INDUSTRIAL ETHERNET FACTS

SYSTEM COMPARISON

The 5 Major Technologies

3rd Edition

PROFINET, POWERLINK, EtherNet/IP, EtherCAT, SERCOS III
How the Systems Work

The User Organizations
A Look behind the Scenes

Investment Viability and Performance
Everything You Need to Know!

OPC UA
More than just another fieldbus?

PROFIsafe
openSAFETY
CIPSafety
FSoE

Preface

Outsiders are not alone in finding the world of Industrial Ethernet somewhat confusing. Experts who examine the matter are similarly puzzled by a broad and intransparent line-up of competing systems. Most manufacturers provide very little information of that rare sort that captures technical characteristics and specific functionalities of a certain standard in a way that is both comprehensive and easy to comprehend. Users will find themselves even more out of luck if they are seeking material that clearly compares major systems to facilitate an objective assessment.

We too have seen repeated inquiries asking for a general overview of the major systems and wondering "where the differences actually lie". We have therefore decided to dedicate an issue of the Industrial Ethernet Facts to this very topic. In creating this, we have tried to remain as objective as a player in this market can be. Our roundup focuses on technical and economic as well as on strategic criteria, all of which are relevant for a consideration of the long-term viability of investments in Industrial Ethernet equipment. The arguments made in this publication were advanced and substantiated in numerous conversations and discussions with developers and decision-makers in this field. We have made every attempt to verify claims whenever practically possible.

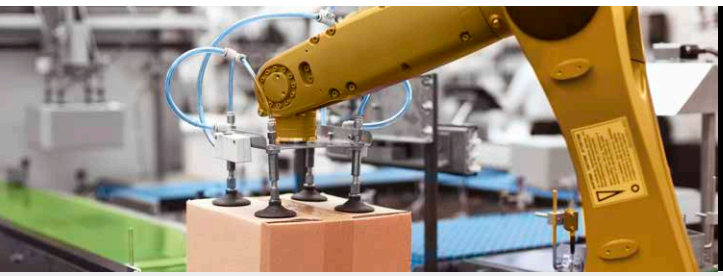
Despite all our efforts, though, we were unable to ascertain exact, verifiable information on some aspects, which prompts us to ask for your help: if you would like to propose any amendments or corrections, please send us an e-mail or simply give us a call. We look forward to any and all support in supplementing this overview, and we welcome all discussions that contribute to making the assessments of the various Industrial Ethernet standards as thorough and objective as possible. This edition of Industrial Ethernet Facts includes feedback submitted by the Industrial Ethernet community after publication of the first two issues in November, 2011 and February, 2013.

Contact: POWERLINK-Office,
phone: +49 33439 539 270
info@ethernet-powerlink.org

Luca Lachello, Software Engineering Manager COMAU Robotics – Italy
Peter Wratil, Managing Director Innotec – Germany
Anton Meindl, President EPSG – Germany
Stefan Schönegger, Business Unit Manager B&R – Austria
Bhagath Singh Karunakaran, CEO Kalycito – India
Huazhen Song, Marketing Manager POWERLINK Association – China
Stéphane Potier, Technology Marketing Manager EPSG – France

Systems Roundup:
The 5 Major Contenders

3rd Edition



Selection of Systems for Review

This issue of Industrial Ethernet Facts compares PROFINET (RT, IRT), POWERLINK, EtherNet/IP, EtherCAT, and SERCOS III, i.e. five out of about 30 Industrial Ethernet systems currently in use around the world.[1] Why these five? The selection was based on technical aspects, standardization status, and strategic market considerations. Relevant issues include e.g. whether a user organization backs the ongoing development of a protocol, whether a protocol is classified in the IEC standard, and whether a system is suitable for hard real-time requirements.

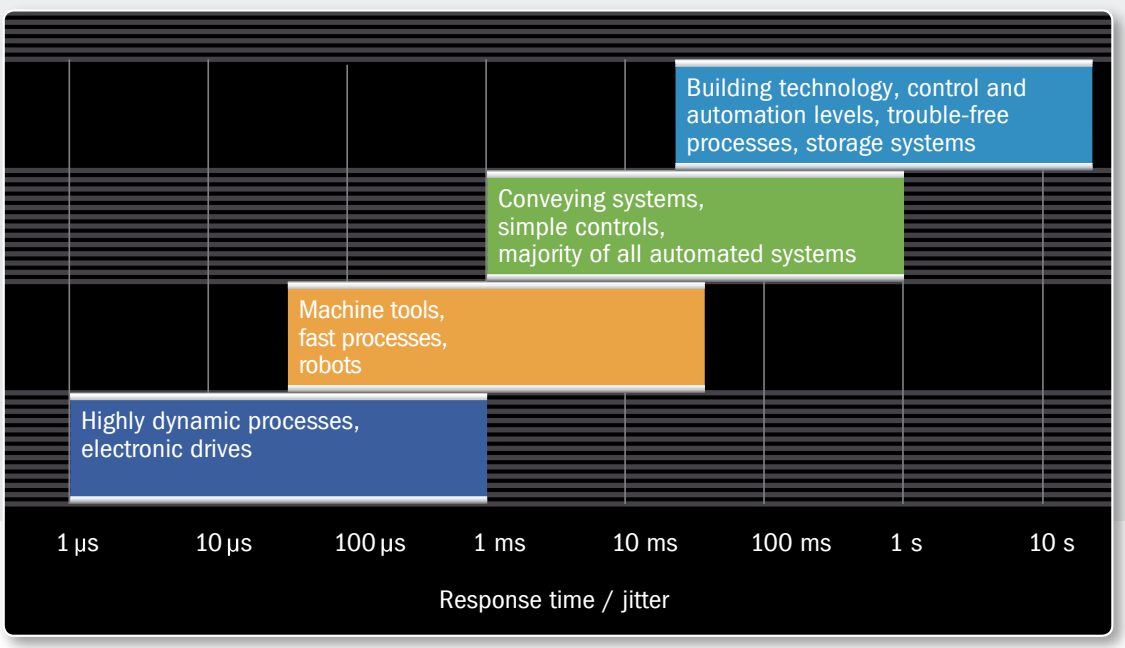
Real-time

A mechanism to resolve data collisions that is part of the IEEE 802.3 Ethernet standard causes irregular delays in data transfer. In order to achieve real-time performance, Industrial Ethernet protocols employ special preventive measures to avoid such collisions. For hard real-time, signal transmission times must stick exactly to a given time frame, or else they will trigger a failure signal. For soft real-time, some deviation within a limited span of time is tolerable. While cycle times of up to several hundred milliseconds may be good enough for soft real-time applications, e.g. for temperature monitoring, digital control systems or Motion Control applications often require cycle times below one millisecond.

1 For a more extensive overview of systems, consult the list on www.pdv.reutlingen-university.de/rte/ compiled by Prof. Dr.-Ing. Jürgen Schwager, head of the Process Data Processing Lab at Reutlingen University.

Market Penetration

Another key aspect in selecting Industrial Ethernet systems for comparison was market penetration: various IMS and ARC surveys indicate that about three quarters of all Industrial Ethernet applications around the world use EtherNet/IP, PROFINET, or Modbus TCP. Next in line are POWERLINK and EtherCAT, two systems particularly suitable for hard real-time requirements. The following roundup does not examine Modbus TCP on its own, since its user organization ODVA has stated that it has been integrated into EtherNet/IP. SERCOS III, however, was included for comparison despite its marginal market share, because this system plays a vital role for fast Motion Control solutions.



Real-time classes and application areas (IAONA classification)

How the Systems Work

Diverse Approaches to Real-time Generation

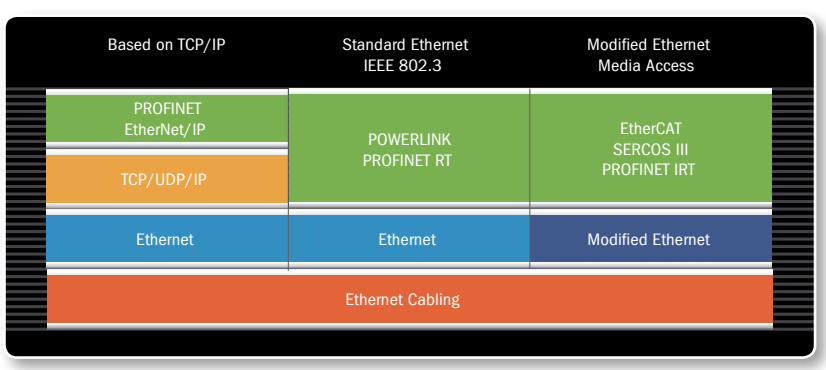
There are three different approaches to building a real-time Ethernet solution:

1. Based on TCP/IP: Protocols are based on standard TCP/IP layers with real-time mechanisms embedded in the top layer. These solutions usually have a limited performance range.
2. Standard Ethernet: Protocols are implemented on top of standard Ethernet layers. These solutions benefit from Ethernet evolution without further investment.
3. Modified Ethernet: The standard Ethernet layer, the Ethernet mechanism and infrastructure are modified. These solutions put performance before standard compliance.

One crucial difference of the various Industrial Ethernet systems compared within this publication lies in how they organize data transfer and how they manage to deliver real-time performance. EtherCAT and SERCOS III communicate using a summation frame method: in each cycle, data for all network nodes is sent in one telegram that travels from one node to another along the ring topology of the network, also collecting node responses on the way. In contrast to that, the single telegram procedure used by the other systems works by sending individual telegrams to the nodes, which also respond individually in separate telegrams.

The systems use three different mechanisms for network access and data synchronization:

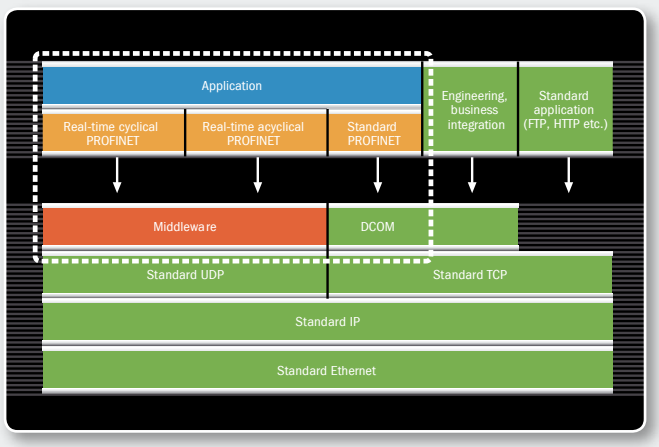
- A master controls the timing on the network. In POWERLINK environments, the master authorizes individual nodes to send data. In EtherCAT and SERCOS III networks, the transfer of summation frame telegrams follows the master's clock.
- PROFINET IRT uses synchronized switches to control communication.
- EtherNet/IP employs CIP Sync to distribute IEEE 1588 compliant time information throughout the network.



Methods for real-time Ethernet implementation

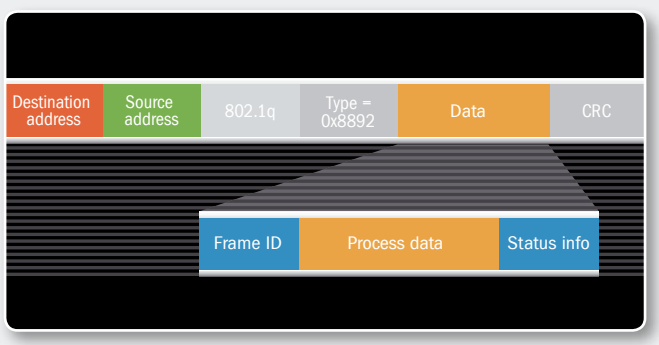
PROFINET Communication

PROFINET ("Process Field Network") is differentiated into different performance classes to address various timing requirements: PROFINET RT for soft real-time, or no real-time requirements at all, and PROFINET IRT for hard real-time performance. The technology was developed by Siemens and the member companies of the PROFIBUS user organization, PNO. The Ethernet-based successor to PROFIBUS DP, PROFINET I/O specifies all data transfer between I/O controllers as well as the parameterization, diagnostics, and layout of a network.



How It Works

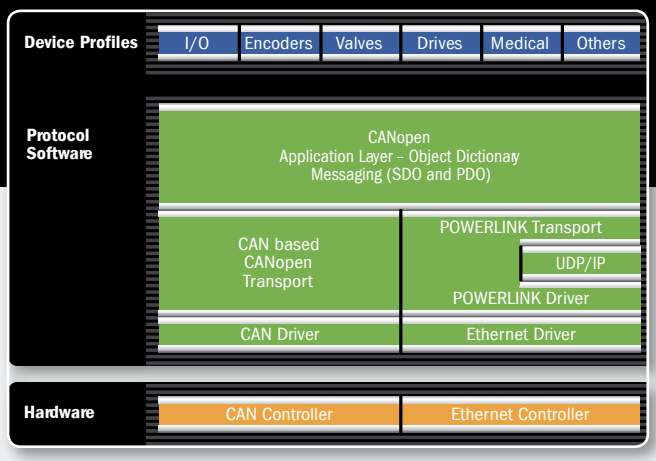
In order to cover the different performance classes, PROFINET makes free use of the producer/consumer principle and resorts to various protocols and services. High-priority payload data sent directly via the Ethernet protocol travels in Ethernet frames with VLAN prioritization, whereas diagnostics and configuration data, for instance, is sent using UDP/IP. That enables the system to achieve cycle times of around 10 ms for I/O applications.



Clock-synchronized cycle times below one millisecond, as required for Motion Control applications, are provided by PROFINET IRT, which implements a time multiplex mode based on specially managed, hardware-synchronized switches. So-called Dynamic Frame Packing (DFP) will in the future give users a new PROFINET variant designed to optimize cycle times making use of the summation frame principle for a certain set of devices in the network.

POWERLINK Communication

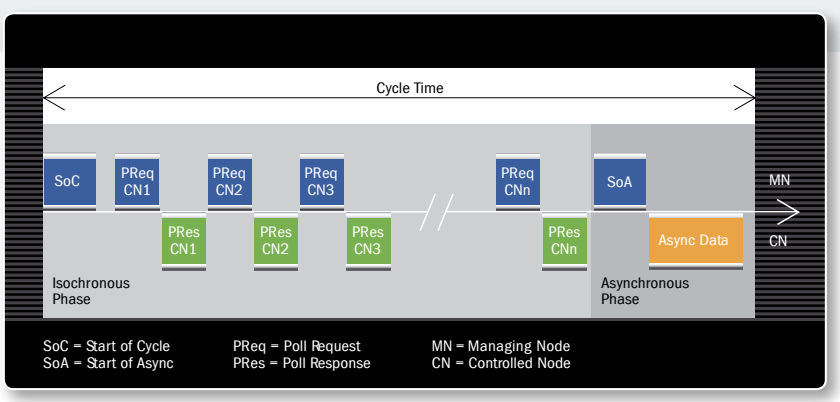
Initially developed by B&R, POWERLINK was introduced in 2001. The Ethernet POWERLINK Standardization Group (EPSG), an independent user organization with a democratic charter, has taken charge of the further development of the technology since 2003. POWERLINK is a completely patent-free, vendor-independent and purely software-based communication system that delivers hard real-time performance. An open source version has also been made available free of charge in 2008. POWERLINK integrates the entire range of CANopen mechanisms and fully complies with the IEEE 802.3 Ethernet standard, i.e. the protocol provides all standard Ethernet features including cross-traffic and hot plugging capability, and allows for deploying any network topology of choice.



Many shared characteristics: the CANopen and POWERLINK OSI model

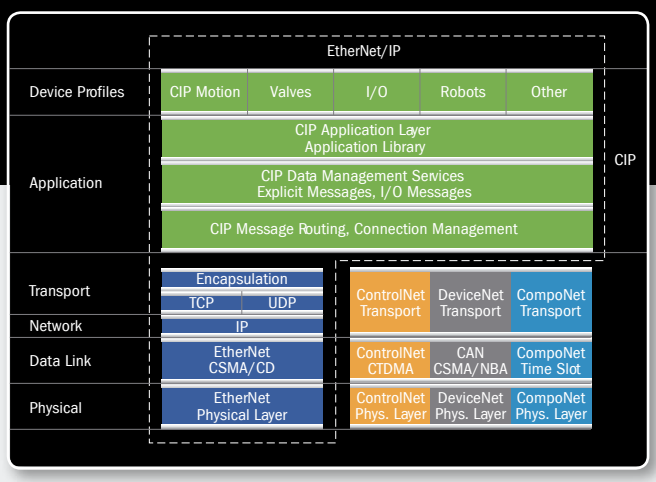
How It Works

POWERLINK uses a mixture of timeslot and polling procedures to achieve isochronous data transfer. In order to ensure co-ordination, a PLC or an Industrial PC is designated to be the so-called Managing Node (MN). This manager enforces the cycle timing that serves to synchronize all devices and controls cyclical data communication. All other devices operate as Controlled Nodes (CN). In the course of one clock cycle, the MN sends so-called "Poll Requests" to one CN after another in a fixed sequence. Every CN replies immediately to this request with a "Poll Response" on which all other nodes can listen in. A POWERLINK cycle consists of three periods. During the "Start Period," the MN sends a "Start of Cycle" (SoC) frame to all CNs to synchronize the devices. Jitter amounts to about 20 nanoseconds. Cyclic isochronous data exchange takes place during the second period ("Cyclic Period"). Multiplexing allows for optimized bandwidth use in this phase. The third period marks the start of the asynchronous phase, which enables the transfer of large, non-time-critical data packets. Such data, e.g. user data or TCP/IP frames, is scattered between the asynchronous phases of several cycles. POWERLINK distinguishes between real-time and non-real-time domains. Since data transfer in the asynchronous period supports standard IP frames, routers separate data safely and transparently from the real-time domains. POWERLINK is very well suited to all sorts of automation applications including I/O, Motion Control, robotics tasks, PLC-to-PLC communication and visualization.



EtherNet/IP Communication

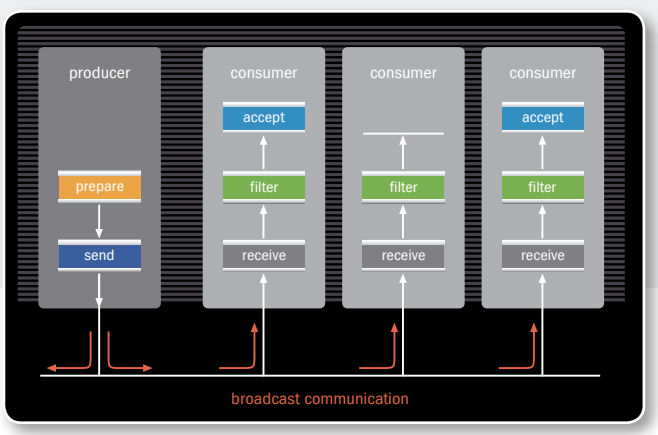
Initially released in 2000, EtherNet/IP is an open industrial standard developed by Allen-Bradley (Rockwell Automation) and the ODVA (Open DeviceNet Vendors Association). The “Ethernet Industrial Protocol” is essentially a port of the CIP application protocol (Common Industrial Protocol), which was already used by ControlNet and DeviceNet, to the Ethernet data transfer protocol. EtherNet/IP is particularly well established on the American market and is often used with Rockwell control systems.



EtherNet/IP layer model

How It Works

EtherNet/IP runs on standard Ethernet hardware and uses both TCP/IP and UDP/IP for data transfer. Due to the producer/consumer functionality supported by the CIP protocol, EtherNet/IP has various communication mechanisms at its disposal, e.g. cyclic polling, time or event triggers, multicast or simple point-to-point connections. The CIP application protocol differentiates between “implicit” I/O messages and “explicit” query/reply telegrams for configuration and data acquisition. While explicit messages are embedded into TCP frames, real-time application data is sent via UDP due to the latter protocol‘s more compact format and smaller overhead. Forming the center of a star topology network, switches prevent collisions of data from devices that are connected using point-to-point connections. EtherNet/IP typically achieves soft real-time performance with cycle times around 10 milliseconds. CIP Sync and CIP Motion as well as precise node synchronization via distributed clocks as specified in the IEEE 1588 standard are used to approach cycle times and jitter values low enough to enable servo motor control.



EtherCAT Communication

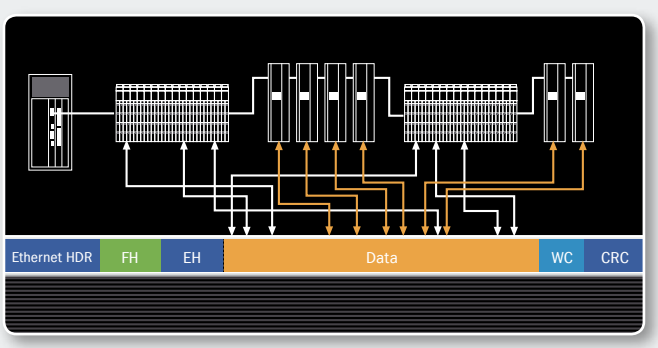
EtherCAT ("Ethernet for Control Automation Technology") was developed by Beckhoff Automation. All users of this technology automatically become members of the EtherCAT Technology Group (ETG).

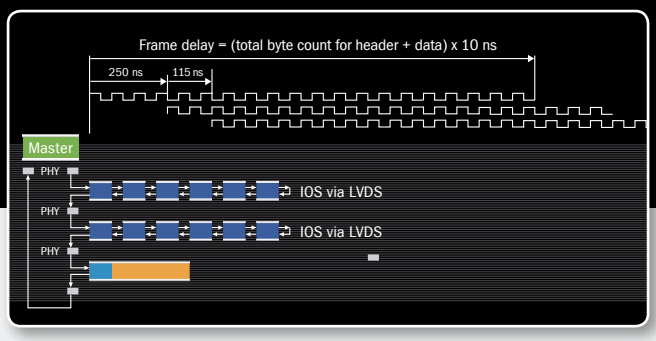
How It Works

EtherCAT is based on the summation frame method: The EtherCAT master transmits an Ethernet frame containing data for all nodes on the network. That frame passes through all nodes in sequence. When it arrives at the last node on a trunk, the frame is turned back again. The nodes process the information in the frame as it passes through in one direction. Each node reads out data addressed to it on the fly, and inserts response data back into the frame. In order to support the bandwidth of 100 Mbit/s, special hardware based on ASICs or FPGAs is required for fast processing as data passes through. In effect, the topology of an EtherCAT network always constitutes a logical ring. Even trunks branching out, which can be hooked up to nodes especially designed for such connections, actually only add a two-way junction where the summation frame telegram travels up and back down the branching line.

Structure of an EtherCAT frame

All EtherCAT telegrams with instructions for individual nodes are contained within the payload data area of a frame. Each EtherCAT frame consists of one header and several EtherCAT commands. Each





of these comprises its own header, instruction data for a slave, and a working counter. Up to 64 Kbytes configurable address space is available for each slave. Addressing proceeds by auto-increment, i.e. each slave counts up the 16-bit address field. Slaves can also be addressed via distributed station addresses, which are assigned by the master in the start-up phase.

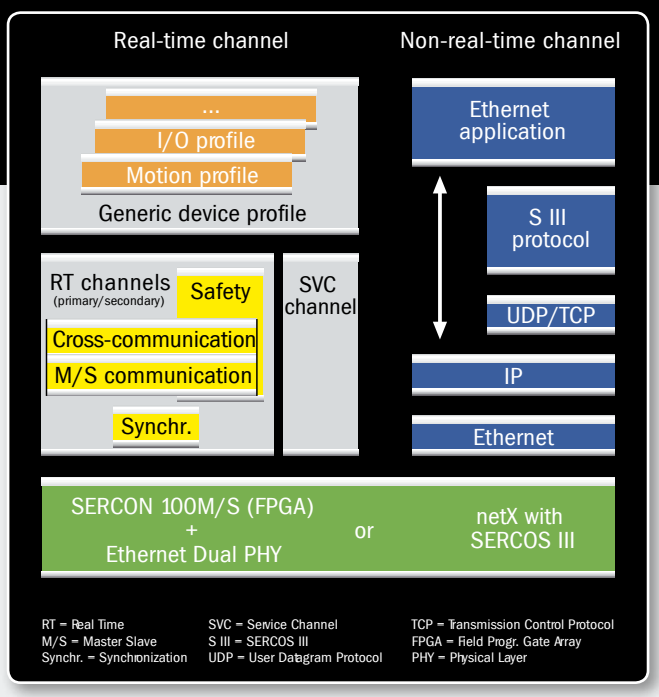
EtherCAT Process Synchronization

Every slave connection provides a real-time clock that is synchronized by the master using a technique similar to IEEE 1588. There are slave devices with and without real-time mechanisms, since these are more demanding on the hardware. Based on the real-time clocks, control signals can be synchronized with high precision. In physical terms, the EtherCAT protocol not only runs on Ethernet, but also on LVDS (Low Voltage Differential Signaling). This standard is used by Beckhoff as an internal bus on the terminals. A PC with a standard Ethernet interface is typically used to implement an EtherCAT master. In contrast to other protocols such as POWERLINK or PROFINET, EtherCAT solely extends to Layers 1 through 3 of the seven-layer OSI model. Hence, in order to achieve application functionality comparable to the other systems, an extra protocol layer (CoE, EoE) needs to be super-imposed.

EtherCAT principle of operation

SERCOS III Communication

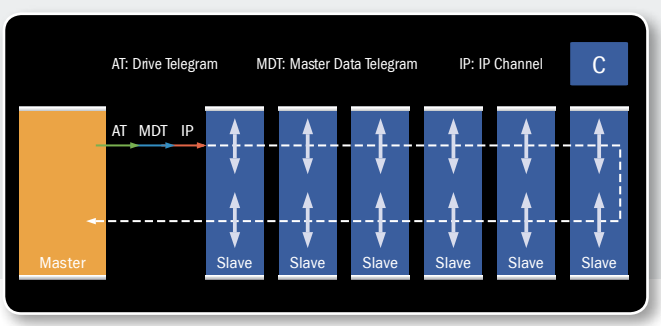
A freely available real-time communication standard for digital drive interfaces, SERCOS III not only specifies the hardware architecture of the physical connections but also a protocol structure and an extensive range of profile definitions. For SERCOS III, effectively the third generation of the Sercos Interface that was originally introduced to the market in 1985, Standard Ethernet according to IEEE 802.3 serves as the data transfer protocol. This communication system is predominantly used in Motion Control-based automation systems. A registered association, sercos International e.V., supports the technology's ongoing development and ensures compliance with the standard.



The specific master/slave communications controller for SERCOS technology is known as SERCON.

How It Works

While specific hardware is categorically needed for the slave, a software solution is also feasible for the master. The sercos user organization provides a SERCOS III IP core to support FPGA-based SERCOS III hardware development. SERCOS III uses a summation frame method. Network nodes must be deployed in a daisy chain or a closed ring. Data is processed while passing through a device, using different types of telegrams for different communication types. Due to the full-duplex capability of the Ethernet connection, a daisy chain actually constitutes a single ring, whereas a proper ring topology will in effect provide a double ring, allowing for redundant data transfer. Direct cross-traffic is enabled by the two communication ports on every node: in a daisy chain as well as a ring network, the real-time telegrams pass through every node on their way back and forth, i.e. they are processed twice per cycle. Hence, devices are capable of communicating with each other within one communication cycle, with no need to route their data through the master.



Besides the real-time channel, which uses time slots with reserved bandwidths to ensure collision-free data transfer, SERCOS III also provides for an optional non-real-time channel. Nodes are synchronized on the hardware level, prompted by the first real-time telegram at the beginning of a communication cycle. The master Synchronization Telegram (MST) is embedded into the first telegram for that purpose. Ensuring high precision by keeping synchronization offsets below 100 nanoseconds, a hardware-based procedure compensates for runtime delays and variations in it resulting from the Ethernet hardware. Various network segments may use different cycle clocks and still achieve fully synchronized operation.

The User Organizations

User independence is another key aspect in the overall assessment of a system. Any unsettled issues regarding brand rights or patents that may limit a user's own developments are crucial factors to consider when making the decision for a system. Legal traps that may cause inconvenience later can be avoided by taking a close look at the creators and the user organizations backing the various solutions.

Criteria	PROFINET RT | IRT	POWERLINK	EtherNet/IP	EtherCAT	SERCOS III
Organization	PNO	EPSG	ODVA	ETG	sercos International
www.	profibus.com	ethernet-powerlink.org	odva.org	ethercat.org	sercos.org

PROFINET – PI

PROFIBUS & PROFINET International (PI) is the international umbrella association for 25 regional PROFIBUS & PROFINET Associations including the user organization PNO, which spells out as PROFIBUS Nutzerorganisation e. V. It runs an office that manages joint projects and disperses information to members and other interested parties. A certification center for PROFIBUS and PROFINET product approvals is affiliated with that office. Adopted on 24 April, 1996, the organization's bylaws specify its duties and responsibilities. Membership is open to all companies, associations, and institutions that support the interests of PI as device vendors, users, systems solution providers or operators of PROFIBUS or PROFINET networks.
www.profibus.com

POWERLINK – EPSG

The Ethernet POWERLINK Standardization Group (EPSG) was founded in 2003 as an independent organization of companies in the drives and automation sector. The group's goal is the standardization and ongoing development of the POWERLINK protocol introduced by B&R in 2001. The EPSG cooperates with standardization organizations such as CAN in Automation (CiA) or the IEC. The EPSG is a registered association established according to Swiss civil law.
www.ethernet-powerlink.org

EtherNet/IP – ODVA

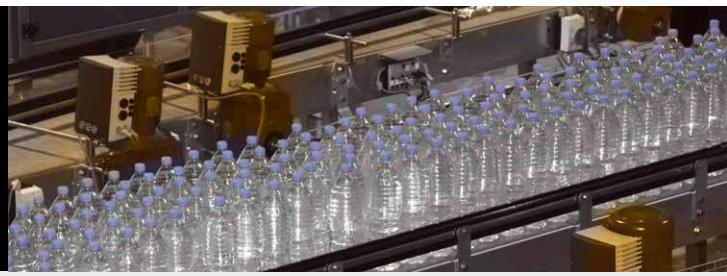
ODVA is the union of all DeviceNet and EtherNet/IP users. The organization attends to the continual development and further distribution of these field buses that are predominantly used in the USA and Asia, but also in Europe. One key aspect of the organization's activities is the development and propagation of the CIP protocol and of other protocols based on it. Users may not only apply the technology but are also invited to contribute to its ongoing development by joining Special Interest Groups (SIG). The ODVA also actively participates in other standardization bodies and industry consortia. The organization's bylaws are relatively complex.
www.odva.org

EtherCAT – ETG

The EtherCAT Technology Group is a forum jointly established by users, OEMs, machine vendors, and other automation suppliers. The group's purpose is to provide support for and to propagate the benefits of EtherCAT as an open technology. A certification lab is affiliated with the organization's head office in Nuremberg. All contractual agreements for use of the technology must be made directly with Beckhoff Automation. Based in Nuremberg, Germany, the EtherCAT Technology Group is a "nicht eingetragener Verein", i.e. a non-registered club in the sense of the German Civil Code.
www.ethercat.org

SERCOS III – sercos International e. V.

sercos International e.V. (SI) is an association entered into the court registry in Frankfurt am Main, Germany. The association's members are manufacturer and users of control systems, drives, and other automation components as well as machine vendors, research institutions, and other associations. There are subsidiary organizations in North America and Asia. A certification lab at the University of Stuttgart is affiliated with the organization's head office.
www.sercos.org



Status, Rights and Licensing

Which is the legal status of the various user organizations? Who owns the technology? Which legal ties, depending on the licensing regime, are binding for developers who use a specific technology? The following pages provide an overview.

Criteria	PROFINET RT | IRT	POWERLINK	EtherNet/IP	EtherCAT	SERCOS III
Type of organization	association +	association +	association +	non-registered club o	association +
Liability	PNO +	EPSG +	ODVA +	**members** o	SERCOS +

EtherCAT Technology Group: the non-registered club is not a legal entity, but is effectively a hybrid between an association and a private partnership, for which legal liabilities remain unclear.

Criteria	PROFINET RT | IRT	POWERLINK	EtherNet/IP	EtherCAT	SERCOS III
Rights owners	members	members	members		members
Brand owners	PNO	EPSG	ODVA		SERCOS

In most cases, the rights to a technology rest with the organization responsible for it. As co-owners, members are therefore entitled to make use of it. If other persons or companies own the rights to a technology, the prospects for future legal use of it remain unclear.

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/ IP	EtherCAT	SERCOS III
Funding obligations	membership fees o	membership fees o	membership fees o	no membership fees +	membership fees o

Membership in the ETG is free of charge. A fee is due for memberships in all other organizations. Annual contributions usually vary with the size of a corporate member. POWERLINK's and sercos' user organizations also allow non-members to develop products and put them on the market.

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/ IP	EtherCAT	SERCOS III
Master and slave specification	PNO +	EPSG +	ODVA +	Beckhoff o	SERCOS o

While communication mechanisms are specified for SERCOS III and EtherCAT, the inner workings of a slave remain undisclosed. Users must resort to an ASIC or an FPGA. FPGA IP code from Beckhoff is available for EtherCAT as object code, the source code is not disclosed.

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/ IP	EtherCAT	SERCOS III
Free source code for master	-	+	-	o	+
Free source code for slave	-	+	+	-	o

PROFINET: *The PROFIBUS user organization (PNO) provides source code and documentations for PROFINET implementations (PROFINET runtime software) to its members. Clause 1.5 of the license agreement for this software gives PNO members the right to use five patents.*

POWERLINK: *POWERLINK master and slave code is freely available under a BSD open source license. The software stack is available on SourceForge.net.*

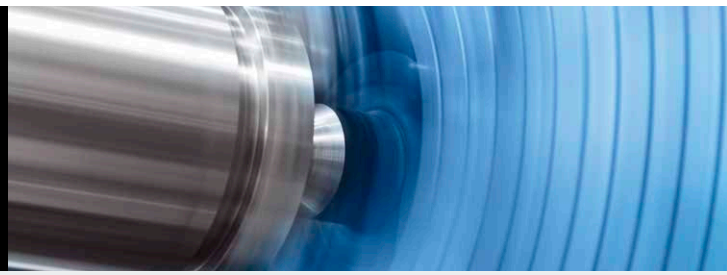
EtherNet/IP: *Stacks are available for purchase from various service providers. An open source variant has been developed by a university.*

EtherCAT: *Slave implementations necessarily require an ASIC or an FPGA. The VHDL or IP code for the FPGA must be purchased from Beckhoff; no source code for it is available. The ETG provides sample source code for the master side. Since the patent holder has not agreed to an open source licensing regime, that source code does not qualify as open source.**

SERCOS III: *Software master is provided free of charge under an LGPL license. ASICs or FPGA code must be purchased for the slave.*

* Source: Open Source Automation Development Lab (www.osadl.org)

Investment Viability



Openness as one issue with a bearing on the long-term viability of investments in a system has already been mentioned. In addition, a number of technical and strategic considerations also play crucial roles in making a safe investment decision for the long term.

Compatibility to Existing Application Profiles

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
	PROFIBUS	CANopen	DeviceNet	CANopen	SERCOS II
Downward compatibility	+	+	+	+	+

EMC Susceptibility/Transmission Reliability

Summation frame protocols are more susceptible to interference than single frame protocols. If a frame is destroyed, summation frame protocols always lose an entire cycle.

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
EMC susceptibility					

Since it uses two telegrams, in this comparison SERCOS III actually provides 50 % better performance than EtherCAT.

Electrical Contact Points

One special EtherCAT feature is the option to route all communication through the internal I/O terminal bus as well. However, the superior performance often cited in connection with this feature is offset by the safety risk due to increased susceptibility for interference (contacts and EMC).

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
Electrical contact points	+	+	+	o	+

Flexible Cabling Topology

EtherCAT and SERCOS III networks always constitute a logical ring. That ring can be physically closed at the master, or, in the case of a daisy chain, closed internally at the last node in the physical line. EtherCAT does provide for trunks to branch out via special junctions, but the entire frame travels up and back down such lateral network lines, i.e. the network as a whole still represents a logical ring.

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
Tree topology	+	+	+	o	o
Star topology	+	+	+	o	o
Ring topology	+	+	+	+	+
Daisy-chain topology	+	+	+	+	+

High Availability

Only in the case of POWERLINK have master and cable redundancy been included in the specifications, and have been implemented in actual projects. For PROFINET and EtherNet/IP, application implementations based on special switches are feasible.

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
Ring redundancy	o	+	o	+	+
Master and cable redundancy	o	+	o	o	-

Hot Plugging Capability

POWERLINK, EtherNet/IP, and PROFINET give users hot plugging capability. Some restrictions apply for SERCOS III and EtherCAT due to the compulsory ring topology. In a physical ring topology, SERCOS III does allow for taking a single node off a network. In this event, the two neighboring nodes close the TX and RX lines. Nodes can then be reached from either side of the master. EtherCAT provides some hot plugging capability: In the EtherCAT Slave Controller, open ports are automatically closed if no link is detected. EtherCAT's distributed clocks, however, requires re-synchronization, which may affect certain applications.

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
Hot plugging	+	+	+	o	o

For technologies based on a logical ring (EtherCAT and SERCOS III), the limitations of the network topology also limit hot plugging capability. Hot pluggable modules can only be connected to one end of a daisy chain (SERCOS III) and distributed clocks require re-synchronization after node failure, which may impose restrictions on applications.

Gigabit Readiness

As EtherNet/IP and POWERLINK are entirely software-based technologies, these protocols can also be used with Gigabit hardware. EtherCAT can be scaled to Gigabit but requires an ASIC redesign. PROFINET IRT also requires some redesign of the hardware, which concerns switches in particular. FPGA solutions can be ported to Gigabit.

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
Gigabit readiness	+ | -	+	+	-	o

sercos International has stated that their IP core is basically Gigabit-ready.

Support of International Standards

The IEC 61158 international standard standardizes protocols (called "Types") for use in industrial control systems. IEC 61784-2 standardizes communication profile families (called "CPF"). GB standards are National Chinese Standards written and issued by the Standardization Authority in China (SAC). They are valid across all industries and nationwide. GB/Z stands for national technical guidelines. These are primarily informative in nature and in no way binding. The highest authorized standardization level for communication technologies is GB/T. As a Chinese recommended industrial standard, GB/T must meet several requirements: It must be fully open technology, widely used and standard technology in the world. It must not be subject to any country or company.

	PROFINET	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
IEC 61158	Type 10	Type 13	Type 2	Type 12	Type 19
IEC 61784-2	CPF 3	CPF 13	CPF 2	CPF 12	CPF 16
GB National Chinese Standard	GB/Z 25105-2010	GB/T 27960-2011	GB/Z 26157-2010	GB/T 31230	

Products on the Market

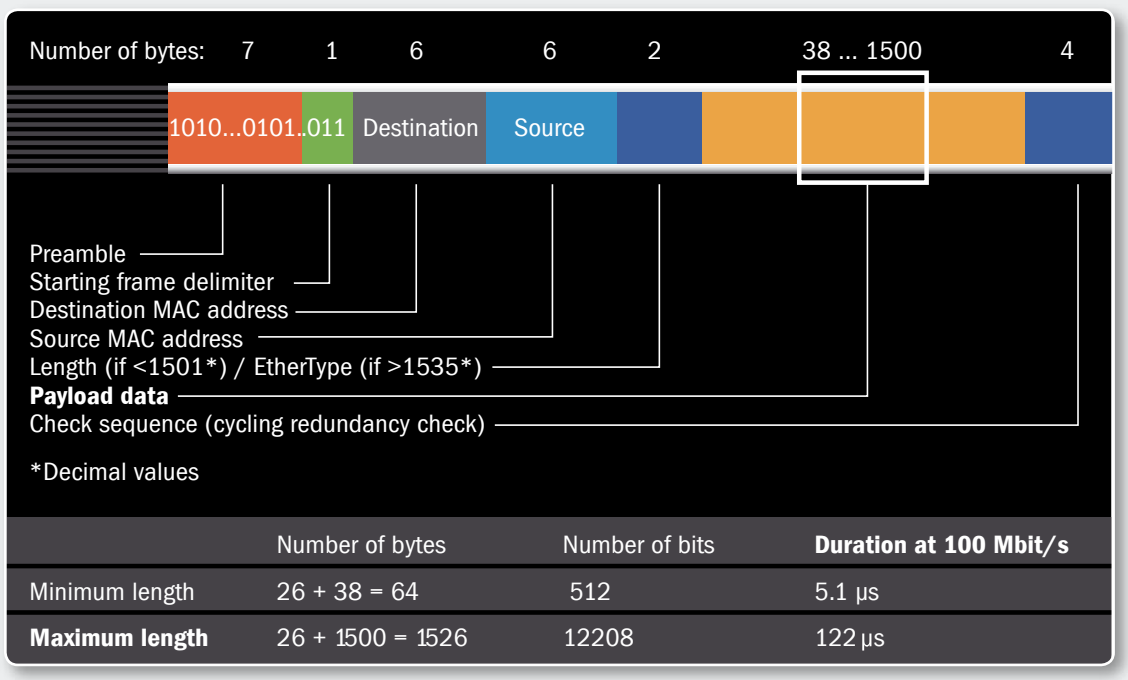
IRT products based on ERTEC technology are generally available on the market. However, the introduction of the DFP feature and the new generation of ASICs in conjunction with it (e.g. the Tiger Chip supplied by Phoenix) has raised doubts concerning the future compatibility of current IRT solutions.

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
Products on the market	+ | o	+	+	+	+

Performance

Theoretically Achievable Cycle Time

The performance of the systems has been the subject of intense debate, which has focused on the theoretical cycle times achievable by Industrial Ethernet systems. The briefest possible cycle time in theory is calculated as follows:



	Number of bytes	Number of bits	**Duration at 100 Mbit/s**
Minimum length	26 + 38 = 64	512	5.1 µs
Maximum length	26 + 1500 = 1526	12208	122 µs

Source: frame makeup as defined in IEEE 802.3
(The interframe gap of .96 µs must be added on top of the 5.1 µs cited above.)

Hence, if a master sends out a frame addressed to itself that does not pass through any other nodes, that frame will be available to the master again after 122 microseconds have elapsed (in the case of a single, maximum-length Ethernet frame).

In theory, it would be possible to process parts of a frame as soon as they are received. However, the CRC bytes that confirm the validity of the data received are last to arrive at the end of a frame. This scenario does not factor in delays affected by PHYs, cables, and Ethernet ports, times for internal data transfer in the master, etc. Moreover, once a signal leaves the master, the time it takes to travel along network lines (5 ns/m) and the processing time inside a slave have to be taken into account as well.

Prospective extensions of a system and possible future requirements need to be carefully considered for selecting either a centralized or a decentralized architecture. One advantage of the decentralized processing of various control loops is that it allows for adding nodes without any noticeable effect on the basic cycle time, i.e. no fundamental changes to the overall concept must be made. Moreover, additional functionality such as condition monitoring or integrated safety technology will have less impact on the control concept than in central architectures, which depend significantly on a low volume of data.

In order to select a solution that is viable for future use as well, wherever possible preference should be given to a decentralized handling of control loops for cycle times below 500 microseconds, especially in drive applications.

Communication Architecture of the Systems

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
Supports central control	+	+	+	+	+
Supports decentral control	+	+	+	-	o

Direct Cross-Traffic

Direct cross-traffic provides crucial benefits particularly in case of very demanding real-time requirements: for fast drive controllers, axes can be synchronized easily and with extreme precision, since all position values can be distributed directly without having to go through a master. That results in lower network load and also ensures that data (e.g. actual angle positions of axes) is available to all relevant nodes within the current cycle. If data needs to pass through a master first, it is not only delayed by one cycle, but overall data traffic on the network is increased as well.

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
Direct cross-traffic	+	+	+	-	+

With POWERLINK and SERCOS III, direct cross-traffic is a feature even for modules that only have slave functionality, while EtherNet/IP requires a module with scanner functionality.

Heavy Data Traffic

In applications involving a large volume of process data, the time required for passing through the nodes greatly impacts the overall cycle time. Data prioritization, on the other hand, enables lower cycle times. Systems that support prioritization mechanisms allow for reading high-priority data once every cycle and polling for data with a lower priority only every n-th cycle.

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
Prioritization	+	+	+	o	+

For POWERLINK, EtherNet/IP, and PROFINET, variable cycle times have been firmly established in the protocols' specifications. SERCOS III has only recently added this feature. For EtherCAT, solutions for this requirement can be implemented as part of a specific application.

Network Load for Safety Communication

Safety over Ethernet is based on a cyclic exchange of protected data between safety nodes (emergency stop switches, drives with Safety controllers). The safeguard procedures in this process involve data duplication and wrapping data in safe "containers". This increases data rates on the network. Solutions using the summation frame method will see the frame count go up, whereas the single frame method will increase the volume of data in each of the frames that are due to be sent anyway. All in all, the theoretically superior performance of the summation frame method is neutralized.

Actual Cycle Time

In solutions using the summation frame method, data must pass twice through each controller. If a signal has to go through many nodes, total transfer time will rise considerably as it makes its way. Raw performance data cited by the organizations supporting such solutions has to be adjusted to account for this effect. Another aspect to consider is that performance depends on implementation specifics, e.g. task classes, in the actual control systems used for an application.

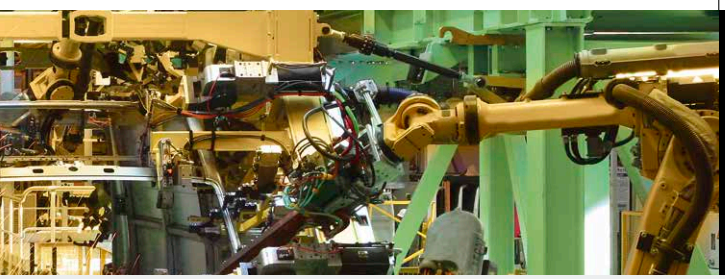
Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
Performance	o	+	+	o	+	+

Jitter

It is crucial for control quality on a network to ensure minimal jitter (clock deviation) and to determine signal delays very precisely. To this end, network nodes must be synchronized as precisely as possible. Competing Ethernet variants employ different mechanisms to achieve that goal. While EtherCAT uses the principle of distributed clocks solved by a proprietary algorithm within the ESC (EtherCAT Slave Controller), synchronization is accomplished via a simple sync signal (SoC) in POWERLINK networks.

Criteria	PROFINET RT | IRT	POWER-LINK	EtherNet/IP	EtherCAT	SERCOS III
Jitter	o	+	+	o	+	+

EtherCAT, POWERLINK, and SERCOS III give users a system with almost no jitter (< 100 ns) at all times. On EtherNet/IP networks, jitter can be considerably reduced with special IEEE 1588 extensions in all components. Reduced jitter can also be achieved in PROFINET IRT applications.



Performance Contest

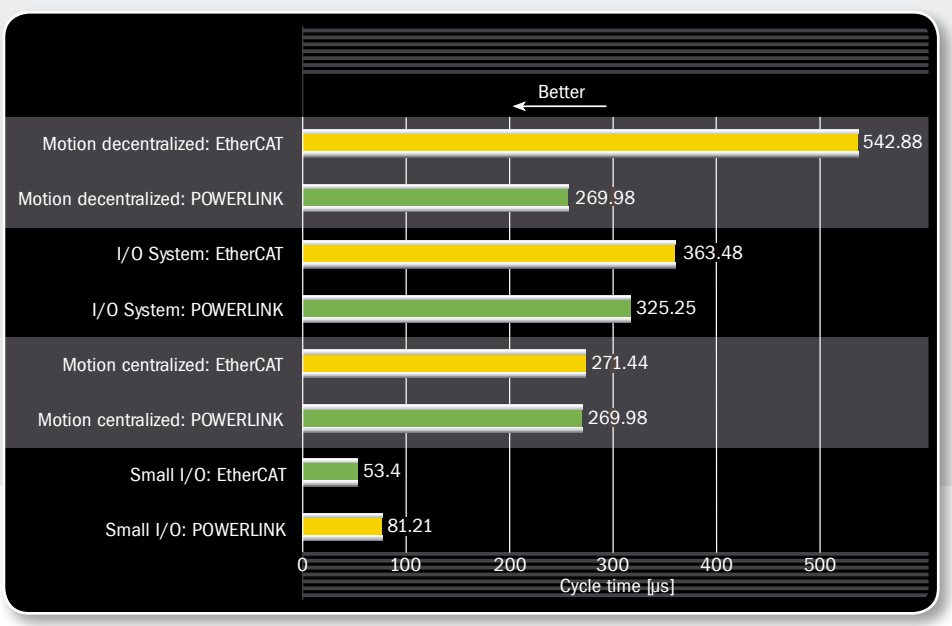
In practice, comparing system performance proves to be a difficult endeavor due to the specific characteristics of the various systems: EtherNet/IP and PROFINET RT are excluded from the start because these systems are only suitable for soft real-time requirements. PROFINET IRT poses problems due to the indispensable switches, which lead to a different application architecture that makes a direct comparison of measurements complicated. The values below were determined based on published calculation schemes.

Test scenarios were

1. a small machine comprising a master and 33 I/O modules (64 analog and 136 digital channels);
2. an I/O system with a master and twelve Ethernet slaves with 33 modules each (in total, 2000 digital and 500 analog channels were taken into account in this application);
3. a Motion Control network with 24 axes and one I/O station with 110 digital and 30 analog I/Os.

In practice, POWERLINK is faster than EtherCAT in most applications. EtherCAT is optimized for applications with only very low network traffic volume. In systems with a heavier data load, there is a disproportionate rise in cycle times in EtherCAT environments. Where decentralized architectures (e.g. for decentralized Motion control) are implemented, EtherCAT suffers greatly from the lack of direct cross-traffic (in both directions), which sharply reduces the performance that can theoretically be achieved. A direct I/O integration of EtherCAT also results in lower sampling rates (I/O system), since the time the signal takes to pass through the I/O has a direct impact on the cycle time within reach. For POWERLINK and SERCOS III, there are no such effects.The publication by Prytz (2008)[1] was used as a reference for the calcu-lations concerning EtherCAT. Delays for signals passing through the EtherCAT ASIC were verified again by measurements. For POWERLINK, applications with actual products were set up for practical measurements, leaving no room for doubt and reconfirming the cited figures.

No tests and calculations were conducted for SERCOS III. However, SERCOS III can be expected to provide a performance level similar to POWERLINK, making it faster than EtherCAT in many applications.



1 G. Prytz, EFTA Conference 2008, A Performance analysis of EtherCAT and PROFINET IRT. Referenced on the EtherCAT Technology Group's website, www.ethercat.org. Last accessed: 14 September, 2011.

Implementation

Implementation costs include development expenses, license costs, and hardware costs. Code availability (program or VHDL in case of a hardware implementation) must be taken into consideration here as well.

Master Implementation

Master designs	PROFINET RT	PROFINET IRT	POWERLINK	EtherNet/IP	EtherCAT	SERCOS III
Master access	–		+	–	o	+
	no open source master available		openPOWERLINK (open source)	no open source master available	patent-protected [1]	common SERCOS III master API (open source)
Implementation costs	o	–	+	o	+	o
	pricey software stack	requires special hardware with coprocessor	runs on standard hardware	pricey software stack	runs on standard hardware	typically with coprocessor support

1 No open source master, only sample code that does not warrant applicability.

All protocols allow for a software implementation of the master on a standard Ethernet chip.

Costs for Potentially Required
Network Components

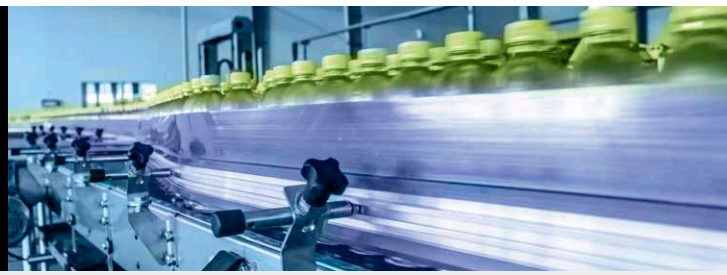
External devices = external switches or hubs

Internal multiports = ports that are directly integrated into the devices, primarily for daisy chain and ring topologies

Network components costs	PROFINET RT	PROFINET IRT	POWERLINK	EtherNet/IP	EtherCAT	SERCOS III
External devices	+	o	+	o	o	o
	standard switch	special switch, IRT support required	standard hubs or switches	managed switch with complex functionality required (IGMP snooping, port mirroring, etc.)	special network components required [1]	designated for future use of external infrastructure devices, but no such use at the time of writing
Internal multiports	o	o	+	o	+	+
	integrated switch	Siemens ASIC required	standard hub	integrated switch, very complex	Beckhoff ASIC required [2] or Beckhoff FPGA IP-Core	FPGA-based technology

1 With EtherCAT, special network components are required for star or tree topologies.

2 Beckhoff ET1100.



Slave Implementation

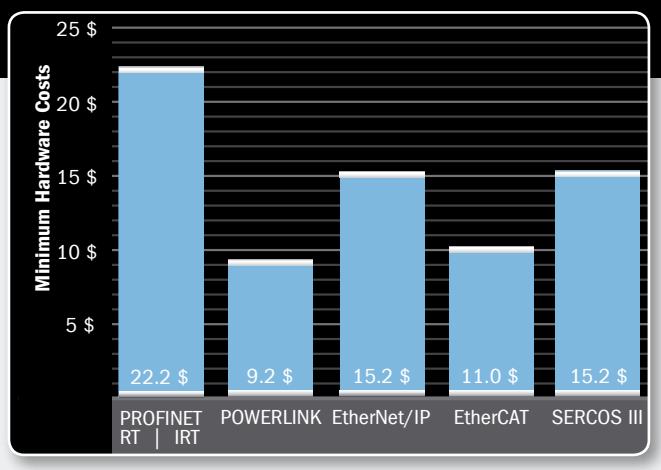
For EtherCAT, SERCOS III, and PROFINET IRT, bus protocol implementations into a slave require hardware solutions (ASICs or FPGAs). For POWERLINK, EtherNet/IP, and PROFINET RT, microcontroller-based software solutions are also feasible. Expenses for software solutions comprise license costs for the stack, possibly complemented by extra costs for more powerful and therefore more expensive controllers. For hardware solutions, users may opt for either FPGA- or ASIC-based communication interfaces. In principle, FPGAs may also be used for software solutions.

An FPGA (Field-Programmable Gate Array) is an integrated circuit that hardware developers can configure themselves. It consists of programmable logic components, so-called logic blocks, and a hierarchy for the reconfigurable component circuitry. All logic functions ASICs are able to execute can be implemented with FPGAs as well. Functionality can be customized before commissioning. The one-off development costs for FPGAs are lower than that of ASICs. FPGAs comprise an attractive technology for Industrial Ethernet solutions primarily due to these lower expenses, their high performance, and multi-protocol capability, but also because they allow for using pre-assembled components to integrate Layer 2 functionality (hubs, switches). However, users need to be aware that the complexity of a protocol has an impact on the volume of code and, by extension, the required number of logic blocks. L2 functionality can also have a substantial bearing on this number. Switches need more blocks than hubs, and complex managed switches require an excessive number of logic blocks. POWERLINK is the least complicated real-time Ethernet solution. Moreover, since POWERLINK only resorts to hubs in its network layout, this protocol requires only a small number of logic blocks, and is suitable for small FPGAs.

EtherCAT and SERCOS III, on the other hand, are more demanding and therefore need many more logic blocks.

Node Connection Costs in Different Real-time Ethernet Environments

The connection costs per node below refer to the running expenses for the hardware. Potentially owed license costs for software stacks etc. have not been taken into account.



The figures in this diagram have been derived from feedback from various manufacturers with implementation experience covering different Industrial Ethernet solutions. Several figures have also been quoted by manufacturers in automation industry magazines. Costs for the PHY (2 × 1.1 $) have been factored in equal measure for all protocols. Connectors are excluded. Cost estimates per node are made for an annual volume of 1000 units.

PROFINET: *The calculation reflects a solution with an ERTEC200 ASIC. Future implementations may also use devices equipped with a TPS1 chip developed by Phoenix Contact. In that case, costs are likely to drop to a level comparable to EtherCAT. POWERLINK's price level will not be met.*

POWERLINK: *The calculation applies to an FPGA-based solution. RAM and flash memory costs have been taken into account.*

EtherNet/IP: *The EtherNet/IP figure applies to a typical FPGA solution.*

EtherCAT: *The calculation is based on the least expensive EtherCAT ASIC solution with two Ethernet ports (ET1100). EtherCAT solutions for FPGAs are much more costly; the difference is most striking for synchronous solutions with real-time clocks.*

SERCOS III: *The SERCOS III figure applies to a typical FPGA solution.*

Operating Costs

Operating costs largely consist of maintenance and network administration expenses. Some technologies such as EtherNet/IP with CIP Sync and PROFINET IRT are highly complex and may therefore entail considerable network administration costs. Moreover, any use of managed switches requires network expertise. In many cases, a network engineer will be needed on location for commissioning and maintenance.

The synchronization technology used by a solution plays a key role for real-time communication. POWERLINK and SERCOS III ensure synchronization via a master-managed mechanism that is very precise and very rarely disturbed by faults. PROFINET IRT and EtherNet/IP with CIP Sync depend on an IEEE 1588 compliant synchronization mechanism. That results in significantly more complex network administration, especially if devices must be isolated because they trigger synchronization faults due to hardware or software failures.

Functions such as hot plugging – i.e. the option to swap devices on a live network – can also help greatly to bring down maintenance costs: replacement devices can be updated and configured without any impairment to the real-time function of the system as a whole.

Costs	PROFINET RT | IRT		POWERLINK	EtherNet/IP	EtherCAT	SERCOS III
Purchase costs	o	-	+	o	+	o
Operating costs	o		+	o	+	+

OPC UA and Industrial Ethernet

What is OPC UA?

OPC Unified Architecture (OPC UA) is a vendor-independent communication protocol for industrial automation applications. It is based on the client-server principle and allows seamless communication, from the ERP system down to individual sensors and actuators. The OPC UA protocol is flexible, platform-independent and possesses built-in safety mechanisms, which is why it is regarded as the ideal communication protocol for the implementation of Industry 4.0.

The origin of OPC

The original OPC – today referred to as OPC Classic – was developed in the 90s for vendor-independent data exchange in industrial production. OPC (OLE for process control) is based on the Microsoft technologies OLE and COM/DCOM.

The development of OPC UA

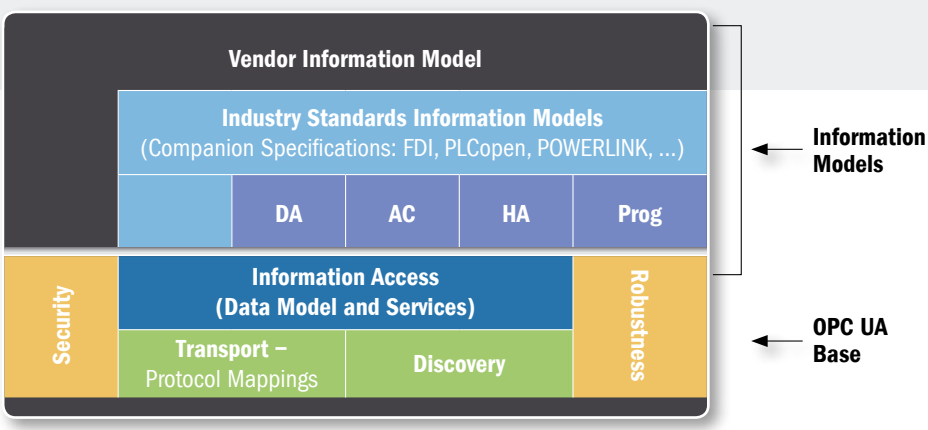
In 2006, the successor standard OPC UA was specified in order to remove the dependency on Windows-based systems and to implement numerous other innovations. The OPC UA protocol is based on a separate communication stack. OPC UA is 100% vendor- and platform-independent and can, for example, be transferred over the Internet. All functions of OPC Classic are contained in OPC UA. The information model was also standardized. Only one server is required to handle process data, alarms, historical data and program calls.

Security completely integrated

The protocol has several integrated safety mechanisms. If need be, user-level security, application-level security and transport-level security can be implemented individually or in combination. Based on secure X.509 certificates, OPC UA meets strict IT security standards.

The OPC Foundation

The OPC Foundation is an independent committee that specifies and develops the OPC UA standard. As of December 2015, the OPC Foundation has more than 450 members, including all of the largest automation manufacturers.



OPC Unified Architecture

What does OPC UA offer users?

OPC UA allows raw data and preprocessed information to be transferred from the sensor and field level to the supervisory control and production planning systems. Interfaces, gateways and the associated loss of information are a thing of the past.

OPC UA enables production data, alarms, events and historical data to be integrated on an OPC UA server. This makes it possible, for example, for a temperature measurement device to be portrayed as an object that contains the temperature value, alarm parameters as well as the corresponding alarm limits. This information is available to every OPC UA client.

Data becomes valuable information

In order for data to be used without vendor or platform restrictions, OPC UA translates it into information that contains the necessary context that allows it to be interpreted and used by any OPC UA-capable device. This process is called data modeling. The OPC UA specifications include general-purpose information models, which can be used as the basis for additional models as needed. The most important models are:

Process data (DA)

Sensors, controllers and position encoders generate process data. The Data Access (DA) information model provides this data to all clients in the network so that it can be post-processed directly. It doesn't matter if the client is a controller, SCADA or ERP system.

Alarm data (AC)

The Alarms and Conditions (AC) information model defines how alarms and conditions are handled. An alarm or condition change triggers what is called an "event". Clients can subscribe to such events and select which of the available accompanying values they want to receive as a part of the notification message (e.g. the message text or acknowledgment behavior).

Historical data (HA)

The Historical Access (HA) information model provides the client access to historical variable values and events. It can read, write or edit this data. The data can be stored in a database, in an archive or in a different memory.

Programs and functions (Prog)

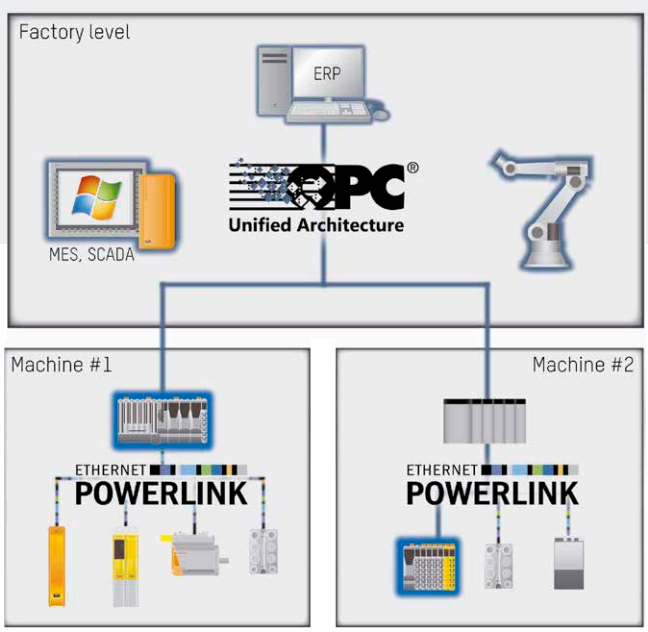
The Programs (Prog) information model calls programs and functions. It can be used to implement batch processes, for example. It sends recipes to the line via OPC UA and returns control values back to the application.

Real-time capability for OPC UA

Until now, OPC UA has had its limitations when it comes to complex processes with real-time requirements. This is why the OPC Foundation is working on 2 expansions that aim to make OPC UA a real-time capable communication standard: The first is a publisher-subscriber model; the other is utilization of the IEEE 802.1 standard for time-sensitive networking (TSN).

Publisher-subscriber model

OPC UA works with a client/server mechanism. A client requests information and receives a response from a server. This approach has its limitations in situations where certain information has to arrive at different clients at a precisely defined point in time. In contrast, the publisher-subscriber model enables one-to-many and many-to-many communication. A server sends (publishes) its data to the network and every client can receive (subscribe to) this data. It is also possible to define the exact interval in which data is to be transferred.



Real-time capability for standard Ethernet

The publisher-subscriber model alone is not enough to give OPC UA real-time capability. That's why the OPC Foundation has implemented Time-Sensitive Networking (TSN). TSN expands the IEEE 802 Ethernet standard with a number of sub-standards that aim to make it real-time capable.

Automotive industry is driving TSN development

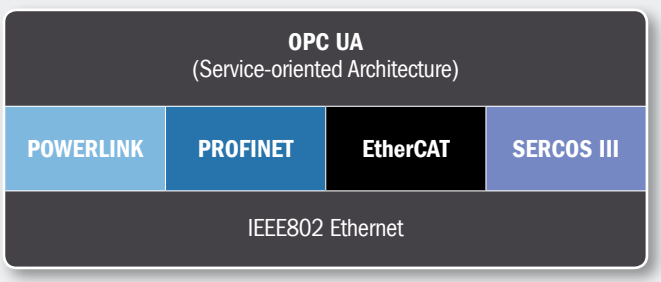
Because the automotive industry relies on TSN, the required semiconductor components will be available very quickly and at comparatively low prices. A widespread goal of the automotive industry is to handle all control tasks and applications that require functional safety over Ethernet. For this to be possible, they will need cycle times in the real-time range and deterministic network behavior.

OPC UA - The production plant standard

OPC UA already plays a central role in the IT-related areas of modern production systems. The addition of TSN and the publisher-subscriber model will greatly expand the range of potential OPC UA applications. Secure, plant-wide Ethernet communication, from the ERP system to the sensor, can be implemented with minimal cost and effort.

OPC UA vs. industrial Ethernet

OPC UA is based on modern service-oriented architectures (SoA) and is the ideal complement to existing fieldbus solutions. OPC UA is the key to 100% a comprehensive and consistent communication solution for production plants – regardless of which individual fieldbus and industrial Ethernet systems are in use. Corresponding companion specifications have already been announced for POWERLINK, PROFINET, EtherCAT and SERCOS. This makes OPC UA the de facto global standard for the upper protocol layers.



OPC UA chosen as de facto standard.

OPC UA and POWERLINK

The OPC Foundation and the EPSG are collaborating on interface-free communication within and between production systems. To achieve this, they are collaborating on a companion specification. All the machine data is mapped from the OPC UA server to the machine controller, so it is provided in a standardized way.

In the future, it will be possible to fully integrate OPC UA into the POWERLINK protocol. In its asynchronous phase – independently of the real-time data – POWERLINK is able to transmit any Ethernet protocol.

As a result, gateways become superfluous, because there is no need for an interface between the worlds of POWERLINK and IT. A SCADA system will be able to take advantage of OPC UA to do things like access a sensor, change parameters or retrieve diagnostic information. All OPC UA services will be available without limitations.

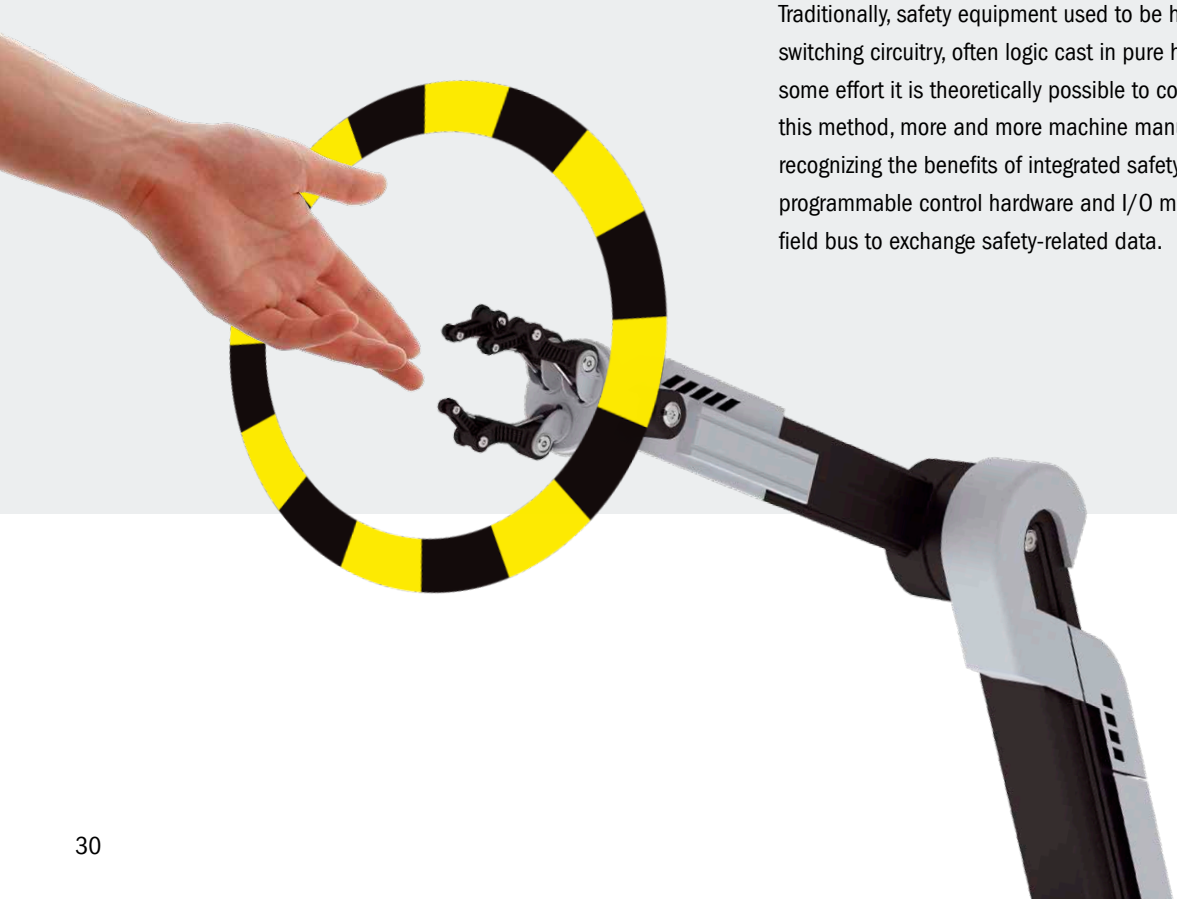
Safety Functionality

Requirements toward safety in production environments have become considerably more demanding over the past decade. Introduction of the 2006/42/EC Machinery Directive by the European Union made machine and plant manufacturers focus their attention on this issue. They are required to design comprehensive solutions to ensure protection of workers against injuries and the machinery itself against damage while maintaining high levels of productivity.

The new standards led to the necessity for new machinery to undergo strict certification procedures and to elevated performance requirements for the safety components used. Supported by a multitude of new and innovative safety products, they also facilitated changes in the approach toward the conceptual design of safety solutions. No longer is an emergency stop immediately halting all parts of a machine the only safe reaction to violations of the machine's safe boundaries. Smart safe reactions such as continued operation at a safe limited speed can in many cases deliver the required level of protection while providing better productivity by reducing the time to resuming full speed. In many instances, it enables a more direct interaction between worker and machine, particularly in teaching and adjustment scenarios.

Network Integrated instead of Hard Wired

Traditionally, safety equipment used to be hard wired with dedicated switching circuitry, often logic cast in pure hardware. Although with some effort it is theoretically possible to cover many cases using this method, more and more machine manufacturers have been recognizing the benefits of integrated safety. It is based on safe programmable control hardware and I/O modules using the existing field bus to exchange safety-related data.



At first glance, the older methods may appear less costly. Due to the lower purchasing costs of their hardware components, this may in many cases be true, but not if safety solutions are viewed in their entirety. Wherever the complexity of such systems goes beyond a single emergency stop button, network-integrated safety systems have become the preferred choice. They lower the number of components as well as required cabling and provide more flexibility of safe logic design by replacing hard wiring with configuration and parameter setting. Also, error diagnostics are greatly simplified. Combined with centralized data storage, this results in faster recovery. Maximum availability of plants and machines is provided by network-integrated safety technology through:

- Safety sensors directly attached to the network
- Direct read-out of component information
- Simplified maintenance due to automated component parameter setting across the network
- Safer operating mode switching due to parameter setting during runtime
- Decreased response time, as latency induced by relays is eliminated
- Modular design supported by network structure and safe software
- Increased availability as a result of comprehensive diagnosis
- Reduction of component count and wiring
- Greater variety of safety functions (safe operating stop, safely limited speed...)

How It Works

Safety applications based on certified software are programmed using function blocks such as counters, timers or speed monitors. Running on dedicated safety controllers, this replaces the traditionally hard-wired safety circuitry. Implementation of the safety application in software reduces the number of both safety components and standard I/O modules. Along with the replacement of discrete cabling by safety data transfer via the existing network connections, this greatly minimizes both costs and complexity of safety installations. Due to the use of existing network connections, varying machine layouts and options do not require dedicated safety connections. This also improves flexibility and freedom of safety application design as well as modifications of existing plants and machines during their lifecycle. Also, diagnostic signals can be transferred without any additional hardware. All in all, using integrated safety speeds up engineering and substantially shortens time to market.

The Black Channel Principle

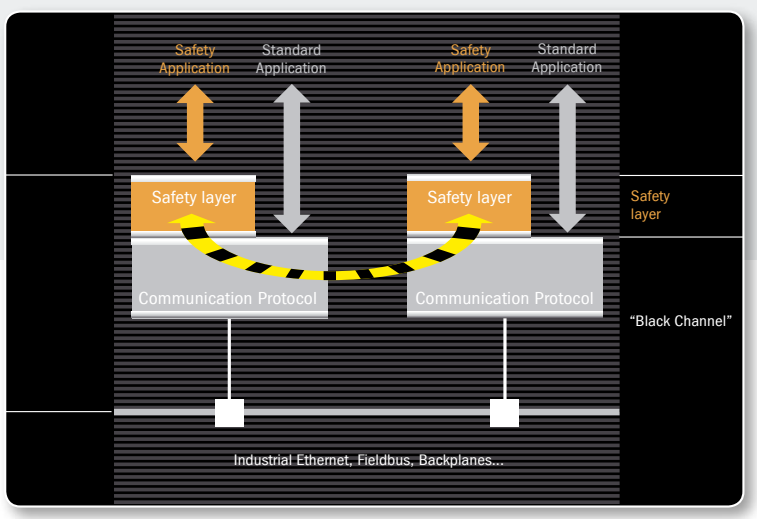
Safety Fieldbus Systems

Safety-oriented field buses simplify placement of components within a plant or machine. In most cases, two cables, one for power and one for communication, are all that is required. Sensors can be attached directly to the safety network. They do not require separate cables for the return of diagnostic signals. This results in a reduction of required hardware components.

Using the Black Channel Principle, safety-relevant data as well as diagnostic information is exchanged via the existing network connections. This enables faster responses. Some protocols also allow optimized parameter settings to be downloaded to the sensors in case of changes to the mode of operation and also prevents the need to adjust parameters on the device itself in case of component replacement. All this adds to a maximized productivity and reduced down time.

Transport of Safety Data via Regular Bus or Network Lines

The Black Channel Principle allows transmission of failsafe and standard data via the same network or bus line. Independent of the regular data transport mechanism used on that line, safety components can transmit data using an isolated safe protocol. As safe fieldbuses are pure application protocols without physical characteristics of their own, available bandwidth and cycle times depend on the data transport protocol used. Possible errors that can occur during data transfer and the appropriate counteractive measures are defined in the IEC 61784-3 standard. Their prevention needs to be implemented as a crucial part of the safety data transmission protocols. The required quality of transmission error detection depends on the safety level that needs to be achieved.



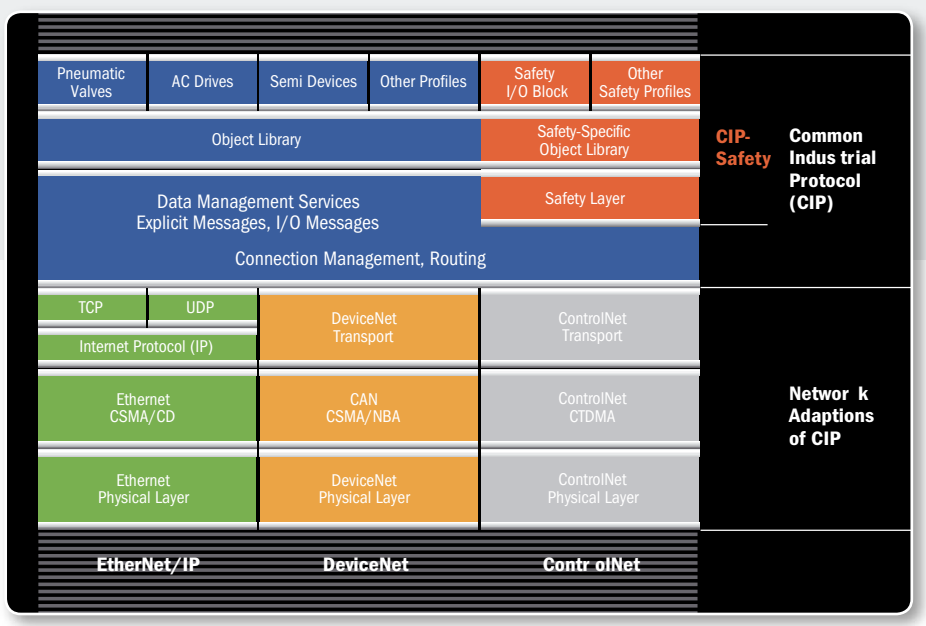
Black-Channel mechanism

How the Safety Systems Work

CIP Safety

The “CIP Safety” protocol was specified for safety data transmission via EtherNet/IP or DeviceNet. Using the pre-existing CIP (Common Industrial Protocol) Services as its foundation, the CIP Safety protocol makes use of the producer-consumer mechanism for the exchange of data between safe nodes. In this context, a consumer is designated “originator” and a producer is called “target”. Safe time synchronization between producers and consumers relies on chronological monitoring. Synchronicity between all nodes throughout the network provided, the time of origination of safe messages can be determined using a time stamp. These methods guarantee that processed data is still up to date. For the transfer of the safe data, “Safety Validator Objects” are used. They organize and guarantee the integrity of messages in a CIP Safety network. These objects also constitute the bridge between the safety communication and the field bus or network used. For data transmission, the protocol provides single transfer or multicast connections. Their use depends on the capability of the channel used to support either of these connections.

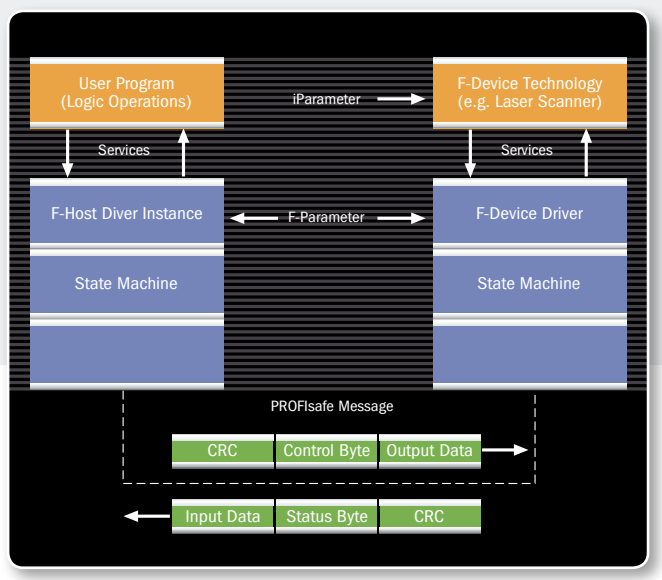
For CRC (cyclic redundancy check) calculation, the CIP Safety protocol makes use of five different formats, ranging from 8 bit to 32 bit CRC. These depend on whether data size is one or two Bytes or between three and 254 bytes and of the data range to be covered by checksum calculation. A “Unique Node Identifier” (UNID) is used for the unique identification of the safe nodes. It is a combination of a network ID and the node address, which is equivalent to the MAC address. It can be set either manually using DIP switches or via software configuration. During the ramp-up phase, the originator checks the presence of the configured UNIDs in the network. Further parameters such as timeout delays, ping intervals or the maximum number of nodes are configured using a Safety Configuration Tool (SNCT).

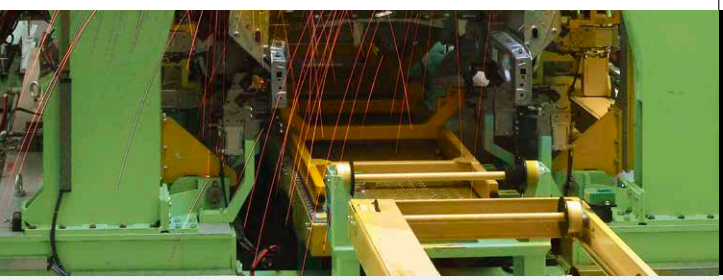


PROFIsafe

PROFIsafe uses the “Master-Slave” mechanism for transmission of safety telegrams. The master, typically called the “F-Host”, cyclically exchanges safety-relevant data with all its configured slaves called “F-Devices”. Each F-Device has an F-Driver organizing the co-ordination of safe messages called “Safety PDUs” (Protocol Data Unit) between the F-Host and F-Slave. CRC calculation of the PDUs depends on the message size to be transferred, the distinction being between “slim PDU” up to 12 bytes and “long PDU” up to 123 bytes. CRC 24 is used for slim PDU calculation, while for long PDUs, CRC 32 is used. As a means for message recipients to determine whether telegrams arrive in the right sequence, PROFIsafe uses consecutive numbers for the safety telegrams. Additionally, monitoring of the tolerance time (F-Watchdog Time) that is reset upon receipt of a telegram ensures that always the currently valid telegrams are read. The so-called F-Parameters (PROFIsafe parameters) supply a unique identifier between F-Host and F-Device.

Although the addresses (Unique Codename) are automatically passed on to the F-Devices, the target addresses need to be adjusted directly at the device via DIP switches. The F-Devices receive their configuration through transfer of the F-Parameter via “GSD” (General Station Description) and of the I-Parameter (individual F-Device Parameter). These parameters are managed within the iPar server, from where they can be transferred to a PROFIsafe Device using standardized interfaces. Usually, the iPar Server comes integrated in a “CPD-Tool” (collaborative product design) engineering tool. For product designers, this means that for the ability to completely configure an F-Device, a GSD file needs to be created and an interface to the CPD-Tool must be provided for each product.





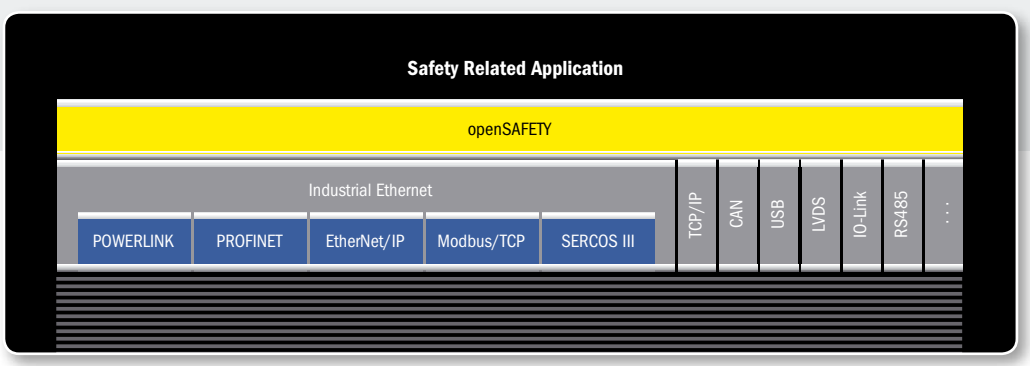
openSAFETY

openSAFETY was designed aiming at transmission of safety relevant data over any field bus or network. It can be used on all field buses, Ethernet-based or not.

For the transmission of safety data, the producer-consumer model is used. The advantage of this model is that all consumers in an openSAFETY network can receive and subsequently process the messages sent by the producer. Each openSAFETY node has a unique UDID (openSAFETY Unique Device Identification) number. During the booting process, the Safety Configuration Manager checks the device type and the UDID and automatically determines that the correct network configuration is being used. After confirmation by the user, the required parameters are then transferred to the safety nodes (SN). Automatic configuration reduces maintenance times and thus increases machine availability.

The openSAFETY Object Dictionary (SOD) manages all parameters and the configuration of each individual node. Upon completion of Node configuration and the booting phase, the cyclic data transfer between producer and Consumer commences. For the transfer of safety-critical process data, this uses Safety Process Data Objects (SPDO). The openSAFETY frame consists of two sub frames. It can transport a maximum of 240 bytes of safety data, using CRC 8 for payloads from 1 to 8 bytes and CRC 16 for payloads from 9 to 254 bytes.

With openSAFETY, very large networks can be created. For each openSAFETY Domain (SD), up to 1023 safe nodes can be connected. As they are addressed by the SCM, no additional hardware switches are required. The maximum total configuration of an openSAFETY network has 1023 openSAFETY Domains with a total of more than a Million safe nodes. Communication between the individual Domains is performed by the openSAFETY Domain Gateway (SDG).

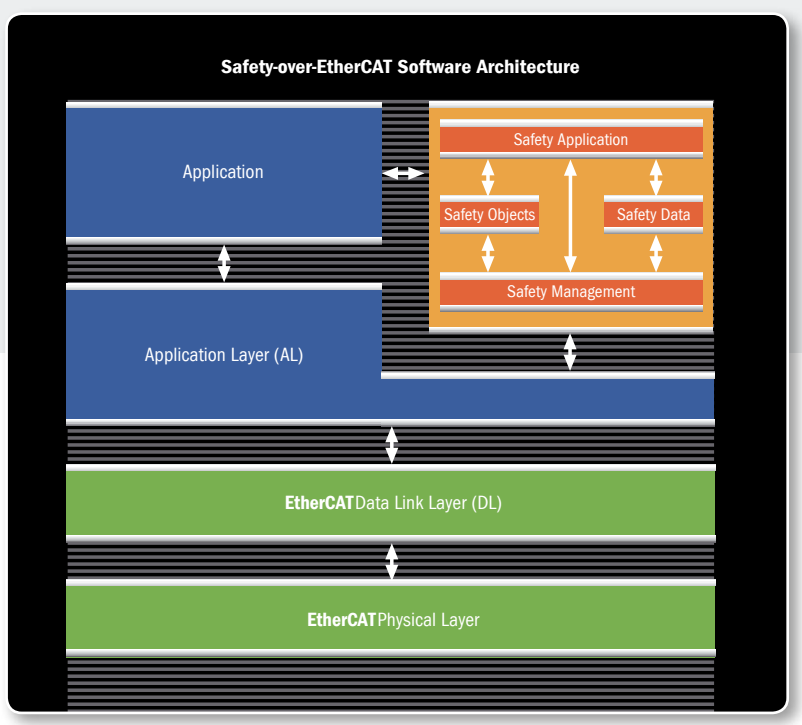


FSoE

Fail Safe over EtherCAT (FSoE) is a transmission scheme for safety data over EtherCAT using an FSoE master and FSoE slaves. In each FSoE cycle, the master sends its Safety PDU (Protocol Data Unit) to the slave, concurrently starting a watchdog timer. The slave verifies and calculates the data received prior to returning it to the master. In this case, the slave also starts a watchdog timer. The master receives and processes the data as described for the slave, stopping the watchdog timer. Only when this cycle is completed, the master generates a new Safety PDU. Due to this mechanism, safe communication always depends on the hardware and topology used.

The address relation between a master and a slave is called “FSoE-Connection”. It is characterized by a unique Connection ID. The 16-bit Connection-ID is transferred by the master to the individual slaves. Users need to take measures to ensure providing each slave with a unique ID. For correct identification of the ramp-up sequence, both the master and the slave generate a “Sequence Number” ranging from 0 to 65535 for every message. This ensures that only currently valid messages are processed. Addressing of the individual devices requires designation of unique Node numbers by hardware setting using DIP switches. Each FSoE master includes an “FSoE master Handler”, which communicates with a slave through an “FSoE slave Handler”. Optionally, an additional “FSoE slave handler” that can be implemented in the master allows communication between different masters within a network. For safeguarding the PDUs to transfer, for every 2 bytes of Safety Data, a CRC 16 is used. This implies that for a 10 Byte transfer, a CRC 16 is applied five times.

Parameter setting as such is not specified. The parameterization process needs to be part of the user-programmed application software. While the FSoE specification does detail the required parameters, users need to ensure for the individual FSoE slaves to receive their correct parameters.



Integrated Safety System Comparison

Certifications

Criteria	CIP Safety	PROFIsafe	openSAFETY	FSoE
Black-Channel based	+	+	+	+
IEC 61784-3	+	+	+	+
Certification body	TÜV Rheinland IFA	TÜV Süd IFA	TÜV Süd TÜV Rheinland	TÜV Süd

Generally speaking, all the various integrated safety technologies equally fulfill safety requirements. They are all based on the "Black Channel" principle, listed in the IEC 61784-3 standard and certified up to SIL 3. Hidden behind the raw safety aspects, however, are relevant criteria that define whether a technology will be adopted by component manufacturers or end customers. The distinguishing differences are the ease of integration of the technologies in the application serving the problem-solving purpose at hand.

Criteria	CIP Safety	PROFIsafe	openSAFETY	FSoE
SIL3 certified (IEC 61508)	+	+	+	+
Suitable for SIL4	o	o	+	o

openSAFETY technology is certified up to SIL3. Though it has not been qualified yet, the core principle of this technology, including probability of failure on demand (PFD), is ready for SIL4.

Technology

Criteria	CIP Safety	PROFIsafe	openSAFETY	FSoE
Payload Data duplication support	+	–	+	–
Multicast messaging support	+	–	+	–
Safety device configuration	+	o	+	o
Safe motion control	o	+	+	+

In the design of safety devices, technology considerations have great significance. Depending on the complexity of Safety frames, their composition can require undesired extra implementation efforts.
Support of multicast messaging helps achieve fast response times. These in turn can be influential for the overall plant or machine design, for instance reducing machine footprints and required floor space.
After maintenance or device replacement, safety slaves should automatically be configured by the safety master. Configuration interfaces need to be specified and unique so that devices can be configured by different masters. For PROFIsafe, the iPar-Server has been developed to cover this requirement. Its interoperability status in the market is unclear, because in the past, configuration data came from the manufacturer of the master used rather than from within the system.

FsOE offers a safe parameterization channel to transfer safe encapsulated data to the safe application, but addressing scheme of the safe application parameters does not exist.

Device Implementation

Criteria	CIP Safety	PROFIsafe	openSAFETY	FSoE
Legal limitation	+	–	+	–
Investment security	o	o	+	o
Time-To-Market	+	+	+	o
Imple-mentation	–	o	+	+
Current market share	o	+	o	–
certified stack available	+	+	+	–

For device manufacturers, independence and implementation costs are the most significant considerations. For implementation, all costs for license fees, software stack, conformance test and certification were taken into account in the comparison. So was the complexity of each technology and its impact on the required resources and costs for implementation.

ProfiSAFE and FSoE are limited to the protocols of their user organizations. This could lead to the requirement to implement several safety protocols if equipment using different automation systems and fieldbuses is combined. CIP Safety requires the implementation of a dedicated CIP Abstraction Layer within the Black Channel, thus increasing engineering efforts.

Criteria	CIP Safety	PROFIsafe	openSAFETY	FSoE
Supported Industrial Ethernet protocols	EhterNet/IP SERCOSIII	PROFINET	PROFINET EtherCAT EtherNet/IP Modbus POWERLINK PROFINET SERCOSIII	EtherCAT
Open-Source Implementation available	–	–	+	–

The openSAFETY stack is currently the only open source software for safety communication. Technically as well as from a legal point of view, openSAFETY is entirely technology-independent.

Integration

Criteria	CIP Safety	PROFIsafe	openSAFETY	FSoE
Stack compatibility	o	o	+	–
Performance	o	o	+	o
Addressing	+	–	+	–
Safe Reaction Time	o	o	+	o

To ensure compatibility between safety products from different manufacturers, compatibility of all stacks on the market is essential.

Open source strategy of openSAFETY guarantees stack compatibility.

In a safety network, all nodes must have unique IDs. To avoid parameter setting errors, addressing should be automated. The PROFIsafe and FSoE protocols, however, require manual address setting for each safety device using DIP switches. This makes installation of safety devices in the control cabinet more complicated. Human error, particularly in maintenance scenarios, could result in faulty parameter setting. It is also very difficult to create modular machine concepts using hardware switches, as this form of addressing is always rigid and components cannot be configured automatically.

Following the producer consumer principle, openSAFETY supports direct cross communication, which results in singularly fast reactions. Routing all safety messages via the master, as in PROFIsafe and FSoE, extends cycle times. Consequently, valuable time for safe reactions is lost.

CIP Safety requires originator functions to support cross-traffic, thus a cross-traffic between slaves (targets) is not possible.

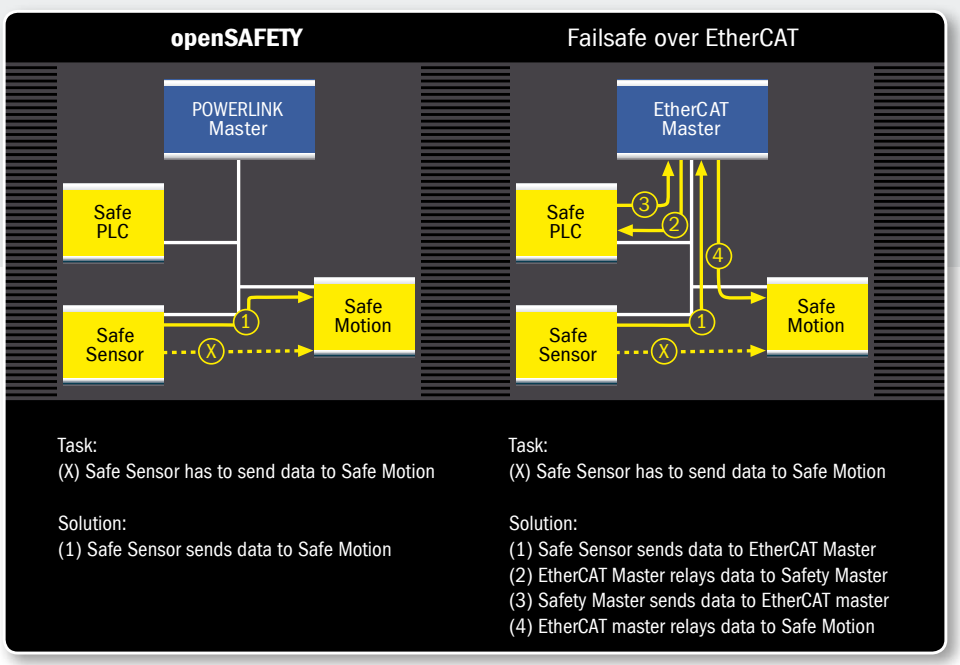
Performance

Since Safety protocols are application protocols, a safety network's performance depends on the underlying data transfer protocol. The base protocol selection determines the available bandwidth and the cycle times, but also functional features such as hot plugging capability or data communication via cross-traffic.

Cross-traffic plays a crucial role in the performance of safety-oriented systems. In networks supporting cross-traffic, safety nodes can transmit signals directly to each other without routing them through a master. This provides for optimized reaction times in hazardous situations. On a network not supporting cross-traffic, safety nodes send their signals to a fieldbus master node, which relays it to the network's safety master for acknowledgement. It is then handed back to the fieldbus master node which forwards it to the receiving safety node. Compared to direct data transfer via cross-traffic, this process causes four times the signal delay – valuable reaction time elapses. Since the emergency stopping distance of an axis increases with the square of the fault response time and negative acceleration, quadrupling the signal transfer time will result in a 16-fold extension of the emergency stopping distance.

Criteria	CIP Safety	PROFIsafe	openSAFETY	FSoE
CRC range	8-32 bits	24-32 bits	8-16 bits	16 bits
Required CRC computations for 20 bytes net data	2	1	2	10
Number of different CRC	5	2	2	1

The required number of different checksums increases implementation complexity, resulting in higher development costs. Additionally, computation of multiple CRCs may result in significantly slower reaction to safety violations.



Example for shorter signal transfer times due to cross-traffic: Cross-traffic enables safety nodes to directly communicate with each other (left), whereas signal paths are quadrupled in a system that does not support cross-traffic (right).

Masthead

"INDUSTRIAL**ETHERNET**FACTS" is an information service provided by the EPSG – ETHERNET POWERLINK STANDARDIZATION GROUP.

POWERLINK-Office
Bonsaiweg 6
15370 Fredersdorf · Germany
Phone: +49 33439 539 270
Fax: +49 33439 539 272
info@ethernet-powerlink.org
www.ethernet-powerlink.org

MM-BR-PL-IEF-EN-03 INDUSTRIAL**ETHERNET**FACTS MÄRZ 2016 ENGLISH