Analysis of the feasibility of remote access to industrial wireless networks by means of VPN

Rodolfo Bruno Hecht, Max Feldman, Tiago Rodrigo Cruz, Ederson Ribas Machado, Ivan Müller
Electrical Engineering postgraduate program
Universidade Federal do Rio Grande do Sul
Porto Alegre, Brazil
rodolfo.hecht@ufrgs.br, max.feldman@ufrgs.br, tiagorcruz1@gmail.com, edersonrmachado@gmail.com, ivan.muller@ufrgs.br

***Abstract*—Many types of industries require their plants to be geographically located at distant points from the headquarters that control their administrative operations. For example, basic industries such as mining, oil and gas and energy, which transform raw materials for use in other processes, usually have their facilities close to primary sources, imposing the need to implement a remote monitoring strategy. This work presents a remote interconnection solution between a field device of a wirelessHART network and a remote operator collecting related latency data, at the time of its measurement, in a secure and reliable way through the use of a virtual private network on the Internet. Measurements were performed at regional and international locations and statistical comparisons of the results were performed.**

***Keywords*—virtual private network, industrial remote monitoring, network control systems, industry 4.0**

I. Introduction

Currently industrial plants and processes are experiencing the introduction of new technologies brought by industry 4.0. Traditional production and manufacturing models and methods will undergo a [1] transformation, where all the aforementioned emerging technologies will make use of information and communication technologies to connect all subsystems, internal and external processes, suppliers and customers, of so that the exchange of information permeates the entire value chain by building a huge database (Big Data) and cloud computing [2]. Considering the arguments presented above, industry 4.0 is essential to overcome the challenge of industrial communication [3].

The expected impact on industry productivity is comparable to that provided by the Internet in several other fields, such as e-commerce, personal communications and banking transactions [4]. Thus more and more these interactions allow exchange information and / or make decisions autonomously, a paradigm that extended to the industrial environment and the entire production chain [5].

Remote access to industrial equipment is defined as the ability of an organization's users and operators to access its physical resources, data and private systems that reside on a physically or logically protected network from external networks that must be considered from outside the organization [6].

Remote access solutions usually need to support multiple security objectives, and the most significant are [6], [7]:

- Confidentiality;
- Integrity;
- Availability.

This work uses an implanted VPN architecture from a software defined network (SDN), considering aspects of authentication, encrypted transmission and reception of data and creation of invisible tunnel, within the means of Internet communication. VPN technology is widely used in corporate environments [8] The VPN established by an SDN has the advantage of not requiring a specific server to create access rules, authentication, and maintain communication. All VPN tasks are performed by rules of software-defined network. In this context, this work focuses on studying the latency behavior of a *wireless*HART (WH) network being accessed remotely.

II. Methodology and Implementation

An overview of the set of methods and materials used in the development of this work, as well as their implementation are presented in this section.

A. View of the remote connection environment

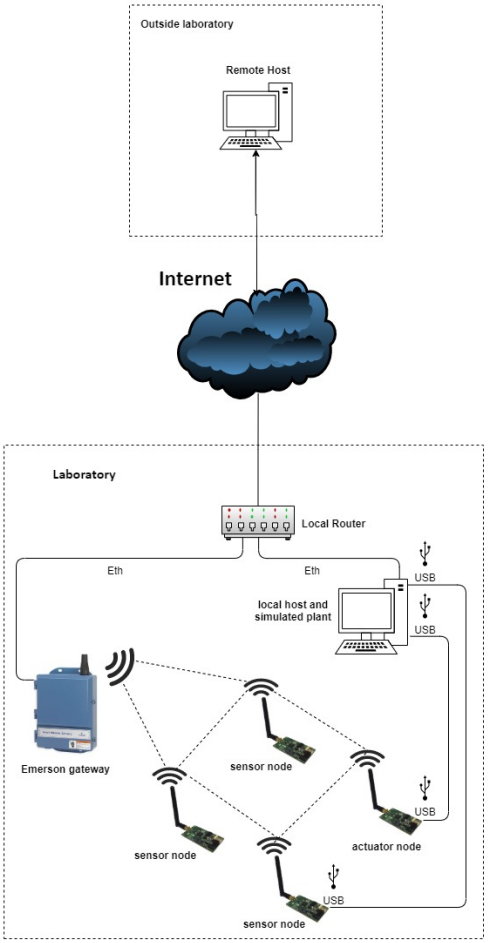
The total network architecture considered in this work can be divided into two parts: the internal network of the plant and the external network, and both are connected to each other through the Internet. The internal network is composed by WH field devices communicating with an industrial gateway, which is, besides gateway, network and security manager and access point to the field devices. The gateway is used in a laboratory environment for industrial automation research.

The gateway uses the HART command standard to transmit and receive information from the *field device* (FD), field devices that act as sensors or actuators in the plant. The equipment used has one of its Ethernet ports connected to a local network, and in this one, the device that acts as a local host (PC) is connected. This *host* has USB ports available to connect to some of the FDs, which emulate sensors and actuators of a simulated plant in order to simulate a NSC. A VPN interconnecting the local and remote *host* provides the necessary connectivity so that the remote *host* can communicate with the gateway, and consequently with the FDs. Through this architecture the remote *host*, in any geographical

position, distant from the laboratory, can communicate with the gateway and the FDs connected to it.

An overview of the proposal of this work can be obtained by the analysis of Figure 1, where the main components of the architecture can be seen.

Figure 1: Proposal overview



Source: author

B. Latency capture strategy

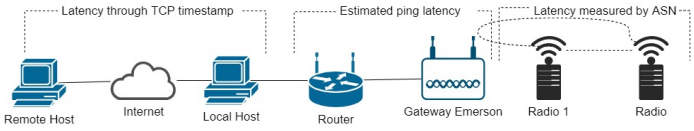
To capture the end-to-end latency measured between the remote host to the gateway and the FD devices it was chosen to separate the measurements into three steps with independent measurements:

- perform latency measurements between remote host and local host - VPN latency;
- perform latency measurements between local host and gateway - local network latency;
- perform latency measurements between gateway and connected FD - WH latency.

Fig. 2 reveals how the latency capture strategy was considered.

This strategy was necessary because some components of the remote interconnect use different means of connection and communication protocols.

Figure 2: Latency capture scheme *one-way*



Source: Author

C. Specifying the elements of the environment

The devices used in the experiment, in summary, are detailed below:

- **Gateway**
  The commercial device Emerson Wireless 1420A gateway [9] performs the role of Network Manager, gateway and access point of the network.
- **Field devices** The field devices were prepared in the laboratory, and are WH compatible radios and are composed of a Freescale MC13224 microcontroller, an integrated IEEE 802.15.4 radio transceiver and several peripherals responsible for other features necessary for a WH device. To analyze the latency of the devices' end-to-end communications, it was necessary to change the firmware previously developed [10], something that was only possible due to the access to the WH protocol stack. To adapt the firmware, making the changes in these radios, the IDE IAR tool Embedded Workbench 5.4 was used. These modifications were already useful in carrying out the work of [11]. The modifications in firmware allow obtaining the Absolute Slot Number (ASN) of the messages that arrive and leave the device, both in uplink and in downlink.
- **Local and remote host** The local and remote hosts have Ubuntu 20.04.1 LTS 64-bit operating system.
- **Router** The wireless router supports the 802.11b&g standard based on 802.11n technology and offers 802.11n performance of up to 150Mbps [12].

D. Physical interconnection for remote access

The elements required for remote access interconnection are detailed below.

1) Physical-logical connection establishment between local "host, router and gateway: .

The connection from the local host to the gateway occurs through a physical link with UTP cable (unshielded twist pair) connected to the router's switch ports forming the local network.

The local and gateway are configured with IPv4 addresses known, fixed and registered in the DHCP service (Dynamic Host Configuration Protocol) of the router, facilitating the search of the remote host and the forwarding of packets on the local network. The router establishes Internet access via its named WAN (*Wide Access Network*) port with a UTP cable connection to the local network.

2) Local host - Remote host connection establishment: The remote *host* and the local *host* are connected over the internet via a VPN. This VPN sets up a logical interface between the *hosts* that will contain an IP address assigned to each *host*

providing data communication, authentication encryption and communication.

3) Connection Establishment of FD to Gateway: The connection between FD and gateway occurs over the WH network.

E. Preparing the remote access environment

The environment encompasses setting up a "continuous" communication path between a remote *host* to a gateway and the connected FDs. In this way the remote access environment is prepared with the VPN installation. For latency collection two scripts were developed in Python language, one installed in the remote *host* and the other installed in a local *host*. These applications are responsible for forwarding commands from the remote *host* to the local *host*, the gateway and the interconnected field devices. The local *host* and gateway respond with the capture values of the times in the sections of this communication. At the end, the script installed on the remote *host* consolidates the latencies of the entire path on the remote *host*. A third script was developed to send a read command, remotely, of a process variable of a FD.

1) Establishment of VPN for interconnection host local-host remote: The creation of the VPN is performed through access to the website of ZeroTier platform [13]. Each remote host and also the local host need a specific configuration to register the *NetwokID* (VPN name determined on the ZeroTier platform), and incorporates authentication and communication encryption, and, furthermore, it creates a logic board on each host that will contain an IP address assigned within the VPN address range created. The remote host participates in a VPN network with a class and range of IP addresses different from the local network, so these networks do not communicate with each other. To overcome this obstacle it is necessary to apply some changes to the *iptables* module of the local host operating system. To forward the VPN traffic to the LAN, a special configuration was made on the local host by changing instructions in the iptables control, activating the Network address translation (NAT) service and the service Masquerade from the local host linked to the gateway. The remote connection method using a VPN tunnel will allow you to link the host through the internet and treat them as if they were in the same place. The VPN used in this work uses an SDN operation platform. SDN technology is relatively new and its attraction is to provide a dynamic network structure whose existence is entirely composed of software.

2) Configuration of remote host and local host: Both the remote host and the local host must have Python version 3 or higher. Complementing the preparation of the host, it is necessary to install the modules numpy, socket, time, struct, os, datetime and reduce.

To obtain an equality in the clock of the hosts we use a synchronization with an NTP server (Network Time Protocol) that offers reliable time references [14].

The preparation of remote host and local host to join the VPN is performed with the following operations performed through an Ubuntu console terminal according to ZeroTier's instructions for VPN client installation.

After installing and configuring the VPN client, we need to obtain a ZeroTier address and perform the join operation that will make the junction in the VPN network, always through an Ubuntu console terminal according to ZeroTier's instructions.

The remote host and the local host are already recognized by the VPN, but they need to be authorized to transmit or receive communications.

3) Latency capture scripts: To verify the feasibility of using it in monitoring and control systems as the events occur remotely, with NCS as local controller or even remote, and analyze the latency of this communication, two scripts were developed in Python language that perform all the functions of capture and consolidation of latency values at each measurement performed. These scripts perform all the functions of sending commands to the NCS, capture and consolidate the latency values.The two scripts developed in Python act together from the latency act as follows:

- Main script - installed on the remote host;
  - Send command 814 (inform active FD) to the gateway to confirm continuity of communication;
  - Selects FD for capturing latency samples in communication;
  - Synchronises the clocks of the local host and remote host via a worldwide server offering the Network Time protocol;
  - Captures the time from the remote host clock and requests the value from the local host clock for measuring the latency of the stretch;
  - Requests the tempop value of the "ping"command between local host and gateway for measuring the latency of the stretch;
  - Requests latency between gateway and FD within the WH network;
  - Receives the consolidated latency values.
- Secondary script - installed on the local Host;
  - Responds to the connection requested by the main script;
  - Ssynchronises the local *host*'s clock with an NTP server;
  - Collects the synchronized clock time from *host* and forwards it to the main script;
  - Performs the estimation of the latency value between local *host* and gateway and sends to the main script;
  - Forwards the collected data to the main script, waiting for the next request.

The sequence of the latency capture operation is shown in Figure 3.

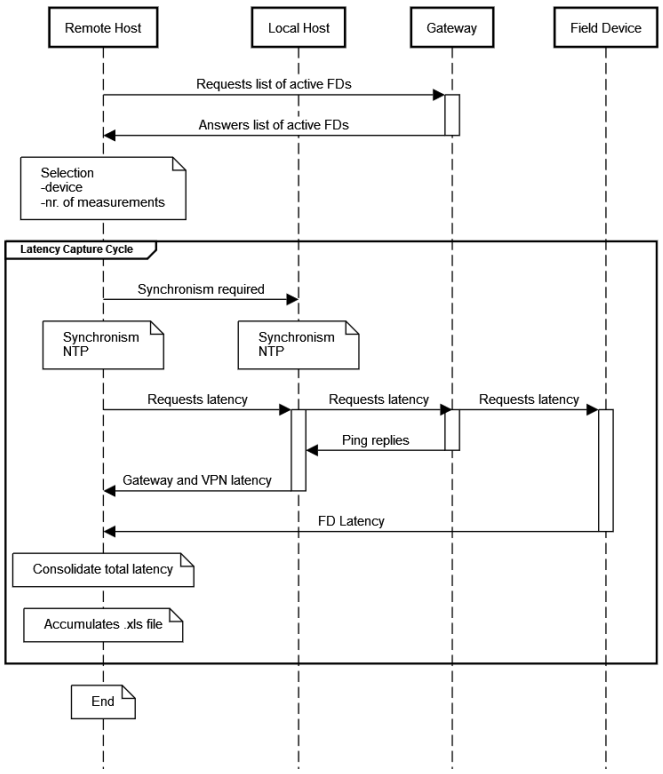
F. Consolidation of latencies

The stretchs analyzed to obtain the end-to-end total latency are treated as follows:

1) Remote Host - local host: At each collection cycle, the main script executes the difference between the value collected in the time.time() command between the remote host and the local host and through the difference in times we obtain the latency of the representative stretch of the VPN.

2) Local Host - gateway: At each collection cycle, the main script receives from the script installed in the remote *host* the latency estimate of that stretch in milliseconds through the

Figure 3: Sequential diagram of end-to-end latency capture



Source: Author

calculation of half the time obtained by executing the *ping* command directed to the gateway IP address. The use of the *ping* command was necessary to estimate the latency in the stretch *host* local and gateway, since the gateway does not allow running a script, internally.

3) gateway - Field Device: Between the gateway and the FD, the connection takes place using the WH communication protocol. To obtain this latency, the strategy described in [15] was used, through the analysis of the difference between the ASN value obtained in the gateway and the FD ASN during the execution of a WH command.

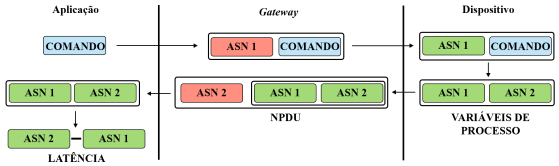
A modification was made to the FD's firmware so that they can receive commands directly from host through script, which are normally restricted to the network manager and the gateway, and so on get the ASN values was done. The main script receives the ASN values and calculates the latency between the FD and the gateway from the difference of the collected ASN values, multiplying by a coefficient of 10 milliseconds, relative to the *interval slot*, and getting the latency value between gateway and FD.

Finally, at each capture cycle, the latency between the gateway and the modified FD is obtained using two modified WH commands, 130 and 131, which respond with the ASN values of the gateway and the FD forwarding to remote host for consolidation.

The modified commands get the assigned values of ASN0 obtained on arrival of the command to gateway and the values of ASN1 on arrival of the command to the destined FD.

In Figure 4 explains the method to determine the latency value using ASN values.

Figure 4: Method to determine WH latency one-way

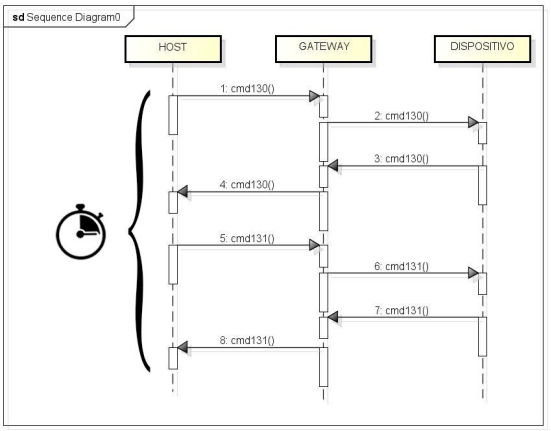


Source: [15]

As each slot has a predetermined time of 10 ms, this metric was used to obtain the latency between gateway and FD by multiplying the value found between the difference of ASN0 and ASN1 multiplied by 10 ms. Thus, a part of the script implemented on the remote host used the latency capture stretch between the gateway and a chosen FD.

Figure 5 demonstrates how the WH latency one-way is obtained.

Figure 5: End-to-end WH latency cycle



Source: [15]

III. Case Study

This chapter presents the results of the experiments carried out together with the details of the latency analysis and statistics obtained in the measurements.

A. Experiment

In order to evaluate the performance of the proposed technique, a remote access experiment was designed and executed in a real WH network to quickly collect total latency data and analyze their differences and the possibility of exercising supervision and control. The objectives of the experiment are:

- verify if there is a significant difference in the latency measurements of a remote access performed directly within the industrial local network directly connected to the industrial gateway when compared to the external remote access, in a regional, national or international location;
- determine which component stretch of the total latency measurement in remote access of an industrial network has the greatest significance.

- verify the effect of the total latency measures with the alteration of the WH network topology, imposing to a certain FD an indirect communication route with the gateway.
- demonstrate the reading of a variable of a FD within the WH network, through several simultaneous remote accesses, enabling multiple remote supervision of the WH network.

The experimental bench used includes the following equipment:

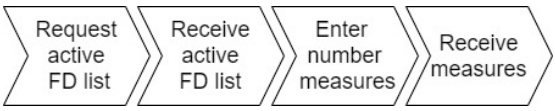
- Five radios that act as field devices with the firmware modified so that it accepts special commands 130 and 131 in order to capture and transmit the ASN values in order to consolidate the latency value within the WH network for the proposed technique ;
- a computer to act as the local host and to perform the local latency collections, and the gateway.

To support the objectives listed, a script to capture latencies was performed at the locations below:

- Brasil - Porto Alegre - Neighborhood Mont Serrat;
- Chile - Santiago - Universidad de Concepcion;
- Alemanha - Magdeburg - Saxônia-Anhalt

The operation of script is described in a simplified way in Figure 6.

Figure 6: Script operation



Source: Author

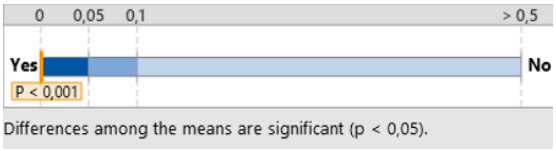
100 latency measurements were made within the laboratory and, successively, another 100 measurements from the remote locations available for analysis of this work.

B. Case study - Analysis of measured latencies in remote access

An analysis of variances (ANOVA - Analysis of Variance) considering "local" as a controllable factor and the analysis of the response "total latency" allows us to assess the significant differences. Through the concept of statistical inference, it can be stated that the measurements obtained represent the characteristics of this type of measurement in the localities. A hypothesis test supports the proposed objective and checks whether there is a significant difference in the measures of local latency with direct access to the WH network and remote accesses. In statistics, it is understood that the statistical power of a hypothesis test is the probability of rejecting H_0 when H_0 is false [16].

For this experiment, the null hypothesis is to confirm that all means in the locations are equal, while the alternative hypothesis is that not all means are equal. A significance level (denoted as α or alpha) of 0.05 is usual. A $P - value \leq \alpha$ means that the differences between some of the medians are statistically significant [17]. Analysis of variance shows that value-$P = 0$ is less than α. This is well evidenced in Figure 7.

Figure 7: Análise de significância



Source: Author

To assist in this task, the Minitab statistical software was used. Minitab calculates, from information on variability and desired statistical power, how large the sample must be for a test with its specified power to detect each difference found. Since sample sizes are whole numbers, the actual power of the test may be slightly larger than the power value specified. So by increasing the sample size, the power of the test will also increase [17].

Results

Statistical analysis using an ANOVA resulted in the P value being equal to zero.

The significance analysis allows us to affirm that there are significant differences between the means of the total latency measures in all locations.

An analysis of the statistical power of the results ensure that the number of measurements was sufficient to support the results found.

The analysis of variance and statistics values in the I table support the estimation of statistical power for the 100 measurements performed at each location.

Table I: 100 measurement statistics

Local	*Measurements*	*Average[ms]*	*S.D.[ms]*
BR-Porto Alegre-Lab.	100	1146,3	674,4
BR-Porto Alegre-Home	100	1423,9	795,5
CL-Univer. Conception	100	1711,3	803,0
DE-Magdeburg	100	1951,7	891,0

The square root of the root mean square error (631573) estimates the maximum difference between the measurement means is 794.72. In the I table, it is observed that the largest standard deviation between the locations is DE-Magdeburg with 891.0 ms, so this is the value chosen for the maximum difference in the calculation of statistical power.

Table II: ANOVA 1 factor α = 0.05 - Assumed S.D. = 794.72

Maximum difference	*Sample Size*	*Power*
891,0	100	0,981292

With 100 measurements, the obtained statistical power of 98.1% was obtained, as shown in the table II, confirming an adequate statistical power to define the existence of significant differences in the averages obtained in the measurements of the different locations.

***- Results*:** As a result, it is possible to declare that the value of P is equal to zero, that is, less than the significance level (α), concluding, with 95 % confidence, and 98% statistical power, that the geographic location of the remote access significantly affects the end-to-end total latency response variable, measured in milliseconds.

C. Case study to determine most relevant latency stretch

For this determination, the averages of the stretches that make up the calculation of latency in each sample were calculated, that is, the latency between host remote and local, between host local and gateway and between gateway and measured FD.

Table III: Latency averages stretch-by-segment

Measured stretch	***Measurements***	***Average[ms]***	***S.D.[ms]***
Latency gateway-FD	400	1422,3	811,2
Latency host local-gateway	400	0,26	0,037
Latency host remote-local	400	135,7	167,5
Latency total	400	1558,3	847,7

***- Results*:**

The table III where the averages of each stretch that make up the total latency are displayed, it can be seen that the value measured within the WH network represents 92.5% of the total average latency measured and shows to be this stretch is the most significant in the composition of the total end-to-end latency of remote access to an industrial network.

IV. Conclusion

The work presented was motivated by one of the main needs of industrial networks, that is, to carry out the control and monitoring of industrial networks in a safe way, analyzing their latency scenarios when the network is accessed remotely. As a way to deal with this issue, a remote access using a VPN provided by an SDN environment was proposed, connecting a remote host installed geographically far from the industrial network, to an industrial gateway installed in a laboratory. The VPN provided by the SDN system eliminates the need to maintain server to support VPN establishment application. Case studies were presented with analyzes of remote access latency from several different geographic locations, national and international. One hundred end-to-end latency measurements were collected through a remote VPN access, connecting each location to the WH network installed in the laboratory.

The data collected served as the basis for the following conclusions:

Analysis of measured latencies in remote access.

Remote remote access on a WH network worked and can be analyzed using a statistical tool. It was an analysis of variance of the obtained measures concluding that, despite the success in establishing remote access in different locations, the average latencies have different intervals. This result indicates that it is possible to perform remote supervision and control in a WH network as long as the system to be controlled has latency times greater than the remote access latency intervals analyzed in each location.

Determination of the most relevant latency stretch

In the analysis of variance, it was concluded that the means of latency measures are different in each location. From this conclusion, an analysis was made in the sums of the total means obtained to determine which stretch could impose the different analysis of variance in each location. It was noticed that the latency between gateway and FD represents 92.5% of the total means. However, latency between remote host and local host, ie remote access by means of VPN has an impact of 8.7% on latency. This section is responsible for the result of the analysis of variance indicating that there are no equal means.

This work concludes that knowing the latency time intervals to perform a remote access to sensor devices and actuators in industrial WH networks, it is possible to design control systems that can be remotely supervised and controlled. Future works will be able to design a remotely operated control system writing and reading FD variables of a WH network considering the latency parameters for each location that is accessed remotely.

Referências

[1] C. B. SILVEIRA, "O que é indústria 4.0 e como ela vai impactar o mundo," *Acesso em*, vol. 15, 2016.

[2] A. L. M. Carmona *et al.*, "Análise dos impactos da indústria 4 na logística empresarial," 2017.

[3] G. Geampalia, F. Hartescu, O. Chenaru, and G. Florea, "Communication technologies for complex industrial systems," in *2017 21st International Conference on Control Systems and Computer Science (CSCS)*, May 2017, pp. 401–405.

[4] J. R. Hahn Filho, "A era da internet industrial e a indústria 4.0," *Produção em Foco*, vol. 6, no. 3, 2016.

[5] A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the internet of things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, 2016.

[6] M. Souppaya and K. Scarfone, "Guide to enterprise telework, remote access, and bring your own device (byod) security," National Institute of Standards and Technology, Tech. Rep., 2016.

[7] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," *IEEE Access*, vol. 2, pp. 1149–1176, 2014.

[8] C. Systems. (2021, Jan.) What is a vpn? - virtual private network.

[9] Emerson. (2020) Process management, gateway smart wireless.

[10] I. Müller, J. M. Winter, C. E. Pereira, and J. C. Netto, "Wirelesshart fast collect: A decentralized approach for intermittent field devices," in *2013 11th IEEE International Conference on Industrial Informatics (INDIN)*, July 2013, pp. 254–259.

[11] C. A. Krötz, "Ferramenta e método para obtenção de parâmetros de confiabilidade fim-a-fim de redes industriais sem fio," Dissertação de Mestrado, Universidade Federal do Rio Grande do Sul, 2019.

[12] TP-Link. (2020) Roteador wireless n 150mbps.

[13] Z. Inc. (2020) Zerotier manual.

[14] NTP.BR. (2021, Jun.) O ntp.

[15] C. A. Krötz, G. P. Cainelli, G. Kunzel, M. Feldman, C. E. Pereira, and I. Muller, "Tool and method for end-to-end reliability analysis of wireless industrial networks." 2019.

[16] D. C. MONTGOMERY and G. C. RUNGER, "Estatística aplicada e probabilidade para engenheiros, 2ª," *Edição. Rio de Janeiro: Editora LTC*, 2003.

[17] Minitab LLC. (2021, Jun.) Interpretar todas as estatísticas e gráficos para poder e tamanho de amostra para teste t pareado.