APPLICATION OF CIP SAFETY PROTOCOL BETWEEN DOUBLE HYDRAULIC PRESS MACHINE AND INDUSTRIAL ROBOT

Radek Štohl, Karel Stibor & Soňa Šedivá

This Publication has to be referred as: Stohl, R[adek]; Stibor, K[arel] & Sediva, S[ona] (2018). Application of CIP Safety Protocol Between Double Hydraulic Press Machine and Industrial Robot, Proceedings of the 29th DAAAM International Symposium, pp.0378-0383, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-20-4, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/29th.daaam.proceedings.054

Abstract

The paper describes a hardwired solution and compares it with the approach based on a current trend in automation, namely, communication control over the Ethernet or via the CIP-Safety protocol, in which all the machines involved can communicate very effectively. The Ethernet can be used to transfer safety information even for the highest safety integrity level, and it also points out that network is not a critical factor in designing safety functions. Further, the paper contains calculation of failure probability per hour for the communicated data, which can be taken into account when users design distributed safety functions. Such a procedure is capable of satisfying not only the hardware reliability requirements but also the demands of end users, who seek to achieve a productivity rate as high as possible.

Keywords: CIP safety; performance level; SIL; ethernet

1. Introduction

The construction of a machine [8] is a major process within the industrial market because machines constitute a central precondition for the general operability of industry. Subsequently, electricity was introduced, rendering machines more accessible, cheaper, and easier to use. Company owners gradually started to realize that safety [2] is important, but they viewed the problem especially from the financial perspective: If a skilled worker was injured, he could not operate the machine, and a substitute usually turned out to be incapable of securing optimal production. The machine, despite consisting of various parts, is safe as a unit; however, if several such units are purchased by a major customer to establish a production line, the client, having joined together multiple machines to form a line, has created one large production machine out of particular units. A mid-size machine is usually equipped with a safety system, interpretable as a set of relays as proposed above; such relays are connected into one CPU, and, as a rule, the safety device offers the possibility of simple programming, with simple logic like AND, OR, timers, and similar components. However, another device, a PLC, is needed to control the non-safety part of the machine. Where two smart devices are involved, then, to enable the best performance, we have to ensure communication between the safety and the PLC systems; ideally, in this context, the information from the safety system is visualized on the operator's screen. This approach too constitutes a very popular, cost-effective solution surpassing the above-indicated method in flexibility.

Real machines, of course, are also completed with other safety capacities, including the prevention of unattended startup or the safe-off function, which, in our case, are materialized via other equipment, such as an overdimensioned lockable main switch. We will concentrate especially on the electrical and electronics-based solution. We can find in a similar way in [1], [6] or [7].

2. CIP-Safety protocol

CIP Safety [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. This protocol [3] 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.

When safety had become a major aspect for machine users and operators, it was to be soon followed by the distributed solution of safety [6]. 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 the EN) 61508. Among the outcomes of the work performed by this committee is also the CIP Safety published by the ODVA on the basis of the CIP.

3. AS-Interface - Safety at Work

The AS-Interface system [8] will be applied mainly at the lowest level of a multi-level automation hierarchy. AS-Interface concentrates on the typical requirements for connecting binary elements with a controlling device. Thus, AS-Interface meets the requirements in machinery and plant construction, where real-time processing, cost effective design, installation, operating, maintenance, and service are essential. To connect this variety of actuators, sensors, or other devices and elements with a controlling device, the AS-Interface is embedded in a structure of two different units, which present three interfaces as shown in Fig. 1.

Fig. 1. Interfaces of AS-Interface [8]

The combined transaction for safe signal transfer mechanism (Safety at Work) is handled according to the specification given below. It uses the standard AS-Interface data transfer mechanisms to build a single bit or two bit (depending on required safety category) safe information channel between safety slaves with the profiles given in slave profiles S-0.B and S-7.B, and a safety control unit.

Safe signal transfer and standard data transfer may be handled on the same network. The safe signal transfer uses a method similar to the one described in EN 50159-1. The safety relevant information consists of one or two bits per slave only (e.g. the output of a safety light barrier, the contact of an emergency stop device). A coding unit is placed between the sensor and the transmission system, which transforms the net information into a sequence of 8 sets of 4 bits of information ("dynamic coding"). On the receiver side a safety control unit built according to DIN V VDE 0801, AK5 interprets the signal. It compares the received codes with internally stored reference codes and from this can derive the state of the slave and of the transmission system. The safety control unit may be a part of the master; alternatively it may be a separate device, called "Safety monitor".

3.1. Safety input slaves

If a safety input slave [8] has two switching states, these states directly control the 4 bits of information transferred from the slave to the master. If the input of the slave is in "ON"-state (e.g. the light path of a safety light curtain is free, a safety door is closed) this state is signalled by transmitting a sequence of 8 sets of 4 bits of information. Every AS-Interface cycles transfers the next set of 4 bits of information. If 8 cycles have been transmitted the complete sequence has been sent. In the 9th cycle the first set is transferred again. If the input of the slave is in "OFF"-state the information "0_{Hex}" is sent. If a safety input slave has two inputs (e.g. redundant contacts) each of the two contacts act independently of each other on two bits (half nibble) of the 4 bits (nibble) of information. The following table shows the 4 possible states of the inputs (see Table 1).

Contact 1	Contact 2	Data D0..D3	Meaning
ON	ON	X X X X	Input in "ON"-state
ON	OFF	X X 0 0	Input in "OFF"-state, only one contact is open
OFF	ON	0 0 X X	Input in "OFF"-state, only one contact is open
OFF	OFF	0 0 0 0	Input in "OFF"-state, both contacts open

Table 1. Table example [8]

3.2. Coding rules

The data bits D0...D3 in the slave answer form a code nibble. 8 code nibbles form a code sequence. Rules for the assembly of a code sequence:

- S1: A sequence consists of eight 4-bit-values where each code nibble is different from each other.
- S2: The values 0000Bin and 1111Bin do not exist within a sequence
- S3: Exactly one value of 0001Bin, 0010Bin or 0011Bin exists in a sequence.
- S4: Exactly one value of 0100Bin, 1000Bin or 1100Bin exists in a sequence.
- S5: Between two values with only 1 bit set are at least 2 values with two or three bits set.
- S6: The value 0000Bin indicates the OFF-state of the sensor.
- S7: The value 1111Bin is reserved for future extensions.
- S8: The stepping of the sequence is delayed by 200 - 900µs after a data-request.

Within an AS-Interface network only different code-sequences are allowed. Following these rules more than 900000 different code-sequences are available. For maximum mixture of the code-sequences on the market, they will be distributed under the control of the AS-International Association. The correctness of the code sequence (nibbles and half nibbles) shall be supervised by the safety control unit. For half nibbles sequence it is mandatory to check for exactly one "00" in the eight value sequence only (Fig. 2).

Fig. 2. State diagram half nibble evaluation [8]

4. Practical Example: a Double Hydraulic Press Machine and Industrial Robot

We will now consider the type C standard EN 693 Machine tools – Safety – Hydraulic presses, as amended (annex 2) in 2012 and standard EN ISO 10218-2 Robots and robotic devices – Safety requirements for industrial robots – Part 2: Robot systems and integration. The documents constitute the most concrete standard existing in machinery safety; interestingly, the fourth chapter of every type C standard comprises a list of typical hazards. A situation scheme is presented in Fig. 3.

Fig. 3. Double Hydraulic Press Machine and Industrial Robot

5. Safety functions

After the safety-related specifications and description of the safety functions have been created for the real machine [4], [5], we can start evaluating the safety functions; however, it is also necessary to create at least a part of the documentation, including the specific cycle time. To possess the latest data, we have to consider the last version of the EN ISO 13849-1 in its third edition of December 2015. For each safety function, we have the same safety function diagram, consisting of one safety input subsystem, one logic subsystem, and one output subsystem.

We identified [6] the mechanical hazards of crushing, shearing, cutting, entanglement, drawing in or trapping, ejection, high pressure fluid ejection, slip, trip, and fall. Further risks then comprised electrical hazards (defined as direct contact and indirect contact), thermal hazards resulting in burns and scalds caused by contact with hot surfaces, noise hazard, and hazards generated by materials and substances in conjunction with the hydraulic system of the press. The remaining safety functions will be solved and put to practice via safety hardware, using the second step of the three-step method to mitigate the probability of risk on the machine. The risk analysis ought to comply with the requirements Performance Level d.

We defined the safety functions as follows:

- The **Emergency stop** safety function is, on the input part, executed via an E-Stop button respecting the EN ISO 13850 standard, which, among other aspects, defines the construction and placing. We use a dual channel connection satisfying the requirements of category 3 connection.
- **Light curtain**: As regards this element, will use the following version: type 4; resolution of 14 mm; protective field of 1800 mm.
- **The prevention of gravity fall** will be ensured by an electromagnetic lock with a one-way travel mechanism. The press can travel upwards, but without an energizing electromagnetic element it cannot travel downwards in any situation.
- **Position sensing** will be secured by the same safety non-contact switches as in the case of the prevention of gravity fall. The safety position of the press is significant due to switching between the movement-regulating valves.

Fig. 4. Logical schemes of our system

5.1. Discrete Solution based on Safety Relays and Safety at Work

The method using older version safety configuration – discrete safety input components connected via AS-Interface safety slaves to cascade designed the AS-I Safety monitors as the safety relays (Fig. 4 part a). The response time of 40 ms is typically for the AS-Interface network with the safety monitor. If we apply this solution on our system, we get the results shown in Table 2.

5.2. Safety Integrated System

Now let us employ the safety integrated system in our set of machinery. One such system ensures the safety of all the machines concerned, and all the corresponding components are connected over a classic Ethernet network. The Ethernet network then facilitates the data exchange between the safety components; this step is made possible via implementing the Ethernet/IP protocol with CIP Safety features inside systems such as GuardLogix (see Table 3).

The Ethernet/IP with CIP Safety is a protocol developed by the independent organization ODVA [3]. The protocol is defined as connected and/or unconnected, and it runs the classic OSI-ISO model, devices lacking an inside driver simply do not understand. The Ethernet/IP enables us to eliminate the need of special equipment such as particular switches. On the network part of the application, the diagnostics are not necessary, because this section only serves to transport information. The second part of the device consists in a distributed input or output or another CPU. Here, the information is checked for consistency, and it is decided if the given data have passed the reliability test.

	E-Stop	Safety gate	Light curtain
Category	3	3	4
$MTTF_d$	100 years	100 years	100 years
DC	86.59%	86.59%	99 %
Reaction time (ms)	230	275	300
PL	d	d	e
Cost (€)	1042	1270	1730

Table 2. The complete data for Safety at Work and Safety Relay within discrete outputs

	E-Stop	Safety gate	Light curtain
Category	3	3	4
$MTTF_d$	100 years	100 years	100 years
DC	86.59%	86.59%	99 %
Reaction time (ms)	225	280	285
PL	d	d	e
Cost (€)	1050	1570	2170

Table 3. The complete data for the integrated safety system

6. Conclusion

In terms of the analyzed problem between two solutions - via Safety at Work, and CIP Safety; an interesting task consists in comparing the cost of the discussed approaches. The comparison proposed below assumes only the safety portion of a machine, and the prices are based on relevant price lists. Comparing the solutions discussed herein, namely, the safety relays with safety inputs via simple communication (AS-Interface network) and the total control systems, we can point out that the values are improved partially in standard safety functions and significantly as regards the communication with other machines. End users will be capable in such more complex situations; safety communication constitutes a very useful tool. The volume of the hardware needed and the number of wires required will be substantially reduced and programming the cascade connecting safety monitors will not be complicated too. Based on evaluating the discussed approaches, we can claim that applying an integrated system improves the safety and helps end users to reduce their maintenance-related costs.

7. Acknowledgments

The authors acknowledge financial support from the Ministry of Education, Youth and Sports under projects No. LO1210 - "Energy for Sustainable Development (EN-PUR) " solved in the Centre for Research and Utilization of Renewable Energy. The completion of this paper was made possible by the grant No. FEKT-S-17-4234 - "Industry 4.0 in automation and cybernetics" supported by the Internal science fund of Brno University of Technology.

8. References

- [1] R. Štohl, K. Stibor. (2014). The Common Industrial Protocol in Machine Safety, Annals of DAAAM for 2014 & Proceedings of the 25th International DAAAM Symposium, Vienna, Austria, ISSN: 1877-7058, pp. 773-781.
- [2] P. Blecha, R. Blecha, F. Bradáč. (2009). 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.
- [3] V. Schiffer, D.J. Vangompel, R. Voss. (2006). The Common Industrial Protocol (CIP™) and the Family of CIP Networks. Milwaukee, Wisconsin, USA, ODVA.
- [4] Rockwell Automation. (2011). Safebook 4. Principles of Machine Safety – Legislation, Theory and Practice. SAFEBK-RM002B-EN-P. Rockwell Automation, Inc. Milwaukee, USA.
- [5] Rockwell Automation. (2016). Machinery Safetybook 5. Safety related control systems for machinery. Principles, standards and implementation (Revision 5 of the Safebook series). SAFEBK-RM002C-EN-P. Rockwell Automation, Inc. Milwaukee, USA.
- [6] R. Štohl, K. Stibor. (2016). Cascading safety relays compared to using a network solution. In Proceedings of the 2016 17th International Carpathian Control Conference, ICCC 2016. Tatranska Lomnica: Institute of Electrical and Electronics Engineers Inc., ISBN: 978-1-4673-8606- 7, pp. 729-734.
- [7] R. Štohl, K. Stibor. (2017). The CIP Safety Protocol in Connecting Single Machines to Create Production Lines. In 2017 18th International Carpathian Control Conference (ICCC). Romania: Institute of Electrical and Electronics Engineers Inc., ISBN: 978-1-5090-4863-2, pp. 512-516.
- [8] AS-International Association. (2015). Actuator Sensor Interface (AS-Interface®) - Complete Specification, Version 3.0, Revision 6. AS-International Association. Gelnhausen. Germany.