**Safety on every level**

Development of functionally safe communication between machines

*More networking, more safety, more freedom - these somewhat contradictory requirements also do not end at the most sensitive part of the machine network, the functionally safe communication. A task that is best handled together. PI (PROFIBUS & PROFINET International e.V.) and the OPC Foundation have now signed a Memorandum of Understanding to quickly start up a Joint Working Group to ensure that PROFIsafe will also function between controllers from different manufacturers in the future.*

Previously, functionally safe communication via a fieldbus or Industrial Ethernet was limited to purely Master-Slave or Controller-Device architectures. However, there is currently no cross-manufacturer standard for safe transfers between machines and thus between the controllers used in the machines. Therefore, controllers from different manufacturers cannot currently communicate with each other without additional action being taken.

In view of the increasing use of networking in companies, this situation is unsatisfactory. There are industries with a very heterogeneous automation landscape, such as the Food & Beverage industry, where controllers from different manufacturers must frequently be connected to one another in a functionally safe way. Nowadays, special couplers are required in this case, which is associated with high hardware and engineering costs. At the same time, the use of functionally safe devices has rapidly increased in the past few years. For example, the number of Profisafe nodes installed in the field will be considerably more than 8 million in 2017; with growth rates of approximately 30% per year. There is a growing need for controllers to now communicate with controllers via functionally safe communication.

Functionally safe communication between controllers is always needed when different machines must be safely coordinated with one another. This mostly occurs during interaction between processing machines and the incoming and outgoing transport units. Some typical examples are transfer lines, overhead monorail conveyors, or machine tools with their loading and unloading systems. Where we currently see special cables, couplers or even additional collision detection sensors installed for processing functionally safe signals, considerable overhead can be saved and more flexible concepts can be implemented in the future using safe communication via the existing network. Other application areas can be found in sluice and bridge applications, where the objects must be remotely monitored and safely controlled from a central control room. In this case, long distances must be bridged for the safety signals. Crane applications are also interesting, for example: In large industrial crane applications, several cranes are operated via a central control desk. The responsible person at the control desk must be capable of safely shutting down the respective crane at any time in a hazardous situation. There are also applications in which several "crane trolleys" must be coordinated in order to bear heavy loads. These applications are also safety-relevant and require a considerable exchange of data between the individual controllers.

**Technology – OPC UA as the basis**

Since OPC UA plays an increasingly important role for connections between the controllers, it is logical and sensible to expand the mechanisms from Profisafe to OPC UA as well. To this end, the cornerstone for a Joint Working Group of the OPC Foundation and PI was laid in mid-November, 2017.

The backdrop for this is: The Profisafe solution developed in the 1990s by PI (Profibus & Profinet International) allows functionally safe communication and the transfer of standard process data via the same connection. Due to the advantages connected with it, Profisafe became established on a broad front and is now the world market leader among functionally safe fieldbus protocols. But above all, the technology is stable and fully matured.

The new specification should also benefit from the proven Profisafe mechanisms: A single cable for standard communication and safety-oriented communication. And the proven Black Channel principle, which is popular among many developers because of its simplicity, will be the underlying principle again.

**The Black Channel principle has proven its worth**

The core of the Black Channel principle is to relocate all of the safety-oriented mechanisms in a separate protocol layer. This layer is capable of reliably detecting and correspondingly responding to all of the errors of the subordinate communication layers. This allows the required level of functional safety to be achieved without requiring any changes or even an analysis of the subordinate communication layers. The subordinate communication layers do not have to be considered even for certification. This has the added advantage that the approval for the functional safety remains valid when there is a change in the transfer technology (e.g. for improving performance or due to the use of security technologies).

The Black Channel principle can also be transferred to the controller-controller communication, where the OPC UA communication stack then takes over the role of the black channel. This means that this does not have to be considered during certification and can be adapted or expanded later on at any time. Only the correctness of the implementation of the Profisafe protocol on a functionally safe platform is relevant for certification.

**Resolving questions of detail together**

By retaining this proven principle, PI expects to make things considerably simpler for manufacturers who want to implement Profisafe on OPC UA in their controllers. This ensures a high degree of acceptance among manufacturers, end users and administrative bodies such as the certification centers. But: This will not function without additional work. Ultimately, the user should be able to rely on the fact that he is getting a solution that is easy to handle, sustainable, and compatible with his previous systems.

To name just some of the details that must be taken into consideration: Previously, asymmetrical protocols were used between the host and the device. Now this is shifting in the direction of a symmetrical protocol, because there are two hosts. This requires an adaptation of the state machines of the Profisafe protocol. Instead of the previous two state machines (one for the host, one for the device), there will only be a single machine in the future. When defining this state machine, it is clarified, for example, how a connection will be established, when process values or secure substitute values must be output, or how a restart is to be acknowledged. Some thought must be given to aspects of the configuration because the devices were previously configured via the host. Questions regarding the addressing or authentication must also be discussed. Another important aspect is the definition of the data types and data structures to be transferred and the reliable checking of whether both communication partners actually have the same understanding of how the transferred data are to be interpreted.

The new specification will address both the client/server and Pub/Sub communication models of OPC UA. Pub/Sub-TSN is also considered to ensure that even very short cycle times can be realized in the communication. Therefore, the Profisafe-over-OPC-UA specification to be newly developed will be based on the brand-new OPC-UA-Pub/Sub specification of OPC UA. Of course, the new specification must satisfy the safety requirements of IEC 61784-3 up to SIL 3. The goal is for the established mechanisms that are known by Profisafe, e.g. safety measures for detecting packet loss, data falsification, addressing errors or impermissible delays, to be imported largely without changes. These proven mechanisms are already known to the approval centers – such as TÜV – which is why an easy and quick certification of the protocol and, consequently, of the products can be expected.

**Outlook:**

In the founding phase of the Joint Working Group between the OPC Foundation and PI, as usual a charter (Call for Experts) will first be published, which calls for active collaboration for the specification: Interested collaborators are welcome! One advantage is: PI and the OPC Foundation are not just capable of developing and advancing technologies, they can also establish a testing system and training courses. In addition, there are manufacturer-independent test laboratories, directed by the organizations, where the devices and components can be checked for adhering to the specification to ensure the necessary interoperability. Prepared in this way, controllers and thus machines will be able to safely communicate with one another in the future on the basis of the new 'Profisafe over OPC UA' specification.

((poss. box)) **Proven collaboration**

It has already been shown in the Joint Working Group of the PI and OPC Foundation when an OPC UA Companion specification for PROFINET was created that the path established between PI and the OPC Foundation is the right one. A workgroup that concentrates on the detailed working out of concrete use cases started here in May, 2017. Topics such as asset management and diagnostics, which are found again in the PROFINET specification, are primarily of interest to users. The user now receives all of the information corresponding to a standardized structure in the OPC UA object tree via the mapping. This information can then be further processed in higher-level systems without any problems. Thanks to TCP/IP, the OPC UA access can take place via the controllers, gateways, or even directly to lower-level devices. Thus, starting out in OPC UA can be done flexibly and in stages. The goal of the activities is an OPC UA PROFINET Companion specification in Q2/2019. The device manufacturers can integrate the proven PROFINET services without any changes. The information can then be displayed as per the customer's requirements in the corresponding devices via OPC UA services according to the defined mapping.

**Graphics for illustration:**

Graphic 1: Current number of nodes



Graphic 2: Photo of Tom Burke and Karsten Schneider shaking hands at the SPS/IPC/Drives.

Graphic 3: Principle of operation of the black channel



Graphic 4: The missing block - Fail-safe machine-machine communication



Graphic 5: Reuse of existing PROFIsafe mechanisms for fail-safe controller/controller communication as a core OPC UA function

OPC UA

Pub/Sub

or
Client/Server

OPC UA

Pub/Sub

or
Client/Server

PROFIsafe

over

OPC UA

PROFIsafe

over

OPC UA

Safety application

Safety application

Standard application