevant applications with POWERLINK Safety. But which errors in particular must the protocol be prepared for?

Which error types occur, and why?

The table below (figure 1) lists all error types and the detection methods

continued on page 3 →

Contact:

EPSG POWERLINK-OFFICE
Kurfürstenstraße 112
10787 Berlin · Germany
Phone: +49(0)30-85 08 85-29
Fax: +49(0)30-85 08 85-86
info@ethernet-powerlink.org
www.ethernet-powerlink.org

NEWS

Contact:

EPSG POWERLINK-OFFICE
Kurfürstenstraße 112
10787 Berlin · Germany
Phone: +49(0)30-85 08 85-29
Fax: +49(0)30-85 08 85-86
info@ethernet-powerlink.org
www.ethernet-powerlink.org

continued:

POWERLINK Safety error detection mechanisms

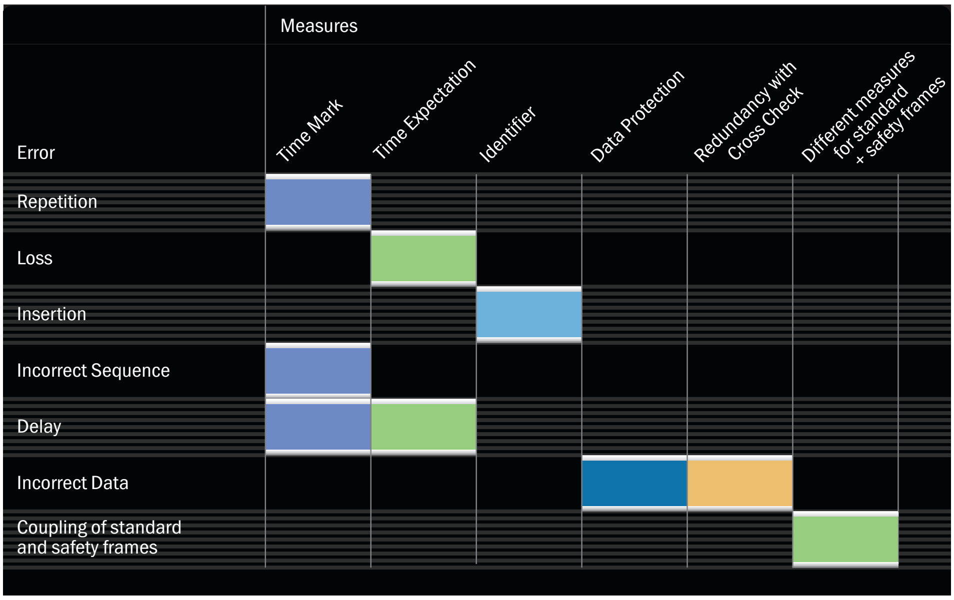

Figure 1: POWERLINK Safety's error detection mechanisms cover the complete spectrum of error types

POWERLINK Safety applies to them. Usually, these errors have the following causes:

- Repetition or duplication of data packets can occur when networks are connected via several gateways. In this error scenario, two gateways transmit the same data, resulting in duplication.
- Data loss occurs when a gateway does not transfer data at all, or routes it to the wrong network.
- Insertions can occur when data packets must be split into several segments due to their size. When networks are connected via several gateways, different transmission routes can result in an incorrect sequence of segments within a packet and in the insertion of segments into other packets.
- In case of high data traffic rates, gateways may delay transmission. If the transmission route leads through two gateways, the chronological data packet sequence can be mixed up because of different delay times.
- Physically corrupted data is usually caused by electromagnetic interference which "flips" single bits or destroys whole sequences
- If a network simultaneously carries standard and safety data, it is possible that standard data is misidentified as safety data. This "masquerade" can lead to serious application malfunctions.

POWERLINK Safety, which is suitable for use in SIL 3-compliant systems, ensures a high degree of safety through the following mechanisms:

continued on page 4 →

NEWS

continued:
POWERLINK Safety error detection mechanisms

Timestamps give data packets unmistakable IDs

The timestamp is one of POWERLINK Safety's most important mechanisms: the sending node stamps each data packet with the sending time, giving it a unique characteristic. Thereby, repetitions, incorrect sequences and delays are exposed and can be handled.

Time synchronization

In order to detect delays, the receiver must know the time difference between the sender's clock and his own. This requires the microcontroller clocks of the sender and receiver to be reliably synchronized.

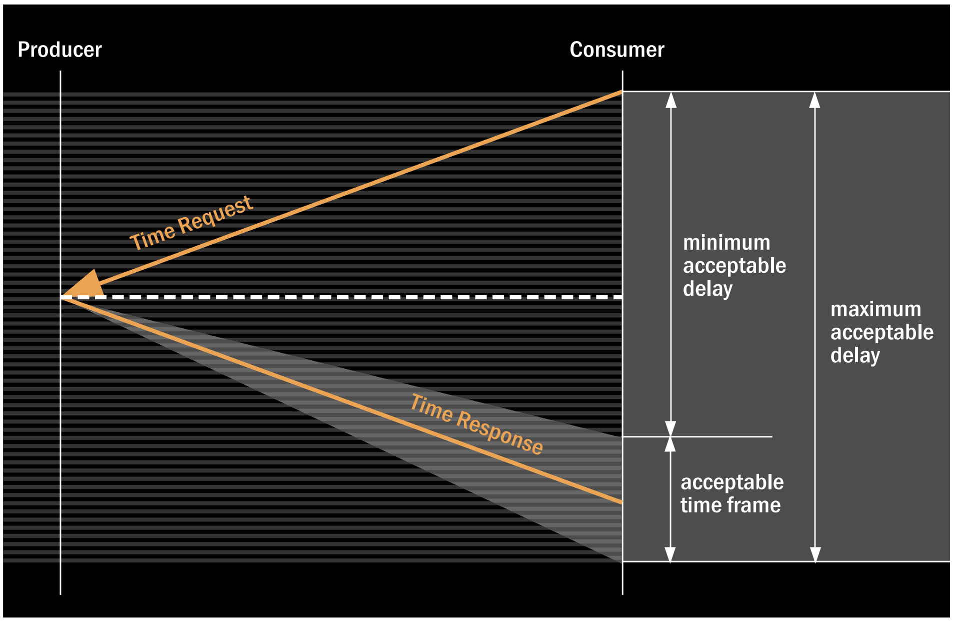

Figure 2: POWERLINK Safety time synchronization diagram

The receiving node (consumer) cyclically sends time requests (TReq) to the producers, who react with time responses (TRes). The consumer processes only time responses received within a response time frame set to a plausible duration.

Time expectation detects unacceptable delays

Thanks to time expectation, consumers can determine whether data cables and nodes are fully functional even when the producer is not currently sending process data. To that purpose, producers continuously send "keep alive signals". If these signals discontinue, the consumer puts the machine into a safe state.

Contact:

EPSG POWERLINK-OFFICE
Kurfürstenstraße 112
10787 Berlin · Germany
Phone: +49(0)30-85 08 85-29
Fax: +49(0)30-85 08 85-86
info@ethernet-powerlink.org
www.ethernet-powerlink.org

continued on page 5 →

NEWS

continued:

POWERLINK Safety error detection mechanisms

Unambiguous frame identification

Inadequate network separation or ambiguous frame IDs can lead consumers to analyze frames which are not intended for them. POWERLINK Safety frames feature an unambiguous identifier which rules out mistakes on the part of the receiver.

Data protection through checksums

The CRC method (Cyclic Redundancy Check) serves to detect changed or destroyed data contents. A checksum is generated from each data set by means of a numerical key. The checksum, which unambiguously encodes data, is attached to each transferred data set. The receiver also calculates the checksum and compares it to the checksum sent with the data set, ignoring the message if the two checksums differ.

POWERLINK Safety Frame

POWERLINK Safety uses yet another method to protect data integrity. The safety protocol duplicates the original frame. Therefore, each POWERLINK Safety frame consists of two subframes with identical payload secured by means of separately generated checksums. The receiving unit compares not only the checksum with the data content, but also checks the two subframes against each other.

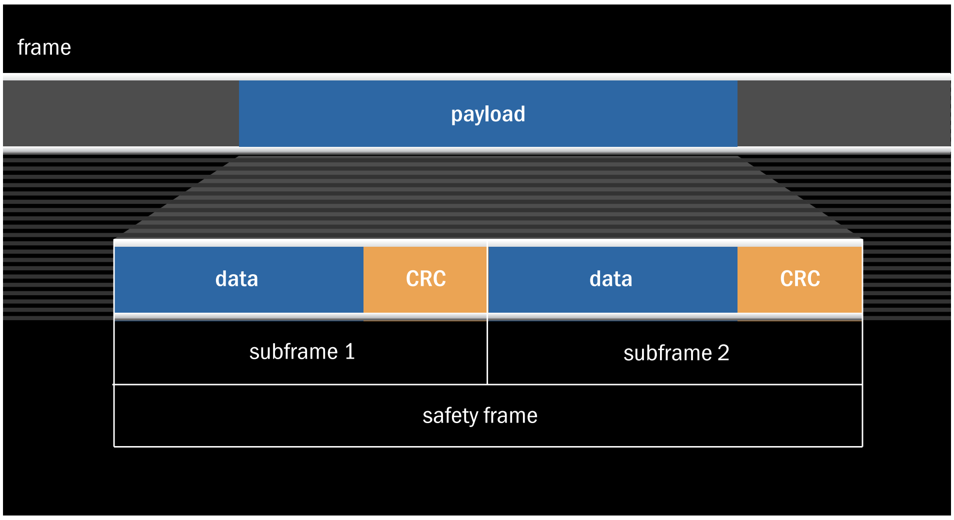

Figure 3: The Safety frame is transported within the payload of a standard frame. It consists of two identical subframes secured by means of separately generated checksums

Camouflage impossible

The list of possible errors concludes with “masquerading”, i.e. standard data accidentally being perceived as safe data. POWERLINK safety frames have a very special format (two subframes with individual checksums), which makes mistakes on the part of the consumer extremely unlikely.

Contact:

EPSG POWERLINK-OFFICE
Kurfürstenstraße 112
10787 Berlin · Germany
Phone: +49(0)30-85 08 85-29
Fax: +49(0)30-85 08 85-86
info@ethernet-powerlink.org
www.ethernet-powerlink.org

NEWS

POWERLINK: safe and secure through separate domains

Industrial Ethernet is sometimes called into question for concerns that Ethernet-based automation networks might not provide sufficient safeguards against attacks. Since Industrial Ethernet enables unified communication structures from control level to field level systems, some have argued that attackers might be able to manipulate processes on the automation level via the internet.

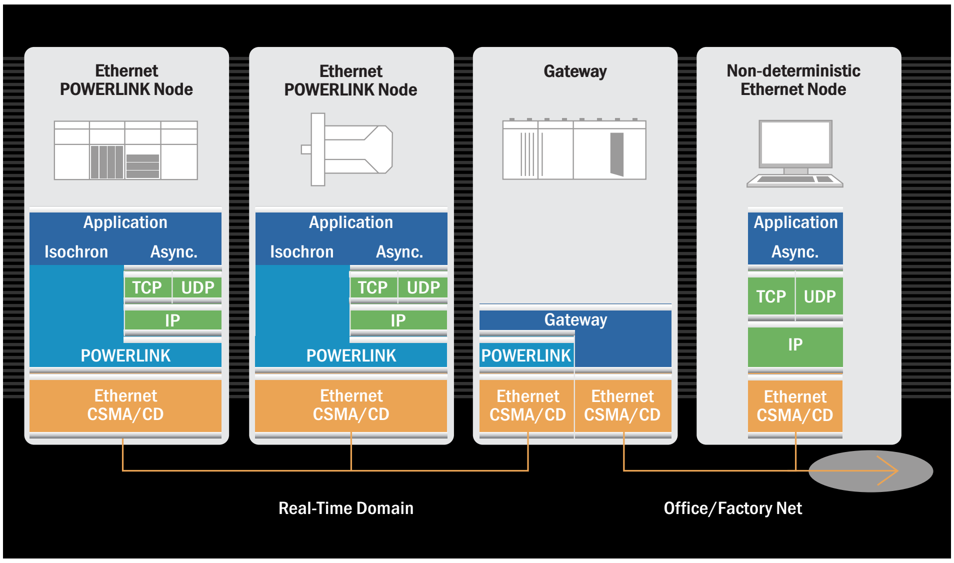

Figure: POWERLINK real-time domains are strictly separated from the network via gateways

In the case of POWERLINK, this concern is unfounded. The communication system is capable of integrating standard Ethernet without compromising high security requirements: POWERLINK real-time domains are strictly separated from non-real-time domains by means of gateways, which are typically directly integrated into the control system. Each POWERLINK-operated machine or plant is an individual network domain represented by a single IP address. The gateways operate similar to a firewall, converting the public IP address via Network Address Translation (NAT) into node IP addresses invisible to the outside. Individual implementations can also include additional safety measures and filter specifications defined at the gateways.

Contact:

EPSG POWERLINK-OFFICE
Kurfürstenstraße 112
10787 Berlin · Germany
Phone: +49(0)30-85 08 85-29
Fax: +49(0)30-85 08 85-86
info@ethernet-powerlink.org
www.ethernet-powerlink.org

Masthead:
“POWERLINK Newsletter” is an information service of the EPSG – Ethernet POWERLINK Standardization Group,
c/o Zürcher Hochschule für Angewandte Wissenschaften, InES, Technikumstrasse 22, 8401 Winterthur, Switzerland

Editorial Office:
Rüdiger Eikmeier (Editor in Chief), Heiko Wittke – gii die Presse-Agentur GmbH,
Immanuelkirchstr. 12, 10405 Berlin, Germany, Tel.: +49 03-53 89 65-0, Fax: +49 03-53 89 65-29