Make CIP Safety Your Safety Protocol

Lechler, Schlechtendahl, Leurs, Verl

Institute for Control Engineering of Machine Tools and Manufacturing Units
(ISW) University Stuttgart
and
Bosch Rexroth

Presented at the ODVA
2012 ODVA Industry Conference & 15th Annual Meeting
October 16-18, 2012
Stone Mountain, Georgia, USA

Abstract

The use of fieldbuses in automation systems instead of hard wired interaction between components provides a number of well-known advantages like lower costs, more flexibility, new functionalities and higher dynamics. For interactions which are needed to fulfill safety requirements, hard-wired connections are still being used in parallel to the fieldbus wire. In order to reap the aforementioned advantages for the case of safety connections, a safety protocol needs to be integrated into the fieldbus communication layers. The inherent failure rate of fieldbus protocols is generally much higher than that allowed in international standards for safety applications. This paper will focus on the steps that are required to adapt the safety protocol CIP Safety™ to a non-CIP fieldbus. It will explain in detail which steps with respect to specification, TÜV involvement, and conformance testing software modification have to be taken to make CIP Safety the safety protocol of a fieldbus. This paper will use the example of the successful CIP Safety integration on top of the existing sercos III communication layer.

Keywords

certification, CIP Safety, sercos

1 Introduction

Optimized exchange of information in automation systems requires a network that allows communicating in real-time, in non-real-time and that includes safe data. sercos III, as an Ethernet-based fieldbus, provides the communication in real-time and non-real-time. Ethernet in general, including sercos III, has a theoretical failure rate of 10^{-3} [1], but SIL 3 [2] requirement for communication of safe data is a guaranteed failure rate of 10^{-7} or better. Therefore, a special safety protocol has to be used to reduce the failure rate. This safety protocol uses mechanisms like check sums, time stamp, redundancy and more to reach the given failure rates. For the calculation of the maximum failure rate, the underlying communication layer (sercos III for example) is called “black channel”. This black channel must not influence the safety telegrams; it only serves as a transport medium.

CIP Safety, as a 7 OSI layer protocol (application layer) [3], is a perfect choice when one must select a safety protocol to extend a lower layer fieldbus for the safety functionality. CIP Safety has been adapted in the past to be used with industrial networks like EtherNet/IP™ and DeviceNet™.

This paper describes how CIP Safety can be adapted to other networks shown by the experience in adapting CIP Safety to sercos. Section 2 shows the necessary modifications regarding the technology and specification. Issues to be considered on CIP Safety and on the fieldbus side are discussed. Section 3 will focus on how TÜV has to be involved in the whole adaptation process. The last section (section 4) will address how the conformance test software for CIP Safety can be connected to already existing conformance test tools of the fieldbus and what changes have to be made to the software.

2 Technology and Specification Work

Using CIP Safety as a safety protocol in non-CIP based networks first includes the choice of an appropriate transport protocol for the safety messages in the underlying network. As sercos is very much focused on real time control loops, the highest priority has been given to these messages in order to guarantee the functionality under any circumstances. Consequently, safety messages are transported using this highest priority scheme inside the sercos RT-channel and thus guaranteed short cycle times inherent to fixed size transport containers are achieved. This sercos III transport protocol is called "Sercos Messaging Protocol" (SMP). Further, an adaptation layer to CIP Safety has to be provided by the non-CIP based fieldbus to implement a basic set of CIP services and objects. The functionality provided by the adaptation layer is described in a sercos "Safety Profile". Subsequent sections describe the structure of Figure 1 from the bottom to the top.

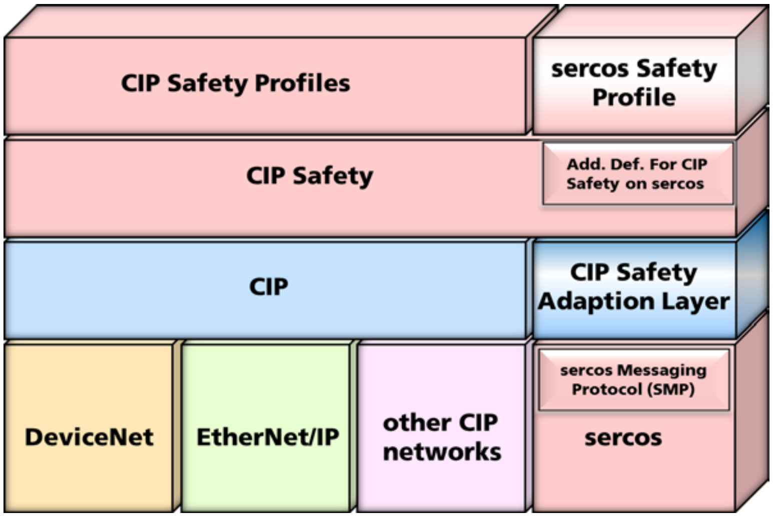

Figure 1: Layer model for CIP Safety on sercos [4]

2.1 Sercos: Transport Layer (Sercos Messaging Protocol)

With sercos communication, the hard real time feature is implemented in the data link layer. Statically configured parameters (IDNs) are cyclically transferred between the various sercos devices on the network. Additional parameters can only be transmitted between the Master and a Slave using the acyclic service channel. The straightforward design for hard realtime, high precision synchronization with minimal jitter and high band width prevents sercos from supporting the following features (comp. [4]):

- A complete application-controlled transmission independent of the time slots of the safety layer
- Flexible multiplexing and fragmentation of data for a better exploitation of the bandwidth available
- Transfer of cyclic messages of variable length

SMP provides a session-based interface which allows for two or more sercos devices to exchange messages of variable length. The exchange takes place without the restrictions listed above. Figure 2 shows how SMP is integrated into the layer model.

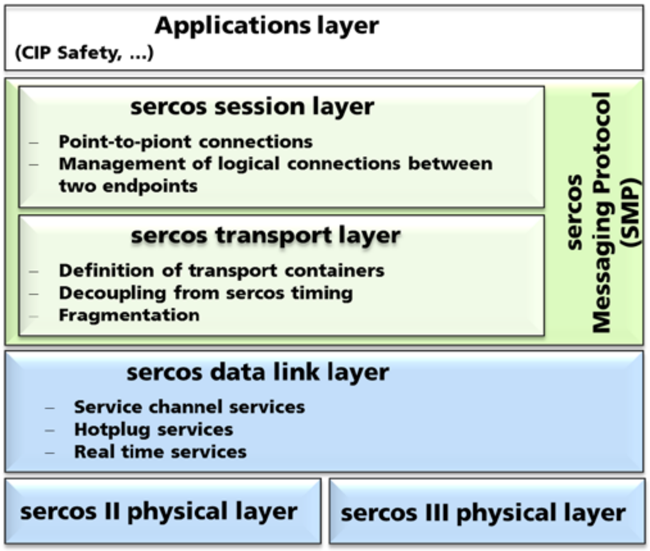
Applications layer
(CIP Safety, ...)
sercos session layer
– Point-to-piont connections
– Management of logical connections between two endpoints
sercos transport layer
– Definition of transport containers
– Decoupling from sercos timing
– Fragmentation
sercos Messaging Protocol (SMP)
sercos data link layer
– Service channel services
– Hotplug services
– Real time services
sercos II physical layer
sercos III physical layer

Figure 2: SMP in layer model [4]

The sercos session layer represents the interface between SMP and the application layer. A session is equivalent to a logical, unidirectional channel between a producer and one or more consumer(s) of a connection. This will be clearly defined by the 8-Bit Session Identifier (SID).

The sercos transport layer provides receive and transmit buffers in order to decouple the higher layers from the sercos cycle. In addition, the transport layer defines SMP containers which can be configured in cyclic real-time data connections. These containers are used for the transmission of safety messages. Enabling the sercos Messaging Protocol requires the configuration of the SMP containers in communication phase 2 (CP2) due to the a priori deterministic approach. This is a restriction of the SMP because when the SMP is in the operating level CP4, safety messages can only be exchanged between devices for which a connection with a transport container has been configured during CP2. Configuration of connections in CP4 is not possible.

The size of the SMP (transport) container can be between 4 and 258 bytes. The first two bytes of the SMP container are used for the Session Control Header. The remaining bytes can be used to transfer – depending on the configured length – up to 256 bytes of user data per sercos cycle. The design of a SMP container is shown in Figure 3.

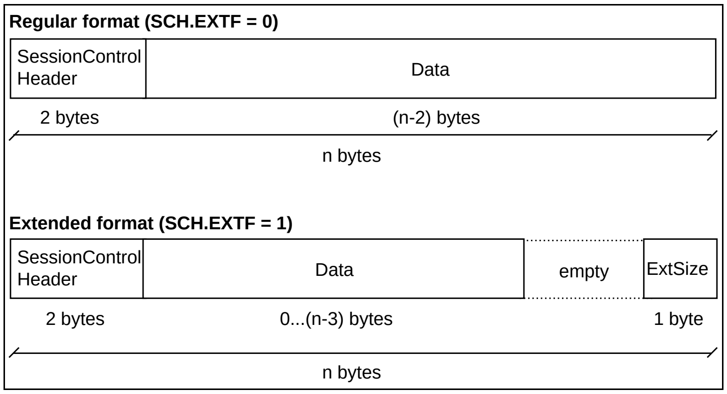

Figure 3: SMP Container [4]

If not enough user data is available to fill the container completely (Figure 3 bottom), the length of the user data is recorded in the last byte of the container. In addition, the flag EXTF is placed in the Session Control Header. The Session Control Header contains information about

- the session ID of the data fragment
- fragmentation information
- priority of the data fragment
- mechanisms for securing the data transfer

2.2 Sercos: Safety Profile (adaptation layer)

Sercos is not based on the Common Industrial Protocol (CIP). Therefore, the adoption of CIP Safety as a safety layer for sercos devices raises the need for an adaptation layer that implements a basic set of CIP objects and services. It is important to mention that the adaptation layer is not part of the safety protocol itself and can be considered as a part of the black channel. The required integrity level is lower than the one necessary for safety.

Figure 4 shows the CIP Safety adaptation layer (CSAL) which makes CIP Safety messages exchangeable between the application layer and the SMP. In the CSAL the objects specific for CIP Safety are received and assigned to the SMP sessions. For the configuration and the establishment of secure connections between CIP Safety devices, objects' acyclical data is exchanged via the CSAL. The assignment of SMP sessions for the cyclical communication for exchanging objects' data including secure process data is also carried out by means of the CSAL.

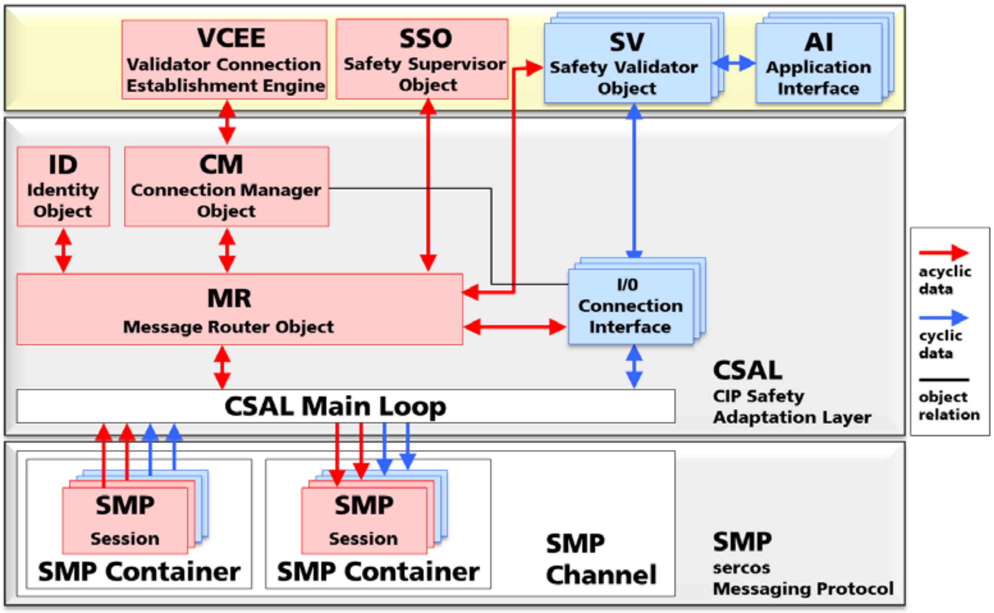

Figure 4: CIP Safety adaption layer [4]

2.3 Specification Adaptation and Review

The technical extensions to use CIP Safety on sercos III need additions in the sercos III specification (SMP, CSAL). Changes to the CIP Safety specification include only:

- Reference to sercos III as communication protocol for CIP Safety
- Methods generating the Unique Node Identifier" (UNID) that consists out of the Safety Network Number (SNN) and the MACID to device identification
- Selection of relevant test cases from Volume 5 (CIP Safety specification) Appendix F

A protocol conformance test specification (PCTS) exists for every fieldbus and technology supported by ODVA including the CIP Safety protocol. The document "CIP Conformance Test Specification: CIP Safety Adaptation" (PUB00170) describes in detail the test cases that have to be executed for the conformance testing of a CIP Safety device. The document includes the test cases described in the CIP Safety specification in Volume 5, Appendix F.

The changes are made in agreement with the ODVA, and they have to be included in the specification according to the Specification Enhancement review process.

3 Concept Validation

In order to validate the CIP Safety on sercos concept, the modified CIP Safety specification including the sercos changes relevant to the safety protocol have to be certified by the TÜV. As part of the certification, TÜV inspects the descriptions of the test cases under which a CIP Safety device is conformance tested. Since CIP Safety is already certified by the TÜV only the sercos-specific extensions have to be approved. For example, there is no need to prove the complex calculation of the failure rates. In addition, the TÜV has to be presented a concept for the tests done in the certification process of the CIP Safety devices. The TÜV expects the certification of the black channel sercos III to be carried out according to the specification of Sercos International. Beyond that a technical facility has to be provided for carrying out the tests described in the specification.

4 Conformance Testing

4.1 Protocol Contformance Test Software (PCTS) structure

For the certification of sercos III the Institute for Control Engineering of Machine Tools and Manufacturing Units (ISW) at the University of Stuttgart developed the PCTS sercos III conformizer. The ODVA already provides a PCTS for CIP Safety on DeviceNet and EtherNet/IP approved by the TÜV. The aim of using unmodified testcases already accepted by TÜV can be achieved by adapting the existing PCTS for CIP Safety onto the sercos transport layer formed by the adapted sercos III PCTS. This solution is accepted by the TÜV if it can be guaranteed that the sercos III conformizer does not affect the safety messages.

The certification tool for CIP Safety consists basically of a user program with a user interface. The configuration of the unsafe and safe communication is carried out by means of the user interface. This enables the required test cases to be selected and started according to the specifications of Volume 5 Appendix F. Most test cases are not contained directly in the user program but mapped as scripts (script language Python). The user program calls them according to the test selection. Each CIP Safety message is transferred to the network stack and the response of the device under test is evaluated. A test report presents the results at the end of the certification process and serves as proof for the TÜV of the successful certification. The certification of CIP Safety devices may only be done by the ODVA itself or ODVA accredited test service providers (TSP).

The sercos III conformizer has a similar structure. The user program is realized as a plugin for the Eclipse framework. The test scripts are implemented in the script language Ruby. Based on the protocol structure of sercos III the telegrams of the sercos III conformizer are generated using hardware support. The communication between the user program and the Ruby scripts is achieved via a middleware (SOAP). For minimal implementation work and no further approval by the TÜV an appropriate interface between the two tools needs to be found.

4.2 Interface for CIP Safety on sercos certification tool

Figure 5 shows the basic architecture of CIP Safety on a sercos certification tool. In order to connect CIP Safety and sercos III certification tools, two interfaces have been implemented. One allows connecting the CIP Safety telegram from the Python test scripts via the CSAL to the sercos SMP sessions. The other interface enables communication between the CSAL and the user program. The user program had to be complemented by a few extensions like the sercos-specific addressing module. The enhanced part of CSAL also takes over the configuration of the sercos III network so that no changes in the user program will be necessary.

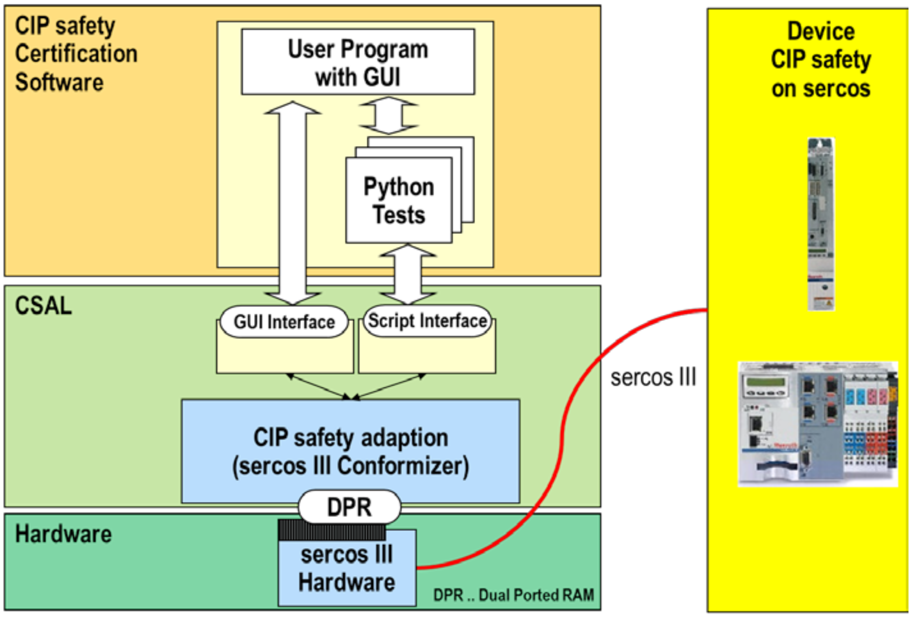

Figure 5: General Architecture of CIP Safety on sercos Certification Tool

5 Conclusion

Making CIP Safety your safety protocol only requires a high-performance communication protocol that allows transporting CIP Safety telegrams in data containers. To achieve this, an appropriate adaptation layer needs to be designed and taken into consideration in the individual technologies specifications. In addition, a concept for connecting existing certification solutions needs to be defined and realized. In cooperation of ODVA and sercos International, this has been successfully achieved including modification of the respective specifications as well as implementation of the necessary technologies.

References (optional):

[1] N.N: Typical Equipment MTBF Values, System Reliability Center, 2001

[2] N.N: IEC 61508, Functional safety of electrical/electronic /programmable electronic safety related systems, Beuth, Berlin, 2010.

[3] N.N.: ISO/IEC 7498-1, Information technology -- Open Systems Interconnection -- Basic Reference Model, Beuth Verlag, Berlin, 1994

[4] N.N.: Specification sercos III V1.1.2, Sercos International, 2012

****

The ideas, opinions, and recommendations expressed herein are intended to describe concepts of the author(s) for the possible use of CIP Networks and do not reflect the ideas, opinions, and recommendation of ODVA per se. Because CIP Networks may be applied in many diverse situations and in conjunction with products and systems from multiple vendors, the reader and those responsible for specifying CIP Networks must determine for themselves the suitability and the suitability of ideas, opinions, and recommendations expressed herein for intended use.