http://journal.unoeste.br/index.php/ce/index
DOI: 10.5747/ce.2020.v12.n2.e318
ISSN on-line 2178-8332

Colloquium Exactarum

Submetido: 20/06/2020 Revisado: 24/08/2020 Aceito: 09/09/2020

MODELING AND VALIDATING A SECURE INTERCONNECTION BETWEEN INDUSTRIAL CONTROL SYSTEM AND CORPORATE NETWORK USING COLORED PETRI NET

MODELAGEM E VALIDAÇÃO DE CONEXÃO SEGURA ENTRE O SISTEMA DE CONTROLE INDUSTRIAL E A REDE CORPORATIVA UTILIZANDO REDES DE PETRI COLORIDA

Adriano Borrego[1]; Adilson Eduardo Guelfi[2]; Anderson Aparecido Alves da Silva[3]; Marcelo Teixeira de Azevedo[4]; Norisvaldo Ferraz Jr[4]; Sergio Takeo Kofuji[4]

[1]IPT. Departamento de Engenharia da Computação, São Paulo, SP. [2]Universidade do Oeste Paulista – UNOESTE, Presidente Prudente, SP. [3]IPT/UNIP/SENAC/USP. Departamento de Engenharia da Computação, São Paulo, SP. [4]Universidade de São Paulo – USP, Departamento de Engenharia Elética, São Paulo, SP
E-mails: a.borrego@gmail.com; guelfi@unoeste.br, anderson.silva@pad.lsi.usp.br, marcelo.azevedo@pad.lsi.usp.br; norisjunior@gmail.com; kofuji@usp.br

ABSTRACT – Industrial Control Systems (ICS) networks offer a high level of automation combined with high levels of control, quality, and process improvement. Since network corporate users have to access the ICS environment, these networks have to be interconnected. However, this interconnection can introduce risks to the systems and manufacturing processes, which leads to the need to ensure the interconnection is done safely. The objective of this paper is to perform modeling and validation of a proposed secure interconnection between ICS and corporate networks using Colored Petri Networks (CPN). In addition to the best practices published in related works, this paper recommends some integrated features like the use of terminal server service, secure manual uplinks, and unidirectional security gateway to enhance environmental security. However, our main contribution is the validation process performed in a CPN, which made it possible to execute queries in the state space resulting from the simulation - that works as a proof of concept. As a result, the paper presents a secure and validated model of interconnection between ICS and corporate networks, capable of being applied to any interconnection environment.
Keywords: ICS Network; Corporate Network; Secure Interconnection; Colored Petri Net.

RESUMO – As redes de sistemas de controle industrial (ICS) oferecem um alto nível de automação combinado com altos níveis de controle,

qualidade e melhoria de processos. Como os usuários corporativos da rede precisam acessar o ambiente ICS, essas redes precisam ser interconectadas. No entanto, essa interconexão pode apresentar riscos aos sistemas e processos de fabricação, o que leva à necessidade de garantir que a interconexão seja feita com segurança. O objetivo deste artigo é realizar modelagem e validação de uma interconexão segura proposta entre o ICS e as redes corporativas usando as Redes de Petri Coloridas (CPN). Além das práticas recomendadas publicadas em trabalhos relacionados, esta pesquisa recomenda alguns recursos integrados, como o uso do serviço de servidor de terminal, uplinks manuais seguros e gateway de segurança unidirecional para aprimorar a segurança do ambiente computacional. Entretanto, nossa principal contribuição é o processo de validação realizado em uma CPN, que possibilitou a execução de consultas no espaço de estados resultantes da simulação - que funciona como prova de conceito. Como resultado, o artigo apresenta um modelo seguro e validado de interconexão entre o ICS e as redes corporativas, capaz de ser aplicado a qualquer ambiente de interconexão.

Palavras-chave: Rede de Sistemas de Controle Industrial; Rede Corporativa; Interconexão Segura; Redes de Petri Colorida.

1. INTRODUCTION

After the automatization process, the industry is facing the irreversible reality of machines replacing people. The use of automated processes is, in many situations, more efficient compared to human operations. The network which interconnects several devices installed in the production areas and links manufacturing process, control devices and monitoring equipment is called Industrial Control Systems (ICS) Network. According to Alcaraz (2013), due to (a) lack of standardization and (b) security concern, historically, ICS networks were isolated without connection to public communication infrastructures, such as the Internet. But the need to remotely control and supervise critical industrial systems has brought the need for interconnection. Many industrial automation systems currently support an Ethernet connection standard, which facilitates interconnections between networks (YADAV; PAUL, 2019; (ZERDAZI; FEZARI, 2019).

For this purpose, updated and accurate information on the processes of the ICS networks is as vital as noted in Mahboob & Zubairi (2010). A possible way to protect the ICS, when the connection between corporate and ICS networks becomes necessary, is the interconnection based on the use of information security mechanisms and access control.

A set of best practices to assist in the interconnection between ICS networks and corporate networks is important.

Guides such as those offered by NIST (2015) help to create topologies to separate networks but do not provide a validation mechanism for the efficiency of the proposed environment. Concerning this deficiency, Colored Petri Networks (CPN) can assist in validating a real scenario. CPN is a mathematical and graphical tool that enables the modeling and analysis of parallel, concurrent, asynchronous, and nondeterministic systems and processes, characterized by discrete states that are abruptly changed by instantaneous events.

There are multiple papers suggesting possible topologies for interconnecting ICS and corporate networks, but few are concerned about validating the effective security of these interconnections. The objective of this paper was to perform modeling and validation of a proposed secure interconnection between ICS and corporate networks using CPN. After the introduction, this paper is divided into five other sections. The literature review presents the concept of the ICS network and the technical security requirements for interconnecting it to other networks and the concept of a CPN. The related works section presents comparisons between this paper and other related works. The proposal section shows the suggested interconnection topology between the ICS and corporate network, which will be validated in section 5, using CPN simulated in the CPNTools (2017). Section 6 presents a deeper comparison between this paper and NIST 2015, highlighting the main advantages of this paper and presenting the conclusions and considerations.

2. LITERATURE REVIEW

This section presents the concepts of the ICS network and the problems related to its security, the technical and security requirements for the interconnection between ICS and corporate networks, and finally, the concepts of a CPN.

2.1. ICS Network

According to NIST (2015), ICS is a generic term encompassing different types of systems and control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., production, transport, energy). These can be an automated or manual system. According to Knapp & Langill (2014), some of the components in ICS networks are sensors, actuators, motors, meters, indicators, and control systems such as PLCs, remote terminal units, among others. They provide a large amount of process data, which, if properly collected and processed, can provide important and accurate information on raw material consumption, energy expenditure, process time, and losses due to failures, which helps in the continuous improvement of industrial processes (WEI, 2007).

Many people misuse the terms ICS and Supervisory Control and Data Acquisition (SCADA). SCADA is one of the possible applications contained within the universe of applications and components of an ICS (AZEVEDO, 2017).

ICS is a set of resources that, to be used, should be interconnected by an ICS network. The ICS network is then the connecting platform for all ICS resources. According to Mahboob & Zubairi (2010), most of the time, companies use only one-level defense, which is insufficient to protect the environment. When interconnecting ICS networks to corporate networks, or even to the Internet, it is important to continue providing a level of security that enables mitigation of possible security breaches (STOIAN *et al*., 2014). Another problem is the lack of tests. Since it is designed for a special application, ICS Network-related software is not used on a large scale. By connecting industrial networks to corporate networks or the Internet, these vulnerabilities become exposed to potential attacks (MAHBOOB; ZUBAIRI, 2010; DONG *et al.*, 2007).

Considering the papers published by Stoian *et al*. (2014), Mahboob & Zubairi (2010), Wei (2007), and NIST (2015), corporate networks and ICS networks should be physically separated. The cabling of the ICS and the corporate networks should be physically separated and have no direct interconnection point. The logical interconnection between ICS networks and corporate networks should contain security controls, such as firewalls, manageable switches, and Intrusion Detection System (IDS). Also, it is desirable to reduce the use of wireless devices and the administrative rights on the equipment installed in the ICS network.

2.2. CPN

According to Murata (1989), Petri Net (PN) was created by Carl Adam Petri in 1962. This is a mathematical and graphical tool to model, analyze, and design parallel, concurrent, asynchronous, and nondeterministic systems and processes, especially those characterized by discrete states that are abruptly altered by instantaneous events. States that PN has stimulated the interest of industry and academy since the 1960s, and is one of the main ways to model systems based on discrete events (UEDA, 2012). The purpose of CPN is to reduce the size of the model, thus allowing the tokens to be individualized through the colors assigned to them, so different processes or resources can be represented in the same network. Colors can represent complex data types, using color nomenclature just to refer to the possibility of distinguishing between the tokens (JENSEN, 2013). According to Maciel (1996), the CPN is composed of three different parts. The first one is the **structure**, which is a directed graph with two types of vertices (places and transitions). Places are represented graphically by ellipses and transitions by rectangles. This representation inherits the characteristic of the original colored nets, which are able to store tokens of different types in each place, and the ability to represent values associated with more complex data types. The second part is the **declarations**, which are composed of the specification of color sets and variable declarations. The last part is the **subscriptions**, varying according to the network component. Places have three types of entries: names, color set, and initialization expression. Transitions have two types of inscriptions: names and expressions. Arcs have only one type of inscription given by the expression. As a way of distinguishing expressions, names are written in normal letters, colors in italic, initialization expressions underlined, and the guard function in square brackets.

3. RELATED WORKS

Works related to the interconnection between ICS and corporate networks had a smaller focus on a method for validating the security of this interconnection. Another topic that can be noticed is that, although there are written works on the importance of protecting ICS networks, and proposals showing how to carry out this activity, it seems they are not focusing on measuring and validating the effectiveness of the approaches concerning security or protection. Table 1 compares this paper with the main related papers described in this section. This comparison is based on ten special criteria: (1) DMZ networks acting as an intermediary network segment between corporate and ICS networks (DMZ); (2) terminal server for remote access to DMZ and ICS network devices (Terminal Service); (3) backup to protect ICS data and configurations (Backup); (4) physical security mechanisms for the ICS network (Physical Security); (5) security policy to protect and control access to ICS networks (Security Policy); (6) firewall to protect and isolate the ICS network segment (Firewall); (7) unidirectional security gateway to transfer data from the ICS network to the DMZ network (Uni. Sec. Gateway ICS --> DMZ); (8) secure manual uplink between the ICS network segment and the corporate network (Secure Manual Uplink); (9) access control to allow the use of the resources on both the ICS and DMZ networks (Access Control); and (10) validation of the topology using CPN (Validation).

It can be observed in Table 1 that only Coates *et al*. (2010) and NIST (2015) propose the use of backups to protect data and configurations. NIST (2015) and Alcaraz (2013) have the closest approach compared to this proposal. One difference is that NIST (2015) recommends the use of unidirectional security gateway between the corporates and ICS network while this paper does not recommend any type of direct communication between these two networks. Hence, the proposal of this paper

is to place the unidirectional security gateway between the DMZ and the ICS network, thus increasing security for the ICS network. Only Coates *et al*. (2010), Amoah *et al.* (2016), and Cárdenas *et al*. (2011) do not use a firewall as a required device.

Table 1. Works Comparison
(Y=YES/N=NO)-A=DMZ; B=TerminalService; C=Backup; D=Physical Security; E=Security Policy; F=Firewall; G=Uni. Sec. Gateway ICS ->DMZ; H=Secure Manual Uplink; I=Access Control; J=Validation

Works Features	Amoha (2016)	NIST (2015)	Stoian *et al*. (2014)	Alcaraz (2013)	Cárdenas *et al.* (2011)	Coates *et al.* (2011)	This Paper
A	N	Y	N	N	N	N	**Y**
B	N	N	N	N	N	N	**Y**
C	N	Y	N	N	N	Y	**Y**
D	N	Y	N	Y	Y	N	**Y**
E	N	Y	N	Y	N	N	**Y**
F	N	Y	Y	Y	N	N	**Y**
G	N	N	N	N	N	N	**Y**
H	N	N	N	N	N	N	**Y**
I	N	Y	Y	Y	Y	N	**Y**
J	Y	N	N	N	N	N	**Y**

Source: (Author, 2020).

The first main contribution associated to this paper is that it proposes a combination of the protection mechanisms used in related works, with existing features such as secure manual uplink, terminal server and the unidirectional security gateway between the ICS network and the DMZ, thus creating a more secure interconnection proposal compared to related works. It also offers a security validation over the interconnection topology, adding an extra level of reliability to the proposal.

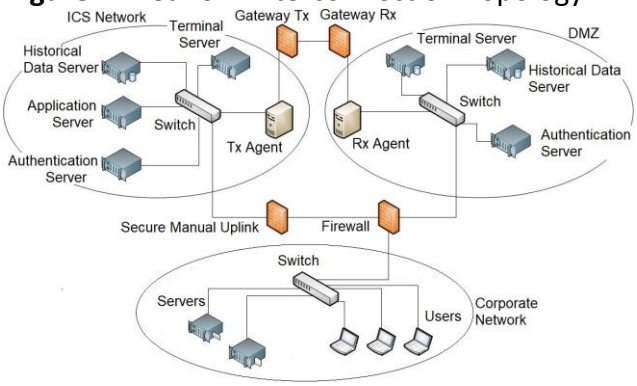
4. SECURE INTERCONNECTION PROPOSAL

Subsection 4.1 presents the secure topology for interconnecting the ICS and corporate networks and its security policy. Subsection 4.2 implements the secure connection topology in CPN.

4.1. Secure Network Interconnection Policy and Topology

Figure 1 presents the ICS and corporate network interconnection topology. In Figure 1, the DMZ, the corporate and the ICS network segments with the following main components: the firewall, the secure manual uplink, the unidirectional security gateway, the terminal servers, the historical data servers, the application server, and the authentication server are shown. A security policy defines who should or should not have access to an environment, equipment, systems, as well as the level of access this person should have. The interconnection between the three network segments is established through the firewall, where there are rules allowing or denying packages to flow.

Figure 1. Network Interconnection Topology.



Source: (Author, 2020).

The protection of the ICS network should not be limited to the logical portion only. It is important to ensure that there is a physical separation among all networks and that access to the physical network is limited to authorized people only.

The use of a DMZ network is strongly recommended to mitigate the risks associated with the ICS network. The DMZ creates an additional layer of access security, preventing critical and sensitive data from being accessed directly from the corporate network. Access attempts originated from the corporate network should be directed to the DMZ network, thus not allowing direct connection to the ICS network.

Only authorized users should be able to access the ICS network, always originating the connection from the DMZ network. Additionally, to access the ICS segment, it is necessary to manually activate the secure manual uplink, installed between the firewall and the ICS network switch.

In the ICS network, there are equipment's such as controllers, meters, servers, desktops, etc. This network is the most critical and sensitive segment of the entire topology. This segment is where important equipment, applications, and data are located.

According to Peshin (2009), secure manual uplink acts as a switch to turn the connection between networks on or off. When a particular authorized user needs access to the server located on the ICS network, a second user should be responsible for manually activating this device. A secure manual uplink works with defined periods in which it maintains the connection active. A physical key is responsible for enabling this connection, and the time it will remain active depends on the set configuration. An example of a possible configuration is the ability to activate the key and let the connection remain on for fifteen, thirty, or forty-five minutes. After this elapsed time, the device will automatically shut down and prevent access to the ICS network. If a problem occurs, such as a power failure, when the device returns to operation, it will be in locked mode, and another manual intervention is required. DMZ access requests to the ICS network can only pass through the secure manual uplink device if it is manually activated.

The main reason for using a terminal server is to reduce the number of devices exposed to less reliable networks. Two terminal servers are used in this proposal, one located in the DMZ network and a second one located in the ICS network. These terminal servers authenticate and allow or deny access requests from the respectively connected networks. Only requests from the terminal server installed on the DMZ network targeting the terminal server on the ICS network are authorized. The terminal server located in the DMZ network is also responsible for connecting users who wish to have access to the resources available in the DMZ network. Only requests coming from the corporate network can connect to the terminal server located in the DMZ network. The use of terminal service creates a single access path to DMZ and ICS networks.

One of the reasons to connect the ICS, DMZ, and the corporate network is to obtain production data in real-time. This data is obtained from devices installed on the ICS network, which then pushes the data into a database. This data should be accessed by certain key people. As there is a high risk of allowing direct access to data in the database located on the ICS network, it is recommended to replicate this information to a database server located in the DMZ

network. So, to ensure that the data flows in only one direction, from the ICS network to the DMZ network, both the ICS network and the DMZ network have a historical data server. These servers are also protected by the unidirectional security gateway (RX Agent and TX Agent, respectively) installed between the ICS and DMZ networks.

The application server is responsible for configuring the controllers scattered over the ICS network. This server should be protected by the firewall and the secure manual uplink installed between the ICS and DMZ networks, so it is not remotely controlled from the corporate network, which could bring high risk to the ICS network.

In order to ensure access to authorized people only, the access control in this paper is based on user account and password. However, it is recommended to use two-factor authentication, thus increasing the level of security in accessing the environment. The authentication server holds the database related to users and passwords and is available for the terminal server to authenticate the user access requests.

In summary, in addition to the topics discussed in sections 2 and 3, this paper considers using three features to leverage the security of the topology: terminal service, unidirectional security gateway, and secure manual uplink. The aim is to contribute improvements to the security of the ICS network when necessary to connect it to less secure networks.

4.2. Modeling the Topology on CPN

The graphical representation of a CPN is given by an active component called transition (rectangle) and another passive component called place (ellipses). The transitions and places are connected by directed arcs (arrows), and they can be either single or multiple directed.

Figure 2 shows a general view of the CPN representing the proposed topology. It is possible to see that there are three segments named ICS segment, DMZ segment, and Corporate segment. Connecting these segments are junctions' points called firewall (FW), switches (SWBIS, SWDMZ, and SWICS), the unidirectional security gateway (GW), and the secure manual uplink (SG). Note that, in addition to modeling, one of the goals of this paper is to validate a secure interconnection between an ICS and a corporate network. To achieve this purpose, the first idea was to validate all possible processes with all segments working together. Since a CPN models all possible process states, initial experiments performed with the integrated segments increased the possibilities of the state space almost to infinity, making the analysis and validation of the proposal too difficult. However, fortunately, validations in separate steps are possible in a CPN. One of the characteristics of this type of analysis is to allow validations of individual segments to be grouped in more complete and complex scenarios. Thus, conclusions can be raised even with the separate execution of the segments. More details on separate segment analysis can be found in section 5.1 Data Analysis.

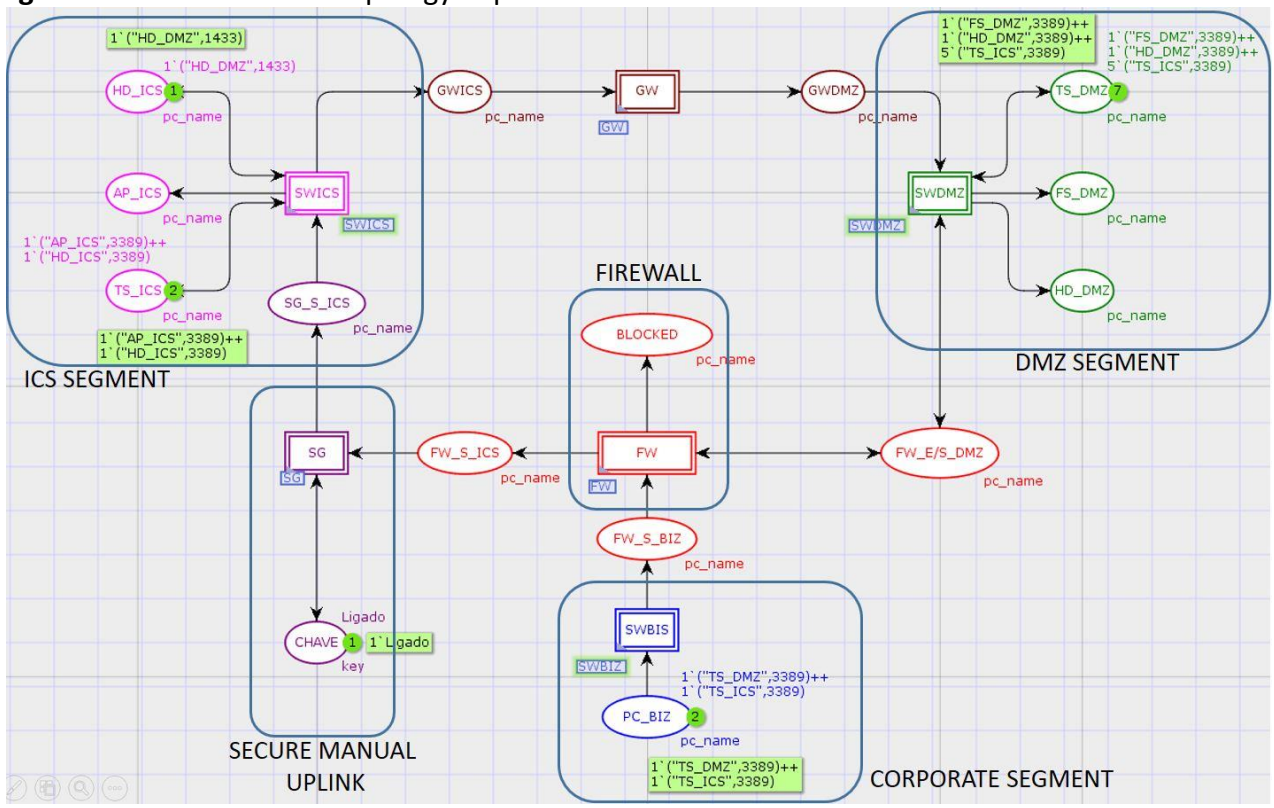
As a means to facilitate the representation and observation of tokens flow among the different places and transitions of the network, it was decided to split the complete design into smaller subparts. Figures 3 to 5, respectively, show the FW, GW, and SG junction points.

Figure 3 represents the FW junction point used to interconnect the ICS, DMZ, and corporate network segments. The SW_S_BIZ place represents the port connecting the firewall to the corporate network segment. The FW_E / S_DMZ place represents the port connecting the firewall to the DMZ network segment. Finally, the FW_S_ICS place represents the port connecting the firewall to the secure manual uplink. All connections not allowed in the firewall are automatically handled by the blocking rule, eliminating the data package.

All tokens coming from the corporate segment reach SW_S_BIZ port, and these

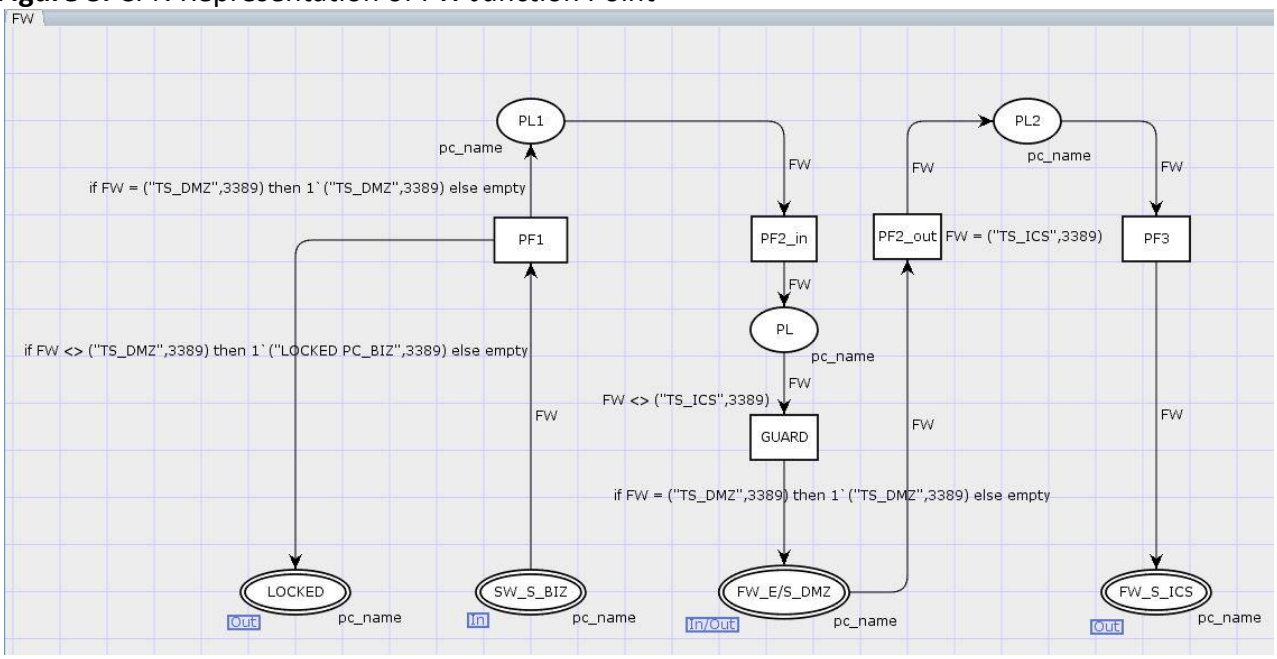
tokens can either be forwarded to the LOCKED place or the DMZ segment, depending on the rules set on the arcs connected to PF1 transition. Before getting to the DMZ segment, the token should fulfill the requirements for passing through PF2_in, GUARD, PL1, and PL and the expressions associated with the arcs connecting the places and the transitions. If all the requirements are met, the token will be allowed to reach FW_E / S_DMZ port and finally access the DMZ segment.

Figure 2. Interconnection Topology Represented in a CPN



Source: (Author, 2020).

Figure 3. CPN Representation of FW Junction Point

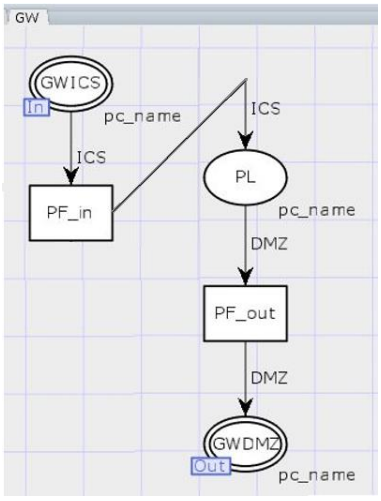


Source: (Author, 2020).

FW_E/S_DMZ port is not only used for receiving tokens from the corporate network and forward them to the DMZ segment, but it is also responsible for receiving the tokens coming from the DMZ segment pointing to the remote places on the ICS segment. FW_ S_ICS port is responsible for forwarding the tokens to the ICS segment. Between FW_E / S_DMZ and FW_ S_ICS ports, there are the PF2_out and PF3 transitions, together with the PL2 place. PF2_out has an expression guard assuring that only tokens pointing to the terminal server on the ICS segment are allowed. Figure 4 represents the GW junction point used to connect the ICS network segment to the DMZ. The GW has two places: (1) GWICS, which is connected to the ICS network segment; (2) GWDMZ, which is connected to the DMZ network segment.

In order to transfer tokens from the ICS to the DMZ segment, the only possible path is through the GW. Tokens from the ICS reach the GWICS port, and it automatically forwards them to the GWDMZ port, which is connected to the DMZ segment. The arcs direction connecting PF_in, PL, and PF_out on the GW assures that the only possible flow will be from the ICS segment to the DMZ segment.

Figure 4. CPN Representation of GW Junction Point

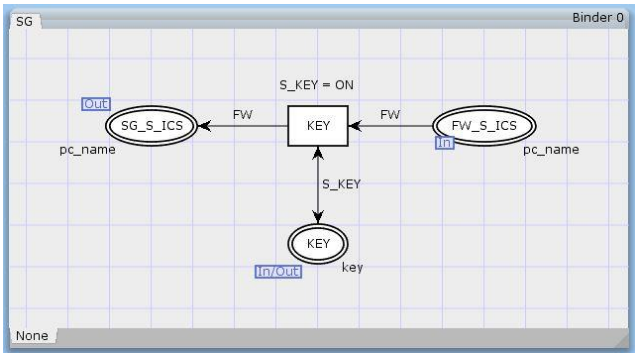


Source: (Author, 2020).

Figure 5 represents the SG junction point installed between the ICS segment and the firewall. The SG has a port called FW_S_ICS, which is used for receiving the tokens from the FW, forwarding them to the SG_S_ICS port, which is connected to the ICS segment. In order to have the tokens crossing the devices and accessing the ICS segment, the transition called KEY has a guard expression associated with it. The tokens will be allowed to pass through the KEY transition only if the status of the KEY place is ON.

When connecting each of the segments using the junction points shown in Figures 3 to 5, it is possible to generate the interconnection topology represented in Figure 2.

Figure 5. CPN Representation of SW Junction Point



Source: (Author, 2020).

5. VALIDATION

As already stated, all tests in this paper are performed using CPN. According to Ueda (2012), in a CPN, a state space is represented by a reachability graph that describes the dynamic behavior of the network. In interpretations made on state space, especially in its representation by a graph of occurrence, information of the nodes and arcs is considered. Using the reachability analysis is possible to indicate if a place is reached by a token when a certain number of transitions are fired in the initial state of the network.

According to Ueda (2012), the problem related to the state space explosion in a CPN can render the reachability analysis infeasible, because the number of nodes in the network becomes exponentially large, causing space state execution time to tend to

infinity. That said, it is important to reduce as much as possible the number of tokens in a given simulation.

According to Ueda (2012) and CPNTools (2017) is a toolkit for creating, editing, simulating, and analyzing a timed and non-timed CPN. The tool has automatic syntax checking, alerting if the correct parameters and codes are being used in the network. The declarations of variables, colors, constants, and functions are made using the Meta-Language (ML). This tool provides appropriate conditions for modeling systems, considering different types of processes. Using CPNTools (2017), it is possible to execute queries to verify that specific states, which should not be reached, are occurring, showing that a security breach exists. It is also possible to execute queries to verify the success of the attempt to reach a specific state that should be accessed, showing that the rules are properly configured. Therefore, by means of the CPNTools (2017), it is possible to validate the secure interconnection scenario between the ICS and the corporate networks, verifying whether or not a given token has reached a place in the CPN. Table 2 presents the description of each of the hosts used in Table 3 and Table 4 and their respective locations.

Table 2. Host Description and Location

Host	Description	Location
HD_ICS	Historical Data Server	ICS
TS_ICS	Terminal Server	ICS
TS_DMZ	Terminal Server	DMZ
PC_BIZ	User Computer	Corporate
HD_DMZ	Historical Data Server	DMZ
AP_ICS	Application Server	ICS

Source: Author.

5.1. Scope

The developments in this paper take place in a real ICS of a food industry that is not highly available. However, due to the simplicity of the architecture, the proposal for secure interconnection between ICS and corporate networks presented here can be easily adapted for use in other environments. It is also worth mentioning that the devices used in this proposal are autonomous, able to carry out their activities yet to occur loss of communication with the network bus.

5.2. Tests

Table 3 shows data flow connection rules between the three network segments. The columns are described as follows: **Source** lists the names of the devices where access requests are originated; **Destination** lists the names of the devices to be accessed; **Dest. Port** lists the port number to be accessed on the remote device; **Path** lists the connection nodes that the access request will go through; **Sec. Man. Uplink** lists the possible states of the secure manual uplink device

The possible states are **ON**, **OFF** or not applicable **N/A**, **ON** means the device is active, **OFF** means the device is not active and **N/A** means that in this path the node secure manual uplink is not used; finally, **Status** lists information about the expected behavior as a result of the access attempt, which can be: **ALLOWED**, if the policy allows access or **DENIED** if the policy denies access.

Table 4 shows the list of tests to be executed on CPNTools (2017). The first five columns of this table have the same information as the first five of Table 3, the difference is in the sixth column, **Expected Result**, which shows the expected statuses resulted from the tests.

The tests listed in Table 4 could be described as follows: (1) get access to allowed states; the expected result is ALLOWED in the column Expected Results of Table 4; or (2) do not get access to states; the expected results are DENIED in the column Expected Results of Table 4.

During the simulations, allowed and denied tokens were created in a given network segment, targeting each of the existing network destinations on the other segments. As an example, if the simulation was executed in the corporate network segment, the tokens were fired, targeting the

remote destinations in the ICS and DMZ network segments.

Table 3. Connection Rules (N/A = Not Applicable)

Source	Destination	Destination Port	Path	Sec. Man. Uplink	Status
HD_ICS	HD_DMZ	1433	Gateway	N/A	Allowed
TS_ICS	AP_ICS	3389	ICS Switch	N/A	Allowed
TS_ICS	HD_ICS	3389	ICS Switch	N/A	Allowed
TS_DMZ	HD_DMZ	3389	DMZ Switch	N/A	Allowed
TS_DMZ	TS_ICS	3389	FW + Man. UpLink	ON	Allowed
TS_DMZ	TS_ICS	3389	FW + Man. UpLink	OFF	Denied
PC_BIZ	TS_DMZ	3389	FW	N/A	Allowed
PC_BIZ	TS_ICS	3389	FW	ON	Denied
PC_BIZ	TS_ICS	3389	FW	OFF	Denied

Source: (Author, 2020).

Table 4. List of Test Simulations on CPN Tools (N/A = Not Applicable)

Source	Destination	Dest. Port	Path	Sec. Man. Uplink	Status
HD_ICS	HD_DMZ	1433	Gateway	N/A	Allowed
TS_ICS	AP_ICS	3389	ICS Switch	N/A	Allowed
TS_ICS	HD_ICS	3389	ICS Switch	N/A	Allowed
TS_DMZ	HD_DMZ	3389	DMZ Switch	N/A	Allowed
TS_DMZ	TS_ICS	3389	FW + Man. UpLink	ON / OFF	Allowed / Denied
PC_BIZ	TS_DMZ	3389	FW	N/A	Allowed
PC_BIZ	TS_ICS	3389	FW + Man. UpLink	ON / OFF	Denied
PC_BIZ	AP_ICS	3389	FW + Man. UpLink	ON	Denied
PC_BIZ	HD_DMZ	3389	FW	N/A	Denied
PC_BIZ	HD_ICS	3389	FW + Man. UpLink	OFF	Denied

Source: (Author, 2020).

Tokens on the remote segments were removed to limit the number of nodes, consequently reducing the state space execution time.

Running the simulations made possible to collect enough data, from the state space tests, to analyze whether the secure interconnection topology proposed is effective.

Using queries on CPNTools (2017), it was possible to indicate whether or not the allowed and denied tokens accessed the different places on the network.

Each of the rows in Table 4 was associated with a state-space query that will be performed within CPNTools (2017). Once each query was executed, the respective result is recorded, each result obtained is compared with the respective expected result **ALLOWED** or **DENIED** from Table 4 and stored for analysis and conclusions.

All simulations were successfully executed in the CPNTools (2017), thus making it possible to run the validation queries on the ML.

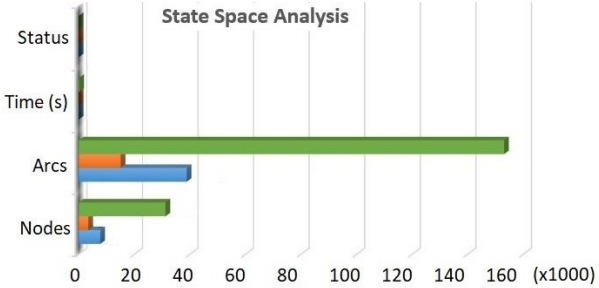
5.3. Data Analysis

The state-space analysis is necessary to make it possible for the queries to show the appropriate results. At the end of the

state space analysis, it is also possible to have access to the directed graph resulting from the state space simulation. The graph is composed of nodes, which are possible network places, and arcs, which are the possible transitions interconnecting each of the nodes. For queries to return the correct results, it is imperative that the state space analysis ends with the status complete. Otherwise, the analysis becomes inconsistent.

Figure 6 shows details about the execution of each of the segmented CPN model simulations. The items are described as follows: **Status** shows whether the execution of the state space has been successfully performed allowing the analysis of state space and consequently the execution of the queries; **Time** shows the total time in seconds required to perform the simulation in the given segment; **Arcs** shows the total number of arcs present in the directed graph resulting from the execution of the state space simulation; **Nodes** shows the total number of nodes present in the directed graph resulting from the execution of the state space simulation.

Figure 6. State Space Analysis



	Nodes	Arcs	Time (s)	Status
Corporate Segment	31,250	153,125	204	1
ICS Segment	3,456	15,120	3	1
DMZ Segment	7,776	38,880	15	1

Source: (Author, 2020).

The simulation was executed in three separate segments to reduce the number of possible states and the execution time. In accordance with Figure 6, the corporate segment was the largest, taking 204 seconds to complete resulting in 31,250 nodes and 153,125 arcs in the state space graph. DMZ segment took 15 seconds to complete resulting in 7,776 nodes and 38,880 arcs in the state space graph. ICS segment was the smallest segment taking 3 seconds to complete resulting in 3,456 nodes and 15.120 arcs in the state space graph.

Tables 5 to 7 respectively show the test results for the DMZ, Corporate, and ICS network segment simulations, validating the proposal of this paper. For each of the segments, the state space analysis was executed with the secure manual uplink key in the **ON** and **OFF** position. These two simulations were necessary to validate the behavior of the network in both cases, when the secure manual uplink was turned on, allowing data flow, and when it was turned off, blocking all data flow.

Tables 5 to 7 have the same columns of Table 4, adding a new column called Validation. This new column is responsible for showing if the query results validate the security policy. If the result listed in this column is **OK**, it means the proposed scenario implemented the security policy correctly and
can be accepted as validated. If all results on Tables 5 to 7 are **OK**, it means this proposed interconnection scenario met the requirements to be considered a valid proposal to securely interconnect ICS and Corporate networks.
Analyzing Tables 5 to 7, it is possible to verify that all state space queries executed presented the results aligned with the expected results listed in Table 4.

Table 5. Test Results for DMZ Network Segment Simulation

Source	Destination	Dst Port	Path	Sec. Man. Uplink	Status	Validation
TS_DMZ	HD_DMZ	3389	DMZ Switch DMZ	ON	Allowed	OK
TS_DMZ	TS_ICS	3389	FW + Man. Uplink	ON	Allowed	OK
TS_DMZ	HD_DMZ	3389	DMZ Switch DMZ	OFF	Allowed	OK
TS_DMZ	TS_ICS	3389	FW + Man. Uplink	OFF	Denied	OK

Source: (Author, 2020).

Table 6. Test Results for Corporate Network Segment Simulation

Source	Destination	Dst Port	Path	Sec. Man. Uplink	Status	Validation
PC_BIZ	TS_DMZ	3389	FW	ON	Allowed	OK
PC_BIZ	TS_ICS	3389	FW + Man. Uplink	ON	Denied	OK
PC_BIZ	AP_ICS	3389	FW + Man. Uplink	ON	Denied	OK
PC_BIZ	HD_DMZ	3389	FW	ON	Denied	OK
PC_BIZ	HD_ICS	3389	FW + Man. Uplink	ON	Denied	OK
PC_BIZ	TS_DMZ	3389	FW	OFF	Allowed	OK
PC_BIZ	TS_ICS	3389	FW + Man. Uplink	OFF	Denied	OK
PC_BIZ	AP_ICS	3389	FW + Man. Uplink	OFF	Denied	OK
PC_BIZ	HD_DMZ	3389	FW	OFF	Denied	OK
PC_BIZ	HD_ICS	3389	FW + Man. Uplink	OFF	Denied	OK

Source: (Author, 2020).

Table 7. Test Results for ICS Network Segment Simulation

Source	Destination	Dst Port	Path	Sec. Man. Uplink	Status	Validation
HD_ICS	HD_DMZ	1433	Gateway	ON	Allowed	OK
TS_ICS	AP_ICS	3389	ICS Switch	ON	Allowed	OK
TS_ICS	HD_ICS	3389	ICS Switch	ON	Allowed	OK
HD_ICS	HD_DMZ	1433	Gateway	OFF	Allowed	OK
TS_ICS	AP_ICS	3389	ICS Switch	OFF	Allowed	OK
TS_ICS	HD_ICS	3389	ICS Switch	OFF	Allowed	OK

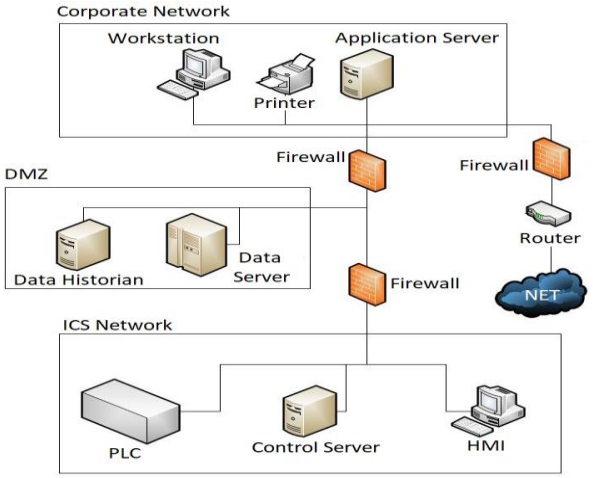
Source: (Author, 2020).

6. DISCUSSION AND CONCLUSION

As mentioned earlier in the related works section, NIST (2015) is the closest proposal compared to this paper, so it was considered important to have a separate section to present a comparison between the two proposals, highlighting the main advantages of this paper compared to NIST (2015). Among the possible topologies proposed by NIST (2015) for segregating networks in different domains, to provide greater security to the ICS network segment, the most complete is the "Paired Firewalls between Corporate Network and ICS Network." In this proposal, it is possible to verify the existence of three network domains (ICS, DMZ, and Corporate). Between the Corporate network and the DMZ network, there is a firewall and between the DMZ network and the ICS network, a second firewall. No direct connection between the corporate network domain and the ICS network domain exists. In order to illustrate the NIST (2015) proposal, Figure 7 presents the suggested topology. By checking Table 1 and Figure 7, it is possible to notice that the

similarities between NIST (2015) and this paper are in the items: DMZ, backup, physical security, security policy, firewall, and access control. On the other hand, the items that this paper proposes as additional points are: terminal service, unidirectional security gateway between the ICS and DMZ network, secure manual uplink, and the validation of the proposed topology.

Figure 7. Paired Firewall between Corporate Network and ICS Network.



Source: (NIST, 2015).

According to NIST (2015), the connection topology between ICS networks and corporate networks should be based on principles such as restriction of logical and physical access to the ICS network. For logical access restriction, some features such as unidirectional security gateways, DMZ protected by firewalls to prevent packets from being exchanged directly between the corporate network and ICS network, and the use of different authentication mechanisms for users of the three networks (Corporate, ICS and DMZ) are needed. It is also necessary to use switches physically and logically separated from the switches installed on the corporate network and the DMZ. Resource sharing between networks should not exist. Dedicated equipment for each of the segments should be used, including the segregated installation of network cabling. The implementation of the ICS network topology should be done in multiple layers. The most critical resources should be installed on the most secure and stable layer of the topology.

According to NIST (2015), to ensure the detection of anomalous or suspicious behavior or even any changes in the policies implemented in the servers or other security devices that protect the networks, a monitoring system should be deployed and continuously updated. Event alerts should be sent to those responsible for information security when a new user is created, or a certificate is generated in the server, a user is added to the server's or firewall's administrator group, a user's security policy is changed on any of the devices in the DMZ or ICS networks, and when users are locked due to invalid password on any of the devices installed on the networks.

Regarding the use of a unidirectional security gateway, NIST (2015) suggests its use for synchronizing historical data from the ICS network directly to a server located on the corporate network. This paper proposes that data synchronization is not performed directly between the historical data server of the ICS network to a server located in the corporate network, but rather the use of unidirectional security gateway between the ICS and DMZ networks, synchronizing the data between the historical data servers on these two networks. For users of the corporate network to view historical data on the DMZ network, they should first authenticate and connect to the terminal server located in the DMZ network. This approach minimizes the risk of intercepting data in the corporate network, which may expose sensitive information from industrial processes.

Considering the access to servers and applications located on the ICS network, NIST (2015) suggests that no access can exist to the ICS network resources remotely. This paper proposes a solution to enable access to these resources without reducing the security of the ICS network. The use of the terminal service, coupled with the use of a secure manual uplink device between the firewall and the ICS network, allows only

manually authorized access to the network resources located on the ICS network. It is important to consider that this access is only allowed if it is originated on the terminal service located in the DMZ network, targeting the terminal service located in the ICS network. In order to access the network resources in the ICS segment, a corporate network user would need to run the following steps: (1) connect to the terminal server located in the DMZ network; (2) contact the ICS network security officer to activate the secure manual uplink; (3) initiate a terminal service connection targeting the terminal server in the ICS network; (4) pass through the firewall rule and authenticate it to the ICS network terminal server.

All connections suggested by NIST (2015) "Paired Firewalls" proposal targets the end devices, which makes it necessary to worry about protecting all resources to be accessed remotely. This paper proposes the use of the terminal service in the DMZ network and the ICS network as a hub point. It considerably reduces the number of firewall rules needed to protect network segments, thereby facilitating rule maintenance and minimizing complexity. Moreover, the hardening of a unique terminal server is simpler compared to having multiple resources to be protected. Other resources often have different operating systems, applications, and physical devices that may have problems after an update is applied to the system.

None of the ICS network protection proposals suggested by NIST (2015) offers validation of the effectiveness of the proposal in terms of security. This paper was not limited to proposing a secure interconnection topology but also to offer a validation using reachability analysis on CPN, ensuring the effectiveness of the proposal. The items considered when preparing the proposed topology included, but were not limited to items such as DMZ, terminal service, physical security of the environments, security policy, firewall utilization, unidirectional security gateway, secure manual uplink, security policy, and validation mechanisms.

The simulations in CPNTools (2017) were executed in three separate segments to reduce the number of possible states and the execution time. Corporate resulted in 31,250 nodes and 153,125 arcs, DMZ resulted in 7,776 nodes and 38,880 arcs and ICS resulted in 3,456 nodes and 15,120 arcs in the state space graph.

The main contributions of this paper include (1) minimizes the number of devices exposed on the ICS and DMZ networks; (2) reduces the complexity of the access control list implemented on firewalls that separate the corporate and ICS networks; (3) the protection of the ICS network is not limited to the logical portion only, so the physical separation among all networks was considered and highlighted that access to the physical network is limited to authorized people only; (4) proposes a topology capable of preventing direct communication between corporate and ICS network devices, reducing exposure to risks, but allowing remote access to ICS devices; (5) the use of the secure manual uplink device increases security for the ICS network segment by providing an additional layer of protection to the firewall; (6) the proposed topology can be easily adapted, being applicable to any separation between corporate and ICS networks; (7) the developed topology presents the best and most current practices in the secure interconnection between ICS and corporate networks; and (8) presents a validation of the proposed interconnection between corporate and ICS networks. This validation helps with decision making when choosing a topology to be implemented.

The main limitations of these results include: (1) the proposed topology considered a limited number of mechanisms to protect the information security, disregarding the use of devices such as intrusion detection and prevention systems, multi-factor authentication, among others; (2) the one-factor authentication approach can create the risk of users using the same

password for all accounts; (3) only the proposed topology suggested in this paper was validated in CPNTools (2017), so not allowing the comparison with other topologies that have already been proposed; and (4) the paper did not consider the validation of a high availability environment.

The secure interconnection topology is feasible and capable of providing security to the ICS network segment. This model is flexible and applicable to any separation between ICS and corporate networks. The use of CPN helps to validate the security of the proposed environment, offering a real contribution in relation to the other works proposing a secure interconnection topology between ICS and corporate networks.

As future works, we suggest the other topologies presented in this paper to be converted into CPN models in order to execute simulations and compare results. In addition, running security topology validation using a different methodology could be considered.

REFERENCES

ALCARAZ, C.; FERNANDEZ, G.; CARVAJAL, F. Security aspects of SCADA and DCS environments**. Lecture Notes in Computer Science**, v. 7130, 2012, p. 120–149, Sept. 2012. https://doi.org/10.1007/978-3-642-28920-0_7

AZEVEDO, M. T. DE. **Transformação digital na indústria: indústria 4.0 e a rede de água inteligente no Brasil.** Tese (Doutorado em Engenharia Elétrica) – Universidade de São Paulo, São Paulo, 2017.

AMOAH, R.; CAMTEPE, S.; FOO, E. Formal modelling and analysis of DNP3 secure authentication. **Journal of Network and Computer Applications**, v. 59, p. 345–360, 2016. https://doi.org/10.1016/j.jnca.2015.05.015

CÁRDENAS, A. A.; AMIN, S.; LIN, Z. S,; *et al*. Attacks against process control systems: Risk assessment, detection, and response. *In:* INTERNATIONAL SYMPOSIUM ON INFORMATION, COMPUTER AND COMMUNICATIONS SECURITY, ASIACCS**.** 6. 2011, , 2011 **Proceedings** […], 2011. p. 355–366. https://doi.org/10.1145/1966913.1966959

COATES, G. M.; HOPKINSON, K. M.; GRAHAM, S. R. *et al*. A trust system architecture for SCADA network security. **IEEE Transactions on Power Delivery**, v. 25, n. 1, p. 158–169, 2010. https://doi.org/10.1109/TPWRD.2009.2034830

CPNTOOLS. **A tool for editing, simulating, and analyzing Colored Petri net.** Disponível em: http://cpntools.org. Acesso em: 10 set. 2020.

DONG, W.; JAFARI, M.; YAN, L. On protecting industrial automation and control systems against electronic attacks. *In:* INTERNATIONAL CONFERENCE ON AUTOMATION SCIENCE AND ENGINEERING**,** 3., **2007**, **Proceedings** […]. Arizona, EU: IEEE, , 2007. p. 176–181

JENSEN, K. **Colored Petri nets: basic concepts, analysis methods and practical use**. Springer Science & Business Media, 2013.

KNAPP, E. D.; LANGILL, J. T. **Industrial Network Security:** Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Syngress, 2014.

MACIEL, P. R. M.; LINS, R. D.; CUNHA, P. R. **Introdução às redes de Petri e aplicações.** 10ª Escola de Computação, Campinas, jul. 1996.

MAHBOOB, A.; ZUBAIRI, J. Intrusion avoidance for SCADA security in industrial plants. *In*: INTERNATIONAL SYMPOSIUM ON COLLABORATIVE TECHNOLOGIES AND SYSTEMS, CTS, 2010. Chicago, IL, EUA,,

2010 p. 447–452. https://doi.org/10.1109/CTS.2010.5478480

MURATA, T. Petri Net : Properties , Analysis and Applications. **Proceedings of the IEEE**, v. 77, n. 4, p. 541–580, 2015. https://doi.org/10.1109/5.24143

NIST **Guide to industrial control systems (ICS) security**. National Institute of Standards and Technology, 2015.

PESHIN, E. **A pragmatic and foolproof approach for connecting critical/industrial networks to external less secure networks**. Modeling Cyber Security: Approaches, Methodology, Strategies, 2009.

STOIAN, I.; CAPATINA, D.; IGNAT, S. *et al*. SCADA and modeling in water management. *In:* INTERNATIONAL CONFERENCE ON AUTOMATION, QUALITY AND TESTING, ROBOTICS, AQTR 2014, **Proceedings […].** Cluj-Napoca, Romênia: IEEE, 2014. https://doi.org/10.1109/AQTR.2014.6857920

UEDA, E. T. **Análise de políticas de controle de acesso baseado em papéis com rede de petri colorida**. Tese (Doutorado em Engenharia Elétrica) - Universidade de São Paulo, São Paulo, 2012.

YADAV, G.; PAUL, K. Assessment of SCADA System Vulnerabilities. INTERNATIONAL CONFERENCE ON EMERGING TECHNOLOGIES AND FACTORY AUTOMATION, ETFA, 24., 2019. , , Zaragoza, Espanha: IEEE, 2019. p. 1737–1744. https://doi.org/10.1109/ETFA.2019.8869541

ZERDAZI, I.; FEZARI, M. SCADA Attack Modeling Using Bond Graph. *In*: INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATION TECHNOLOGIES FOR DISASTER MANAGEMENT, ICT-DM, 6., Paris,França, 2019. Paris: IEEE, , 2019. p. 2019–2020. https://doi.org/10.1109/ICT-DM47966.2019.9032929