Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 100 (2015) 773 – 781

Procedia Engineering

www.elsevier.com/locate/procedia

25th DAAAM International Symposium on Intelligent Manufacturing and Automation, DAAAM 2014

The Common Industrial Protocol in Machine Safety

Stohl Radek[a]*, Stibor Karel[b]

[a]*CEITEC - Central European Institute of Technology, Brno University of Technology, Technicka 10, Brno, 606 00, Czech Republic*
[b]*Faculty of Electrical Engineering and Communication, Brno University of Technology, Technicka 10, Brno, 606 00, Czech Republic*

Abstract

The authors discuss the Common Industrial Protocol (CIP), an instrument used in many types of networks, including EtherNet and DeviceNet. The CIP is classified into a large number of variants, for example CIP Safety, CIP Sync, or CIP Energy, to facilitate easy communication between industrial network components that need to interact with other elements in the given network. Out of these categories, CIP Safety will be described in greater detail, with a particular focus on the principles and applications of this version of the protocol.

Keywords: Common Industrial Protocol; Machine Safety; CIP Safety; CIP Sync; CIP Energy

1. Introduction

The meaning and purpose of *safety* are well known, and all people active in industry should be aware of their functional interpretation. The term *functional safety* covers the overall safety of machines [5], which can be achieved through various means, including fixed or movable guards, electronic, electromechanical or other machine-controlling hardware or applications, and information-related measures that generally help us to decrease the level of risk in machines and processes. The safety-oriented category [1] of the Common Industrial Protocol (CIP) [2, 4] is widely used for instances and fields (such as machinery) where a high degree of Safety Integrity Level is needed.

* Corresponding author. Tel.: +420-541-146-614; fax: +420-541-146-451.
E-mail address: radek.stohl@ceitec.vutbr.cz

doi:10.1016/j.proeng.2015.01.431

The introductory section of this paper comprises an outline of CIP-based network communication, and this part is suitably connected with the actual core of the article, namely the problem of extending the CIP to facilitate the transmission of safety information (CIP Safety [3, 7]). In this context, the authors specify the basic properties and capabilities necessary for the system to be regarded as safe. The final portion of the analysis contains error probability calculation to compare two different types of the emergency stop circuit design: the solution using the traditional relay-based technology, and the approach with a distributed system on a bus, in which communication via the CIP Safety protocol is utilised.

2. Common Industrial Protocol

The Common Industrial Protocol was designed by the ODVA organization. In general terms, the CIP [2, 4] describes connected or unconnected communication. The latter concept denotes communication for hardware which is not capable of building a data package for CIP messages. In controllers, MSG instruction is applied to enable usage on demand. Conversely, the former type of communication is needed for all devices located in the same network and intending to cooperate with each other seamlessly. Controllers use connection for the point-to-point communication path between the source and the destination. If we allude, for example, to the architecture of ControlLogix, then we have to point out that the processor opens the connection to every input, output, communication, or any other card in system; moreover, access is provided in this manner to the communication card or, through this card, to decentralized inputs, outputs, visualization, and all other devices. Every processor has a number of connections which can be opened at a single moment. While the smallest CPU can hold 8 connections, the best processors are capable of supporting up to 500 connections. This is physically represented by some allocated memory, communication time, and resources which have to be reserved on both sides.

Class 1 connections can send and receive data repeatedly at a pre-determined and configured rate. The discussed parameter is referred to as the RPI (Request Packet Interval), and it is always an attribute of definition of this connection. The connection is opened for the entire time during which the network remains operative and the originator is alive. When the target or the originator drop the link, the connection is closed and periodically retried by the originator.

Class 3 connections can be closed by the originator or via timeout; this form of communication is widely used in, for example, HMI interaction.

CIP services are always active and use unconnected communication to open Class 1 or 3 connections; importantly, they do not require user intervention to initiate the link. Based on the specification, we need connection to exchange any data between the members in a network, and data exchange is also necessary to establish the connection. In a network, the UnConnected Message Manager is active, providing the necessary means to communicate without any established connection and allowing “one shot” requests without setting up the connection. The originator sends an UnConnected message to the target in order to establish a connection, and it has to know how to obtain the type of information required from the target. This information can be found in an Electronic Data Sheet file.

3. CIP Safety

CIP Safety (Fig. 1) is an extended version of CIP messaging. As it is an extension, any device which cannot decode CIP safety is not involved in the communication. Identical principles are used for CIP Sync [8] in performing time synchronization, for example with respect to motion control on the axes and CIP Energy in devices measuring power consumption and power network quality.

CIP Safety [1, 3, 7] applies two basic principles of safety engineering practice: redundancy and diversity. CIP Safety uses only Class 1 connection. In any case of closed communication, all the outputs go to the safe state (logical 0). Every input/output card of the network has one connection, which means that the CPU ensures 99.9% diagnostics on every safety card regarding the events occurred and the measures to be adopted for higher SIL ratings. For non-safety IOs, the connection can be set as rack-optimized; thus, in an ideal case, sixty-three IO cards (each can have up to eight IOs) can be communicated over one connection. In safety connection, we can set the Safety Network Number; this is a unique code set up in the course of the programming phase, and it is combined with the node's IP address to get the UNID (Unique Node ID) used for clear identification of the point for communication. The Safety Network Number is generated automatically, but it can be modified by the designer or programmer of the safety system.

The second highly precise technique to be described utilizes time stamps in every data package of the connection. This method is referred to as the Connection Reaction Time Limit (CRTL), and it is available in two forms: the CRTL of the inputs and outputs, both observable from the CPU. The number of inputs multiplied by the RPI value plus the latency of the network will yield the value of the CRTL for the inputs; in the output signal, the aspects considered comprise the Safety Task period and the latency of the network.

The third technique to provide safety information between two members of a safety network is the CRC.

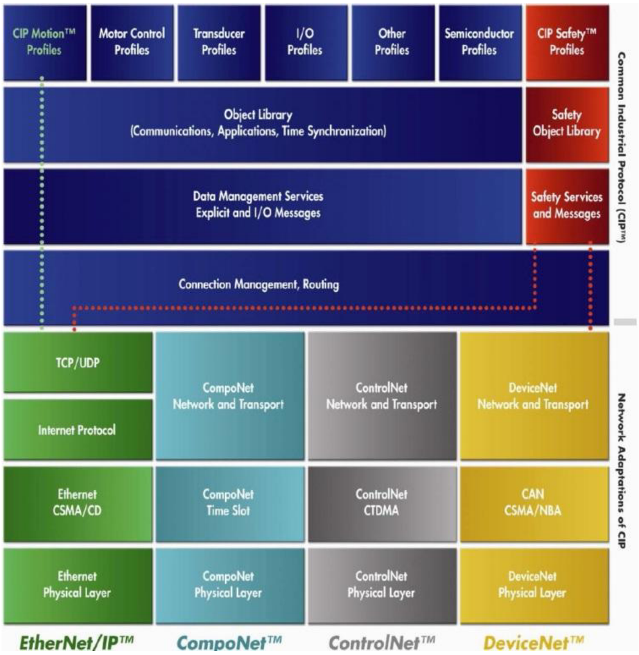
CIP Motion™ Profiles
Motor Control Profiles
Transducer Profiles
I/O Profiles
Other Profiles
Semiconductor Profiles
CIP Safety™ Profiles
Object Library (Communications, Applications, Time Synchronization)
Safety Object Library
Data Management Services Explicit and I/O Messages
Safety Services and Messages
Connection Management, Routing
Common Industrial Protocol (CIP™)
TCP/UDP
Internet Protocol
CompoNet Network and Transport
ControlNet Network and Transport
DeviceNet Network and Transport
Ethernet CSMA/CD
CompoNet Time Slot
ControlNet CTDMA
CAN CSMA/NBA
Ethernet Physical Layer
CompoNet Physical Layer
ControlNet Physical Layer
DeviceNet Physical Layer
Network Adaptations of CIP
EtherNet/IP™
CompoNet™
ControlNet™
DeviceNet™

Fig. 1. CIP Safety in the architecture of an ISO/OSI model [2].

4. Measures to render CIP Safety reliable

Although it is generally known how to transport safety data between two devices, we also have to be sure that the data have been transported to the right device. For this purpose, we use the property of every safety-related device, namely the UNID (Unique Network Identifier). The UNID can be identified as a MAC address, but it can also be modified by the SW designer if necessary. The UNID is encoded and safe–checked in all safety connections. As regards EtherNet [6], the UNID stems from the combination of the SNN (Safety Network Number) and the IP address of a node in the network. Thanks to this feature, the safety architecture is not restricted to one IP address set in the device, and we can use, for example, DHCP or BootP servers to obtain the IP address. The UNID has to be set up manually during the development/maintenance phase by the system designer or supervisor, and setting up the UNID and the IP address is fully independent.

Safety functions originated and were progressively developed in the 1980s and 1990s; at the time, this was the only method to produce safe applications. The actual evolution proceeded from hard-wired emergency stop buttons through switches and safety relays to contactors. Safety functions became very difficult to interconnect when more operational modes were available on one machine (such as a press), and therefore safety elements consumed a substantial part of the operating space of a machine. With the EN954-1 standard, there was also no other procedure to handle safety functions than that constituted by electromechanical devices. However, as both technology and safety keep moving forward, special safety systems started to appear in the late 1990s, facilitating the connectability of all safety devices into a single system and enabling us to decide what safety functions could be materialized on a software basis in conjunction with relevant sensors. From the perspective of legislation, this was nevertheless possible only with difficulty because, according to relevant laws from the given period, at least one emergency stop device had to be an electromechanical apparatus. After new legal standards were adopted in 2002, safety PLCs became applicable without certification restrictions.

Safety PLCs (usually with a redundant processor, networks, and other internal parts) are very effective even when other machine safety projects have to be adapted to the device in a complicated manner. But certain requirements for more complex functions surfaced too, including operation under safe speed or safe position of the proportional valves. Such demands can be satisfied only via microprocessor solutions as these applications are hard to solve by simple relays.

When safety had become a major aspect for machine users and operators, it was to be soon followed by the distributed solution of safety. In Germany, the committee for safety fieldbuses was founded in 1989 with the aim to adapt safety requirements transported over networks in line with the basic bundle of safety standards – the IEC (later also EN) 61508. Among the outcomes of the work performed by this committee there is also the CIP Safety published by the ODVA on the basis of the CIP.

4.1. Measures to keep CIP Safety reliable

Before transporting safety information, we need to create a Safety Channel on the network. The Safety Channel consists of a Client and a Server; on each of these two members, some validator has to be present to confirm whether the information is safe and, more importantly, reliable. The Safety device can be a monitor, a controller, an input or output, and an input or output device (sensor or actuator). The controller and monitor communicate with the I/O devices through I/O modules. This set of devices is referred to as the Safety Chain.

Table 1. Error detection measures [2].

Communication Errors	Measures to Detect Communication Errors				
	Time Expectation via Time Stamp	ID for Send and Receive	Safety CRC	Redundancy with Cross Checking	Diverse Measures
Message Repetition	X		X*		
Message Loss	X		X*		
Message Insertion	X	X	X*		
Incorrect Sequence	X		X*		
Message Corrupt			X	X	
Message Delay	X				
Coupling of Safety and Safety Data		X			
Coupling of Safety and Standard Data	X	X	X	X	X
Increased Age of Data in Bridge	X				

* The Safety CRC provides additional protection for communication errors in fragmented messages.

Whenever the validator checks the reliability of a message (Table 1), it uses the sequence of the pinging source with CRC ending and evaluates the CRC time stamp, time stamp, CRC data, safety data, and CRC complement data. Furthermore, cross checking is also performed within this operation. When the connection is terminated, the application is informed of such termination to be able to execute interventions including the de-energetising of the outputs. The CRCs used for CIP safety purposes are CRC-S1 or S2; these versions contain two bytes, of which one

(8bit) byte is for the CRC safety data, and the other is for the time stamp. The 16bit CRC-S3 is used for the CRC of the safety basic data with lengths from 3 to 250 bytes.

5. Comparison of the wired and network techniques

Let us now compare the outlined approaches for the purpose of very simple statistical data calculation. In this context, let us build a model case with a safety gate including a monitoring electromechanical switch that comprises two contacts connected in wiring category 3. The output will contain two contactors with feedback loop monitoring. Generally, two different solutions are to be performed; while we use a safety module or a relay for the safety logic function in the first method, the second case will involve a safety system using EtherNet/IP.

5.1. The safety relay approach

Safety relay is an incorrect term for a device which should be regularly referred to as a safety module. Some time ago, this safety module consisted of several relays packed in one box; these relays were interconnected to resolve problems related to safety, diagnostics, resetting, and some other safety and non-safety functions using the NO and NC contacts of classical electro-magnetic relays.

In order to evaluate the safety function, we have to define the concrete device for which the manufacturer provides statistical values of dangerous failures. Furthermore, it is necessary to determine the value following from the designer's assumption of how often the safety function will be used; to illustrate this statement, we could refer again to the case where the value expresses simultaneously the frequency of a safety gate opening and the exclusion of a potentially hazardous situation. At this point, let us choose the simplest solution: the designer will include in the manual two elementary parameters, namely the number of switching cycles per twenty years and the probability of a dangerous failure per the same unit of time.

However, to evaluate the SIL CL (Safety Integrity Level Claim Limit), we need also other properties, and these are as follows:

- Hardware Fault Tolerancy (*HFT*)
- Probability of Dangerous Failure per Hour (PFH_D)
- Safety Fail Fraction (*SFF*)
- Diagnostic Coverage
- Architecture of System
- Number of switching cycles per hour
- Test Proof Interval (T_1)
- Diagnostic Test Interval (T_2)
- Number of dangerous cycles which is taken from EN ISO 13849-1 (B_{10d})

Let us now suppose that our safety gate monitoring corresponds to the requirements stipulated by SIL2, which is included in the overview of significant risk assessment documents (Table 2).

Table 2. Architectural constraints on subsystems: the maximum SIL that can be claimed for the safety- related control function using this subsystem (standard IEC 62061).

Safe Failure Fraction (*SFF*)	Hardware Fault Tolerance (*HFT*) (see Note 1)		
	0	1	2
< 60%	Not allowed	SIL1	SIL2
60% … < 90%	SIL1	SIL2	SIL3
90% … <99%	SIL2	SIL3	SIL 3 (see Note 2)
≥ 99%	SIL3	SIL3 (see Note 2)	SIL 3 (see Note 2)

Note 1 A hardware fault tolerance of *N* means that *N*+1 faults could cause a loss of the safety-related control function.
Note 2 A SIL 4 claim limit is not considered in this standard. For SIL 4 see IEC 61508-1.
Note 3 Exception, see 6.7.7 in IEC 62061.

We intend to build a system respecting the provisions of the SIL2, and there are three possibilities of how to satisfy the given specifications. The first option is that we will structure a system comprising a triple channel (*HFT* = 2); in these circumstances, the Safe Failure Fraction rate can equal 60% or less. The second and most common alternative involves a dual channel (*HFT* = 1), where the reliability indicator ranges between 60 and 90% of the SFF. Finally, the last choice consists in a single channel (*HFT* = 0); here, however, it is necessary to reach more than 90% of the *SFF*.

Which of these ways, then, is the easiest one? In response, we could definitely point to the first approach, yet such a solution would not be economical. For machinery safety, only a very limited number of components are connectable via the triple channel in the sensors part, and there is no safety module for the triple channel device; thus, the only method to resolve the problem is to use some type of the safety PLC, which can be adjusted by software. But the modification via software is no simple step either, because the prepared and certified blocks for the evaluation of safety functions are "only" dual channel. The last option (a single channel and *SFF* rate of 90 - 99%) cannot bring the desired benefit, as it simply requires too much diagnostics, thus necessitating the use of difficult systems to detect serious failures. The most advantageous and easy-to-connect procedure will be the middle option, namely a dual channel with a relatively low *SFF* indicator.

Another step is to determine the architecture of entire subsystems. Our safety function consists of three subsystems: an electro-mechanical safety switch; a safety module evaluating signals from the sensor; and a pair of safety contactors controlling the power supply to the motor performing dangerous movements of the machine. Because we have *HFT* = 1, we will use the dual channel configuration. This brings us to the architectures of subsystems C or D; the difference between these two types lies in the Common Cause Failure rate (*CCF*). As it is essential to have a Common Cause Failure in both the electro-mechanical switch and the safety contactors, we need to use type D architecture. The *CCF* is well described in annex F of the IEC 62061 standard. To obtain positive evaluation, we have to adopt some measures to lower the *CCF* indicator. For every single measure, we will receive points to be summarized, and Tab. F.2 of the IEC 62061 standard contains the "beta factor" which will be needed later for our calculations. Even though it is necessary to admit that more fulfilled measures produce more points and a better beta-factor, we also have to note that such conditions result in increased expenditure on the project. Our previous experience nevertheless shows that a score of between 70 and 80 points is reachable with rather small investment and that the beta factor of 2% is low enough to fundamentally influence the PFH_D value at the final stage.

We have to calculate the failure rate for the electromechanical switch and also for the contactors according to formula D.1 from the IEC 62061 standard:

$$\lambda_D = (1-\beta)^2 \cdot \left(\frac{(\lambda_{D1} \cdot \lambda_{D2} \cdot (DC_1 + DC_1)) \cdot T_2}{2} + \frac{(\lambda_{D1} \cdot \lambda_{D2} \cdot (2 - DC_1 - DC_1)) \cdot T_1}{2}\right) + \beta \cdot \left(\frac{\lambda_{D1} + \lambda_{D2}}{2}\right) \quad (1)$$

Further, we will calculate the failure rate of dangerous failures, namely

$$PFH_D = \lambda_D \cdot HFT \cdot h \quad (2)$$

to finally obtain the PFH_D.

These calculations have to be performed for all elements of the inputs and outputs.

If we use the safety electromechanical switch which exhibits B_{10D} 10^6 cycles and the testing interval of 50 ms, the *SFF* rate will be 85%; we will thus obtain $PFH_{Dinputs} = 1.5 \cdot 10^{-7}$.

We will use two contactors, each exhibiting B_{10D} $2 \cdot 10^7$ cycles and the testing interval of 50 ms; the *SFF* indicator will then equal 85%, too. In this manner, we have $PFH_{Doutputs} = 6.2 \cdot 10^{-9}$.

For the safety module, the procedure is simple: we will follow the manufacturer data sheet, which informs us that in SIL 3 we obtain the formula expressed below $PFH_{Doutputs} = 1.2 \cdot 10^{-8}$.

Now, we can define the $PFH_{DSafetyRelay}$ for the complete safety function. According to article 6.6.3.2.3 of the IEC 62061 standard, the complete PFH_D will be calculated as the sum of all partial PFH_{Di} values. For our situation, the equation will be as follows:

$$PFH_{DSafetyRelay} = PFH_{Dinputs} + PFH_{Dlogic} + PFH_{Doutputs} \quad (3)$$

The complete result of the $PFH_{DSafetyRelay}$ is $1.682 \cdot 10^{-7}$. With this outcome, we will proceed to Tab. 3 to find out that our result corresponds to SIL 2.

Table 3. Safety integrity levels (IEC 62061).

Safety Integrity Level (SIL)	Probability of a dangerous Failure per Hour (PFH_D)
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

NOTE: Where the required safety integrity of a SRCF is less than SIL 1, the requirements of category B of ISO 13849-1 should be met as a minimum.

5.2. Solution using safety PLC

The major part of the evaluation will be identical with that outlined in the previous chapter. The inputs and contactors include all properties exhibited by the *CCF*, PFH_D, *SFF* and other parameters; the novel part to be introduced in this section is the logical element. This time, five subsystems are included: the inputs representing the electromechanical switch; the distributed safety inputs connected over EtherNet/IP; the safety CPU; the distributed safety outputs connected over EtherNet/IP, too; and safety contactors functioning as actuators.

The equation for the calculation will remain virtually unchanged; the only difference will consist in the overall $PFH_{DSafetyPLC}$, as indicated below:

$$PFH_{DSafetyPLC} = PFH_{Dinputs} + PFH_{DCPUinputs} + PFH_{DCPU} + PFH_{DCPUoutputs} + PFH_{Doutputs} \quad (4)$$

For the values of the inputs and outputs, we will use the data from the part describing the safety module, where the value $PFH_{Dinputs} = 1.5 \cdot 10^{-7}$ represents the safety electromechanical switch and $1.2 \cdot 10^{-8}$ relates to the redundant safety contactors. The distributed safety inputs (Allen Bradley – 1734-IB8S) exhibit $PFH_{DCPUinputs} = 5.1 \cdot 10^{-10}$, and the distributed safety outputs (Allen Bradley 1734-OB8S) are expressed as $PFH_{DCPUoutputs} = 5.14 \cdot 10^{-10}$. The safety CPU (Allen Bradley 1756-L71S) then has $PFH_{DCPU} = 1.2 \cdot 10^{-9}$. We can thus see that the overall $PFH_{DSafetyPLC}$ equals $1.63224 \cdot 10^{-7}$.

In view of the preceding facts, it is possible to claim that using the safety PLC is more reliable than applying the safety module. To substantiate this statement, we can introduce the following description:

The EtherNet/IP with the CIP Safety protocol is certified up to the SIL3, which represents the values of $PFH_D = 10^{-8}$ and lower. Thanks to the CRC and the other measures specified above, the probability of residual errors in the network oscillates between the values 10^{-19} and 10^{-20}. In this context, the PFH_D value will then be approximately $9 \cdot 10^{-13}$, this being a number we can neglect in calculations even for the SIL3.

5.3. Comparison of simple architectures

In the chapters above, we made simple calculations of an architecture based on safety modules and a safety PLC with distributed inputs and outputs. When considering only the PFH_D value, we can highlight the safety PLC as a slightly better solution.

5.4. Advantages of safety modules

In the safety domain, the time response exhibits a critical value. The typical response time of safety modules is approximately 10 ms. Compared to this, the safety PLC displays a significantly higher value because a simple safety program exhibits a scan time of about 25 ms; however, we also have to account for the reaction time of the inputs, (which equals 16.2 ms in our case) and the reaction time of the outputs (6.2 ms). The last value relates to the

Ethernet network. We have thus described a simple solution with no Ethernet switch or devices such as drives or the HMI; even though the expectable latency of the network oscillates around 3 ms, this value is subject to further growth proportional to the traffic increase within the network. The reaction time of the proposed simple solution reaches approximately 50 ms, and this is still a very low number. Controlling fast actions, such as those performed by the clutch-brake valve on an eccentric press, requires a very long time; therefore, the period necessary for fast action control is up to 5 ms.

5.5. Advantages of safety PLCs.

Connecting more safety modules together is not a difficult task when the logical function AND is available between the particular modules and the safe state of the machine. With a more complex function for the safety modules (OR) and wherever more demanding logical linkage between such modules is needed, the number of output contacts begins to grow dramatically. As this number expands, the PFH_D increases as well. However, the count of contacts may become so high that, for the same safety function with the same hardware but more contacts at the output side, degradation of the PFH_D will occur (such as the demotion from the SIL2 to the SIL1). Furthermore, we have to consider that the response times can grow too. With the safety PLC, the situation is nevertheless very simple: all the safety inputs and outputs are wired, and the logical function will be defined in the control safety software. There will remain the same PFH_D, and the time response increase will be neglectable.

Conclusion

This paper describes the Common Industrial Protocol, a technique used in many types of networks, including EtherNet/IP or DeviceNet. The Common Industrial Protocol Safety is presented in detail with a particular focus on its principles and applications, and a simple example of the safety problem is analyzed. The proposed solutions comprise the classical wired approach and the method employing CIP Safety integrated in Ethernet/IP. The result obtained from the comparison of both solutions is as follows: The differences in the base safety function between the solutions remain very small (if we compare $PFH_{DSafetyRelay} = 1.682\cdot10^{-7}$ and $PFH_{DSafetyPLC} = 1.63224\cdot10^{-7}$, we obtain the difference of only $4.98\cdot10^{-9}$), but the procedure using CIP Safety brings more additional features, for example the advantage of safety module diagnostics. The situation nevertheless changes if we need to apply complex functions (such as OR). The classical solution requires more safety input/output contacts, and the parameter PFH_D increases more than with Safety PLCs.

Acknowledgements

The completion of this paper was made possible by grant No. FEKT-S-14-2429 - "The research of new control methods, measurement procedures and intelligent instruments in automation", and the related financial assistance was provided from the internal science fund of Brno University of Technology. This work was realized in CEITEC - Central European Institute of Technology with research infrastructure supported by the project CZ.1.05/1.1.00/02.0068 financed from European Regional Development Fund.

References

[1] D.A. Vasko, A. Kucharski, CIP Safety on Ethernet/IP, CIP Networks Conference & 11th Annual Meeting, Phoenix, Arizona, 2006.

[2] V. Schiffer, D.J. Vangompel, R. Voss, The Common Industrial Protocol (CIP™) and the Family of CIP Networks. Milwaukee, Wisconsin, USA, ODVA, 2006.

[3] The CIP Networks Library: Volume 5 - CIP Safety. Milwaukee, Wisconsin, USA, ODVA, 2013.

[4] D.-S. Kim, S. Lee, Feasibility analysis of hybrid control networks based on common industrial protocol. Computer standards&Interfaces. Vol. 33 (2011), Issue 4, ISSN 0920-5489, pp. 357-366.

[5] P. Blecha, R. Blecha, F. Bradáč, System approach to risk assessment in safety assurance of machinery with regard to directive 2006/42/EC, Annals of DAAAM for 2009 & Proceedings of the 20th International DAAAM Symposium, Vienna, Austria, ISSN 1726-9679, ISBN 978-3-901509-70-4, pp. 0159-0160.

[6] G. Enstad, J. Ralston, Applying wireless to EtherNet/IP pipeline automation, Pipeline and Gas Journal, Vol. 238 (2011), Issue 2, ISSN: 0032-0188, pp. 48-51.

[7] R.S.H. Piggin, Developments in real‐time control with EtherNet/IP, Assembly Automation, Vol. 27 (2007), Issue 2, ISSN: 0144-5154, pp. 109-117.

[8] L. Teschler, Safe and sync’ed up, Machine Design, Vol. 76 (2004), Issue 15, ISSN 0024-9114, pp 68-72.