A hybrid intrusion detection system in industry 4.0 based on ISA95 standard

Salwa Alem, David Espes, Eric Martin, Laurent Nana, Florent de Lamotte

A hybrid intrusion detection system in industry 4.0 based on ISA95 standard

Salwa Alem[a,*], David Espes[b], Eric Martin[a], Laurent Nana[b], Florent De Lamotte[a],
[a]University Bretagne Sud, Lab-STICC (Laboratoire des Sciences et Techniques de l'Information de la Communication et de la Connaissance), Lorient, France
[b]University of Western Brittany, Lab-STICC (Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance), Brest, France

***Abstract*—Today with the emergence of an industrial information system (IIS) in industry of the future that includes the connection between all trades, applications and the converged technologies between Information Technology (IT) and Operational Technology (OT), cybersecurity has become an emergency. Industrial IDS are no longer enough to counter cyberattacks because of their natures, which is usually misuse and are unable to detect attacks that target the application layer of Open Systems Interconnection model (OSI). Therefore, cybersecurity in industrial systems adopts known IT security solutions, such as Intrusion Detection System (IDS) which has to be modified, completed and adapted to work in industrial field. We propose to deepen this approach by developing an adapted IDS to monitor industrial systems against illegitimate access and detect abnormal activities. For this purpose, we expose in this paper our efficient hybrid intrusion detection solution based on International Society of Automation 95 standard (ISA95 standard) and Neural network. Our research work is focused on Manufacturing Executive System (MES) which represents the central and main element in the industry.**

Keywords: Industry 4.0, cyber physical system, intrusion detection system, ISA95, artificial intelligence.

I. Introduction

Industry 4.0 is faced with several challenges which are summarized in flexibility, agility and corporate social responsibility requirements (CSR). The advent of this fourth industrial generation makes all devices connected and opened to the outside world, deports and stores most data in media other than the usual local hard drive as in the cloud, and connects especially the information technology (IT) world with operational technology (OT) world. This convergence is done through the Manufacturing Executive System (MES). The MES is the industrial management system that bridges the gap between the information system (IS) at the top level of the factory, namely enterprise resource planning (ERP) and the field level called the automation systems [1]. It centralizes all information concerning the production, maintenance, stock and products quality. Now that this border is opened, any attacks made in the past in the IT world can be replayed in the OT world. The notion of cybersecurity became an urgent need in industry of the future.

*Corresponding author.
Email address: salwa.alem@univ-ubs.fr

In these last years, industries were victims of attacks that came from the IT world and spread to the OT world as Stuxnet in Iran, Slammer in US, Shamoon in Saudi Arabia, Black energy in Ukraine, and Energetic bear in US. Unfortunately, the OT world today does not have all the tools to protect itself. Until now the factories mainly use as protection mechanisms, firewalls that enforce access control. While these mechanisms are very useful to restrict access to or from some parts of the network, they cannot detect attacks. As detection mechanisms, factories mainly use misuse IDS such as Bro, snort, Suricata. These IDS do not cover the wide range of industrial protocols because they mainly focus on the detection of attacks based on the Modbus protocol. Their approach consists of searching for the activity of the monitored element for the signatures of known attacks. This approach applied to intrusion detection, is very similar to that of antivirus tools and has the same disadvantages as this one. The hackers can change these signatures. Therefore, they are no longer recognized by the IDS. The main advantages of this approach are that this model is very easy to implement and optimize. It allows the separation of the software from the signatures database, thus the update can be done independently. However, their major disadvantages are the need for a daily update and the fact that they detect only known attacks. In addition, this detection system depend on the quality of signatures database. If the signatures are wrong the detection is ineffective. Another kind of IDS is the behavioral IDS used primarily in the IT world. Its implementation always requires a learning phase during which it learns the normal behavior of the monitored elements. Any other activity that deviates from the normal behavior learned is considered as abnormal. The main added value of these IDS is the fact that they detect unknown attacks like Zero-day attacks. The disadvantages of this technique are that it does not assess the degree of criticality of the attack. In addition, with this behavioral IDS it is difficult to define normal behavior especially in the IT world which changes all the time. Because of this last disadvantage, it generates a lot of false positives. For all the elements previously mentioned and thanks to MESA model that gives us a succession of transactions, step by step at the physical level, to realize a production order (PO), we can easily define a reference behavior on which a hybrid IDS can be based. Our approach is

composed of two steps. The first one is our semantic IDS based on MESA model which allows us doing the first checking level by verifying the anomalies related to the execution of PO at the application level of the industrial information system (IIS) and not at the machine (field level). By studying this model, our proposed IDS can detect 13 anomalies. In the second part of the approach, we will use the network traffic to train our neural network. Hence, we are able to distinguish anomalies from a real intrusion and reduce false positives thanks to MESA model which takes into account several anomalies related to the equipment maintenance or the stock for example. The paper is organized as follows. Section 1 provides a context and positioning of our research work. Section 2 discusses related works. Section 3 presents our approach including its two steps. Section 4 explains the experimentation environment and gives some results. And finally we finish this paper by a conclusion and perspectives.

II. CONTEXT AND POSITIONING

A. Research work positioning

Today industries need a strong security strategy. Firewalls and antivirus are not enough to protect against elaborate attacks. Their protection abilities are very limited and allow only the access control. Misuses IDS are limited because of their inability to detect attacks that do not belong to their signature databases. For all these reasons, our research focuses on behavioral IDS for overall efficiency going up to the application layer using AI techniques. For high learning efficiency, we will use the MESA model of the ISA95 standard that allows to knows the expected sequence of a production order within a factory. Consequently, the definition of a reference behavior will be precise and complete thanks to this model, and our neural network will trained from the network traffic to distinguish dysfunction from intrusion. Thus and thanks to this model, we will reduce the rate of false positives that represent a disadvantage for this kind of IDS in the IT world.

B. New cybersecurity strategy is required in industry

A few years ago factories were isolated of the outside world and so only enforced physical security. With the use of IP-based technologies and the convergence between IT and OT, factories are vulnerable to cyberattacks. Then over the years, factories are starting to use security mechanisms such as antivirus, firewall and misuse IDS. The problem with these means is that they are very limited if they work separately. In [2] and [3], the authors propose the features of firewall and misuse IDS are resumed in TABLE I.

To be effective, both of them have to work in a complementary way to. Firewalls represent the first security barrier allowing control access and IDS strengthen further security by analyzing flows authorized by firewalls. Regarding IDS, they are mainly used in IT world due to their working process that we will explain later in this paragraph. IDS can be classified according to the approach used in two kind of IDS: either misuse or behavioral.

- Misuse IDS is based on a set of attack descriptions, also called attack signatures [10]. It consists of defining attack scenarios and looking for traces of these scenarios. It uses either the machine log and this is called HIDS (Host Intrusion Detection System), or NIDS (Network Intrusion Detection System). Misuse IDS are the most used in industry.
- Behavioral IDS related to models of the normal behavior of a computer system [11]. The principle of this approach is to define a behavior reference representing the normal behavior then any activity which deviates from this reference behavior is considered as intrusion.

Thanks to MESA Model, using a behavioral IDS is now possible. This model is an abstract model of the industry including management and execution functions, different activities allowing the planing and execution of PO and the various information exchanges between these activities. Therefore, planing and execution of PO follow an accurate model that is considered by behavioral IDS as a reference. This model is explained in details in the next paragraph.

C. TOWARD AN EFFICIENT IDS BASED ON ISA95 STANDARD

The MESA model defines a generic model of operational activities [12]. It is applied to either production, maintenance, quality or stocks. This model defines information flows by categories. The data structures are detailed in 8 models (see Fig 1):

- 4 models for resource data (personnel, equipment, materials and energy, process segment).
- 4 operational data models (production capability, product definition, PPO and EPO).

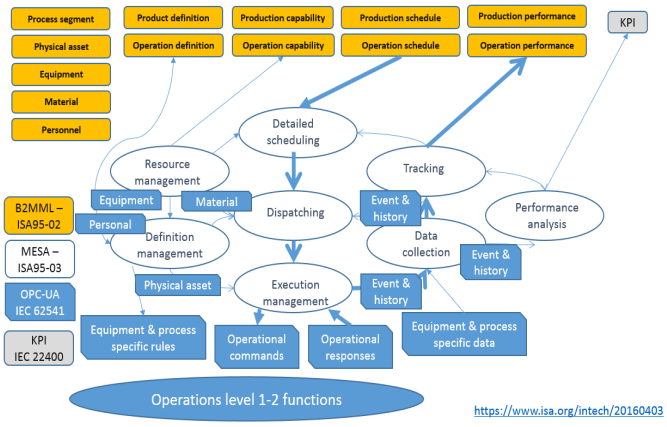

Fig. 1: Information exchange models for manufacturing operations management

The OPC Foundation, the ISA95 committee, and MESA merged their efforts to make a new model which adds ISA-95 object model representations of equipment, personnel, material, and physical assets to OPC UA 95 specification. The goal of this model is to show how OPC Foundation, the ISA95

	Firewall	IDS
Principle of working	Filters traffic based on IP address and port numbers and provides mechanism for access control to network resources.	Detects real time traffic and looks for traffic patterns or signatures of attack or deviation from the normal behavior and then generates alerts.
Advantages	* Can be hardware, software, or both. * Are network-based or host-based firewalls.	* Treat the attacks occurred in the application layer. * Treat Known and unknown attacks.
Disadvantages	* Certain threats that cannot be controlled by the firewall. * Cannot protect against malicious insiders. * It cannot give protection against connections that do not pass through it. * Cannot protect against threats new to it. * Protection against viruses is not good enough. * A firewall has to be set up by the administrator.	* Noisy and bad packets corrupt and limit the IDS. * False positives and true negatives. * Constant updating for misuse IDS is required so as to protect against new attacks and vulnerabilities. * For misuse IDS there will be lag between a new threat discovery and its signature being applied to the IDS. During this delay time the IDS will be unable to identify the threat. * Encrypted packets are not processed by most intrusion detection devices.

TABLE I: Firewalls and IDS features

committee, and MESA standards can be used together in a federated system architecture [4]

In Figure 1, B2MML defines products, material, personal, process information. This information is executed into MESA model which generates the data in the physical level. In this new architecture every material is a data publisher and exposes selected information using standard exchange models. this model has been designed to take into account exhaustively all the hazards that can happen in a factory. Therefore, anomalies related to production, maintenance hazards, inventory or quality are already taken into account. Thus, defining a behavioral IDS thanks to this model is now more precise with fewer false positives.

III. RELATED WORKS

Because of the importance of cybersecurity that has emerged with industry 4.0, several authors have proposed an industrial IDS. They mainly target the SCADA system or the field level. These IDS are split between misuse IDS, by specification or behavioral IDS that summerized as follows:

- Misuse IDS: In [5], authors propose a hybrid approach based on two types of solutions: the filter approach and the IDS to detect intrusions that can bring ICS into critical states. They use the notion of distance which will make it possible to control the distance to the critical states and thus to prevent drifts towards these states. In [6], the authors propose a comprehensive SCADA-specific IDS that is tailored for cybersecurity of IEC 61850 based SCADA networks. It consists of four modules: Access Control Detection (ACD), Protocol Whitelisting Detection (PWD), Model-Based Detection (MBD), and Multi-Parameter based Detection (MPD). Their IDS targets malformed packet attack, DoS attack, address resolution protocol (ARP) spoofing attack, and man-in the-middle (MITM) attack. Authors show that their results are better than four other works in term of accuracy detection and process time. In [7], authors target the cyber and physical part of an electrical system. Their HC-NIDS approach generates intrusion detection rules for environments that use microprocessor-based controllers and packet communications. The newness of their NIDS is that they integrate the rules of communication and security between a conventional network and a computer. These rules are coupled with information related to the

physical constraints of a system and the execution of their hybrid model of Programmable Logic Controller (PLC). The purpose of this hybridization is to mitigate cyber-physical vulnerabilities. The experimental results demonstrate the capabilities of the HC-NIDS for detecting a wide range of attacks by using the physical constraints and the overall expected behavior of the studied physical system in addition to the common communication rules that are included in their HC-NIDS

- By specification IDS: In [8], the authors propose a resilient architecture based on several principles, firstly the secured "vertical" flows (data exchanges with SCADA) in network separated from the real-time network. Secondly, the authors put probes able to detecting the Ethernet storms as well as the usurped GOOSE and transferring alerts from Ethernet IDS to SCADA. Therefore, the rewriting IED control is programmed by taking into account IDS alerts sent through SCADA. In [14], authors rely on the results of runtime checking and specification analysis to automatically infer and monitor process specifications. The specifications are represented by sets of temporal security properties on states and events corresponding to sensors and actuators.
- Behavioral IDS: In [9], the authors propose a NIDS approach for patterns learning for an industrial control network traffic. The information contained in all the cycles identified is the model of communications of the industrial control network. Their research work only targets the SCADA system. In [13], they expose an intrusion detection module that is able to detect malicious network traffic in a ICS. The Output of its detection module is communicated to the system by files containing information about the source, time and severity of the intrusion. Their results about the accuracy of the classification of the data is high but they have to improve the accuracy of their IDS with more attributes in the future. In [15], a IDS with an unsupervised learning approach is proposed. It consists of two techniques. The first is used to identify coherent and inconsistent states from unlabeled SCADA data. This is done by giving an inconsistency score to each observation using the neighbor k-nearest density factor. The second is based on proximity-based detection rules for each behavior, whether inconsistent or consistent. This approach detects 90 % of coherent and inconsistent states. In [16], the authors propose an improvement of the OCSVM method, This method takes place in an intrusion detection model based on this technique and propose an algorithm. The method takes place in several stages: Capture the data, extract the code from the function, get the samples from the learning and then test these samples. Preprocessing and normalizing the data is the step where the Modbus function sequences must be converted into short sequences, then build sample data according to the frequency of the short sequences of each mode where OCSVM can be calculated. They choose the kernel function and the appropriate parameter that reflects the accuracy rate of the model and its generalization capability as well as the other parameters to calculate the decision function and finally calculate the decision function. In this work, authors use the PSO-OCSVM model. The implementation results showed that this model has a higher classification capacity and the learning time is smaller than the traditional method. They also deduce that the model is more concise and has a strong capacity for generalization.

All these works target either the PLC level or SCADA systems but none of them deals with security of data exchange at the MES level. Our work targets the MES level based on ISA95 standard.

IV. PROPOSED APPROACH

A. RESEARCH WORK BASIS

Since the MESA model takes into account anomalies produced in the PLC, our approach focuses on the intrusions targeting the industrial information system at the MES level. Thanks to this model a list of 13 anomalies was identified (see Table II). Verifying these anomalies allows the checking of the sequencing of the execution of the PO. This first verification is done from the Business To Manufacturing Markup Language (B2MML) files comparing. Then, we added the key performance indicators (KPIs) in order to complete this model and check the temporality of this execution. These two checking steps allowed us to develop our semantic IDS. Then by analyzing the network traffic, we will develop the second intelligent behavioral IDS thanks to the neural networks. At the time of writing this paper, the development of the semantic IDS is almost finished. The next step will be analyzing the network traffic that will feed our intelligent behavioral IDS based on neural networks.

B. GLOBAL VIEW

According to [18], the two main functions of cybersecurity in ICS (Industrial Control System) are availability and integrity. Faced to the multitude of research works dealing with the data integrity and the shortage of works focusing on the integrity of the application, our approach targets the integrity of the application at the MES (Manufacturing Executive System) level which represents the central and primary element of industry of the future. The overall approach of this work consists of two IDS. The first one is a semantic IDS whose role is to check that the planned production order (which is requested by the scheduler) corresponds to the actually executed production order (what is actually produced). The inputs of this IDS are composed mainly of two B2MML files: the planned production order (PPO) and the executed production order (EPO). The PPO file represents the planning of the production order with its various parameters and its different resources (the estimated time per segment, the estimated total time of production, the estimated time between segments...). The EPO file contains all the information related to a production order that are gathered during its execution (such as the resources actually the used time per segment,

Anomalies	MESA /KPIs	Technique
Check that the response matches with the request segment	MESA	ID of OperationsResponse (in EPO file) = ID of OperationsRequest (in PPO file)
Check that the order of the segments is respected	MESA	startTime (S1) $\leq$ startTime (S2) $\leq$ StartTime (S3) (in EPO file)
Check the personal skills planned/used	MESA	PersonnelClassID (PPO file, node: PersonalRequirement) = PersonnelClassID (EPO file, node: PersonalActual)
Check that the PO is executed with the right equipment	MESA	EquipmentClassID (PPO file, node: EquipmentRequirement) = EquipmentClassID (File: EPO , node: EquipmentlActual)
Check that the PO is executed with the correct material	MESA	MaterialClassID (PPO file, node: MaterialRequirement) = MaterialClassID (EPO file, node: MaterialActual)
Check that the total expected time (AOET) is correct	KPIs	If AOET in SegmentParameter (SegmentRequirement (PPO file)) = APT in SegmentResponse (EPO file) (+/- 3 seconds[1])
Check the duration per segment (APT) is correct	KPIs	If APT in SegmentParameter (SegmentRequirement (PPO file)) = APT in SegmentResponse (EPO file) (+/- 3 seconds)
Check times between segments (ATT) is correct	KPIs	If ATT in SegmentParameter (SegmentRequirement (PPO file)) = APT in SegmentResponse (EPO file) (+/- 3 seconds)
Request arrives while the PO is not launched	MESA	segmentState(PPO file) = Released, performanceState (EPO file) = holding, Published Date and segmentData=0
Check that the quantity requested is the one manufactured	MESA	If Produced Quantity (PQ) in SegmentParameter (SegmentRequirement (PPO file)) = Produced Quantity (PQ) in SegmentResponse (EPO file)
Check if resources are available before launching the PO	MESA	Check Quantity of EquipementCapability, MaterialCapability, PersonnelCapability (Operation Capability file[2]) $\geq$ Quantity of EquipmentCapability, MaterialCapability, PersonnelActual (PPO file)
Equipment down, while sending data	MESA	Check in EPO file for production if starts time = 0
Check the launching order of PO	MESA	EndTime (Node: OperationsSchedule) (PO1) $\leq$ EndTime (Node: OperationsSchedule) (PO2) EndTime (Node: OperationsPerformance) (PO1) $\geq$ EndTime (Node: OperationsPerformance) (PO2)
Check if equipment is down while continuing to send data	MESA	Check in (EPO file, SegmentData $\neq$ 0, and in (equipment file[3], node: TestResult stringValue = Fail)

TABLE II: Anomalies taken into account in this work according to MESA model and KPIs

[1]:arbitrary, can be modified according to industrial need

[2]: file giving available resources (personal, material, equipment...)

[3]: file giving equipment resources

the used total time of production, the used time between segments.....). Our IDS compares these files and returns the results of the comparison to the operator. In the case of a deviation between the two PO, the notification will be quite explicit indicating more precisely the kind of the anomaly that is raised. At this point, our IDS can only tell us an anomaly that may be a malfunction or a real intrusion. To distinct the type of anomaly, a complementary step is required. This step is based on a behavioral IDS using neural network. It will have as inputs the system calls of the operating system of the automaton as well as the execution traces of the PLC code execution. Thus, it will be possible to decide the nature of the anomaly.

Therefore, our hybrid (semantic and behavioral) IDS is an intelligent IDS based on a standard and using powerful machine learning techniques.

C. A SEMANTIC IDS USING B2MML IMPLEMENTATION

The first part of our hybrid IDS is the semantic IDS which consists, as mentioned previously, of comparing the planned PO with the actually executed PO based on the ISA95 standard and its implementation in B2MML.

The ISA95 standard business model explains the different information exchanges required for the planning and execution of an PO (Fig 1). The implementation of this standard is the B2MML files. In this work, we use the schedule operation and the definition operation as schemes representing the planned PO, and the performance operation represents the PO actually executing.

The following figures (Fig 2 and Fig 3) show the detailed principle of this IDS:

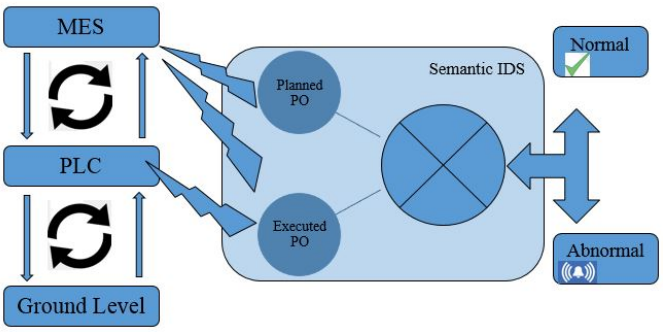

Fig. 2: Semantic IDS

all information concerning the planned PO and the executed PO is retrieved from the MES database. In addition to this information, we decided to create the KPIs in the PLC program and retrieve them from the network traffic.

Once the segment data is retrieved from both sides (the automaton and the MES), our IDS compares the semantics of the PO and checks the compliance of the PO. In case of a deviation between the B2MML files an alert is raised and sent to the operator.

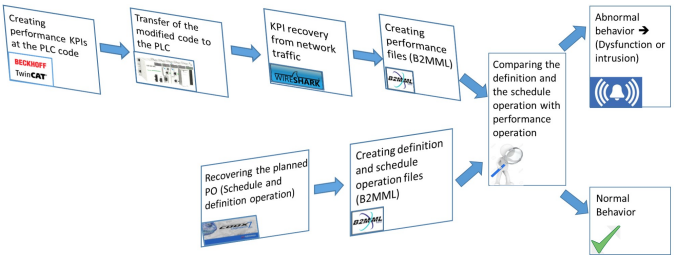

Fig. 3: Semantic IDS principle

D. AN INTELLIGENT IDS USING NEURAL NETWORK

The second step of this approach is to refine the intrusion detection so as to be able to make the difference between dysfunction and a real intrusion. To reach this goal, we intend to use the network traffic in order to define a normal behavior and to distinguish it from another abnormal behavior (Fig 4). In this part we will use the neural networks. Hence, we propose a behavioral IDS that will complement the IDS by specifications proposed in the first part of this approach. This IDS will be based on neural networks and supervised learning whose the main objective is to define rules for classifying objects in classes based on qualitative or quantitative variables characterizing these objects. This IDS will have as input the network traffic which will allow him to define the normal behavior of IIS and as outputs the result of the classification (dysfunction or intrusion)

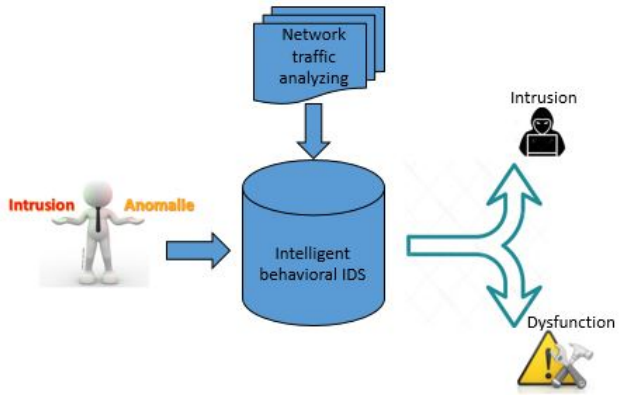

Fig. 4: Intelligent behavioral IDS

V. EXPERIMENTATION AND RESULTS

A. EXPERIMENTAL FRAMEWORK

In this research work, we used Beckhoff PLC whose OS (operating system) is a windows 7 using Twincat 3 as runtime and modbus/TCP as protocol. To remain compliant with the ISA95 standard, we have chosen a MES called COOX, that is compatible with this same standard. Thus our security solution will be fully standardized ISA95. The first step of this experiment part is firstly, the creation of B2MML files

from XSD schemas. B2MML files may be created using the tool mentioned in [20]. This tool retrieve the appropriate data from the MES database automatically and fill B2MML files with them. During this step, the planned production order file is created.
Then Then, KPI are added on the process field. To control the temporal aspects of the executed PO, the KPI needed are: - APT (Actual production time): it gives the time per segment or per work unit, - ATT (Actual transport time): it gives the time between segments, - AOET (Actual Order Execution Time): it indicates the total time of production. They are retrieved from the network traffic between the MES and the PLC and will then complete executed production order file. Semantic IDS will compare the semantics between the two PO and raise an alert if a deviation is detected.

B. RESULTS

1) Creation of the B2MML files:: Thanks to B2MML standard [18], we used XSD shemas which give an image of the MES database therefore, they give all details about the planned and the executed PO with all parameters (start time, end time, personnel, equipment and material required, segment parameters...) planned PO and executed PO files are created.
Planned PO file consists of several fields containing general information about operation production, followed by a node called OperationRequest which in turn consists of SegmentRequirements node and another for SegmentResponse. SegmentRequirements node contains general information about segment such as start time, end time, type of operation, and a nested node of the parameter segments such as time per segment and produced quantity. It also consists of estimated personnel, equipment, material and physical asset and finally the last node on the segment responses which represents the estimated parameter.
Executed PO file consists of fields containing general information about the operation and a node named OperationResponses, which in turn consists of the SegmentResponses node. SegmentResponses node contains general information about segment such as start time, end time, type of operation. A nested node of SegmentData containing actual data (actually made) such as duration per segment and produced quantity (added KPIs). It also consists of actual personnel, equipment, material and physical asset responses. Figures 6 and 7 show respectively parts of both files:

2) Creation of KPI:: KPIs were created in Beckhoff program using visual studio and Twincat 3 (see Fig 7). Then a production cycle were launched. During a production run, the previously mentioned KPIs were retrieved to complete our B2MML files representing the planned PO and the executed PO. The goal of this KPIs is to check the temporal aspects of the execution of the PO. To be compliant with the MESA model, these KPI are required. The programmer should systematically add these KPI in their program.

3) Semantic IDS:: After creating KPI and B2MML files, it comes the role of our semantic IDS which is detecting the

```
<b2mml:OperationsSchedule xmlns:b2mml="http://www.mesa.org/xml/B2MML-V0600"
    <b2mml:ID>Ordo-26032019</b2mml:ID>
    <b2mml:Description>Déplacement des palettes</b2mml:Description>
    <b2mml:HierarchyScope>
        <b2mml:EquipmentID>Convoy-SCAP</b2mml:EquipmentID>
        <b2mml:EquipmentElementLevel>Unité</b2mml:EquipmentElementLevel>
    </b2mml:HierarchyScope>
    <b2mml:OperationsType>Mixe</b2mml:OperationsType>
    <b2mml:StartTime>09:00:00 26-03-2019</b2mml:StartTime>
    <b2mml:EndTime>09:05:00 26-03-2019</b2mml:EndTime>
                                .
                                .
    <b2mml:SegmentParameter>
        <b2mml:ID>APT-S4</b2mml:ID>
        <b2mml:Description>la durée dans poste 4</b2mml:Description>
        <b2mml:Value>
            <b2mml:ValueString>1,450</b2mml:ValueString>
```

Fig. 5: Planned production order file

```
<b2mml:OperationsPerformance xmlns:b2mml="http://www.mesa.org/xml/B2MML-V0600"
    <b2mml:ID>Op-def1</b2mml:ID>
    <b2mml:Description>Déplacement des palettes</b2mml:Description>
    <b2mml:HierarchyScope>
        <b2mml:EquipmentID>normalizedString</b2mml:EquipmentID>
        <b2mml:EquipmentElementLevel>Unité</b2mml:EquipmentElementLevel>
    </b2mml:HierarchyScope>
    <b2mml:OperationsType>Production</b2mml:OperationsType>
    <b2mml:OperationsScheduleID>Ordo-26032019</b2mml:OperationsScheduleID>
    <b2mml:StartTime>09:00:00 26-03-2019</b2mml:StartTime>
    <b2mml:EndTime>09:05:00 26-03-2019</b2mml:EndTime>
                                .
                                .
    <b2mml:SegmentParameter>
        <b2mml:ID>APT-S4</b2mml:ID>
        <b2mml:Description>la durée dans poste 4</b2mml:Description>
        <b2mml:Value>
            <b2mml:ValueString>1,450</b2mml:ValueString>
```

Fig. 6: Executed production order file

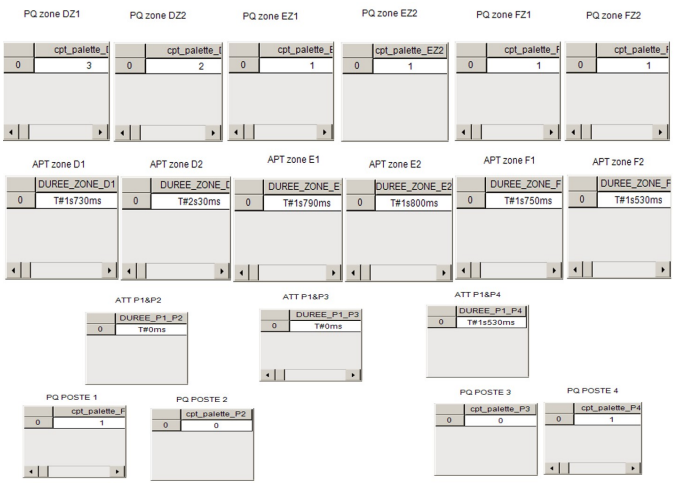

Fig. 7: Temporal key performance indicators

different anomalies. Semantic IDS can handles several anomalies. In this article, we look at fourteen kinds of anomalies:

- Compliance between segment request in (PPO file) and segment response (EPO): it is the action to check that the EPO response is the expected one i.e., the response is related to the PPO request and not forged by an attacker.
- Sequencing segment control: the IDS checks that the segment order is respected.
- Compliance between the personnel class in PPO file and the one in EPO file which checks that the right used staff is the planned one.
- Compliance between the equipment class in PPO file and

the one in EPO file which checks that the right used machine is the planned one.
- Compliance between the materialclass in PPO file and the one in EPO file which checks that the right used material is the planned one.
- Compliance between APT, ATT, AOET and produced quantity excepted with those realized.
- Equipment down control: IDS checks that equipment is not working.
- Equipment down control: IDS Check that the equipment is down or compromised while continuing to send data
- Compliance resource: IDS checks resources before launching PO.
- Compliance of the sequencing of PO execution : IDS verifies that the first planned PO is executed firstly and the last one is executed in the end of the planning.
- Compliance between PO launching and request: which check if Request arrives while the OF is not launched.

Based on this matrix of anomalies as a basis for work, we developed a semantic IDS to browse our B2MML files (PPO and EPO) and then check the conformity of the OF. This verification is an anomaly anomaly or a set of anomaly that interests us or all the anomalies at once (see Fig 8)

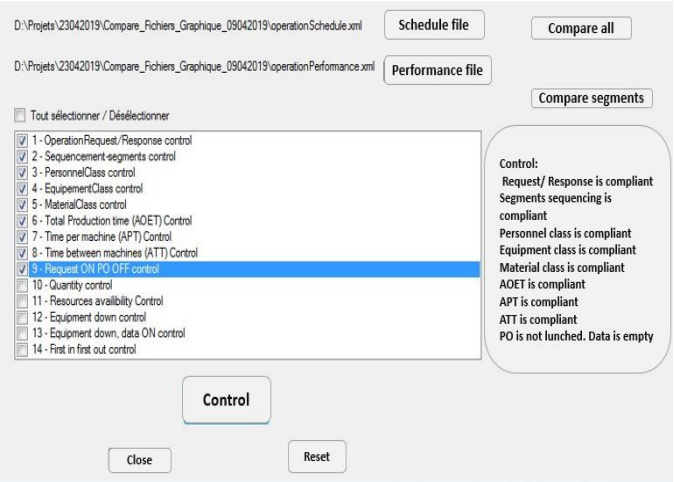

Fig. 8: Semantic IDS tool

At this stage, the IDS can detect an anomaly. However it cannot know the nature of the anomaly (malfunction or intrusion). Hence the goal of our intelligent behavioral IDS is to refine intrusion detection thanks to network traffic between COOX MES and Beckhoff PLC and also the PLC code execution traces.

VI. Conclusion and perspectives

This work proposes an efficient and intelligent way without any latency in industrial control systems through the proposal of a behavioral IDS. Due to the information provided by the MESA model, a low rate of false positive alarms is expected. To manage the dynamic aspect of ICS, specific KPI are required. All programmers should add these KPI during the implementation phase to monitor the temporal aspects of an industrial workshop. At this moment, our semantic IDS can detect 13 anomalies. However it is not able to distinct an attack from a failure. In future works, new features will be added to our semantic IDS. Neural network will be used to detect attacks in the network traffic. It is also planned to explore another track that consists of analyzing the traces of PLC code execution in order to couple it with network traces for a better analysis of an industrial behavior.

References

[1] G. Rajesri and C. D. R, Manufacturing Execution System Design using ISA-95, vol. 980, pp. 248252, 2014.

[2] C. V. Jean-Francois MICHEL, Annie NORMAND, Cyberscurit dans lindustrie, 2016.

[3] Kaspersky Lab, La cyberscurit industrielle est diffrente, 2016.

[4] D. Brandl, Factory Automation: New integration architectures for federated systems - ISA, 2016. [Online]. Available: https://www.isa.org/intech/20160403/. [Accessed: 06-Jun-2018].

[5] F. Sicard et al., Approche filtre base sur la notion de distance pour la dtection des cyberattaques To cite this version: HAL Id: hal-01562589 Approche filtre base sur la notion de distance pour la dtection des cyberattaques, 2017.

[6] J. Lee, H. A. Kao, and S. Yang, Service innovation and smart analytics for Industry 4.0 and big data environment, Procedia CIRP, vol. 16, pp. 38, 2014.

[7] G. Koutsandria, V. Muthukumar, M. Parvania, S. Peisert, C. McParlan, and A. Scaglione, A Hybrid Network IDS for Protective Digital Reays in the Power Transmission Grid, vol. 71, pp. 908913, 2006.

[8] S. Mocanu, P. Bellemain, J. Thiriet, and E. Savary, Architecture des systmes dautomatisation des postes rsiliente aux attaques des trames GOOSE, pp. 110, 2013.

[9] R. R. R. Barbosa, R. Sadre, and A. Pras, Exploiting traffic periodicity in industrial control networks, Int. J. Crit. Infrastruct. Prot., vol. 13, pp. 5262, 2016.

[10] S. Kumar, and E. Spafford, A Software Architecture to Support Misuse Intrusion Detection, Department of Computer Sciences, Purdue University, Mar. 1995.

[11] D. E. Denning, An intrusion detection model, in IEEE Transactions on software engeneering, SE-13 :222232, 1987.

[12] M. E. Systems, Production , gestion et MES: LISA95 devient internationale, pp. 25, 2003.

[13] L. A. Maglaras and J. Jiang, Intrusion detection in SCADA systems using machine learning techniques, 2014 Sci. Inf. Conf., no. August, pp. 626631, 2014.

[14] O. Koucham, G. Hiet, and J. Thiriet, Secure IT Systems, vol. 10014, pp. 2036, 2016.

[15] A. Almalawi, X. Yu, Z. Tari, A. Fahad, and I. Khalil, An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems, Comput. Secur., vol. 46, pp. 94110, 2014.

[16] W. Shang, L. Li, M. Wan, and P. Zeng, Industrial communication intrusion detection algorithm based on improved one-class SVM, 2015 World Congr. Ind. Control Syst. Secur. WCICSS 2015, pp. 2125, 2016.

[17] ANSSI, Cybersecurity for Industrial Control Systems Classification Method and Key Measures, 2014.

[18] "https://services.mesa.org/ResourceLibrary/ShowResource/0f47758b-60f0-40c6-a71b-fa7b2363fb3a"

[19] E. Moones, Proposition d une approche m ethodologique d interop erabilit e multi-niveaux dans un environnement de PLM collaboratif Th ‘ ese, 2017.