Malicious Anomaly Detection Approaches Robustness in Manufacturing ICSs

Amaury Beaudet, Cédric Escudero, Eric Zamaï

Malicious Anomaly Detection Approaches Robustness in Manufacturing ICSs

Amaury Beaudet * **Cédric Escudero** ** **Éric Zamaï** ***

* *Ampère Lab - INSA Lyon, CNRS, 69621 Villeurbanne cedex (e-mail: amaury.beaudet@insa-lyon.fr).*
** *Ampère Lab - INSA Lyon, 69621 Villeurbanne cedex (e-mail: cedric.escudero@insa-lyon.fr).*
*** *Ampère Lab - INSA Lyon, 69621 Villeurbanne cedex(e-mail: eric.zamai@insa-lyon.fr)*

Abstract: For the past decade, manufacturing Industrial Control Systems (ICSs) have suffered from targeted attacks against their physical system and their control integrity, resulting in financial and material losses. Among protective answers to this malicious threat, Anomaly Detection Systems (ADS) based on behavioral models of the ICS are highly regarded for their ability to detect zero-day attacks. However, the design of accurate and non-obsolescent detection models is not as an easy task in a constantly changing ICS environment. Thus, this paper provides an overview of the behavioral ADSs detection flaws issued from the ICS unpredictable management and its heterogeneous environment. Behavioral models will be introduced in light of four attributes: their design method, the modeled ICS behavior, the lifecycle of the design and the model nature. Then, each of these attributes will be discussed in regard of their detection robustness to the different environmental factors and uncertainties they are affected by.

Keywords: Cyber-security, ICS, Anomaly Detection Systems, Manufacturing Systems

1. INTRODUCTION

An Industrial Control Systems (ICSs) is a structure of hardware and software components interconnected together through an industrial network to achieve the following objectives: controlling and monitoring a large physical system. ICSs are deployed in different industrial sectors, like manufacturing systems, power systems or nuclear facilities. Originally, ICSs were considered as secured from malicious cyber attacks by the air-gap separating their Information Technologies (ITs), implemented in business networks, and their Operational Technologies (OTs), employed in ICSs and industrial networks. This air-gap was assumed by the numerous proprietary protocols in OT levels and the clear network segregation between IT and OT levels. However, the recent convergence of IT technologies to the OT levels erased this gap and brought new threats to the ICSs (Stouffer et al. (2015)). Modern attacks against ICSs, like the Stuxnet attack, illustrate this trend and provide a glimpse of the financial, material and human losses a successful attack targeting an ICS and in particular its physical system could cause.

Against these new attack threats, manufacturing systems are highly vulnerable. Protecting them against these threats can be achieved using different methods aiming for instance to prevent attacks, to detect them or to assess ICS cyber vulnerabilities. Among theses solutions, Anomaly Detection Systems (ADSs) based on models of normal behaviors of manufacturing ICSs (behavioral ADSs) are highly rated (Mitchell and Chen (2014)). However, in many instances, implementing this kind of solution rests upon strong, yet unfounded, hypotheses of stability and determinism regarding the ICS normal runing. On the whole, in real systems, behavioral ADSs have to cope with the uncertain and heterogeneous environment of manufacturing ICSs (e.g. ICS rescheduling, human intervention (Vieira et al., 2003; Escudero et al., 2018). This paper offers a first answer to this problematic by giving an overview of the flaws behavioral ADSs detection mechanisms could encountered in manufacturing ICSs. The objective of this work is to provide an analysis method to orientate the choice of the behavioral model main features to make the detection more robust against the different environmental factors and uncertainties.

The paper is organized as follows. In section 2, manufacturing ICSs and the attack threats they have to face are introduced. In section 3, behavioral ADSs are presented. Main features of behavioral models are reviewed, supported by the related works. Concurrently, flaws affecting detection mechanisms of behavioral ADSs are detailed. In section 4, manufacturing ICS uncertainties and its heterogeneous environment are described via different factors. For each of them, engendered effects on detection are depicted according to the features of behavioral ADSs models. In section 5, the ADSs detection flaws originated from the manufacturing environment are summarized in a table and illustrated with an example. Section 6 concludes this paper and exposes our future research axes.

2. MANUFACTURING ICSs

A manufacturing ICS aims at controlling a physical system operating on a product flow, defined as a process where

a product is manufactured through different operations and production cells. In order to control the product flow, manufacturing ICSs are organized following the CIM architecture (Escudero et al. (2018)). In this model, the ICS is split into horizontal layers as follow:

- **Product flow:** sequence of operations performed on the product through different productions cells in order to make it reach a desired state.
- **0 - Operative part:** actuators and sensors transforming the product and monitoring its flow through the ICS.
- **1 - Control layer:** controllers (e.g. Programmable Logic Controller (PLC), PID controllers) operate on a production cell by manipulating actuators. The control is based on a predefined control law updated in real time with sensors data.
- **2 - Supervision layer:** Collection of data acquired from all controllers via Remote Terminal Units (RTUs), the whole product flow is supervised and monitored in real-time by operators.
- **3 - Planning layer:** the production scheduling is planned according to client orders, ICS state and available resources.

The different layers communicate together by sending orders to the layer below them and receiving reports (e.g. order executed, sensors data, alarms) from this layer. These communications are called control messages. On the networks between OT layers (0,1,2), industrial protocols are employed to structure and offer specific services to the communication between control devices. Industrial protocols are myriad (e.g. Modbus TCP-IP, OPC-UA) and each of them owns a dedicated frame format and communication rules (Galloway and Hancke (2013)).

Because of new attack threats, manufacturing systems are vulnerable. Apart from protecting the product flow and the ICS availability, integrity and confidentiality (Escudero et al. (2018)), manufacturing ICSs own other particularities and constraints that need to be addressed. First, a manufacturing system prioritizes **profitability** over other objectives (e.g. safety, security, sustainability). Profitability is a combination of productivity, product quality, cost reduction and customers satisfaction, which lead modern ICSs to be highly flexible and agile (Panetto et al. (2019)). Then, manufacturing ICSs follow **recipes** to control the product flow. An ICS **Recipe** defines the parameters and sequences of physical operations the product will go through to reach its final desired state. Recipes can be either consistent over time or renewed every time a new customer order is registered (Vieira et al. (2003)). Thirdly, in manufacturing ICSs, the **human operator** is responsible for the productivity goals. It is allowed to intervene on the ICS whenever it is required, from modifying the ICS scheduling to removing a flawed product from the production line (Escudero et al. (2018)). Finally, manufacturing environment offers a high **diversity** of inter components architectures and technologies employed among existing systems (Stouffer et al. (2015)). All these particularities make the manufacturing environment and ICSs normal behaviors more likely uncertain and heterogeneous. Therefore, these particularities need to be considered in the design of behavioral ADSs.

3. BEHAVIOR-BASED ANOMALY DETECTION

Among security solutions, behavioral ADSs are highly rated for protecting manufacturing ICSs against attack threats. Indeed, as decision support methods (e.g. alarms, detection metrics), ADSs do not interfere with production flow, neither consume exuberant control resources (e.g. PLC's CPU, network bandwidth) except for reading or retrieving ICS data. Moreover, behavioral ADSs are able to detect unknown attacks since they rely on models of the normal functioning of the ICS to perform detection. In detail, if a deviation is monitored between the ADS models and the real-time observations of the system, an anomaly detection occurs, even if the anomaly nature (malicious or natural) is unknown. However, one shortcoming remains. As the ICS normal functioning might not be consistent over time, the behavioral ADS can trigger false detection.

With this problematic in mind, we intend to analyse the main features of ADS models with the aim to further evaluate their robustness to the uncertainties and heterogeneity of manufacturing ICSs. In this paper, only ADSs considering several PLCs and positioned on the communication between levels 1-2 or on level 2 are reviewed.

3.1 Behavioral Model Features

In the literature, behavioral ADSs have been surveyed with different perspectives. In this paper, ADSs are reviewed regarding the ICS normal behaviors they are monitoring and the hypotheses they take to model these behaviors. Depending on these hypotheses, the resulting models will be more or less robust to the ICS environment uncertainties and heterogeneity. Hence, the selected model features (Fig 1) showcase: What ICS behavior is modeled (Modeled Behavior) and if this behavior is viewed as deterministic or stochastic (Model Nature), How this behavior is modeled and from which knowledge (Model Design Method) and When, during the ICS lifecycle, is the behavior studied for modeling (Model Design Lifecycle).

Modeled Behavior. An ADS positioned between the level 1-2 or on level 2 can rely on either a network model or a control model. The first category is designed from the normal behavior of the ICS industrial network, divided into the network traffic and the protocols specifications (Rakas et al. (2020)). Network traffic models study the communication patterns (e.g. frequencies, sequences, or periodicity of messages) and quantitative metrics (e.g. message length, bandwith, communication delays) of the industrial network, whereas protocols models focus on the protocol specifications behaviors (e.g. ports used, function codes, request/response scheme). The second category gathers all the ADS modeling the normal control behavior of the ICS. These models represent either the controlled physical system behavior (product flow and operative part), the control flow behavior (control laws and control messages), or both.

Model Nature. A behavioral model nature represents the degree of determinism of the model. This feature is either described as deterministic or stochastic. For instance, a Deterministic Finite Automaton (DFA) modeling offline PLCs control laws is considered as highly deterministic,

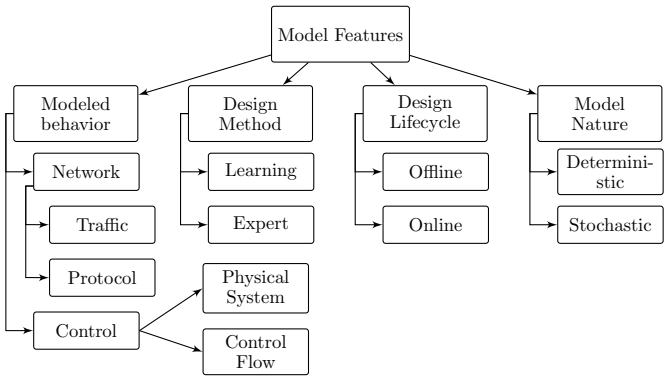

Fig. 1. Detection Model Features

whereas a Bayesian network predicting the product recipes shifts is more probabilistic.

Model Design Method. Behavioral models can either be designed based on learning methods, expert knowledge or both (Mitchell and Chen (2014)). Learning methods need a extended learning phase (up to several months) before being effective, unlike expert ones that are immediately effective after their implementation.

Model Design Lifecycle. Behavioral models are designed either offline, online or both. This feature describes the chronological positioning of the ICS normal behavior modeled in the ADS. This positioning is either at a fixed date (offline) or continuously updated based on the real-time ICS functioning (online).

3.2 Related Works

Behavioral ADSs are well represented in the literature. A glimpse of these ADSs is given in Table 1 regarding the different features of the models employed by the authors. The chosen ADSs represent a restricted part of the existing literature and were selected based on our own knowledge to illustrate all the ADSs models features.

Table 1. Behavioral ADSs References

	Modeled Behavior				Design Method		Design Lifecycle		Model Nature	
	Network		Control							
	Traffic	Protocol	Physical System	Control Flow	Learning	Expert	Offline	Online	Determin.	Stochastic
Refs	[1]	[2]	[3] [5]	[4]	[1] [5]	[3]	[2] [4]	[4]	[3] [4]	[1]

[1] = (Caselli et al. (2015)), [2] = (Yusheng et al. (2017)), [3] = (Khalili and Sami (2015)), [4] = (Adepu et al. (2020)), [5] = (Lin et al. (2018))

In Table 1, the quoted ADSs are usually evaluated based on their detection results and their ability to avoid detection errors. In the next section, the different detection flaws a behavioral ADS can encounter are introduced.

3.3 Detection mechanisms flaws

A behavioral ADS is expected to detect all anomalies resulting from attacks it was designed for without miss interpreting any ICS normal behavior with a malicious one. An ADS needs also to be functional and maintains its detection efficiency as long as the ICS operates and for a large scope of manufacturing ICSs. These requirements translate themselves into the following detection flaws a behavioral ADS aims to minimize.

- **False Positive (FP)**. The ADS detects and interprets a normal ICS behavior as an anomaly.
- **Miss Detection**. The ADS misses the detection of an anomaly. This is also called a False Negative (FN).
- **Outdated detection**. The ADS detection model does not match consistently over time with the ICS normal behaviors. This results in a important rate of False Positive and an inefficient detection.
- **Detection Coverage**. The ADS has a high detection rate for a restrained set of manufacturing ICSs configurations and, in contrast, does not cover efficiently ICSs out of its scope.

The different detection flaws are originated for the most part from the model inability to cope with the manufacturing ICS heterogeneous environment and its uncertain behaviors. This detection concern is addressed in the remainder of this paper.

4. ICS ENVIRONMENTAL FACTORS

Manufacturing ICSs are characterized by a heterogeneous and uncertain environment (Escudero et al., 2018) that may affect the detection quality of behavioral ADSs. In this section, the ICS environment heterogeneity and uncertainty are broken down separately into different factors. Each of them will be introduced and described in regard of the detection flaws they can infer into behavioral ADSs according to the different ADSs models features.

4.1 A Heterogeneous Environment

Manufacturing ICSs are viewed as heterogeneous as they may differ from each other in physical, architectural and technological aspects. This heterogeneity can be highlighted through the 3 environmental factors: Protocols diversity, Architectural diversity, and Outsourced resources.

Protocols diversity reflects the vast range of industrial protocols that can be found in manufacturing ICSs. Each protocol offers its own message frame, services and communication specifications. This factor can infer coverage issue to network ADSs modeling specifications or traffic patterns for a specific protocol (Yusheng et al. (2017)).

Architectural diversity refers to the ICS network configurations heterogeneity and to emerging decentralized architectures. **ICS network configuration** defines how the different ICS devices are interconnected between the levels 0 and 2. ICS network configurations involve different physical inter-devices architectures(e.g. serial, parallel, star), network devices (e.g. switch, protocols gateway, modems), and communication paths between devices (e.g. parallel networks, intermediary devices) (Samad et al. (2007)). This factor can result in information misses for deterministic ADSs focusing on network models, either when an awaited message takes an alternative path (FP), or when an anomaly routes through another network path (FN). This configuration heterogeneity brings also coverage issues to ADSs based on traffic models. **Decentralized architecture** designates emerging inter-devices structures where the traditional master-slave access-method is substi-

tuted by self operating and self communicating control devices (Panetto et al. (2019)). This factor condemns offline traffic-based ADSs to process FPs or become outdated as communication patterns between devices are constantly reconfigured. Control flow based ADSs may also be affected when control devices are self-reconfigurable.

Outsourced resources gather all the services and software implemented on the business network (IT levels) for productivity enhancing and remote use, yet authorized to access the ICS network and devices (Samad et al. (2007)). Outsourced resources are for example maintenance remote operations, devices update by manufacturers or statistical tools for diagnostic. These resources originate spontaneous messages on the industrial networks resulting in FPs for network, offline or learning based ADS. In some extent, the implementation of a new outsourced resource can make a network ADS detection become outdated.

4.2 An Uncertain Environment

Manufacturing ICSs are operating in an uncertain environment as they are influenced by miscellaneous, unpredictable and spontaneous events. In manufacturing systems, the uncertainty origins can be broken down into 3 main environmental factors : Uncertain scheduling, Human intervention and Physical system alteration.

Uncertain Scheduling depicts the constantly evolving production scheduling and the regular renewal of product recipes a manufacturing system faces. In manufacturing ICS, **Real-time Scheduling** is commonly calculated and validated by operators on a daily basis based on the ICS tasks list, the available resources and the scheduling priorities. However, the planned scheduling is rarely followed and left unchanged due to unexpected events and decisions (Vieira et al. (2003)). For instance, an actuator failure happens, shuts down an entire production cell for several hours and prevents from manufacturing the scheduled product. In response, the real-time scheduling is modified to start the manufacturing of another product whose flow does not route through the failed cell. Then, depending on the class of the ICS, either low-mix/high-volume or high-mix/low-volume (Abu Samah et al. (2015)), the **Recipes** might be modified regularly. For instance, in the semi-conductor industry, wafer recipes are renewed often when new customer orders are scheduled. These two factors bring uncertainties to the ICS and may cause outdated detection for offline ADS and learning based ADS as they design their model on past data and knowledge that become irrelevant when scheduling and recipes change. Deterministic ADS will also be subject to FP and outdated detection when unable to tackle stochastic scheduling and recipes evolution. Between control and network based ADSs, the second category suffers more from these factors as non modeled communication can appear on the ICS network (FP) while their control meaning is still predictable. At last, expert based model ADSs are vulnerable to scheduling variability (FP, Outdated detection) since even with deep knowledge, an expert may be unable to model the uncertain scheduling changes (Sicard et al. (2019)).

Human Intervention designates the actions and decisions an operator can perform on the ICS (Escudero et al. (2018); Panetto et al. (2019)). A human intervention can be defined by its localization (e.g. operative part, product flaw, supervision), its nature (e.g. repair, replace, reconfigure) and its justification (e.g. component failure, product low-quality, productivity drop). For instance, when a product obstructs a production line, an operator intervenes on the physical system to remove it. Another example is the operator decision to stop via the supervision a chemical ICS process when a boiler pressure is abnormally low and could mean a tank leak. Both example reveal potential detection flaws for behavioral ADSs. First, the intervention localization can interfere on ADS models awareness when, for instance an operator modifies manually the physical system without the ADS being noticed. This factor engenders FP for deterministic or offline ADSs as they miss expected events and detect non modeled one. More generally, depending on the intervention localization and nature, network based and control based ADSs produce FPs. The first category does when the intervention engenders unexpected messages on the network. For example, traffic based ADSs may detect FPs every time a spontaneous message is emitted on network 1-2 from a supervisory operator. The second category produces FPs when the intervention modifies the physical system or the ICS control behaviors. Finally, FPs and outdated detection are also a real concern for learning based ADS as learning data are polluted by frequent human interventions (e.g. missed data during an intervention or a shut down, spontaneous messages).

Physical System Alteration gathers both natural alterations (e.g. component failures, aging) and maintenance operations (e.g. component replacement, corrective maintenance). **Natural alterations** (Nguyen et al. (2016)) are either sudden, like a component failure, or progressive, such as components aging. The first category is a source of FPs for behavioral ADSs as it makes deviate suddenly the ICS physical system behavior. Deterministic and control based ADSs are the most affected by this flaw. For instance, a sensor failure would make an ADS modeling the normal sequences of control messages raise a FP. Progressive natural alterations will, in contrast, make the ICS normal behavior deviate gradually and reach a new normal behavior after a certain time. This uncertainty is a cause for outdated detection from offline ADSs and from learning based ADSs. Control based ADSs are also subject to this flaw as they rely on models of the physical system behavior. **Maintenance operations** (Abu Samah et al. (2015)) are either reactive, when a failure occurs, or preventive, when the operation is planned and aims to predict forthcoming failures. In both cases, the ICS post-maintenance behavior may deviate from the anterior one. For instance, a sensor fails and is substituted by an available one, yet slower and from another manufacturer. This may result in a change of the physical system timing behavior. In another context, a predictive maintenance is planned to replace half the hydraulic cylinders of an ICS. This maintenance can turn the ICS behavior into a more reactive and responsive one. In both examples, the ICS behavior is modified and may occasion FP or even outdated detection to behavioral ADSs. In particular, offline, deterministic and control based ADSs will suffer from uncertain changes of the physical system they are unaware of. Finally, due to poorly documented maintenance operations, expert based ADSs can produce FPs or outdated detection flaws.

Table 2. Behavioral ADSs Detection Flaws

	Modeled Behavior				Model Design Method		Model Design Lifecycle		Model Nature	
	Network		Control		Learning	Expert	Offline	Online	Determin.	Stochastic
	Traffic	Protocol	Physical System	Control Flow						
Protocol Diversity	Cov.	Cov.	-	-	-	-	-	-	-	-
Network Configuration	FP/Cov. Miss.	FP Miss.	-	-	-	-	-	-	-	-
Decentralized Architecture	-	FP Out.	-	FP Out.	-	-	FP Out.	-	-	-
Outsourced Resources	FP Out.	FP Out.	-	-	FP.	-	FP.	-	-	-
Real-time Scheduling	FP.	FP.	-	-	FP Out.	FP Out.	FP Out.	-	FP Out.	-
Recipes Renewal	FP.	FP.	-	-	FP Out.	-	FP Out.	-	FP Out.	-
Human Intervention	FP.	FP.	FP.	FP.	FP Out.	-	FP.	-	FP.	-
Natural Alterations	-	-	FP Out.	FP Out.	Out.	-	Out.	-	-	-
Maintenance Operations	-	-	FP Out.	FP Out.	-	-	FP Out.	-	FP Out.	-

Legend : (-) Blank cells illustrate factors that do not theoretically impact detection results of ADSs with the corresponding feature.

5. CONSEQUENCES ON ANOMALY DETECTION

5.1 Table Analysis

In this section, all the detection flaws previously exposed are gathered and highlighted in Table 2. This table was fulfilled by answering the following question for every cell (every combination of environmental factor & model feature): "How does the chosen factor affect the normal behavior of the ICS, and how does it degrade the detection results of ADSs modeling this behavior and designed with the selected model feature ? " For example, the factor *Maintenance Operations* affects the behavior of the ICS *Physical System* when a physical component is modified for maintenance reasons. If this modification is slight (e.g. tool renewal), *FPs* will be produced by the ADS until the ICS behavior returns to its former state, whereas if the change is significant (e.g. addition of sensors/actuators), the ICS physical system behavior will be definitively reshaped and the ADS will perform *Outdated Detection*.

In this paper, the main objective is to give a method to analyze and orientate the choice of the behavioral ADS model features by studying the effects of environment heterogeneity and uncertainty on ADSs detection efficiency.

Environment heterogeneity leads to coverage flaws to network ADSs as a significant diversity exists among protocols and network configurations. Yet, this flaw is not as a priority for ADSs as the detection quality (FPs, Outdated and Miss detection). The heterogeneity factors mainly impact the detection quality of network-based ADS and offline-based ADSs. Indeed, service-oriented architectures are prioritized for modern ICSs, and industrial networks (level 1-2) are becoming more uncertain as they tend to offer more connectivity, accessibility and freedom to new services, devices and technologies connected to them.

Environment uncertainty causes FPs and outdated detection to control- and network-based ADSs depending on the localization of the hazardous events (e.g. network for planning uncertainties, control for physical alterations and both for human interventions). The main singularities about uncertainty factors concern the ADS design Method, Lifecycle and Nature. Indeed, this table highlights the high rate of FPs and outdated detection flaws, for learning based, offline based and deterministic ADSs. The first two features develop these flaws since their design relies on past data and knowledge to model the ICS behavior while not considering present and future modifications. The third feature experiences detection flaws due to its inability to deal with stochastic and spontaneous events occurring in uncertain environments.

Among all ADS features, stochastic, expert, online, and control-based ADSs seem to provide ideal answers to manufacturing uncertainties. Yet, this statement relies on some limitations. First, if they are designed with substantial margins and flexibility, stochastic and online-based ADSs can perform miss detection when they interpret attacks as ICS uncertainties. Besides, expert control-based ADSs suffer from model complexity explosion and coverage flaws.

5.2 Example

This example illustrates how an ADS based on a behavioral model $N1$ is affected by detection flaws when the manufacturing ICS behavior is altered by environmental uncertainties (recipe change, human intervention). The new behaviors are modeled through $N2$ and $N3$.

Let $N1(P, T, F, W, m0)$ be a Petri Net representing a manufacturing process with 3 operations, where $P = (p1, p2, p3)$ are the operations, $T = (t1, t2)$ the transitions, $F = ((p1, t1), (t1, p2), (p2, t2), (t2, p3))$ the arcs, whose weights $w \in W$ are equal to 1 and $m0(p1) = 1$ is the initial marking of the process. $N1$ is illustrated in Fig 2.

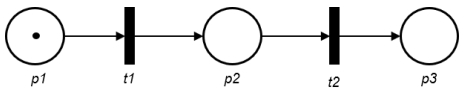

Fig. 2. Petri Net $N1$

This Petri Net is implemented in a behavioral ADS (Expert, deterministic, offline, control based) to represent the normal sequential behavior of the product flow. If the product flow deviates from this model, the ADS detects an anomaly and raises an alarm. However, this ADS detects FPs when the product flow is modified by environmental events and then deviates from the expected flow described in $N1$. Let $N2$ and $N3$ be two Petri Nets based on $N1$, yet updated to showcase the effect of two uncertainties, a change of recipe and a human intervention.

In $N2$ (Fig. 3), two places $p0a$ and $p0b$ are added to represent the initial choice of recipe between a and b, and a parallel path to the original one describes the realization of

the recipe b with a new place $p2b$ and two new transitions $t1b$ and $t2b$. In $N2$, the recipe b was chosen ($m0(p0b) = 1$), which means the token will now transit through $p2b$ to reach $p3$ from $p1$. Considering the ADS model $N1$, this new path means the non realization of the operation $p2$ between $p1$ and $p3$. This results in a false anomaly detection (FP).

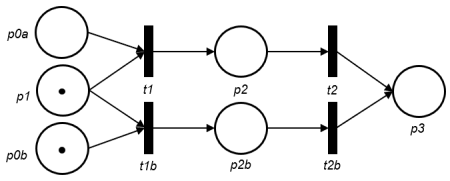

Fig. 3. Petri Net $N2$

In $N3$ (Fig. 4), a place pF is added to symbolize that the place $p2$ is free or not. In normal situation, $p2$ is initially free ($m0(pF) = 1$) and the process follows $N1$. However, in some situation, a product can get blocked on the production line between $p1$ and $p3$, resulting in $p2$ being not free ($m0(pF) = 0$). In this case, $t1$ can not be enabled and $p1$ keeps getting fed with products ($tokens$) from previous places ($p0$). To face this problematic, an operator (pOP) is requested (tOP) when $p1$ is overloaded ($w(p1, tOP) = 2$). The operator unloads manually $p1$ to feed $p3$ ($t1b$) and thus, keeps the process operational. Considering the ADS model $N1$, the human intervention means the non realization of operation $p2$ and, such as $N2$, results in a FP for the ADS.

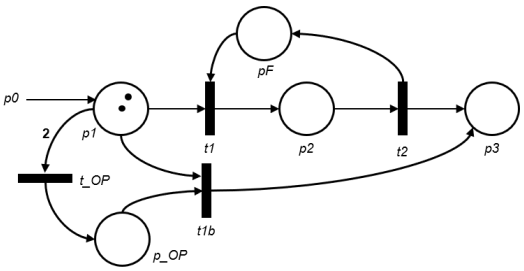

Fig. 4. Petri Net $N3$

6. CONCLUSION AND FUTURE WORKS

In this paper, behavioral ADSs were presented in regards with the main features of their models. Concurrently, the manufacturing ICSs environment was introduced in highlights of its heterogeneity and its uncertainty. An overview of the effects of this environment on behavioral ADSs detection results was submitted and illustrated through a table and an example. The main objective of this paper is to provide a method to orientate the choice of the ADS model features considering the ICS environmental characteristics. Nonetheless, this paper has to cope with some limitations and investigations that need to be addressed. First, an experimentation should be conducted on a test bed to demonstrate the validity of the ICS environmental effects on ADS detection results. Stochastic and online ADS should as well be further studied and modeled in order to prove their feasibility and their good detection results on manufacturing ICSs. Secondly, within the architectural heterogeneity factor, we have not considered independently all the existing architectural frameworks and their security practices. Indeed, depending on the framework, detection results could vary from one ICS to another. This limitation needs to be further addressed. Finally, based on a deep knowledge of the environmental uncertainties, a future work could be conducted around the ability for an ADS to distinct between attacks and other anomalies.

REFERENCES

Abu Samah, A., Shahzad, M.K., Zamaï, É., and Hubac, S. (2015). Effective Maintenance by Reducing Failure-Cause Misdiagnosis in Semiconductor Industry (SI). *IJPHM*, 6(009), 18.

Adepu, S., Brasser, F., Garcia, L., Rodler, M., Davi, L., Sadeghi, A., and Zonouz, S. (2020). Control Behavior Integrity for Distributed Cyber-Physical Systems. In *2020 ACM/IEEE 11th ICCPS*, 30–40.

Caselli, M., Zambon, E., and Kargl, F. (2015). Sequence-aware Intrusion Detection in Industrial Control Systems. *CPSS '15*, 13–24. ACM, New York, NY, USA.

Escudero, C., Sicard, F., and Zamai, E. (2018). Process-Aware Model based IDSs for Industrial Control Systems Cybersecurity: Approaches, Limits and Further Research. In *IEEE 23rd ETFA*, volume 1, 605–612.

Galloway, B. and Hancke, G.P. (2013). Introduction to Industrial Control Networks. *IEEE Commun. Surv. Tutor.*, 15(2), 860–880.

Khalili, A. and Sami, A. (2015). SysDetect: A systematic approach to critical state determination for Industrial Intrusion Detection Systems using Apriori algorithm. *J. Process Control*, 32, 154–160.

Lin, Q., Adepu, S., Verwer, S., and Mathur, A. (2018). TABOR: A Graphical Model-based Approach for Anomaly Detection in Industrial Control Systems. *ASIACCS '18*, 525–536. New York, NY, USA.

Mitchell, R. and Chen, I.R. (2014). A Survey of Intrusion Detection Techniques for Cyber-physical Systems. *ACM Comput. Surv.*, 46(4), 55:1–55:29.

Nguyen, D.T., Duong, Q.B., Zamai, E., and Shahzad, M.K. (2016). Fault diagnosis for the complex manufacturing system. *Proc. Inst. Mech. Eng. O. J. Risk. Reliab.*, 230(2), 178–194.

Panetto, H., Iung, B., Ivanov, D., Weichhart, G., and Wang, X. (2019). Challenges for the cyber-physical manufacturing enterprises of the future. *Annu. Rev. in Control*, 47, 200–213.

Rakas, S.V.B., Stojanović, M.D., and Marković-Petrović, J.D. (2020). A Review of Research Work on Network-Based SCADA Intrusion Detection Systems. *IEEE Access*, 8, 93083–93108.

Samad, T., McLaughlin, P., and Lu, J. (2007). System architecture for process automation: Review and trends. *J. Process Control*, 17(3), 191–201.

Sicard, F., Zamaï, r., and Flaus, J.M. (2019). An approach based on behavioral models and critical states distance notion for improving cybersecurity of industrial control systems. *Reliab. Eng. Syst. Saf.*, 188, 584 – 603.

Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., and Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security. *NIST Special Publication*, 255.

Vieira, G.E., Herrmann, J.W., and Lin, E. (2003). Rescheduling Manufacturing Systems: A Framework of Strategies, Policies, and Methods. *J. Sched.*, 6(1), 39–62.

Yusheng, W., Kefeng, F., Yingxu, L., Zenghui, L., Ruikang, Z., Xiangzhen, Y., and Lin, L. (2017). Intrusion Detection of Industrial Control System Based on Modbus TCP Protocol. In *IEEE 13th ISADS*, 156–162.