atp magazin

SONDERDRUCK

Transforming Automation
Ausgabe 1-2/2023

Peer-Review: 30.11.2022

The Next Generation: Ethernet-APL for Safety Systems

Contribution for the NAMUR Annual General Meeting 2022

Karl-Heinz Niemann, Hochschule Hannover; Marc Risser, BASF SE

This paper reflects the content of the presentation "The Next Generation: Ethernet-APL for Safety Systems" at the NAMUR Annual General Meeting 2022. It deals with the use of the Ethernet Advanced Physical Layer (Ethernet-APL) in combination with the PROFINET/PROFIsafe protocol for safety applications. It describes the virtues of the digital communication between the field and safety system. In parallel the aspect of OT security for this use case is touched as well. The paper proposes a secure architecture, where safety- and non-safety field communications are still separated. At the end a set of requirements for the development of future APL devices is described.

#Safety #Ethernet-APL #PROFINET/PROFIsafe #Field communication #OT security

Die nächste Generation: Ethernet-APL für Sicherheitssysteme

Beitrag zur NAMUR-Jahreshauptversammlung 2022

Dieser Beitrag gibt den Inhalt des Vortrags „The Next Generation: Ethernet-APL for Safety Systems" auf der NAMUR-Hauptsitzung 2022 wieder. Er befasst sich mit der Nutzung des Ethernet Advanced Physical Layer (Ethernet-APL) in Kombination mit dem PROFINET/PROFIsafe-Protokoll für Sicherheitsanwendungen und beschreibt die Vorzüge der digitalen Kommunikation zwischen Feld und Sicherheitssystem. Parallel dazu wird auch der Aspekt der OT-Security für diesen Anwendungsfall behandelt. Der Beitrag schlägt eine sichere Architektur vor, bei der die sicherheitsgerichtete und die nicht sicherheitsgerichtete Feldkommunikation getrennt sind. Abschließend wird eine Reihe von Anforderungen für die Entwicklung zukünftiger APL-Geräte beschrieben.

#Safety #Ethernet-APL #PROFINET/PROFIsafe #Feldkommunikation #OT security

1. Communication in the field

This chapter gives an overview on the evolvement of the communication in the field for the process industry.

1.1 The evolvement of digital communication

Since decades the 4…20 mA current loop signal [1] was and still is the work horse in the process industry to connect field devices to the automation system. As the current loop signal is able to transmit the analog measurement signal only, the HART protocol [2] was developed in the eighties of the last century, to add digital communication to the current loop signal. Unfortunately, the access to the digital data often needs additional interface modules and data conversion [3] when transferring HART data via a remote IO to asset management applications.

For this reason, digital fieldbuses like PROFIBUS PA [4] and Foundation Fieldbus H1 [5] have been developed in order to close the analog gap between the sensor and the automation system. In an atp article dated in the year 2000 one of the authors of this paper wrote:

"The advance of intelligent field devices is opening up access to internal data of the field device. If the classic 4...20 mA interface could just signal the measured value and some fault messages, [...] today's fieldbus-based field devices offer a much wider range of diagnostic information […] like a variety of different views of their internal state, input and output states, diagnostic and maintenance information and on control behaviour. A crucial factor in the use of digital field devices is the way in which this information is made available to the user."[6]

Even though this statement, dated 22 years ago, is still valid today, the advantages of the digital communication in the field are undisputed, the use of digital sensor / actuator busses like PROFIBUS PA [4] or Foundation Fieldbus H1 [5] is not widespread. This applies for control systems, but especially for safety system. The reasons for this are manifold:

- The fieldbus technology is perceived as complex in comparison to the 4…20 mA current loop.
- The integration of the field devices via the integration technologies FDT [7, 8] and FDI [9, 10] requires the support by corresponding device integration modules like

Device Type Managers (DTMs) resp. FDI Packages as well as by the automation system.

» Remote IOs are required in addition to the digital field devices in order to collect data from simple binary sensors like limit switches.

» The parallel use of e.g., Ethernet, PROFIBUS DP and PROFIBUS PA requires personnel with skills in these areas.

The described issues explain to a certain extent, why the digital communication in the field is still behind and why the benefits of digital communication in the field are not leveraged.

1.2 Converged digital communication with Ethernet-APL

In the year 2021, the *Ethernet Advanced Physical Layer* (APL) was introduced to the market during the 2021 Achema Pulse Event. Ethernet-APL is based on the 2-wire Ethernet Standard IEEE 802.cg [11]. This standard provides a 10 Mbit/s full duplex data communication as well as power delivery via the two wires of the communication line. For the use in the process industry, e.g. the operation in a potentially explosive atmosphere and for the use in harsh environments, additional features have been defined in the Ethernet-APL port profile specification [12]. Ethernet-APL allows connecting sensors and actuators directly to an Ethernet network. The development of Ethernet-APL was done under the consideration of the NAMUR position paper for an Ethernet communication system in the process industry [13].

Figure 1 shows the structure of an APL system, by using PROFINET as a communication protocol between the sensors / actuators and the controller of the automation system. The controller is connected via PROFINET (e. g. 100 Mbit/s or faster) and network switches to the APL field switches. The APL field switches (only one shown in Figure 1) receive auxiliary power and convey power and data to the APL field devices that are connected to the APL field switch via the Ethernet-APL spurs. This means that the APL field switch needs an auxiliary power supply (yellow arrow). Other topologies with a powered trunk are also possible. In this case an APL trunk cable conveys data and power to the APL field switches. The spur length can be up to 200 m. Operation of the field devices and field switches in areas with potentially explosive atmosphere is possible. A description of the Ethernet-APL engineering process can be found in [14].

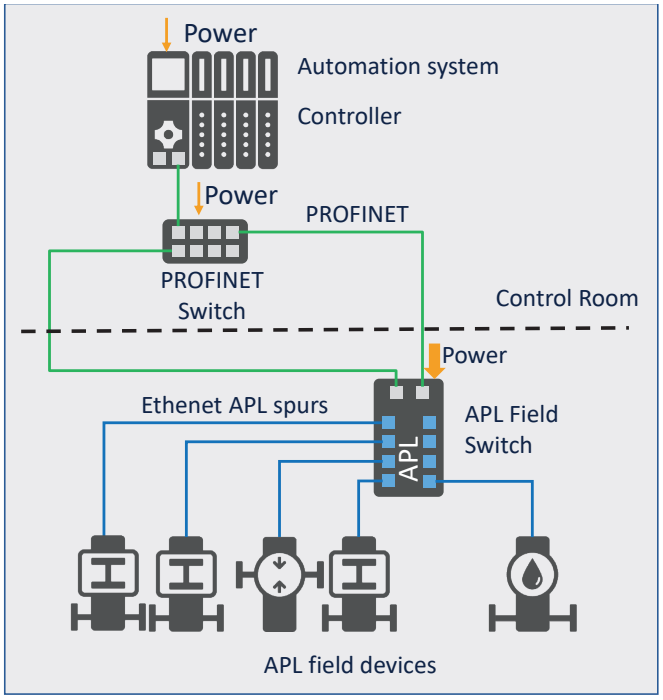


Figure 1: Structure of an Ethernet APL System.

Figure 2 compares the features of the Ethernet Advanced Physical layer with the 4…20 mA current loop. In the first run, it can be seen that Ethernet-APL provides a 10 Mbit/s fully digital communication, while the current loop delivers the measurement value as analogue value. The digital HART communication is very slow, compared to Ethernet-APL. Both concepts are suitable for areas with potentially explosive atmosphere. Ethernet-APL allows a direct connection of the field devices to the APL power switch. Explosion protection measures like barriers or supply isolators are not needed. Both concepts deliver power via the two-wire connection.

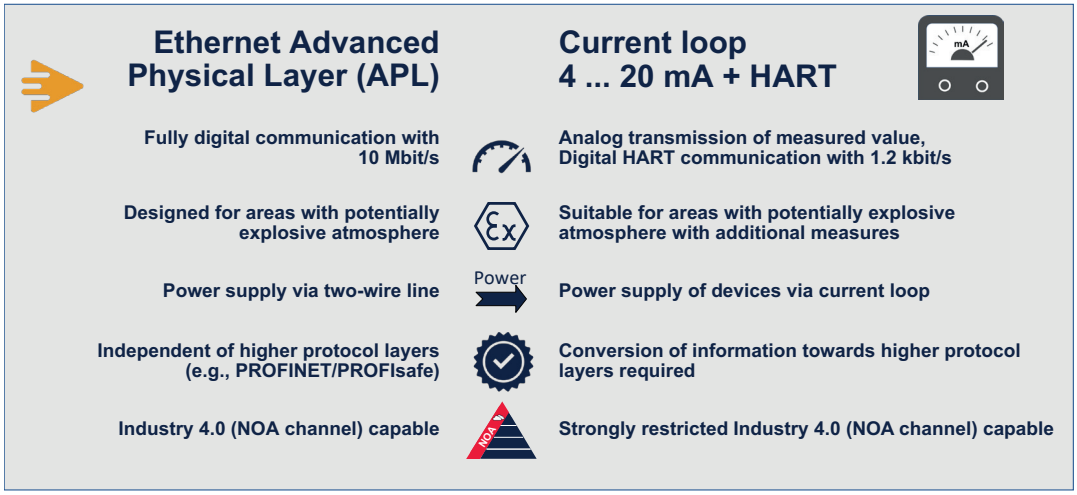


Figure 2: Comparison of Ethernet APL with current loop.

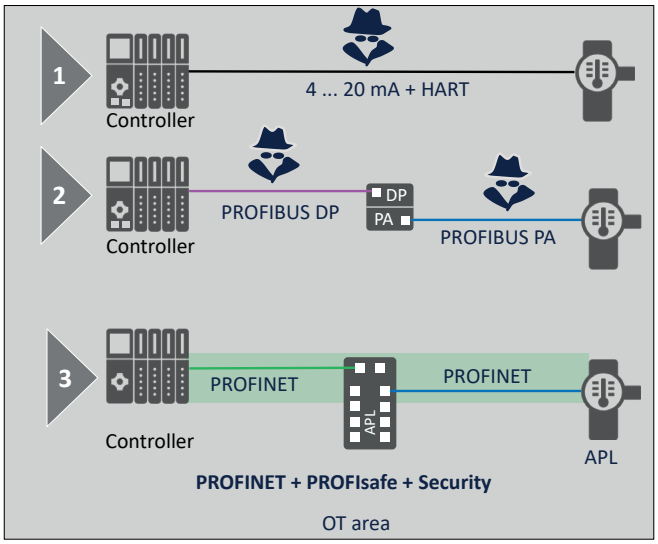


Figure 3: Attack vectors for sensors.

Ethernet-APL is a physical layer for Ethernet. This implies that it can be combined with a variety of industrial Ethernet protocols that make use of Ethernet, like PROFINET, OPC UA, EtherNet IP or HART IP. This allows for example that the field device can directly talk to the controller, as shown in Figure 1. Solely the Ethernet switches are needed to establish the communication. This is not possible with the current loop connection. HART communication needs an additional interface and a conversion to one of the industrial Ethernet protocols.

The access to diagnostic and other supplementary information is one of the key features of the NAMUR Open Architecture (NOA) [15, 16]. The use of Ethernet-APL simplifies this access by using a converged network architecture. This means that only one network infrastructure is needed for all means of communication. Media disruption is not any longer an issue.

1.3 Digital Communication and OT-Security

The direct connection of field devices to the automation network opens pandora's box of cyber security. The field devices are directly accessible on the automation network and therefore prone to OT security attacks.

Figure 3 shows possible attack scenarios for different stages of technology. It is assumed that an internal offender has access to the plant and the components installed in the plant. Already in 2013, the federal office for information security (Bundesamt für Sicherheit in der Informationstechnik, BSI) pointed out the relevance of internal offenders in the OT domain [17]. Further information about internal offenders can be found in [18].

Example 1 shows the classical 4…20 mA current loop with HART protocol. It is obvious that in internal offender can easily hook up to the current loop with a handheld terminal and change e. g. the measurement range of the device. From this point in time the device will deliver wrong measurement values via the current loop interface. Further attack scenarios with respect to HART can be found in [19].

Example 2 shows a control system that uses POFIBUS DP, a DP to PA Coupler and PROFIBUS PA to connect a field device to the controller. Both protocols are prone to a number of attacks as the protocol lacks integrity protection as well as it does not check the authenticity of information. So, configuration changes of man in the middle attacks are possible. A set of attack scenarios for PROFIBUS can be found in [20].

Example 3 now shows the situation for a digital communication with PROFINET. The controller communicates e.g., via 100 Mbit/s PROFINET. The APL Field switch converts the physical layer to the APL physics. It can be seen that controller and APL field device have a direct connection via Ethernet. In addition, the two devices do not have a point-to-point connection only, but they are part of a larger automation network that may span the whole plant. As of today, PROFINET products are prone to cyber-attacks as described in [21], but PROFIBUS and *PROFINET International* (PI) works on a security layer for PROFINET. The basic concepts are described in [22].

Since June 2022 the PROFINET Specification V2.4 MU3 is available [23, 24]. This version describes the major relevant security measures to ensure integrity and authenticity on a PROFINET network. This means that known attacks like a "man in the middle attack" are not any longer possible. If desired, also the confidentiality of the communication can be ensured, even though this is not a typical requirement. For sure, denial of service attacks are still possible. This kind of attack needs to be mitigated by the defense in depth concept. For future APL applications, the use of the PROFINET security layer will be the key measure against internal as well as external offenders. The PROFINET security concept is expected to comply with NAMUR recommendation NE 153 [25]. A detailed analysis of the security considerations for the integration of APL devices in an automation system is provided in [26].

2. The safety domain

Due to long lifecycles and high investment cost for new plants, process automation has a rather conservative and slow approach when adapting new technologies. This effect is multiplied in process safety by the general high demands of safety applications. Within process automation a technology break between control- and safety applications developed (see Figure 4).

When today a new plant is built in the process industry, the control application will use fieldbus technology for the integration of field devices.

At the same time, safety systems in the process industry still rely on the use of 4…20 mA current loops.

This is reasonable, as safety systems tend to employ tried and tested technology. Even though digital safety communication has been available for safety applications for many years and is already used in other industries as standard.

This leads to a situation, as shown in Figure 4. There is a technology gap between process control and process safety. Besides this technology gap, further challenges, as shown in Figure 5, apply.

Companies in the process industry experience a shift of functionality from process control into the direction of safety systems. This is caused by a higher number of safety functions, compared to the past. At the same time, high requirements for

documentation and regular testing of the safety functions applies. In addition, the demographic change may lead to a lack of qualified staff in the plants.
One of the key objectives of a digital safety communication is to lower the effort for testing and documentation (through automation) as well as to increase the use of predictive diagnosis for safety related field devices for e.g., proof test time extension.
As a result, now the process industry has the opportunity to use the Ethernet-APL in combination with the PROFINET/PROFIsafe technology in order to close the gap and bring the field communication to a new level.
The next section will describe how digital communication in the field can leverage the operational cost of safety systems during the lifecycle of the plant.

3. Synergies between Ethernet-APL and Safety-Applications

The possibility to connect an Ethernet-APL field device via Ethernet/PROFINET to a controller, yields several advantages:

- All Ethernet communication, no media breaks
- Staff needs to be trained on a single technology
- High data rate, compared to HART and Fieldbuses
- Integrated plant network based on Ethernet
- OT security aspects handled via PROFINET security concept (see chapter 1.3)

Some drawbacks need to be considered as well:

- During the ramp up of the APL technology a parallel use of fieldbus technology needs to be considered.
- APL is intended to allow the re-use of PROFIBUS PA cabling / FF-H1 cabling, but the quality of the cable needs to be measured, prior to reusing it.
- In case a powered trunk is used, a power budget calculation is necessary.

In parallel to that it would be beneficial to use the same infrastructure also for a safety-related communication. In 2021 the NAMUR defined requirements for the use of APL for safety applications [27]. Before going into detail, one principle of the safety communication shall be elaborated, the integrity protection of the safety related data.
Figure 6 shows on the upper side a simplified explanation of a data integrity protection for a non-safety communication. Three bytes of data shall be protected by a checksum. In this case the checksum is just the sum of the data. The sender calculates the checksum, concatenates it to the data and submits data plus checksum. The receiver computes the checksum himself and compares the calculated checksum

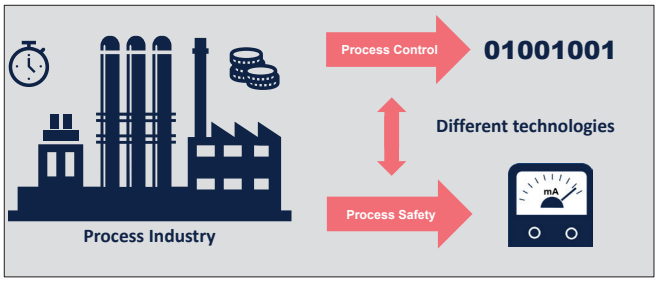


Figure 4: The technology gap between process control and process safety.

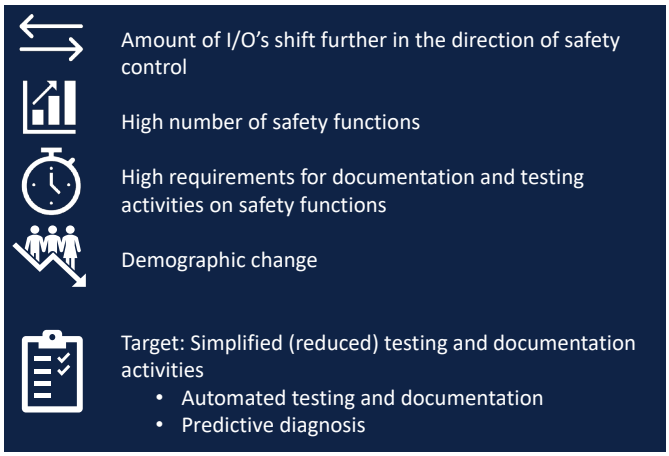


Figure 5: Challenges in the safety domain.

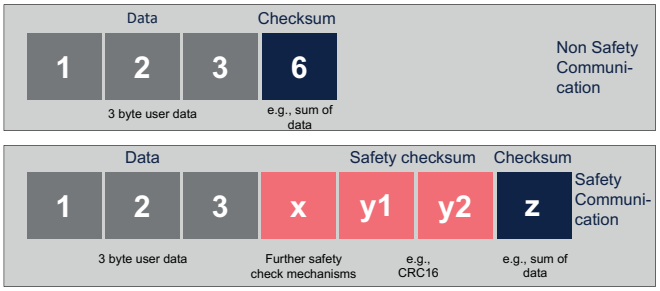


Figure 6: Basic data integrity protection mechanisms.

to the received checksum. In case both checksums are identical, the data packet is considered to be intact.
In case data bytes or the checksum get damaged (modified) during the transmission, the algorithm at the receiver will identify a difference between the checksum received and the checksum calculated and discard the package. This ensures that only intact data packet get processed by the receiver.
Due to the simplicity of the chosen algorithm, it is obvious that multiple transmission errors might lead to a situation where the data is damaged, but the checksum is still o.k. Assume that the first byte is changed from 1 to 2 and that the second byte is changed from 2 to 1. In this case the checksum is still the same and the package would be identified as intact. In real life the algorithms are better than described and the likelihood of such an undetected error is pretty low. Nevertheless, for safety applications a higher degree of integrity protection is needed. Usually it is not possible to change the integrity protection algorithm of the protocol used, as it might be in the market for decades and backwards

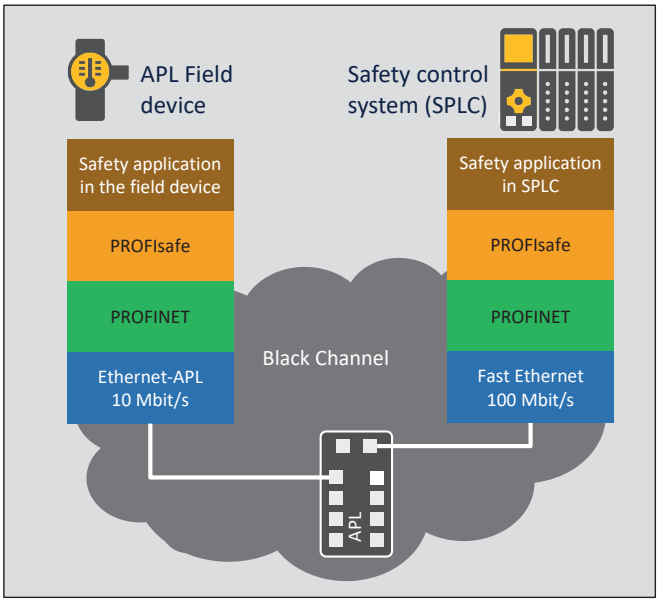


Figure 7: PROFIsafe communication with PROFINET and Ethernet APL.

compatibility needs to be ensured. Therefore, safety protocols add additional protection mechanisms are added to the data frame, but do not touch the original mechanism.
The lower part of Figure 6 shows such an extended protection. In the first run, additional safety check mechanisms, like a sequence counter x, are added to the frame. This ensures the correctness of the sequence of information. On top of that, an additional checksum is added to the data frame. A more sophisticated algorithm, the Cyclic Redundancy Check 16 (CRC 16) [28] y1 and y2 is used in this example. In the end, the "normal" checksum z of the data packet gets calculated, as in the previous example. The described mechanism allows to leave the used protocol and the used data protection mechanism unchanged. The safety layer does not even know the integrity protection mechanism of the underlying communication channel in detail but takes care of the data protection itself. The use of a transport channel with unknown or insufficient data integrity mechanisms is called using a "black channel". PROFIBUS as well as PROFINET use the black channel concept and add the additional integrity protection mechanism by the PROFIsafe safety profile (layer) [29]. So, if Ethernet-APL field devices shall be used in combination with PROFIsafe, the structure shown in Figure 7 results.
On the left side, the APL field device is shown. The device runs a safety application in order to provide a measurement value for the safety application running in the safety control system on the right side. The safety application in the field device sends data to the network. The data passes the PROFIsafe layer that ensures the safe communication, e.g., by adding an additional checksum, a sequence number and other additional information to the data packet. The data then runs through the PROFINET protocol stack and leaves the device via the Ethernet-APL connection. The data runs through the APL field switch. This switch processes the data and delivers it to the 100 Mbit/s Fast Ethernet connection in the right side. There the controller receives the data, runs it though the PROFIsafe layer, checks the safety integrity and delivers it to the safety application in the *safety programmable logic controller* (SPLC). On this basis, automation systems can run safety functions in combination with the Ethernet APL field devices. If this principle is transferred to a plant, a structure shown in Figure 8 is the result.
Figure 8 shows the parallel operation of a safety infrastructure and a control infrastructure. The right side of the image shows the controller of a DCS. The controller uses PROFINET as communication protocol. A media redundancy (ring redundancy) is used. The field devices are connected to the controller via the APL switch. A detailed overview on possible Ethernet-APL topologies can be found in [14]. This

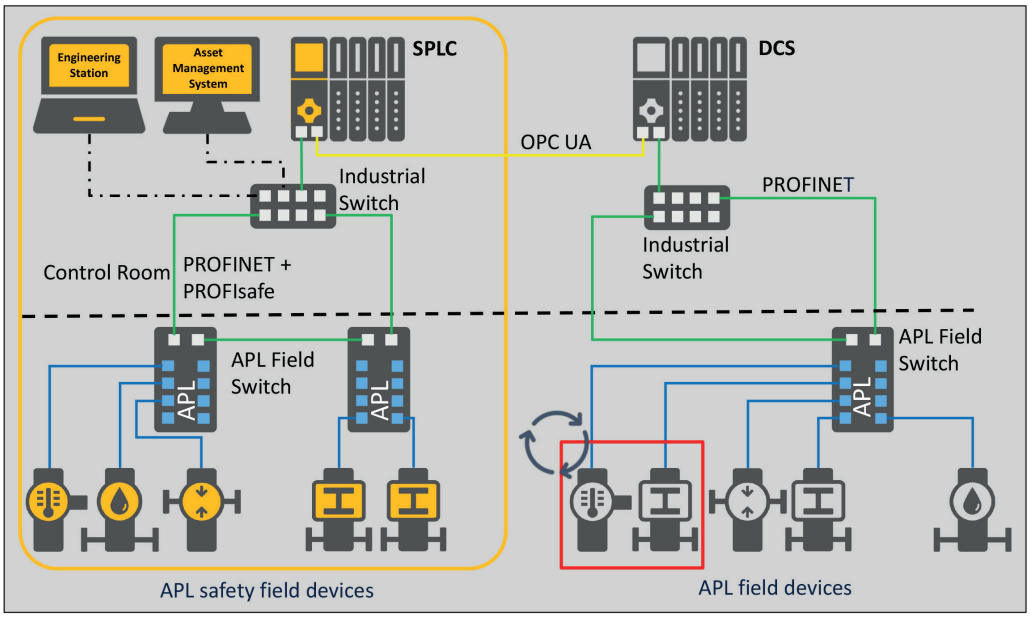


Figure 8: Safety Application and DCS in parallel.

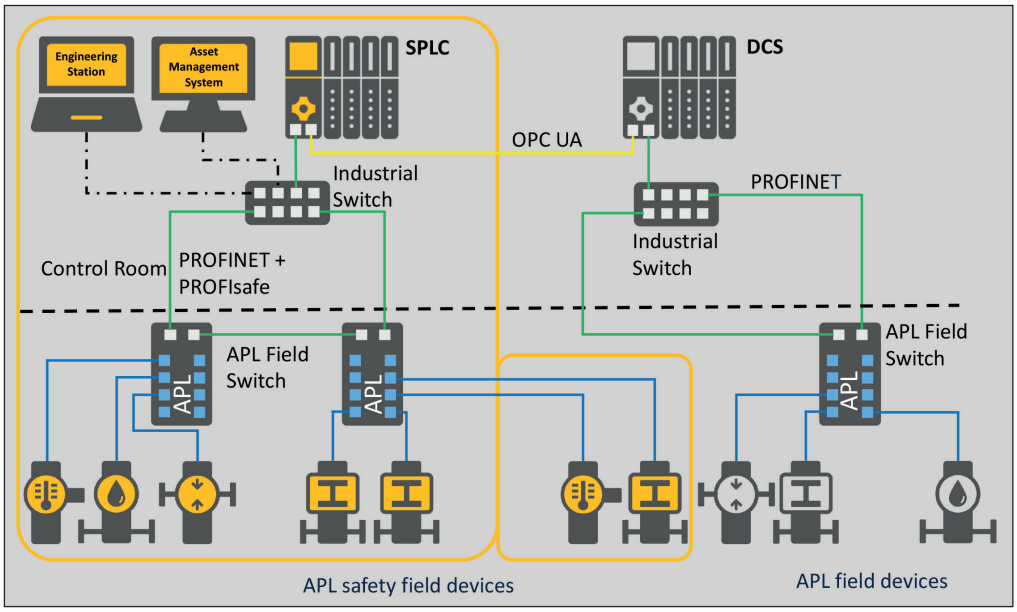


Figure 9: Migration of APL field device.

topology allows a direct communication between the controller and the APL field devices without any interfacing or data conversion. Only Ethernet switches are needed.
The left side of Figure 8 shows a safety system that is also based on PROFINET in combination with Ethernet-APL and PROFIsafe. The APL field devices are certified for use in safety applications (shown by the amber color). The safety controller (SPLC) is also certified for the use in safety applications. Besides these components, Figure 8 shows the dedicated engineering station and the dedicated asset management system. It is obvious that both of them can directly communicate with the APL field devices. This eases the maintenance and test process of the safety system and especially of the safety field devices. Recurring tests of the APL safety devices can be initiated and documented by the asset management system. Further information about this system approach can be found in [30–32].
Figure 8 shows a separation between the control system and the safety system. This separation yields advantages with respect to availability and security, even though increased effort is needed for the duplicated infrastructure [33]. In case information exchange between control system and safety system is needed, an OPC UA server to server communication can be used [34] to connect the two automation systems.
One use case for the shown system is the re-allocation (e.g., in case of new safety perceptions) of a field device from the control system to the safety system. Figure 8 shows two devices marked with a red frame. These devices shall be disconnected from the control system and re-allocated to the safety system. The necessary steps are:

» Disconnect the devices from the control system and disable the devices in the configuration of the DCS.

» Activate the PROFINET safety layer in the device. This implies that the device is certified as safety device and that the device supports the enabling and disabling of the safety function.

» Re-connect the devices to the safety system and integrate them into the safety function.

Figure 9 shows the re-allocated devices that are now used for the safety system. This option yields certain advantages for the plant owner:

» One set of APL field devices can be used for safety and non-safety application. The provisioning of spare parts is simplified by this concept.

» Due to the black channel principle, switches as well as APL field switches can be used for safety and non-safety applications.

» This infrastructure enables all NOA use cases - not only on the process control path, also on the important process safety path.

4. Challenges for using APL in safety systems

Besides the promising concepts, described in the previous chapters, there is still some work to do. The main requirements for the next steps are:

» The APL field devices shall be developed according to the IEC 61508 series of safety standards.

» The safety functionality shall be configurable (switch on, switch off) on the APL field devices. This allows using them for safety and non-safety applications and reduces the amount of spare parts (see example in Fig. 8 and Fig. 9).

» The APL field devices shall be developed according to the secure development lifecycle described in IEC 62443-4-1 [36].

» The devices shall support PROFINET in combination with PROFIsafe.

» The PROFINET/PROFIsafe PA Profiles [38] shall be considered.

The requirements listed above require certain precautions when developing Ethernet-APL field devices. Especially, reserves with respect to memory and computing power and an option for secure or at least protected boot and the provision of a secure element (e.g., Trusted platform module or similar) shall be considered.
Besides these technical requirements, accompanying measures for technology introduction shall be taken. The new founded NAMUR APL task force is a first, valuable step in the right direction.
From the end users' point of view, the use of APL with PROFINET/PROFIsafe shall simplify the work in all life cycle phases, compared to the current situation.

Acknowledgements

The authors would like to thank the NAMUR User Association of Automation Technology in Process Industries for the opportunity to present this paper at the NAMUR Annual General Meeting on the 10th and 11th November 2022 in Neuss/ Germany.

References

[1] DIN IEC 60381-1. (1985). Analoge Signale für Regel- und Steueranlagen; Analoge Gleichstromsignale. DIN: www.beuth.de.

[2] HART Communication Foundation (Fieldcomm Group). (2013). *HART Communication Application Guide*. Retrieved from: https://www.fieldcommgroup.org/sites/default/files/imce_files/technology/documents/HART_ApplicationGuide_r7.1.pdf

[3] PROFIBUS Nutzerorganisation e.V. (2018). *HART Integration in PROFINET IO: Amendment 4 to Fieldbus Integration into PROFINET IO*. Retrieved from: https://de.profibus.com/downloads/fieldbus-integration-into-profinet-io-guideline

[4] Diedrich, C., Bangemann, T. (2007). *Profibus PA: Instrumentation Technology for the Process Industry*. Oldenbourg Industrieverlag.

[5] Verhappen, I., Pereira, A. (2009). *Foundation fieldbus, 3rd ed*. Research Triangle Park. NC: ISA.

[6] Kaiser, V., Niemann, K. H., Otte, R., Wippermann, B., Koschel, J., Muller, U., Nicklaus, E. (2000). Asset Management-Asset Optimization-Technik und Beitrag zur Wertschöpfung. *atp magazin, 42*(12), 28-40.

[7] IEC 62453-1. (2016). Field device tool (FDT) interface specification – Part 1: Overview and guidance. IEC: www.iec.ch

[8] Simon, R. (2005). *Field Device Tool-FDT*. Oldenbourg Industrieverlag.

[9] IEC 62769-1. (2021). Field Device Integration (FDI) - Part 1: Overview. IEC: www.iec.ch

[10] Grossmann, D., Braun, M., Danzer, B., Kaiser, A., Riedl, M. (2016). *FDI-Field Device Integration: Handbook for the unified Device Integration Technology*. VDE Verlag GmbH.

[11] IEEE 802.3cg. (2019). IEEE Standard for Ethernet - Amendment 5: Physical Layer Specifications and Management Parameters for 10 Mb/s Operation and Associated Power Delivery over a Single Balanced Pair of Conductors. IEC: www.iec.ch

[12] PROFIBUS Nutzerorganisation e.V. (2021). *Port Profile Specification Ethernet-APL: Ethernet-APL Network and Port Requirements*. Retrieved from: https://www.profibus.com/download/port-profile-specification-ethernet-apl.

[13] NAMUR. (2016). *Position paper: An Ethernet communication system for the process industry.* Retrieved from: http://www.namur.net/fileadmin/media_www/Dokumente/Anforderung_Ethernet-NAMUR_2016-02-25_EN.pdf.

[14] APL Project and PROFIBUS und PROFINET International. (2022). *Ethernet APL Engineering Guideline. Planning, installation and commissioning of Ethernet-APL networks*. Retrieved from: https://www.ethernet-apl.org/wp-content/uploads/APL-Engineering-Guideline-V114_1.14.pdf.

[15] NE 175. (2020). NAMUR Open Architecture - NOA Konzept. NAMUR: www.namur.net

[16] Tauchnitz, T. (Ed.). (2021). *NAMUR Open Architecture (NOA): Das Konzept zur Öffnung der Prozessautomatisierung*. Vulkan-Verlag GmbH.

[17] Bundesamt für Sicherheit in der Informationstechnik (BSI). *Industrial Control System Security: Innentäter*. Retrieved from: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/BSI-CS_061.html.

[18] Cybersecurity & Infrastructure Security Agency. (2022). *Insider Threat Mitigation*. Retrieved from: https://www.cisa.gov/insider-threat-mitigation.

[19] Bhurke, A. U., Kazi, F. (2021). Methods of Formal Analysis for ICS Protocols and HART-IP CPN modelling. In *2021 Asian Conference on Innovation in Technology (ASIANCON)* (pp. 1-7). IEEE. doi: 10.1109/ASIANCON51346.2021.9544603.

[20] Watson, V., Lou, X., Gao, Y. (2017). A Review of PROFIBUS Protocol Vulnerabilities - Considerations for Implementing Authentication and Authorization Controls. In *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications, Madrid, Spain, 2017*, pp. 444–449. doi: 10.5220/0006426504440449.

[21] Mehner, S., König, H. (2019). No need to marry to change your name! Attacking profinet io automation networks using DCP. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 396-414). Springer, Cham.

[22] PROFIBUS Nutzerorganisation e.V. (2019). *Security Extensions for PROFINET - PI White Paper for PROFINET*. Retrieved from: https://www.profibus.com/download/pi-white-paper-security-extensions-for-profinet

[23] PROFIBUS Nutzerorganisation e.V. (2022). *Application Layer protocol for decentralized periphery. Technical Specification for PROFINET IO: Version 2.4 MU3*. Retrieved from: https://www.profibus.com/download/profinet-specification.

[24] PROFIBUS Nutzerorganisation e.V. (2022). *Application Layer services for decentralized periphery: Technical Specification for PROFINET IO, Version 2.4 MU3*. Retrieved from: https://de.profibus.com/downloads/profinet-specification/.

[25] NE 153. (2015). Automation Security 2020 – Design, Implementierung und Betrieb industrieller Automatisierungssysteme. NAMUR: www.namur.net

[26] Niemann, K. H., Merklin, S. (2022). OT security requirements for Ethernet-APL field devices: Technological change can yield improved protection. *atp magazin, 64*(5), 44-51. https://doi.org/10.25968/opus-2288.

[27] NAMUR Working Group 2.6 Digital Process Communication. (2021). *Ethernet APL for functional safety applications*. Retrieved from: https://www.namur.net/fileadmin/media_www/Dokumente/AK_Position_2.6_Ethernet_APL_2021-07-09_EN.pdf

[28] Jetzek, U. (2018). *Galois Fields, Linear Feedback Shift Registers and their Applications.* Carl Hanser Verlag GmbH Co KG.

[29] PROFIBUS Nutzerorganisation e.V. (2016). *PROFIsafe System Description Technology and Application*. Retrieved from: https://www.profibus.com/download/profisafe-technology-and-application-system-description

[30] Meurer, A., Risser, M., Roser, M. (2022). Ethernet-APL für hochverfügbare Sicherheitsanwendungen: Vorteile über den gesamten Lebenszyklus von Prozessanlagen. *atp magazin, 63*(5), 76-81. doi: 10.17560/atp.v63i5.2595.

[31] Risser, M., Ziegler, A., Salzmann, P., Roser, M. (2021). Ethernet-APL für hochverfügbare Sicherheitsanwendungen: Vorteile über den gesamten Lebenszyklus von Prozessanlagen. In *22. Leitkongress der Mess- und Automatisierungstechnik Automation 2021 -Navigating towards resilient Production, VDI Wissensforum GmbH, Ed.*, pp. 209–220.

[32] Ditting, S., Rogoll., G., Hähniche, J., Ziegler, A., Risser, M., Siebert, H., Stadler, R., Niedermayer, G. (2021). *Ethernet-APL in the Field for high-availability Safety Applications: Safety over Ethernet APL*. Retrieved from: https://www.endress.com/_storage/asset/9323211/storage/master/file/34108340/download/Whitepaper%20APL-SIF_final-EN.PDF

[33] NAMUR Working Group 2.6 Digital Process Communication. (2021). *Ethernet APL for functional safety applications*. Retrieved from: https://www.namur.net/fileadmin/media_www/Dokumente/AK_Position_2.6_Ethernet-APL_2021-07-09_DE.pdf

[34] IEC TR 62541-1. (2020). OPC unified architecture - Part 1: Overview and concepts. IEC: www.iec.ch

[35] DIN EN 61508-3. (2011). Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme - Teil 3: Anforderungen an Software. DIN: www.beuth.de

[36] DIN EN IEC 62443-4-1. (2018). IT -Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung. DIN: www.beuth.de

[37] DIN EN IEC 62443-4-2. (2019). IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS). DIN: www.beuth.de

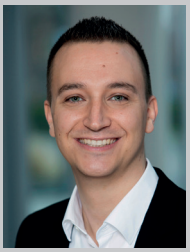
[38] PROFIBUS Nutzerorganisation e.V. (2022). *Profile for Process Control Devices: (PA Profile Version 4.02MU1).* Retrieved from: https://www.profibus.com/download/process-control-devices

AUTHORS

Prof. Dr.-Ing. Karl-Heinz Niemann (born 1959) represents the areas of industrial informatics and automation technology at Hannover University of Applied Sciences and Arts since 2005. From 2002 to 2005, he was responsible for the area of process data processing at the University of Applied Sciences and Arts Northeast Lower Saxony (today Leuphana University). Prior to that, he held leading positions in the development of process control systems, at ABB, Elsag Bailey and Hartmann & Braun. ORCID: https://orcid.org/0000-0001-8931-6789

Prof. Dr.-Ing. Karl-Heinz Niemann
Hannover University of Applied Sciences
P.O. Box 92 02 61
30441 Hannover
✆ +49 511 92961264
@ karl-heinz.niemann@hs-hannover.de

Marc Risser, M.Sc. (born 1988) heads as an Automation Manager the Safety Systems Technology Team in the Center of Technical Expertise - Automation Technology in BASF SE. His team is involved in the standardization of software and hardware solutions for the implementation of safety applications. The focus of his work is on new technologies in the field of functional safety.



Marc Risser, M.Sc.
BASF SE
Carl-Bosch-Strasse 38
67056 Ludwigshafen am Rhein
@ marc.risser@basf.com