Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

Proposal

Master of Communication Systems and Networking

Security Analysis of Industrial Bus Protocols

by

Zain Umer Javaid

First supervisor:	Professor Dr. Karl Jonas
Second supervisor:	Prof. Dr. John Doe
External supervisor:	Jonas Stein
External company	Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung (IFA)
Handed in:	March 2, 2020

Introduction: The German institute "Bundesamt für Sicherheit in der Informationtechnik (BSI)" published their fifth annual report in 2014. It entailed a description about an attack on an unspecified German steel mill. According to the report, spear phishing emails were sent to the employees to access the office network, which later helped the attacker to access the plant network [LAC14]. The technical capabilities of attacker estimated were significantly advance. The attacker had acquired significant knowledge about the plant control system. Several internal devices and components were compromised, subsequently incurring damage to equipment and control process. The BSI considered this attack as a Advanced Persistent Threat [BSI14, Cob15]. Such criminal activities must be considered for Industrial Control System (ICS) security.

In December 2017 FireEye published a report about a new ICS attack. The malware was named as "TRITON". In the meantime, the malware was called as "TRISIS" by DRAGOS and "HATMAN" by the US Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). FireEye claimed that a petrochemical processing plant in Saudi Arabia was the victim of this malware [HF+18]. The culprit targeted SIS (Safety Instrumented Systems) devices. SIS are specially designed to control devices, that deal with functional safety. The malware attacked a Triconex safety controller by Schneider Electric and manipulated its memory firmware. The attack consisted of two parts. First, the intruder entered the operational technology network via the IT network. Second, the malicious content was injected which enabled the attacker to read and modify the memory content of the SIS controller. TRITON is considered as one of the most perilous malware with the ability to produce immense physical damage. However, a minor error in the malicious code prevented the plant from the planned destruction [DPDC18, Slo19].

Industrial control system (ICS) is a general term that encompasses a combination of control systems, equipments, networks and operations involved in industrial processes [SFS11]. There are many characteristics which are kept at precedence while designing an ICS. These characteristics include timed performance, availability, communications, reliability and safe usage. Moreover, ICS deals with sensitive applications like a reactive chemical process, high temperature furnaces, high voltage devices, cutting machines, high pressure operations, burners. All of these characteristics and applications makes an ICS extremely sensitive. If these control systems are compromised, they pose a very serious threat for occupational safety and health. Therefore, a high security implementation is required, which not only maintains the system integrity during normal operation but also in the event of a attack [SFS15].

With the advancement in technology, many of IT capabilities become part of ICS. ICS manages the physical, real-world devices and IT deals with the data to maintain communication among these devices. Prevalent automation and computerization have introduced many security implications in ICS. An evolved system pays the price in terms of malware propagation and some unusual attacks. [GH12, Zha10].

The involvement of real-time equipment management in ICS puts a great emphasis on safety, security and quality of services of such systems. It is a matter of imperative concern how Industrial control systems can be secured. There are several techniques when a malicious intruder can attack and compromise the security of ICS. The attacker can intercept the protocol frames involved in ICS, exploit the weakness in software or can utilise other data frames connected with ICS [LSB+17]. All security devices and mechanisms (such as networking and communication system, protocols, software) involved in ICS are of great importance. For this reason, we are always interested in the security analyses and testing of the existing mechanisms used for industrial communication and monitoring [KG13].

One of the important aspects in an industrial control system is functional safety. Functional safety is an integral part of ICS and kept at precedence. A safety function is a "function of a machine whose failure can result in an immediate increase of the risk(s)" [fSC10]. Functional safety is defined as the "part of overall safety that depends on a system or equipment operating correctly in response to its inputs" [C+08]. In an industrial system, the proper functioning of equipment is very essential. Any small error or negligence in the communication between devices and their control equipment could lead to an immense hazardous situation and effects the reliability of the system. Functional Safety flow diagram is described in the following figure:

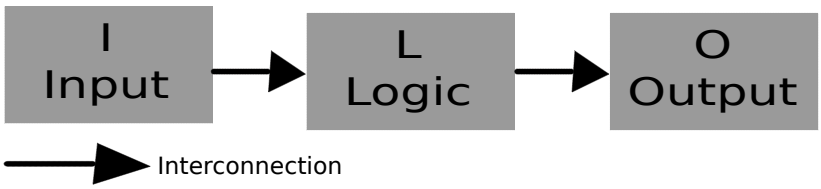

Figure 1: Functional Safety Flow Diagram [HSA+19]

Several networking protocols are designed to control industrial devices. These protocols

in particular deal with the safety devices such as safety switches, sensors, light curtains, laser scanners and pressure sensitive mats. PROFIsafe is an open standard protocol introduced by PI developers used in safety applications. [Zur14, BRS09] PROFIsafe is based on "Black Channel" principle. Black Channel principle allows the communication of failsafe and standard data via same network. The safety protocol is tunnelled with the underlying network. Safety devices can transmit their message using safety protocol. [RF11]. The communication model is depicted as:

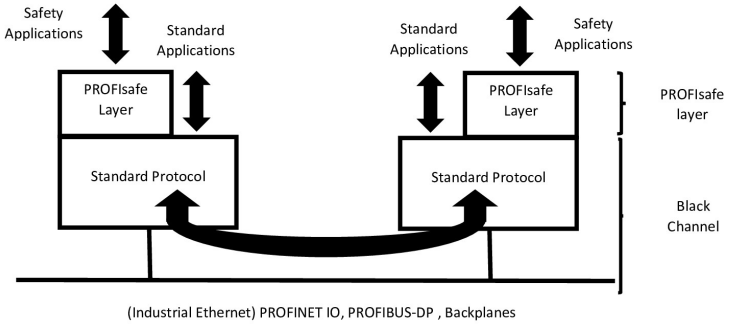

Figure 2: Black Channel Approach [RF11]

In this thesis, we analyse the security related measures of the safety protocol "PROFIsafe".

1. Motivation

The ICS structure stands on the safety and reliability of its components and equipments. However, the migration of industrial systems towards communication technologies and open protocols have introduced new breaches and backdoors in the ICS, impacting its safety and reliability. Since, for a safe and secure industrial system every component is required to be analysed and secured. In this thesis, we will investigate one of the open source functional safety protocol used in ICS. We will try to find the backdoors and flaws in the protocol which can be exploited to make an ICS vulnerable and insecure.

- The industrial control system can be accessed by unauthenticated adversaries.
- PROFIsafe is one of the safety protocols used by ICS.
- The structure of PROFIsafe needs a thorough study so that it can be analysed to evaluate its strengths and weaknesses against attacks.

2. Questions

In this thesis we will address following major questions:

- What knowledge about the attacks on industrial networks-especially PROFIsafe is available?
- What are the principles of the PROFIsafe protocol and what is the common relation to other protocols?
- What are the core specifications of PROFIsafe that may impact the system integrity?
- What limitations exist in industrial communication protocol?
- How can we attack the system using PROFIsafe as safety protocol?
- What are the possible attacks?
- How can we prevent the system from a specific attack?
- How secure are the existing communications protocols (in particular PROFIsafe)?
- Can the security model of the protocol (PROfisafe) be compromised?

3. Objectives

The aims of this research work are:

- Initially, the ICS protocol will be studied and analysed.
- Protocol specifications will be analysed and work flow will be understood.
- Protocol workflow and communication model will be monitored, and packet flow will be examined using Wireshark plugin.
- The third objective is to find the weakness in protocol specification or in communication flow which may debilitate the protocol design and endanger the system security.
- The next objective will be to examine the integrity of the protocol. For this purpose we will try to attack the protocol using one or two methods, such as packet manipulation or making use of a fake sequence number.

- The results from our research work will be a set of safety suggestions and recommendations improving the security between safety applications.
- During this, I would like to participate in security conference. This will allow myself to keep up-to-date with the latest research in the security field.
  - SECCAMP COLOGNE
  - RUHRSEC
  - FrOSCon

4. Theory References

The following are some books and literature that are helpful to understand Industrial Control System and communication protocols:

- Richard Zurawski. Industrial Communication Technology Handbook, Second Edition, ISA Group, San Francisco, California, USA.
- J. Rofár and M. Franeková. FUNCTIONAL SAFETY SPECIFICATION OF COMMUNICATION PROFILE PROFISAFE, Department of Control and Information Systems, Faculty of Electrical Engineering, University of Žilina, Univerzitná 1, 010 26 Žilina.
- Gerhard Goos, Juris Hartmanis and Jan van Leeuwen. Computer Safety, Reliability, and Security, 28th International Conference, SAFECOMP 2009 Hamburg, Germany, September 15-18, 2009.
- PROFIsafe System Description Technology and Application, PROFIBUS and PROFINET International Support Centre.
- DACFEY DZUNG, MARTIN NAEDELE, THOMAS P. VON HOFF AND MARIO CREVATIN. Security for Industrial Communication Systems, PROCEEDINGS OF THE IEEE, VOL. 93, NO. 6, JUNE 2005.
- Safety Technology for PROFIBUS and PROFINET,PROFIsafe, PROFIBUS and PROFINET International Support Center. PROFIBUS Nutzerorganisation e.V. (PNO), Germany.

5. Method

We will utilise two tools which are robust and well known in the industry to evaluate the design and strength of the industrial protocol. They will be leveraged to orchestrate an attack and analyse its response. The following strategies will be adopted:

- Wireshark, to monitor the packet flow strategy of the protocol and analyse its structure.
- Some penetrations software (such as SCAPY, NMAP) to attack the protocol and test its security portfolio.

6. Evaluation Strategy

To evaluate the results, a qualitative analysis will be performed. Safety communication protocol holds some safety measures or checksum (defined by ICE-61784-3) for a secure and successful transmission. These safety measures include repetition, deletion, insertion, sequence number, data corruption, delay, masquerade and loop-back of messages [RF11].

These characteristics will determine the functionality and strength of the protocol. We will observe the impact of the attack on these safety parameters and control system. The results will be deduced by the reaction of the system and that will lead us to conclude whether the system is secure and robust when under attack.

A. Thesis Outline

1. Chapter 1: Industrial Control Systems
2. Chapter 2: Industrial Control Systems Networking Protocols
3. Chapter 3: PROFIsafe Protocol
4. Chapter 4: Analysis of PROFIsafe Protocol Architecture(Wireshark Plugin)
5. Chapter 5: Attacking the Protocol
6. Chapter 6: Conclusion

B. Tasks and Time Distribution

	Task	Time(weeks)
1	Protocol Introduction and Understanding	2 Weeks
2	Examine the Protocol Architecture(PDU and packet flow) using Wireshark	7 weeks
3	Presentation (Conference)	1 week
4	Attacking and Result deduction	4 weeks
5	Thesis Writing	5 weeks

C. References

References

[BRS09] Bettina Buth, Gerd Rabe, and Till Seyfarth. *Computer Safety, Reliability, and Security: 28th International Conference, SAFECOMP 2009, Hamburg, Germany, September 15-18, 2009. Proceedings*, volume 5775. Springer, 2009.

[BSI14] The state of it security in germany 2014. 2014.

[C+08] International Electrotechnical Commission et al. Iec 61508 second edition: Functional safety of electrical/electronic/programmable electronic systems. *Committee Draft for Vote (CDV)*, 2008.

[Cob15] Pamela Cobb. German steel mill meltdown: Rising stakes in the internet of things. *IBM Security Intelligence Blog*, 14, 2015.

[DPDC18] AC Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. Triton: The first ics cyber attack on safety instrument systems. In *Proc. Black Hat USA*, pages 1–26, 2018.

[fSC10] European Committee for Standardization (CEN). Safety of machinery–general principles for design–risk assessment and risk reduction, 2010.

[GH12] Brendan Galloway and Gerhard P Hancke. Introduction to industrial control networks. *IEEE Communications surveys & tutorials*, 15(2):860–880, 2012.

[HF+18] Kevin E Hemsley, E Fisher, et al. History of industrial control system cyber incidents. Technical report, Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.

[HSA+19] Michael Hauke, M Schaefer, R Apfeld, T Boemer, M Huelke, T Borowski, K-H Büllesbach, M Dorra, HG Foermer-Schaefer, J Uppenkamp, et al. *Functional safety of machine controls: application of EN ISO 13849*. DGUV/IFA, 2019.

[KG13] Maryna Krotofil and Dieter Gollmann. Industrial control systems security: What is happening? In *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, pages 670–675. IEEE, 2013.

[LAC14] Robert M Lee, Michael J Assante, and Tim Conway. German steel mill cyber attack. *Industrial Control Systems*, 30:62, 2014.

[LSB+17] Anil Lamba, Satinderjeet Singh, Singh Balvinder, Natasha Dutta, and Sivakumar Rela. Mitigating cyber security threats of industrial control systems (scada & dcs). In *3rd International Conference on Emerging Technologies in Engineering, Biomedical, Medical and Science (ETEBMS–July 2017)*, 2017.

[RF11] Jan Rofar and Maria Franekova. Functional safety specification of communication profile profisafe. *Advances in Electrical and Electronic Engineering*, 5(1):158–161, 2011.

[SFS11] Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ics) security. *NIST special publication*, 800(82):16–16, 2011.

[SFS15] Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ics) security. *NIST Special Publication Revision 2*, 800(82):16–16, 2015.

[Slo19] J Slowik. Defense informs offense improves defense: How to comprom. In *In Depth Security Vol. III: Proceedings of the DeepSec Conferences*, volume 3, page 183. BoD–Books on Demand, 2019.

[Zha10] Peng Zhang. *Advanced industrial control technology*. William Andrew, 2010.

[Zur14] Richard Zurawski. *Industrial communication technology handbook*. CRC Press, 2014.