# A Review of PROFIBUS Protocol Vulnerabilities
## *Considerations for Implementing Authentication and Authorization Controls*

Venesa Watson[1,2], Xinxin Lou[1,3] and Yuan Gao[1,4]
*[1]AREVA GmbH, Erlangen, Germany*
*[2]Faculty of Science and Engineering, University of Siegen, Siegen, Germany*
*[3]Department of Computer Networks and Distributed Systems, Bielefeld University, Bielefeld, Germany*
*[4]Department of Computer Science, Otto-von-Guericke University, Magdeburg, Germany*

Keywords: PROFIBUS, Industrial Networks, Security, OPC UA, Defense-In-Depth.

Abstract: PROFIBUS is a standard for fieldbus communication, used in industrial networks to support real-time command and control. Similar to network protocols developed then, availability is the security objective prioritized in the PROFIBUS design. Confidentiality and integrity were of lesser importance, as industrial protocols were not intended for public access. However, the publicized weaknesses in industrial technologies, including the inclusion of publicly available technology and protocols in industrial networks, presents major risks to industrial networks. This paper investigates the security risks of and provides suggested security solutions for PROFIBUS. The objective is to review the PROFIBUS protocol, to establish the purposefulness of the design and its suitability for the applications where it forms a core part of the infrastructure. The security risks of this protocol are then assessed from successful and possible attacks, based on the vulnerabilities. Proposed security solutions are reviewed and additional recommendations made concerning the use of OPC UA, accompanied by an analysis of the cost of these solutions to the efficiency and safety of the PROFIBUS. The findings of this paper indicate that a defense-in-depth approach is more feasible security solution, with strong security controls being implemented at networks interconnecting with the PROFIBUS networks.

## 1 INTRODUCTION

Industrial networks, like those in nuclear power plants, are isolated from public networks, such as the Internet. These networks primarily use specialized protocols that were not initially developed with security features as a part of their design, as they were not intended for public availability. In fact, industrial networks comprised of trusted devices with little or no connection with the public space. As such, cyber-security was not seen as integral, but rather as a compensating control. Today, whilst these specialized protocols remain in use mostly in industrial networks, information about their vulnerabilities is now publicly available. Furthermore, given that these networks are increasingly targeted by persistent and sophisticated attacks, the lack of security for these protocols represents a major risk to industrial networks (Knapp and Langill, 2015). This paper will focus on just one industrial protocol, namely PROFIBUS.

PROFIBUS is an international open standard defined by IEC 61158/IEC 61784-1, for fieldbus communication in automation technology. PROFIBUS has three specifications: PROFIBUS Fieldbus Message Specification (FMS), for data communication between PCs and Programmable Logic Controllers (PLCs); PROFIBUS Fieldbus Decentralized Peripherals (DP), connects distributed field devices to a centralized controller, for example; and PROFIBUS Process Automation (PA), developed with technology that transports both power and data over the same cable at a reduced level that decreases the probability of explosions, in hazard-prone areas (Acromag Incorporate, 2002, and Siemens, 2010). Per ISO 7498, PROFIBUS is oriented to the OSI model (Table 1) (Applied Tech Systems, 2016). At the physical layer, RS485 is a shielded twisted pair (STP) copper cable, with special advantage for communication over long distances and for use in noisy environments. Fiber-Optic cable offers similar advantages, but is recommended for areas with high EMI. Manchester Bus Powered

Watson, V., Lou, X. and Gao, Y.
A Review of PROFIBUS Protocol Vulnerabilities - Considerations for Implementing Authentication and Authorization Controls.
DOI: 10.5220/0006426504440449
In *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT*, pages 444-449
ISBN: 978-989-758-259-2

(MBP) technology is made especially for use in hazardous areas. Layer 2 is referred to as the Fieldbus Data Link (FDL) layer. Here, the medium access control (MAC) mechanism is defined for fieldbus, and the master-slave and token-passing principles are combined for communication between stations (masters and slaves). Token-passing coordinates the communication among the masters. The token is passed in ascending order according to the station address, and the master in possession of the token is authorized to transmit to any other station. The stations communicate using telegrams, which can have a maximum size of 249 bytes (Figure 1) (Felser, 2013). At the application layer, three messaging protocols are defined for PROFIBUS DP: DP-V0 for cyclic exchange of data and diagnosis; DP-V1 for acyclic data exchange and alarm handling; and DP-V2 for isochronous mode and data exchange broadcast (slave to slave communication) (Siemens, 2010).

The PROFIBUS protocol stack and the format of the telegrams demonstrate the lack of confidentiality and integrity checks on this protocol. There are no controls for authentication or authorization defined at any layer of its OSI model, and the telegrams are transmitted in clear-text. These features provide a possible attack path in industrial networks, where PROFIBUS is used.

This paper is structured in the following way: Section 2 briefly looks at the features of PROFIBUS that make it suitable for use in the industrial setting, and at possible exploits. Section 3 discusses proposed security controls to address the PROFIBUS vulnerabilities, and highlights considerations for the feasibility of implementing these solutions. The conclusion provides an overview of the PROFIBUS security vulnerabilities and possible security controls, and ideas for further research.

Table 1: The OSI Model for the PROFIBUS Protocol (Applied Tech Systems, 2016).

| | User Program | Application profiles |
|---|---|---|
| 7 | Application | DP-V0; DP-V1; DP-V2 |
| 6 | Presentation | NOT USED |
| 5 | Session | |
| 4 | Transport | |
| 3 | Network | |
| 2 | Data link | Master-Slave; Token-Passing |
| 1 | Physical | RS485; Fiber-Optic; MBP |
| | OSI Model | PROFIBUS OSI Model |

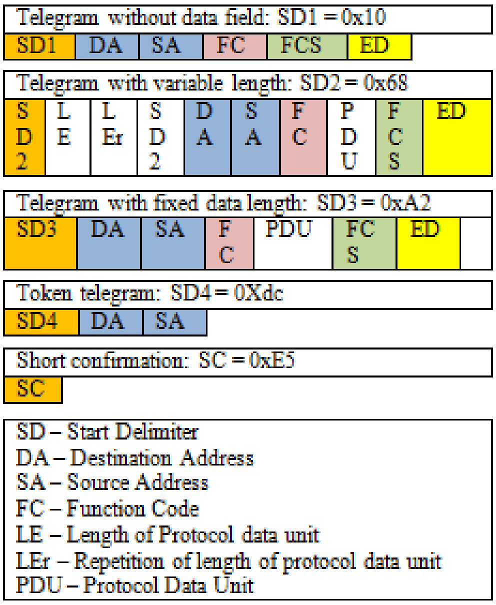
Telegram without data field: SD1 = 0x10
SD1 DA SA FC FCS ED
Telegram with variable length: SD2 = 0x68
SD2 LE LEr SD2 DA SA FC PDU FCS ED
Telegram with fixed data length: SD3 = 0xA2
SD3 DA SA FC PDU FCS ED
Token telegram: SD4 = 0Xdc
SD4 DA SA
Short confirmation: SC = 0xE5
SC
SD – Start Delimiter
DA – Destination Address
SA – Source Address
FC – Function Code
LE – Length of Protocol data unit
LEr – Repetition of length of protocol data unit
PDU – Protocol Data Unit

Figure 1: PROFIBUS Telegram Formats (Felser, 2013).

## 2 PROFIBUS FEATURES AND VULNERABILITIES

PROFIBUS stands out from other fieldbus systems because it offers an extraordinary breadth of applications (Profibus International 2013). PROFIBUS can be used for fast and cost-effective production in a wide area of applications – such as factory automation, process automation and building automation. As an open standard, PROFIBUS is compatible with a wide range of components from different manufacturers. This protocol boasts further advantageous features, which include network components suitable for hazardous industrial environments; high security of investment, as existing networks can be extended without any adverse impacts; and high levels of operational reliability and plant availability, due to different diagnostics options. And whilst it is mainly used at the field level of an industrial network architecture, PROFIBUS can also be used at the control level. PROFIBUS flexible, durable and safety-oriented, which contributes to its success and wide use. However, the security holes in PROFIBUS are of concern. Lack of authorization and authentication control suggests that a rogue device can be connected to and communicate on PROFIBUS, gaining access to the clear-text telegrams.

In an attack tree analysis of an industrial network segment that has a PROFIBUS backbone, a connected controller is considered as a prime target, as it is a device that can issue commands to disrupt the functioning of the plant. Typical attack goals include: gain access to the controller (master), disable, write data to and/compromise master. With access to the master, an attacker can also gain access to slaves, to achieve goals as above, in addition to reading data from the slave or programming the slave (Bryes et al., 2004). Access to a controller allows an attacker to monitor the network communication, map the network topology and spoof and/or capture, interpret and use the commands observed. Once an attacker achieves network access, sniffing the network is a relatively easier task, especially where there is no confidentiality control in place. Such a network attack is possible through PROFIBUS, as it lacks authentication and authorization controls to verify connected masters, to validate the communication and to restrict communication to legitimate components. The infamous Stuxnet worm is an example of an attack that exploited these vulnerabilities. Stuxnet is a sophisticated malware that was injected into the SCADA system at a uranium enrichment facility in Iran. This worm compromised PLCs, and whilst operating as a logic bomb, monitored the clear-text communication on a PROFIBUS DP network, waiting for specific data before executing its payload (Knapp and Langill, 2015, and Abouzakhar, 2013). With authentication and authorization controls in place on the PROFIBUS network, it is possible to assume that this attack would not have been successful or as successful.

## 3 CONSIDERATIONS FOR PROFIBUS SECURTIY

Authorization and authentication controls are used to ensure that rights and privileges for access, modification and creation are given to the approved individual or system, to maintain confidentiality and integrity. Cryptography is the most appropriate solution, and possibly the only real solution for authenticating network devices and for verifying communication integrity. However, cryptographic controls come at a cost to efficiency. Integrity verification, encryption and decryption all require additional processing time. This additional time is unfavourable in industrial networks, where system reaction time is critical due to the heavy reliance on the information transmitted between masters and slaves. This information is used to monitor and control the environment, which is important to maintaining safety - the protection of life and the environment from harm and danger. As such, security controls for integrity and confidentiality should not affect availability, that is, the reaction time or real-time responsiveness of the system.

The PROFIBUS MAC mechanism is based on the Timed Token (TT) protocol, which specifies the amount of time given to a master or slave to transmit data. This impacts the bus cycle time (time taken for the exchange of data between master and slaves or between slaves, which influences the reaction time of the connected components by between 2 to 20 percent (Felser, 2013, Profibus International, 2009, and Tovar and Vasques, 1999). Typically, the favourable maximum PROFIBUS bus cycle time is less than 10ms, at the field level of an industrial network. Other factors that contribute to system reaction time include: transmission time, protocol processing time, and access and queuing delays (Profibus International, 2009, and Tovar and Vasques, 1999). Emphasis is placed on the real-time requirement at the field level. Hence, the processing time of a cryptographic solution is an important factor in determining the most suitable option for implementation here. Additional cryptographic concerns include the need for additional computing resources, the complexity the control introduces, and maintaining system reliability.

In securing PROFIBUS, two options are presented: using existing secure protocols, particularly those for Ethernet technology, or integrating authentication controls on PROFIBUS itself.

### 3.1 Secure PROFIBUS with Ethernet Technology

In Treytl et al., (2004), the authors propose the use of IPSec to support confidentiality and integrity on the PROFIBUS network. However, their work considered IP-based fieldbus technology, which has the advantage of deploying existing, compatible encryption protocols. An example of this is PROFINET, which is a category of industrial Ethernet that integrates the PROFIBUS technology with Ethernet technology (Siemens, 2017a). IPSec has two security mechanisms: Authentication Header (AH) and Encapsulating Security Payload (ESP), which support authentication, confidentiality (ESP only) and integrity. IPsec also has two data transfer modes: transport mode, where only the payload of the packet is encrypted; and tunnel mode, where the entire packet is encrypted. These features highlight the flexibility and suitability of IPSec in fulfilling the necessary security needs of PROFIBUS. AH and ESP can be used on their own or can be combined. AH provides integrity of the immutable elements of the IP header, but whilst ESP also provides authenticity, this is does not include the outer IP header, hence why a combination would be desirable. However, in addition to the overhead in encrypting and decrypting network packets, using a combination of AH and ESP would exponentially increase the required SAs. In that, let n be the number of fieldbus nodes, *n squared* represents the number of SAs required (Treytl et al., 2004). It is suggested that this exponential resource requirements could be alleviated by having masters provide SA functions for all connected slaves.

The proposals given in Treytl et al., (2004) and Udayakumar and Ananthi (2015) suggest the use of a symmetric key algorithm to reduce the processing time and complexity. DES was identified as the selected algorithm, which has a key size of 56-bits. However, DES is known to be weak due to this short key size, and can be broken in less than a week.

## 3.2 Secure Fieldbus Architecture

The Open Connectivity Unified Architecture (OPC UA) is a platform-independent standard that provides interoperability for devices from different manufacturers, allowing them to communicate by sending Messages between OPC UA clients and Servers. In part 2 of this multipart standard, a security model is defined, which aims to secure the communication facilitated by OPC UA, to assure the identity of Clients and Servers and to resists attacks (IEC, 2016a). According to its scope, OPC UA is applicable to manufacturing software used in industrial applications, such as Control Systems, Enterprise Resource Planning, Manufacturing Execution Systems and Field Devices.

OPC UA security concerns itself with the following factors: the authentication of users, the verifiability of claims of functionality, the authentication of Clients and Servers, and the integrity and confidentiality of their communications (IEC, 2016a and 2016b). In a typical industrial network, OPC UA servers and clients are placed in the control zone, which is just above the field level, where the PROFIBUS predominantly features (Knapp and Langill, 2015). However, OPC UA merely provides support for the implementation of controls, and can be integrated at the other network levels (IEC, 2016b). IEC (2015) outlines four security policies defined for OPC UA:

- None – a suite of algorithms that does not provide any security settings, for configurations with the lowest security needs;
- Basic128Rsa15 – a suite of algorithms that uses RSA15 as the Key-Wrap-algorithm and 128-bit for encryption algorithms, for configurations with the lowest security needs;
- Basic256 – a suite of algorithms that are for 256-bit encryption algorithms, for configurations with medium to high security needs; and
- Basic256Sha256– a suite of algorithms that are for 256-bit encryption algorithms, for configurations with high security needs.

The features of OPC UA that make it robust against attacks that target communication data, are described in part 5 (IEC, 2016a). Such attacks include message flooding, eavesdropping, message spoofing, session hijacking, rogue server and compromising user credentials. By protecting against these and other attacks, the OPC UA security mechanisms work to secure application authentication, user authentication, authorization, confidentiality, integrity, auditability and availability. Furthermore, OPC UA provides the additional resources and support for the use of cryptographic controls, such as a key management server and key exchange services, removing the burden from the industrial network components. On the surface, these features make OPC UA suitable for securing PROFIBUS. However, the cryptographic controls, as indicated by the above security policies, are considered as resource- intensive. In fact, Post et al., (2009) expresses concern about the communication delay inflicted by encryption. This is supported by the formula for estimating PROFIBUS DP and PA bus cycle times (Figure 2) (Profibus International, 2009). This formula indicates that the bus cycle time increases with increasing transmission rate and slaves. To maintain a bus cycle time of less than 10ms, the transmission rate must remain at 1.5Mbits/s, whilst also observing the number of slaves connected (Profibus International, 2009). Therefore, the additional bits from the encryption key size and cipher, as well as plans to expand the network, must be considered when selecting an OPC UA security policy, particularly for the field level. For example, consider a network segment with a PROFIBUS backbone that has its maximum slaves connected, that is, 32 slaves. Using the formula in figure 2, (with $L_O = L_I = 5$ bytes and $T_r = 1.5$Mbits/s), the bus cycle time is 9.1 ms. Adding to the telegram overhead, the cipher bits and key size bits of a suitable algorithm for the following OPC UA security policies: Basic128Rsa15 (AES 128-bit cipher and 128-bit key length) and Basic256Sha256 (AES 128-bit cipher and 256 bit key length), the respective bus cycle times are 14.6ms and 17.3ms. For DES (64-bit cipher and 56 bit key), the bus cycle time is 11.7ms. These values indicate that these security policies at the field level may not be favourable, as it concerns the effect on system reaction time. To support these controls whilst maintaining the required bus cycle time, the formula suggests that Basic128Rsa15 can facilitate up to 22 slaves (10ms), up to 18 slaves with Basic256Sha256 (9.7ms), and 27 slaves with DES. However, DES is too weak to be considered for implementation. Discounting the number of connected slaves, these controls are likely to have negligible disadvantages at higher network levels, such as at the control level and operations management level, where bus cycle times are far greater than 10ms.

$$T_{cycle} = \frac{\sum_{i=1}^{n}(T_O + Bit \,.\, (L_O + L_I)_i)}{\mathrm{T}_r}$$

$\mathbf{T_{cycle}}$ = cycle time in ms
**n** = total number of slaves
**i** = slaves run available
$\mathbf{T_O}$ = telegram overhead (317 bits)
Bit
= PROFIBUS DP data format: $11(\frac{bit}{byte})$ **or**
= PROFIBUS PA data format: $8(\frac{bit}{byte})$
$\mathbf{(L_O + L_I)_i}$ = Sum of slave output and input in bytes
$\mathbf{T_r}$ = Transmission rate in Kbits/s

Figure 2: Formula for estimating PROFIBUS Dp and PA bus cycle times (Profibus International, 2009).

IEC (2016a and 2015) acknowledges that the system designers have final decision on the security controls and the network level for implementation. As such, following a defense-in-depth approach, stronger controls can be implemented at the non-time-critical levels of the industrial network, whilst using secure, but lighter controls at the field level. This proposition is also supported because physical security at the field level is and will become increasingly stringent. In addition, Post et al., (2009) postulates that confidentiality is not necessary at the field level, given that the events at this level are time critical. Therefore, implementing stronger, more resource-intensive authentication and authorization controls above the field level, through OPC UA, is recommended. The goal of this strategy would then be to provide a layer of defense above the field level, to supplement the stringent physical security controls and reduce the probability of an attack at the field level. In time however, OPC UA may provide additional support for time-critical services, as there are plans for extensions in the area of Time-Sensitive Networks (TSN) for this standard (Zvie, 2017). Assuming that cryptography will also be included in the specifications to support time-critical networks, consideration should be given to the optimization of encryption, to reduce the overhead.

## 4 CONCLUSIONS

Developing and deploying a secure PROFIBUS is possible, but requires thorough consideration and testing, to maintain system availability, and by extension, functional safety. Implementing cryptographic controls to address the confidentiality and integrity gaps in PROFIBUS, particularly at the field level, suggests unfavourable consequences for system reaction time. Nevertheless, OPC UA presents an option for a defense-in-depth approach to secure the PROFIBUS network by implementing strong security at the network levels above the field level. Other research suggests that authorization and authentication controls be implemented at the field level network, which is not as feasible, due to processing overhead and additional resource requirements. These security controls are best implemented above the field level, where the identified drawbacks are negligible. By leveraging authentication and authorization controls, of differing strengths, at the higher level, this approach should supplement the physical security measures implemented at the field level.

Furthermore, the development of a thorough attack tree analysis for PROFIBUS is required to assist in determining all possible attack goals and their attack paths, and in measuring the risks, impact and probability, so that appropriate measures are implemented to thwart these attacks. Additionally, test cases are necessary to simulate and observe cryptography in action on a PROFIBUS network, to determine the suitability and the ease of implementation of the chosen cryptographic algorithms. Further suggestions for future research, include a study to determine if and where controls (particularly, data encryption) for preserving confidentiality are necessary when other controls are in place to guarantee authentication and integrity, for time-sensitive networks; and for methods for accelerating or optimizing cryptographic processes. Also to be considered is that specification and enforcement of detailed activity-related security controls, like limited range modifications of set-points in automation equipment by predefined end-users, could be the next security defense-in-depth level on secure application level network communication.

## ACKNOWLEDGEMENTS

Some of the addressed cybersecurity related topics are being elaborated as part of AREVA GmbH's participation in the "SMARTEST" R&D (2015-2018) with German University partners, partially funded by German Ministry BMWi.

## REFERENCES

Abouzakhar, N., 2013, 'Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations', in R. Kuusisto and E. Kurkinen (eds.), *Proceedings of the 12th European Conference on Information Warfare and Security, Jyväskylä, Finland, July 11-12, 2013*. Academic Conferences and Publishing International Limited, UK, 1-10.

Acromag Incorporated, 2002, *Introduction to Profibus DP*, viewed 26 January 2017, from http://www.diit.unict.it/users/scava/dispense/II/Profibus.pdf.

Applied Tech Systems, 2016, *PROFIBUS Technology*, viewed on 26 January 2017, from: http://www.ats-global.com/Profibus-technology_230_nlnl.

Bryes, E., Franz, M. & Miller, D., 2004, 'The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems', International Infrastructure Security Survivability Workshop (IISW), viewed on 13 December 2016, from https://www.researchgate.net/publication/228952316_The_use_of_attack_trees_in_assessing_vulnerabilities_in_SCADA_systems.

Felser, M., 2013, *PROFIBUS Manual: A collection of Information Explaining PROFIBUS Networks*, 1.2.3 edn, Profibus.felser.ch, viewed 26 January 2017, from http://Profibus.felser.ch/en/

International Electrotechnical Commission (IEC), 2015. *IEC TR 62541-7 Ed. 2.0. International Standard OPC Unified Architecture – Part 7: Profiles*. Switzerland: IEC.

International Electrotechnical Commission (IEC), 2016a. *IEC TR 62541-1 Ed. 2.0. Technical Report OPC Unified Architecture – Part 1: Overview and concepts.* Switzerland: IEC.

International Electrotechnical Commission (IEC), 2016b. *IEC TR 62541-2 Ed. 2.0. Technical Report OPC Unified Architecture – Part 2: Security Model*. Switzerland: IEC.

Knapp, E.D. & Langill, J.T., 2015, *Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, 2nd edn., Syngress (Elsevier), Massachusetts, USA.

Post, O., Seppälä, J. & Koivisto, H., 2009, 'The Performance of OPC-UA Security Model at Field Device Level', in J. Ferrier, J. Filipe and J. Cetto (eds.), *Proceedings of the 6th International Conference on Informatics in Control, Automation and Robotic, Intelligent Control Systems and Optimization, Milan, Italy, July 2-5, 2009.* Scitepress, Portugal, 337-341.

Profibus International, 2009, *PROFIBUS Installation Guideline for Planning Version 1.0*, viewed May 16, 2017, from http://www.profibus.com/uploads/media/PROFIBUS_Planning_8012_V10_Aug09.pdf.

Profibus International, 2013, *PROFIBUS and Integrated Safety architectures in Ex areas*, viewed January 26, 2017, from http://www.Profibus.com/newsroom/detail-view/article/Profibus-in-ex-area/

Siemens, 2010, *Network solutions for PROFIBUS according to IEC 61158/61784*, viewed January 26, 2017, from https://www.industry.siemens.nl/automation/nl/nl/industriele-communicatie/Profibus/Documents/Network_solutions_for_PROFIBUS_en.pdf.

Siemens, 2017a, *From PROFIBUS to PROFINET*, viewed January 26, 2017, from http://w3.siemens.com/mcms/automation/en/industrial-communications/profinet/Profibus/pages/Profibus.aspx.

Tovar, E. & Vasques, F., 1999, 'Real-time Fieldbus Communications Using Profibus Networks' *IEEE transactions on Industrial Electronics*. 46 (6), 1241-1251.

Treytl, A., Sauter, T., & Schwaiger, C., 2004, 'Security Measures for Industrial Fieldbus Systems – State of the Art Solutions for IP-based Approaches', in T. Sauter (ed.), *Proceedings of the IEEE International Workshop on Factory Communication Systems, Vienna, Austria, September 22-24, 2004,* IEEE Press, USA, 201-209.

Udayakumar, S. & Ananthi, S., 2015, 'Fieldbus Protocol for Secured Wireless Sensor Network Communication in Process Automation', *International Journal of Emerging Trends in Electrical and Electronics (IJETEE)* 11(5), 92-96, viewed on January 26, 2017, from www.ijetee.org/Docs/Volume%2011/Issue%205/14.pdf.

Zvie, 2017, 'Industrie 4.0 Plug-and-Produce for Adaptable Factories: Example Use Case Definition, Models, and Implementation', unpublished.