



Industrial Ethernet in process automation

... and explosion protection?

by André Fritsch



Figure 1: Explosion protected Ethernet for process engineering

Not so long ago, bus technology was more or less unacceptable in process automation, particularly in hazardous areas. Approximately 20 years ago the first fieldbus solutions were based on largely proprietary solutions. In 1988 R.STAHL was the first to announce a remote I/O system for hazardous areas in zone 1, at that time called 'Fieldbus System ICS MUX'. A very interesting system approach that was received with enthusiasm, and in particular by Norwegian offshore industry. The ICS MUX systems are still in use there today. The worldwide acceptance of this new technology was, however, way below expectations at the time and the technology only really became established 12 years later with the successor IS1.

General scepticism towards fieldbuses in hazardous areas has mellowed significantly in recent years and now almost everybody accepts bus solutions like Profibus DP or FOUNDATION™ fieldbus H1.

The next technological step now appears to be beginning – Industrial Ethernet. Even though Ethernet was invented in the 70s, it took a very long time for Ethernet to become established as the standard for the office world. As a result of the step-by-step installation of Ethernet systems in factory automation in recent years, this technology appears to be awakening interest for process automation. Along with various other companies and organisations, the two ›big players‹, Profibus and Fieldbus Foundation, are already offering Ethernet-based solutions: Profibus with ProfiNet and the Fieldbus Foundation with FF High Speed Ethernet (FF HSE)

Unlike factory automation, process automation is very closely linked to the topic of explosion protection, in particular in sectors such as oil & gas, chemicals, pharmaceuticals or petrochemicals. But are there any solutions for explosion protection with Ethernet? There are actually several approaches with solutions that all have advantages and disadvantages. A classic intrinsically safe Ethernet is possible – but is it practical and cost-effective? Ethernet over optical fibre has practical advantages – but what is the situation here with explosion protection? Does it always have to be type of protection intrinsically safe ›i‹ – which other types of protection could be used? And how do the apparatus and applications then appear? In the following we will address these issues, list the advantages and disadvantages of the solutions, and derive the best possible solution.

What is Ethernet? A look back

There is a nice story about the origin of Ethernet. A man called Robert Metcalfe invented the technology in 1973 during his work at the Xerox Palo Alto Research Centre (PARC). He sent his boss a note (Figure 2) about the capability of this new technology ... and the Ethernet standard was born. A nice story but not true. From 1973 to 1976 Robert Metcalfe worked with his team on a new, proprietary communication bus for Xerox. The first name for this bus was also not Ethernet but ›Alto Aloha Network‹ and it was only renamed ›Ethernet‹ after the imaginary ether in 1976. With a bus speed of 2.94 MHz, it was miles away from today's transmission speeds, and many years would pass before people begin to talk about Gigabit Ethernet.

In 1979 Robert Metcalfe left Xerox and founded his own company, 3COM. With DEC, Intel and Xerox, he began to standardize Ethernet. In 1980, IEEE (Institute of Electrical and Electronics Engineers) working group 802 started its standardization work (Table 1). One of the next milestones, and as a result an increase in acceptance, came with the change from coax cables (10Base2) to much cheaper and easier to install twisted pair copper cable (10Base-T). The first installations with optical fibres (10Base-F) still operated with a transmission speed of 10 Mbits/s. The next step came with the introduction of the 100 Mbit/s data rate, which is currently in use often under the name Fast Ethernet (100Base-T for copper cable, 100Base-FX for optical fibre). Since approx. 1995 a working group

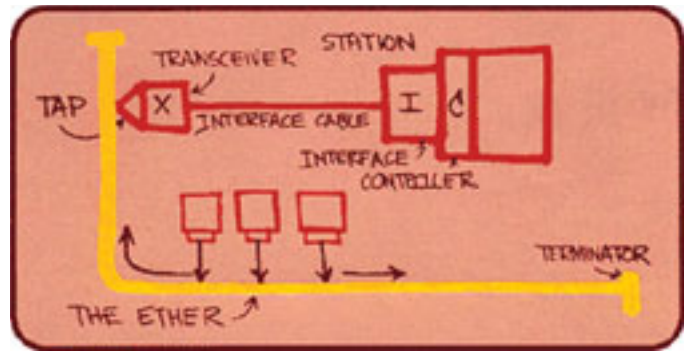


Figure 2: First Ethernet structure from Robert Metcalfe in 1973

has been addressing Gigabit Ethernet and has already standardized 1 Gbit/s (1000Base-T and 1000Base-SX or LX) and 10 Gbit/s (10Gbase). 10Gbit/s Ethernet is still very new on the market and not yet used widely. Some other well-known working groups related to Ethernet are the ›Power over Ethernet‹ group IEEE802.3af and the wireless LAN group IEEE802.11.

Ethernet technology – a short introduction

The first Ethernet systems in the 1970s were still ›real‹ bus systems with a trunk and spurs (see Figure 2). These days Ethernet is no longer installed as a bus, even though the term bus or even fieldbus is used colloquially in relation to Ethernet. Modern installations have star or mesh structures (Figure 3). While a star is very easy to install with every device in a network connected to exactly one other device, mesh networks are significantly more complex and require more intelligence in network management. As a result these structures have higher availability. If a device fails, the data are forwarded via a different device. The Internet is probably the best and largest example of a meshed network.

Even though over the years a large number of changes and improvements have been introduced and the modern Ethernet is very different to the initial version, the basic communication structure is still the same. It is based on the so-called ›Carrier Sense Multiple Access with Collision Detection‹ or CSMA/CD for short. The principle can be compared with a discussion group. Everyone uses the same medium (e.g. the air or a telephone line). If someone wants to say something, he/she waits until the person speaking has finished or takes a break and then talks. If two or more people start to talk at the same time, they stop, wait a moment and then continue in the hope that the others will react a little slower. →

Active Working Groups	
IEEE P802.3ap	Backplane Ethernet Task Force
IEEE P802.3ar	Congestion Management Task Force
IEEE P802.3as	Frame Expansion Task Force
IEEE P802.3at	DTE Power Enhancements Task Force
IEEE P802.3av	10Gb/s PHY for EPON Task Force
IEEE 802.3aw	10GBASE-T Corrigendum
IEEE 802.3ax	Link Aggregation Task Force
IEEE 802.3ay	Maintenance #9 (Revision) Task Force
IEEE 802.3	Higher Speed Study Group
IEEE 802.3	Energy Efficient Ethernet Study Group
IEEE Std 1802.3-2001	Conformance test reaffirmation
Completed work	
IEEE 802.3	Trunking Study Group
IEEE 802.3	Higher Speed Study Group
IEEE 802.3	DTE Power via MDI Study Group
IEEE 802.3	10GBASE-CX4 Study Group
IEEE 802.3	10GBASE-T Study Group
IEEE 802.3	Backplane Ethernet Study Group
IEEE 802.3	10Gb/s on FDDI-grade MM fiber Study Group
IEEE 802.3	Power over Ethernet Plus Study Group
IEEE 802.3	Residential Ethernet Study Group
IEEE Std 802.3z-1998	Gigabit Ethernet
IEEE Std 802.3aa-1998	Maintenance #5
IEEE Std 802.3ab-1999	1000BASE-T
IEEE Std 802.3ac-1998	VLAN TAG
IEEE Std 802.3ad-2000	Link Aggregation
IEEE Std 802.3ae-2002	10Gb/s Ethernet
IEEE Std 802.3af-2003	DTE Power via MDI
IEEE Std 802.3ag-2002	Maintenance #6 (Revision)
IEEE Std 802.3ah-2004	Ethernet in the First Mile
IEEE Std 802.3aj-2003	Maintenance #7
IEEE Std 802.3ak-2004	10GBASE-CX4
IEEE Std 802.3REV am-2005	Maintenance #8 (Revision)
IEEE Std 802.3an-2006	10GBASE-T
IEEE Std 802.3aq-2006	10GBASE-LRM
IEEE Std 802.3	DTE Power Isolation Corrigendum
IEEE Std 1802.3-2001	Conformance Test Maintenance #1
IEEE P802.3	Ethernet over LAPS liaison Ad hoc
IEEE P802.3	Static Discharge in Copper Cables Ad hoc
IEEE P802.3	100BASE-FX over dual Single Mode Fibre Call for interest

Table 1: Overview of the IEEE 802.3 Ethernet working groups

This system works very well if there are only a few participants in the group. The more participants, the more likely a collision and the slower the group will progress. The problem described is not particularly critical for Ethernet connections in everyday use. Everyone is familiar with the phenomenon that sometimes the network access becomes very slow or even stops completely for no apparent reason. This is a typical sign of an overload where too many devices are communicating on the network at the same time resulting in frequent collisions. Typically an office network should be utilized to a maximum of 50 ... 60% to guarantee acceptable response times. Slower access here may be tedious, but are not normally critical, unless you need to print an important document for your boss at the time.

The situation is different for automation technology. If it cannot be guaranteed that information is available in a defined time, it will not be possible to correctly control many systems. Control functions without guaranteed response or reaction times are mostly unacceptable. This behaviour is described with the term »real time«. One measure to achieve real time capability was to increase the data rate from 10Mbit/s to 100Mbit/s or even Gigabit. The faster the network, the lower the probability that collisions will occur, and the more likely the information can be transmitted on the first attempt. This makes it possible to react significantly faster to collisions that have occurred and for data to reach its destination quickly despite repetition. Another measure is to limit the number of devices in the network, which must be taken into account when planning network structures. In industrial applications, networks should therefore be utilized to max. 8 ... 10%.

Industrial Ethernet for process automation

By taking the measures stated above, reaction times of approx. 100 ms or less can be guaranteed. It is from this point that the technology becomes interesting in principle for process automation. However, a protocol is required that must also meet the requirements stated above, in short that is »real time«. Standard Ethernet protocols like TCP or UDP are too slow and unreliable, so special real time protocols have been developed. Using these protocols, response times of approx. 10 ms are possible; on the usage of special, proprietary Ethernet hardware even 1 ms is possible. Unfortunately, a large number of different protocols have been developed over the years, such that today there are more than 20 protocols and of these, as many as 11 are standardized worldwide as an IEC standard (Table 2). And of course, they are all incompatible with each other and therefore truly reactionary.

Other differences between Ethernet and Industrial Ethernet are primarily in the hardware. The requirements in industry are very different to those in the office world. For this reason, all components like cables, connectors, switches, hubs or media converters are of significantly more robust design. Installation is typically on 35 mm DIN rails, the supply of power is 24 V DC, and an expanded operating temperature range and higher IP degree ratings are required. The cables only differ slightly, except that armoured cables are used outdoors. Different cables of varying quality (and price) are used depending on the data transmission speed. These are the CAT5 cables for Ethernet up to 1 Gbit/s or CAT7 cables for up to 10 Gbit/s.



In general, three different transmission media can be used: copper, optical fibre and rf (wireless). Although wireless transmission in accordance with the WLAN standard is not part of the Ethernet standard IEEE802.3, it is in principle possible to support the Ethernet data format and to communicate with these systems.

Industrial Ethernet is already used very frequently for automation (Figure 4). The majority of applications are in factory automation, in the automotive sector or the control of machinery. According to a market study by Frost & Sullivan, the international Industrial Ethernet market has been growing at approx. 50% per year since 2000. Other market studies have yielded similar results.

The usage of Ethernet is somewhat behind this development for process automation in sectors like oil & gas, chemicals, pharmaceuticals etc. Many sector-specific requirements have not yet been met, e.g. many applications in the oil & gas sector require redundant structures. Although there are some Ethernet solutions with redundancy (spanning tree or rapid spanning tree), the reaction and switching times are in the order of seconds and therefore much slower than the values required in process automation of 100... 500 ms. Even typical process protocols like ProfiNet or in particular Fieldbus Foundation™ High Speed Ethernet (FF HSE) are still in the specification phase in relation to the requirements

of the process industry. In both organizations, working groups are currently tackling the integration of Ethernet and also the interfacing of remote I/O systems via Ethernet to the process world. It is expected that the first solutions will come onto the market from 2009.

Explosion protection for Industrial Ethernet – types of protection

The requirement for explosion protected solutions is typical for the sectors mentioned. Many applications are installed in zone 2 or zone 1. In principle, there are several ways in which Industrial Ethernet can be designed for explosion protection. The solutions depend on the cable or transmission medium used and the actions necessary in the hazardous areas, e.g. making and breaking connections in operation, maintenance work on systems in operation, replacement or addition of components etc. Some types of protection that can be used are very well known, e.g. intrinsically safe or flameproof enclosure. Others such as inherently safe optical radiation or explosion protection for radio waves are still very much new territory. In the following we will look in more detail at the various possibilities. →

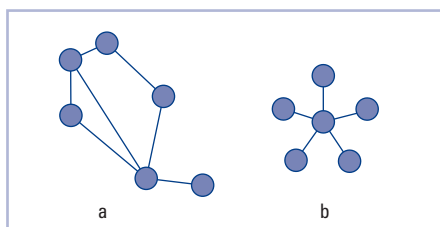


Figure 3:
a) mesh network
b) star network

IEC/PAS 62030 (Ed. 1.0)	Digital data communications for measurement and control – Fieldbus for use in industrial control systems – Section 1: MODBUS® Application Protocol Specification V1.1 a – Section 2: Real-Time Publish-Subscribe (RTPS) Wire Protocol Specification V1.1a – Section 2: Real-Time Publish-Subscribe (RTPS) Wire Protocol Specification Version 1.0	2004-11
IEC/PAS 62405 (Ed. 1.0)	Real-time Ethernet Vnet/IP™ specification	2005-06
IEC/PAS 62406 (Ed. 1.0)	Real-time Ethernet TCnet (Time-Critical Control Network)	2005-08
IEC/PAS 62407 (Ed. 1.0)	Real-time Ethernet control automation technology (EtherCATTM)	2005-06
IEC/PAS 62408 (Ed. 1.0)	Real-time Ethernet Powerlink (EPL)	2005-06
IEC/PAS 62409 (Ed. 1.0)	Real-time Ethernet for Plant Automation (EPA) (R)	2005-06
IEC/PAS 62410 (Ed. 1.0)	Real-time Ethernet SERCOS III	2005-08
IEC/PAS 62411 (Ed. 1.0)	Real-time Ethernet PROFINET IO	2005-06
IEC/PAS 62412 (Ed. 1.0)	Real-time Ethernet P-NET on IP specification	2005-08
IEC/PAS 62413 (Ed. 1.0)	Real-time Ethernet - EtherNet/IP (TM) with time synchronization	2005-07
IEC 61158-2 (Ed. 3.0)	Fieldbus Foundation - High Speed Ethernet (FF-HSE)	2003-05

Table 2: IEC standardized real time ethernet protocols

The classic: intrinsic safety

If consideration is given to the topic of explosion protection in process automation, initial thoughts are mostly of the type of protection intrinsically safe »i«, (IEC 60079 -11 [19]).

Intrinsic safety is based on the fact that a specific amount of energy is required to ignite an explosive atmosphere. The amount of energy in an intrinsically safe circuit is reduced to a safe level by limiting current and voltage so that sparks or other thermal effects no longer represent sources of ignition. This situation applies under normal operating conditions and also under certain fault conditions. The resulting advantage, which makes it possible to work on, install and maintain live equipment in hazardous areas has made this type of protection the most widely used in process automation today. Intrinsic safety is typically used for 4...20 mA signals, and also for fieldbuses like Profibus PA or Foundation Fieldbus H1, as well as for Profibus DP as mentioned above. This situation of course suggests the application of this principle for Ethernet.

Similar to conventional installations with intrinsically safe circuits, e.g. for 4...20 mA signals, an item of so-called »associated apparatus« is required. This apparatus isolates the intrinsically safe circuits in zone 1 from the non-intrinsically safe circuits in the safe area. Initially, safety barriers without electrical isolation were used for this purpose. In modern systems, however, electrical isolators are increasingly used. The result is that simpler installa-

tion, higher transmission accuracy and significantly more robust EMC properties for earthing and screening can be achieved.

These electrical isolators are therefore also appropriate for an intrinsically safe Ethernet installation with copper cables. The electrical isolators must be of a special design that can cope with the high transmission rates and be very robust to external interference. Due to the high transmission rate for Industrial Ethernet of 100 Mbit/s, special attention must be paid to the usual components such as Zener diodes, transistors, transmitters and optocouplers in the Ex i isolators. Without appropriate high quality components and a clean high frequency design, signal distortion, and as a result transmission errors, will occur.

As no Ethernet installation can go without corresponding switches, hubs or routers, it would seem sensible to integrate the isolator functionality into these modules. In this way possible signal corruption or interference due to additional connectors and contact resistances is elegantly eliminated at the same time.

Today there are only a few products on the market that use the classic intrinsic safety for Ethernet. As the safety-related parameters for these apparatus are not standardized, as has happened, e.g., with the FISCO model for fieldbus, different devices from different manufacturers are not currently compatible without additional measures and it is correspondingly difficult to verify intrinsic safety.

Perhaps the biggest problem is the 100 Mbit/s Ethernet itself, specifically in the form of the cable lengths. Copper cables – specified according to the Ethernet standard as CAT5 or CAT7 – permit maximum distances of approx. 100 m if laid correctly with optimal screening. They are therefore often much too short for applications in process technology.

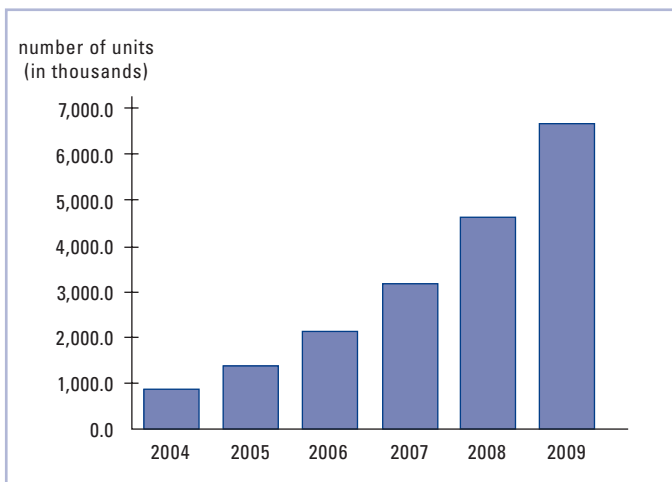


Figure 4: Industrial Ethernet device supply – market analysis and outlook up to 2009 from the ARC, date 2005



Figure 5: Flameproof connectors miniCLIX for Industrial Ethernet



Figure 6: Ex d connector system with hot-plugging functionality

Flameproof enclosures ›d‹ and increased safety ›e‹

Another type of protection that can be considered is flameproof enclosures ›d‹ (IEC 60079-1 [17]), mostly in combination with increased safety ›e‹ (IEC 60079-7 [18]) in the form of a connection box. This solution is based on the requirement that although an explosion can occur inside an enclosure, the energy from the explosion must not escape to the outside, or only an insufficient amount of energy can escape to the outside, and the explosion must not destroy the enclosure. Although Ethernet devices could be installed in appropriate flameproof enclosures, there is then again the problem with the cables that must be connected to the enclosure in some way. Whether as direct flameproof cable entry or indirectly using a connection box in type of protection increased safety ›e‹, specially designed cable glands are needed that, on the one hand, transmit the high frequency Ethernet without distortion, and on the other hand do not allow the energy from the explosion to escape to the outside. These Ethernet-flameproof cable glands are also already available on the market. However, there is again also the problem of reachable transmission distance and appropriate careful screening with copper cables.

Even the requirement for pluggable connections that can be made during operation, that is similar to an intrinsically safe solution, is met by a few products. R.STAHL has launched the special connector system in type of protection flameproof enclosures ›d‹ miniCLIX for this purpose (Figure 5 and 6).

The principle of operation of these Exd connectors is as follows: in a first step the electrical circuit is isolated. As the connector is not yet separated mechanically, any sparks produced remain inside a tiny flameproof space. Only after a short delay can the connector also be separated mechanically. As standard Ethernet connectors are not used here, miniCLIX of course had to be verified as ›Ethernet-compatible‹ through extensive testing.

Even though this solution appears to be very elegant, it still does not deal with the problem of cable lengths and appropriate careful installation. There is also the problem that the Ethernet devices with the connector pins must be switched off prior to isolation, as Ethernet operates bi-directionally. If this problem is not addressed there would be open connector contacts in the hazardous area, and that is not allowed. As discussed later the solution is transmission using optical fibres.

Example of application using Ethernet

Typical applications are, e.g., in the area of operator and monitoring systems. Modern operator interfaces with large, high resolution monitors and a high level of functionality up to and including so-called open HMI systems (Figure 7), which have PC functionality, are increasingly also used in hazardous areas zone 1. These powerful systems also need correspondingly fast bus interfaces with high data rates. Industrial Ethernet is particularly well suited to this task. Depending on the application and requirements, the connection is made using the Exd or Exe technology mentioned above. In mobile applications, the connection system miniCLIX mentioned can be used.

Explosion protection using optical fibres

Up until now it is clear that for solutions based on the use of copper cables, the maximum cable length remains a possible obstacle. It would seem obvious than to ask the question what can be done with optical fibres? Optical fibres make greater distances possible between components in a plant that even high quality screened CAT7 twisted pair cable can not achieve. Depending on the fibre used, distances of 2000 m or more are possible. →

And explosion protection? Is this even necessary at all for a bit of light? This need is easy to explain: if you focus sunlight on some straw using a simple magnifying glass, as is well known the straw will start to burn after a short time (Figure 8). If light is focussed on a small point, the energy is bundled – at the focal point the energy is many times higher. An optical conductor focuses light on a very small point. As early as the 90s the PTB in Germany began investigations on the topic of optical energy in hazardous areas. In 1996 the PTB report W-67 ›Welzel, M.M., Entzündung von explosionsfähigen Dampf/Luft- und Gas/Luft-Gemischen durch kontinuierliche optische Strahlung‹ was published [14]. In August 2006, IEC 60079-28 ›Explosive atmospheres – Part 28: Protection of equipment and transmission systems using optical radiation‹ was published [21]. The European implementation appeared in October 2007; it will also be included as appropriate in the next issue of IEC 60079-0.

In general, four possible ignition mechanisms are considered:

- › heating of particles by optical radiation and reaching a surface temperature capable of causing ignition
- › thermal ignition of a quantity of gas due to the optical wavelength matching an absorption band for the gas, this is a type of resonance effect
- › photochemical ignition due to photochemical dissociation of oxygen molecules caused by radiation in the ultraviolet range
- › direct laser-induced flashover of a gas at the focal point of a powerful beam and production of plasma or a shock wave that can both act as sources of ignition.

In practice users will most frequently come across the mechanism first mentioned (see experiment in Figure 8). The standard also describes three possible types of protection methods.

- › inherently safe optical radiation ›op is‹
- › protected optical radiation ›op pr‹
- › optical systems with interlock ›op sh‹

The principle of inherently safe optical radiation is very similar to electrical intrinsic safety. It is based on limiting the optical energy in a system, e.g. in an optical fibre, in normal operation and in certain fault conditions. For example, the maximum optical radiant power allowed for use in hazardous areas zone 1 and explosion group IIB for temperature class T4 is limited to 35 mW.

There are also additional requirements for pulsed radiation. This type of protection ›op is‹ is very suitable for Industrial Ethernet. The advantages of electrical intrinsic safety are transferred to optical fibre and as a result provide a high level of flexibility. Optical fibre conductors can be connected and disconnected during operation in hazardous areas; installation and maintenance work on ›normal‹ equipment is then possible.



Figure 7: Modern open HMI system with Ethernet interface

The only thing missing for a complete solution is an appropriate optical isolator. Apparatus based on the principle of inherently safe optical radiation were developed very early for the intrinsically safe Profibus DP. The first was placed on the market by R. STAHL for the in-house remote I/O system IS1 at the end of the 90's. Successor products permit installation of an optical ring in hazardous areas, and provide convenient diagnostics and signalling features for fibre fracture or signal level (Figure 9). For Industrial Ethernet there is currently only one apparent solution that has been integrated into a switch.

Applications are here again in operator interfaces. With the protection method inherently safe optical radiation an interface in operation can be disconnected or connected to the bus, a feature that is particularly advantageous for mobile applications and constantly changing locations.



Remote I/O on the optically inherently safe Ethernet

For some years remote I/O systems and/or fieldbus installations have been increasingly replacing the point to point connection with conventional isolators. Less wiring effort, better and more comprehensive diagnostics, as well as space savings in the control room are some of the reasons why users are increasingly changing to these technologies. On remote I/O systems, e.g. the system IS1 from R. STAHL, Profibus DP is used these days in the majority of cases as the bus protocol. Profibus DP is still one of the few fieldbuses that can transmit the amount of data produced by a remote I/O system in an acceptable time, and that allows larger system structures to be designed cost-effectively. Furthermore, it is available in an explosion protected version both for copper and optical fibre cables (see above).

With Industrial Ethernet new opportunities are opening up where interfacing can be made faster and more effective, and where it can be integrated into existing structures of a plant significantly more easily and more optimally – keyword ›vertical integration‹. As a consequence, since the start of 2007 the large fieldbus organisations Profibus International and Fieldbus Foundation™ have been tackling the integration of remote I/O technology into their system architectures, ProfiNet for the Profibus organisation and FF HSE for the Fieldbus Foundation™. R. STAHL

is actively involved in these working groups and will announce corresponding solutions for the IS1 system when the new specifications are available. It can be assumed that corresponding equipment will be launched in 2009, and that the first applications and systems could also go into operation then. One open point is unfortunately still the support for the protocols by the process control systems. Only very few support the ProfiNet protocol, or even FF HSE. In the context of open system solutions, it is to be hoped that this situation will change in the near future.

On the other hand, it is not absolutely necessary to wait for the ›grand solution‹, as the majority of control systems already support a simple but still very effective Ethernet real time protocol, Modbus TCP. There are already installations in safe areas. And with the appearance of the new remote I/O system IS1-Ethernet from R. STAHL, the first fieldbus solution is available for hazardous areas zone 1 (Figure 10). This system support Modbus TCP with a flexible hardware platform can also be used in the future for the ProfiNet and FF HSE specifications when they are available. Although compared to the more powerful protocols Profinet or even FF HSE, Modbus TCP does not provide any integrated diagnostics and parameter configuration functions, R. STAHL has developed a very powerful DTM for this interface for simple and effective integration. →



Figure 8: Optical energy can cause ignitions and explosions!



Figure 9: Optical fibre isolating repeaters for Profibus DP, for Profibus DP with optical ring and for Industrial Ethernet (fltr)



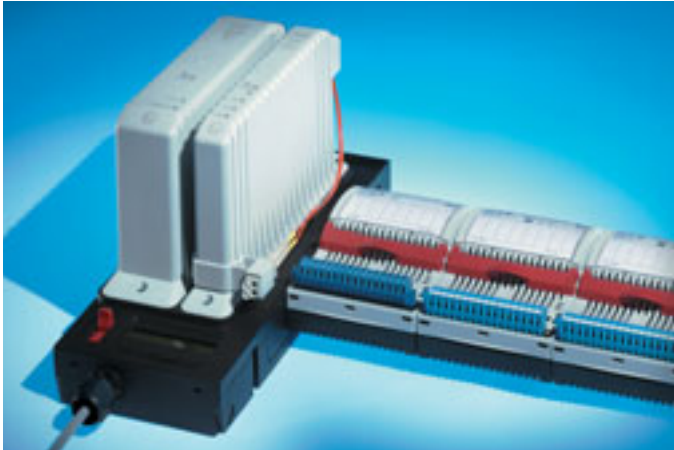


Figure 10: Remote I/O system IS1 with Industrial Ethernet

Protected optical radiation and interlocking with cut-off

Protected optical radiation ›op pr‹ is based on the concept that the radiation cannot escape from its confinement. Optical fibre cables must be designed to be correspondingly robust or laid so they are protected against damaging effects. Enclosures for, e.g., connectors must be designed such that an explosion in the interior cannot cause ignition of the surrounding atmosphere and no hazardous quantities of optical energy can escape. As a result this type of protection method is very similar to the type of protection flameproof enclosures ›d‹. Special cable glands are again necessary here (Figure 11).

There are no connectors for this situation such that this type of protection will initially be limited to a few fixed installation applications.

The principle of interlocking and cut-off ›op sh‹ was used a few years ago in a similar form by Fuji for a transmitter. The protection principle for this type of protection method is based on a risk analysis. Anybody who is reminded of the topic of functional safety as per IEC 61508 [12] and IEC 61511 [13] would be right: IEC 60079-28 refers to these standards.

Explosion group	Effective power limits
IIA	6 W (mean value over 100 µs)
IIB	3.5 W (mean value over 100 µs)
IIC	2 W (mean value over 100 µs)

Table 3: Limits for radio waves hazardous areas (VDE0848, section 4.4)

No wires: wireless and WLAN

Wireless interfaces in hazardous areas can also already be found in a few applications; there are also several suitable types of protection here. As wireless solutions for process automation will only slowly become established over the coming years, these type of protection methods will not be covered in more detail here. The requirements on the explosion protection for electromagnetic radiation is only defined with the issue of IEC 60079-0 edition 5 [10]. Currently only the German VDE 0848 from 2001 [15] is available as a basis (Table 3).

Today applications have already been implemented wirelessly, e.g. monitoring of tank farms and pipelines, access control or portable diagnostics. The fieldbus organizations are also active in the wireless technology sector. Only recently the working groups from HART, Profibus and the Fieldbus Foundation™ formed a joint group to define a common solution for process automation. The first products, e.g. a wireless FF HSE gateway, are expected to reach the prototype stage by the end of the year. R. STAHL is also actively involved here, and is contributing its knowledge particularly on the topic of explosion protection.



Figure 11: Flameproof gland for optical fibres

While in the cable-based Ethernet world, the switch is the central component between the field level and the control system, an access point is used in wireless applications. Here R. STAHL launched the first solutions for hazardous areas zone 1 as early as last year. The solution is based on industrial access points installed in suitable enclosures with appropriate antennae in type of protection increased safety »e« to suit the requirements of zone 1 or zone 2 (Figure 12). However, intrinsically safe solutions are also now available. The connection of the access point to the control system is in turn made using cable-based Ethernet, with either copper or optical fibre cables and the type of protection methods described above.

Outlook

Industrial Ethernet has taken a hold in process automation. There are still questions and risks, as with all new technologies. The opinion that Ethernet will make everything easier and better may justifiably be doubted in some cases. How the two major solutions Profinet and FF HSE will be accepted by the end user and the control system manufacturers is still uncertain. The question of »if« and »how« for the explosion protection have, however, already been answered.



Figure 12: Wireless LAN access point for hazardous areas

References

- [1] »Profibus International« in the internet at www.profibus.org
- [2] »Fieldbus Foundation« in the internet at www.fieldbus.org
- [3] PROFINET: PROFINET Technology and Application – System Description; Order no. 4.132
- [4] FF HSE: FF-007 Foundation Technical Specifications (H1+HSE)
- [5] IEC 61158-2: Digital data communication for measurement and control – Fieldbus for use in industrial control systems – Part 2: Physical layer specification and service definition
- [6] IEEE 802: LAN/MAN Standards Committee develops Local Area Network standards and Metropolitan Area Network standards. The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs. An individual Working Group provides the focus for each area
- [7] IEEE 802.11: IEEE Wireless Communication Standards; 25th August 2004
- [8] TCP: Transmission Control Protocol acc. to standards RFC793 and RFC 1323
- [9] UDP: User Datagram Protocol acc. to standard RFC 768
- [10] Frost&Sullivan in the internet at www.frost.com; market analysis
- [11] »ARC Advisory Group« in the internet at www.arcweb.com
- [12] IEC 61508: Functional Safety of electrical/electronic/programmable electronic systems (1998-12)
- [13] IEC 61511: Functional safety – Safety instrumented systems for the process industry sector (2004-11)
- [14] M. M. Welzel, Entzündung von explosionsfähigen Dampf/Luft- und Gas/Luft-Gemischen durch kontinuierliche optische Strahlung, PTB Bericht W-67: Wirtschaftsverlag NW 1996
- [15] VDE 0848-5: Sicherheit in elektrischen und magnetischen Feldern Teil 5 Explosionsschutz 2001-01
- [16] IEC 60079-0 Ed.5.0: Explosive atmospheres – Part 0: Equipment general requirements (2007-10)
- [17] IEC 60079-1: Explosive atmospheres – Part 1: Equipment protection by flameproof enclosures »d« (2007-04)
- [18] IEC 60079-7: Explosive atmospheres – Part 7: Equipment protection by increased safety »e« (2006-07)
- [19] IEC 60079-11: Explosive atmospheres – Part 11: Equipment protection by intrinsic safety »i« (2006-07)
- [20] IEC 60079-27: Electrical apparatus for explosive gas atmospheres – Part 27: Fieldbus Intrinsically Safe Concept (FISCO) and Fieldbus non-incendive concept (FNICO) (2005-04)
- [21] IEC 60079-28: Explosive atmospheres – Part 28: Protection of equipment and transmission systems using optical radiation (2006-08)