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 in industry of the future which includes the connection between all trades, applications and the converged technologies between information technology and operational technology, cybersecurity has become urgent. Industrial Intrusion Detection System are no longer sufficient to counter cyberattacks because of their natures, which is usually misuse, and are unable to detect attacks that target the application layer of the Open Systems Interconnection model. Therefore, cybersecurity in industrial systems adopts known information technology security solutions, such as an Intrusion Detection System 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 and neural network. Our research work is focused on Manufacturing Executive System which represents the central and main element in industry.**

Keywords: Industry 4.0, cyber physical system (CPS), intrusion detection system (IDS), ISA95, artificial intelligence.

I. Introduction

Industry 4.0 is faced with several challenges which are summarized as flexibility, agility and corporate social responsibility requirements (CSR). The advent of this fourth industrial generation means that all devices are connected and open to the outside world, most data is deported and stored in media other than the usual local hard drive such as in the Cloud, and the information technology (IT) world is specifically connected to the operational technology (OT) world. This convergence is performed 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 open, any attacks made in the past in the IT world can be replayed in the OT world. The notion of cybersecurity has become an urgent need in industry of the future.

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

In recent years, industries have been victims of attacks that came from the IT world and spread to the OT world such as Stuxnet in Iran, Slammer in US, Shamoon in Saudi Arabia, and Black energy in Ukraine [21]. Unfortunately, the OT world today does not have all the tools necessary to protect itself. Until now factories have mainly used firewalls as protection mechanisms 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.
Factories mainly use misuse IDS such as Suricata and Snort as detection mechanisms. Their approach consists of searching for the activity of the monitored element among known signatures attacks. The main advantage of this approach is that it allows the separation of the software from the signatures database, thus the update can be done independently. However, its major disadvantages are that the hackers can change these signatures. Therefore, they are no longer recognized by the IDS. They need a daily update and the detect only previously known attacks. In addition, this detection system depends on the quality of the signatures database. Both of Snort and Suricata have their specific limitations which discouraged us to use them. For instance, Snort is not suitable with high-speed networks, its decoders are limited, and its signatures base is unreliable [2]. Another kind of IDS is the behavioral one which is 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[22]. 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. There some IDS which are both misuse and behavioral such as Bro but the problem with Bro the fact that it is difficult to set up and configure because of its used scripting language and the need to have a solid knowledge in UNIX environment to handle it [2].

For all of the elements previously mentioned and thanks to MESA model (see Fig 1) that gives us a succession of transac-

tions, 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. This model defines a general request-response cycle that starts with requests or schedules, converts them into a work schedule, dispatches work according to the schedule, manages the execution of work, collects data and converts the collected data back into responses [3].

Our approach is composed of two steps. The first step is our semantic IDS based on the MESA model which enables the first of verification by checking the anomalies related to the execution of the 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 step, we use 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 illustrates results. The paper is completed by a conclusion and perspectives.

II. CONTEXT AND POSITIONING

A. Research work positioning

Today's industries need a strong security strategy. Firewalls and antivirus protection are not enough efficient 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 use the MESA model of the ISA95 standard that knows the expected sequence of a production order within a factory. Consequently, the definition of a reference behavior will be precise and complete due to this model, and our neural network will be 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 from the outside world and so only enforced physical security. With the use of IP-based technologies and the convergence between IT and OT, factories have become vulnerable to cyberattacks. Then over the years, factories started to use security mechanisms such as antivirus's, firewalls and misuse IDS. The problem with these means is that they are very limited if they work separately. In [4] and [5], the authors summarize the advantages and the limitations of firewall and IDS. The main difference between the two securing means is that the firewalls function is the access control and the fact that they are very limited for detecting intrusions. As for IDS, their main function is the attacks detection using either the misuse approach or the behavioral approach.

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

- Misuse IDS is based on a set of attack descriptions, also called attack signatures [11]. 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 commonly used in industry.
- Behavioral IDS relates to models of the normal behavior of a computer system [12]. 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 an intrusion.

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

C. TOWARDS AN EFFICIENT IDS BASED ON THE ISA95 STANDARD

The MESA model defines a generic model of operational activities [13]. 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 resource data models (personnel, equipment, materials and energy, process segment).
- 4 operational data models (production capability, product definition, PPO and EPO).

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 an OPC UA 95 specification. The aim of this model is to show how the OPC Foundation, the ISA95 committee, and MESA standards can be used together in a federated system architecture [6].

In Figure 1, B2MML defines products, material, personnel and process information. This information is implemented into the MESA model which generates the data in the physical level. In this new architecture every material is a data publisher

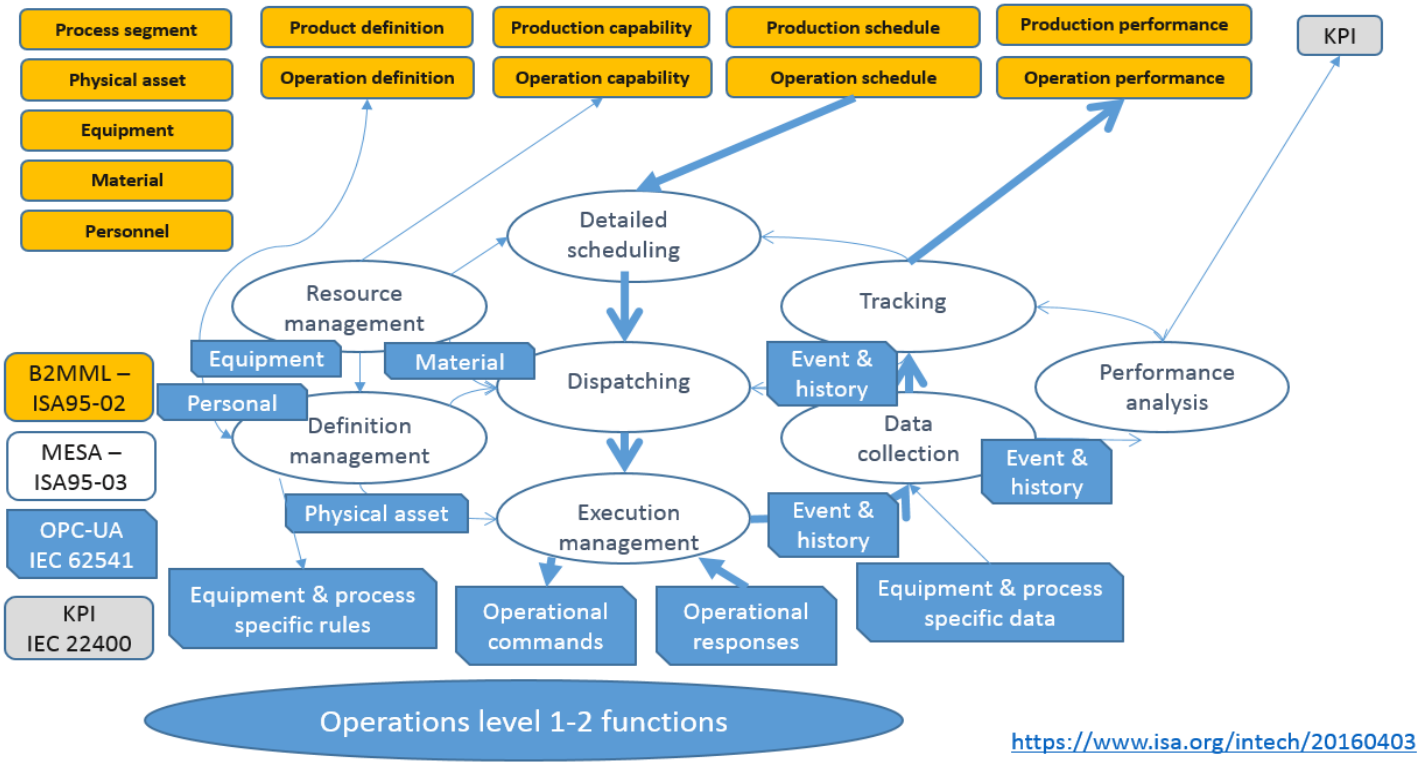

Fig. 1: Information exchange models for manufacturing operations management

and exposes selected information using standard exchange models. This model has been designed to take into account exhaustively, all the hazards that can occur in a factory. Therefore, anomalies related to production, maintenance hazards, inventory or quality have already been taken into account. Thus, defining a behavioral IDS using 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 a misuse IDS, by specifications or a behavioral IDS that are summarized as follows:

- Misuse IDS: In [7], authors propose propose an IDS which consists of two modules for collect of the incoming and the outgoing metadata from the network nodes, an anomaly detection controller and a rules database. The controller receives the metadata coming from the collection modules, it sends them to a logical engine for the analysis according to the rules stored in the database. These rules represent patterns describing normal behavior. If there is a difference with this normal behavior, an alert is raised by an alert generator. In [8], the authors propose a comprehensive SCADA-specific IDS that is tailored for the 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). The authors demonstrate that their results are better than four other works in terms of accuracy detection and process time. In [9], the 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 novelty 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 a 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 [10], the authors propose a resilient architecture based on several principles, firstly the secured ”vertical” flows (data exchanges with SCADA) in a network separated from the real-time network. Secondly, the authors positioned probes capable of detecting Ethernet storms as well as the usurped GOOSE and transferring alerts from an Ethernet IDS to SCADA.

Therefore, the rewritten IED control is programmed by taking into account IDS alerts sent through SCADA. In [16], 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 [14], the authors propose a NIDS approach. They propose learning patterns for an industrial control network traffic. The information contained in all the cycles identified is the communication model of the industrial control network. This research work targets only the SCADA system. In [17], an IDS with an unsupervised learning approach is proposed. It consists of two techniques. The first is used to identify consistent 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 consistent and inconsistent states. In [18], 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: data capture, extracting the code from the function, obtaining samples from the learning and then testing these samples. Preprocessing and normalizing the data is the step where the Modbus function sequences must be converted into short sequences, then sample data is build according to the frequency of the short sequences of each mode where OCSVM can be calculated.
  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 have been chosen. In this work, authors use the PSO-OCSVM model. The implementation results show that this model has a higher classification capacity and the learning time is less 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 the 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 industrial information systems at the MES level. Using this model, a list of 13 anomalies was identified (see Table I). Verifying these anomalies enables the checking of the sequencing of the execution of the PO to be checked. This first verification is performed from the Business To Manufacturing Markup Language (B2MML) files comparison. Then, we added the key performance indicators (KPIs) in order to complete this model and check the temporality of this execution. These two verification steps enabled us to develop our semantic IDS. Then by analyzing the network traffic, we will develop the second intelligent behavioral IDS using the neural networks. At the time of writing this paper, the development of the semantic IDS was almost finished. The next step will be to analyze the network traffic that will feed our intelligent behavioral IDS based on neural networks.

B. GLOBAL VIEW

According to [20], the two main functions of cybersecurity in an ICS (Industrial Control System) are availability and integrity. Faced with the multitude of research works that deal with data integrity, and the shortage of studies 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 (that 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 used per segment, the total time taken for production, the time taken 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 anomaly that is raised. At this point, our IDS can only tell us that an anomaly that may be a malfunction or a real intrusion. To distinguish the type of anomaly, a complementary step is required. This step is based on a behavioral IDS using a 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 on the nature of the anomaly.

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

C. A SEMANTIC IDS USING B2MML IMPLEMENTATION

The first step of our hybrid IDS is the semantic IDS which consists, as mentioned previously, of comparing the planned PO with the PO actually executed 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

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 personnel skills planned/used	MESA	PersonnelClassID (PPO file, node: PersonnellRequirement) = PersonnelClassID (EPO file, node: PersonnelActual)
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 is broken 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 I: 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 (personnel, material, equipment...)

[3]: file giving equipment resources

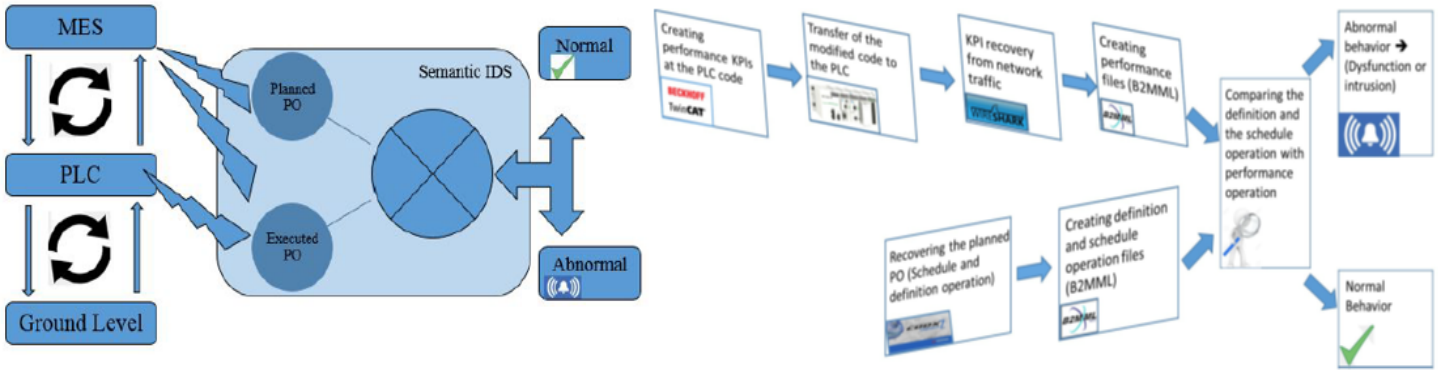

Fig. 2: Semantic IDS principle

of a PO (Fig 1). The implementation of this standard is through the B2MML files. In this work, we use the operation schedule and the operation definition as schemes representing the planned PO, and the performance operation represents the PO actually executed. Fig 2 illustrates the detailed principle of this 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 the case of a deviation between the B2MML files an alert is raised and sent to the operator.

D. AN INTELLIGENT IDS USING A NEURAL NETWORK

The second step of this approach is to refine the intrusion detection to be able to distinguish the difference between a dysfunction and a real intrusion. To reach this goal, we intend use the network traffic in order to define a normal behavior and to distinguish it from another abnormal behavior. In this section, we will use the neural networks. Therefore, 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 main objective is to define the rules for classifying objects in classes based on qualitative or quantitative variables characterizing these objects. This IDS will have the network traffic as input which will enable it to define the normal behavior of the Industrial Information System (IIS) and as outputs the results of the classification (dysfunction or intrusion)

V. EXPERIMENTATION AND RESULTS

A. EXPERIMENTAL FRAMEWORK

It should be mentioned in this section that this work is still at the beginning of its evaluation and that more mature results will be presented shortly. We used for our experimentation, Beckhoff PLC whose OS (operating system) is 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 experimental part is firstly, the creation of B2MML files from XSD schemas. B2MML files may be created using the tool mentioned in [22]. This tool retrieves the appropriate data from the MES database automatically and fills B2MML files with them. During this step, the planned production order file is created.

Then, KPIs are added to 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 the executed production order file. The 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**:* Due to B2MML standard [19], we used XSD schemas which give an image of the MES database. Therefore, they give all details about the planned and the executed PO with all the parameters (start time, end time, personnel, equipment and material required, segment parameters...) planned PO and executed PO files are created (see Fig 3). The planned PO file consists of several fields containing general information about production operation, followed by a node called OperationRequest which in turn consists of a SegmentRequirements node and another for SegmentResponse. The SegmentRequirements node contains general information about the segments such as start time, end time, type of operation, and a nested node of the parameter segments such as time per segment and quantity produced. It also consists of estimated personnel, equipment, material and physical assets and finally the last node on the segment responses which represents the estimated parameter.

The Executed PO file consists of fields containing general information about the operation and a node named OperationResponses, which in turn consists of the SegmentRe-

```
<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>
```

```
<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. 3: Planned production order file

sponses node. The SegmentResponses node contains general information about the 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.

*2) **Creation of KPIs**:* KPIs were created in the Beckhoff program using Visual Studio and Twincat 3 (see Fig 4). Then a production cycle vas launched. During a production run, the previously mentioned KPIs were retrieved to complete our B2MML files representing the planned PO and the executed one. The aim of these KPIs is to check the temporal aspects of the execution of the PO. To be compliant with the MESA model, these KPIs are required. The programmer should systematically add these KPIs to their program.

*3) **Semantic IDS**:* After creating KPI and B2MML files, it is then the role of our semantic IDS to detect the different anomalies. The semantic IDS can handle several anomalies. In this article, we looked at fourteen kinds of anomalies:

- The compliance between the segment request in the PPO file and the segment response in the EPO file: the action is 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.

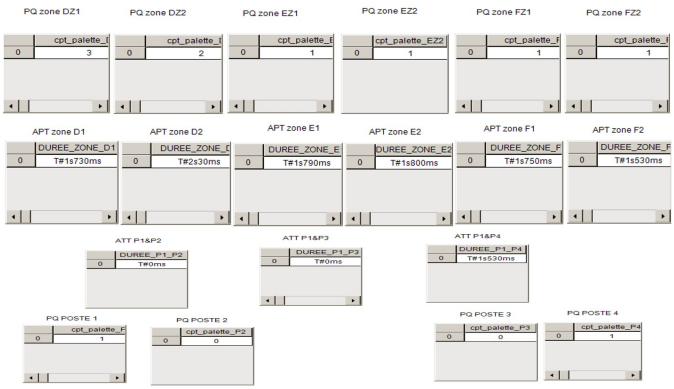

Fig. 4: Temporal key performance indicators

- Compliance between the personnel class in the PPO file and the one in the EPO file which checks that the staff used are the ones that were planned to be used.
- Compliance between the equipment class in the PPO file and the one in the EPO file which checks that the machine used is the one that was planned to be used.
- Compliance between the materialclass in the PPO file and the one in the EPO file which checks that the materials used are the ones that were planned to be used.
- Compliance between APT, ATT, AOET and the expected produced quantity with those actually produced.
- Equipment down control: IDS checks that the equipment is not working.
- Equipment down control: IDS checks that the equipment has broken down or is compromised whilst continuing to send data
- Compliance resource: IDS checks resources before launching the PO.
- Compliance of the sequencing of the PO execution : IDS checks that the first planned PO is executed first and the last one is executed at the end of the planning.
- Compliance between the PO launch and request: which checks if the request arrives while the OF is not launched.

Based on this matrix of anomalies as a basis for our work, we developed a semantic IDS. User browses B2MML files (PPO and EPO) and then checks the conformity of the PO. One or a set of anomalies that interests operator can be chosen according to his requirements (see Fig 6)

At this stage, the IDS can detect an anomaly. However, it cannot determine the nature of the anomaly (malfunction or intrusion). Hence, the aim of our intelligent behavioral IDS is to refine intrusion detection using network traffic between COOX MES and Beckhoff PLC and also the PLC code execution traces. As previously mentioned, intelligent behavioral IDS will be based on the neural network. This latter will be trained and tested by a data set which we will build from the actual data collected from our laboratory production line. In this data set, several attacks scenarios will be put in place. The simulated attacks will be DOS, MITM attacks and OS Beckhoff's vulnerabilities exploitation (Windows 7).

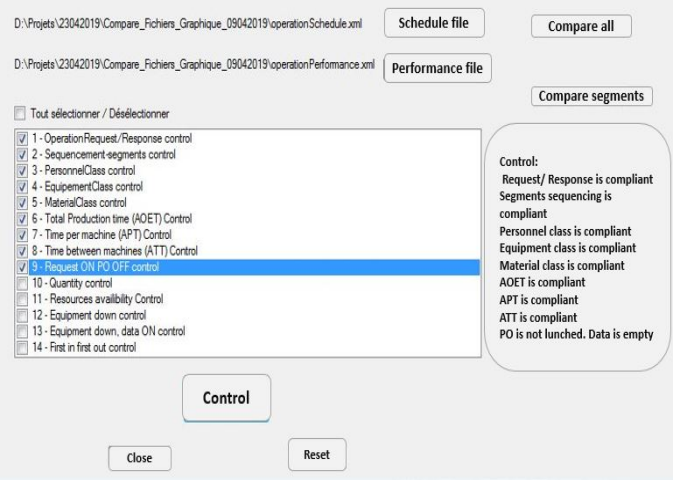

Fig. 5: Semantic IDS tool

A tool analyzing and extracting the metrics from a network capture will be developed, allowing us getting a training set for RNs. This tool will be based on the work quoted by [] and enriched according to our needs. Knowing the main limitation of this existing tool (OSI application protocols are not supported), we decided to develop our own tool that analyzes even Modbus protocol.

This approach has some limitations that are summarized in the following points:

- This approach is valid for industries that are compatible with the ISA95 standard since it is based on the use of the B2MML schemas that are implemented.
- The ISA95 standard already takes certain anomalies related to the maintenance, stock and conformity of the material into account. Nevertheless, if human intervention occurs during the industrial process for any reason, this may increase the number of false positives. This point can be mitigated with the automation aspect and predictive maintenance of the industry of the future.
- For intelligent IDS, if the system or the production chain changes, another learning phase must be done to learn the new behavior of the new system.
- The interpretability of the KPIs must be dynamic and adaptable to each production line.

VI. Conclusion and perspectives

This work proposes an efficient and intelligent method 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 thanks to the fact that the MESA model takes already into account false alerts raised because of the scheduled maintenance, the non-provisioning of the inventory, or the non-compliant product. Then comes the step of the second IDS which defines the nature of the alert raised.

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 the moment, our semantic IDS can detect 13 anomalies. However it is not able to distinguish an attack from a failure. In future works, more matures results will be exhibited, 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 avenues that consist of analyzing the traces of PLC code execution in order to couple it with network traces for a deeper analysis of industrial behavior.

References

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

[2] P. Mehra, A brief study and comparison of Snort and Bro Open Source Network Intrusion Detection Systems; International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Int. J. Adv. Res. Comput. Commun. Eng. Vol. 1, Issue 6, August 2012, vol. 1, no. 6, pp. 383386, 2012.

[3] "sagaweb.afnor.org/fr-FR/sw/Consultation/Xml/1282104/?lng=FR&supNumDos=FA149598"

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

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

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

[7] RA Mixer, GK Law, AE Cutchin, Anomaly detection in industrial communications networks, US Patent App. 10/291,506, 2019.

[8] 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.

[9] 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.

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

[11] V. K. C. Sriram Sundar Rajan, An Overview of Intrusion Detection System, Int. J. Res. Appl. Sci. Eng. Technol., vol. 3, no. VI, pp. 559563, 2015.

[12] M. Dacier and A. Wespi, Towards a taxonomy of intrusion-detection systems, 1999.

[13] C. Johnsson, ISA 95 - how and where can it be applied?, Instrumentation, Syst. Autom. Soc., no. August, pp. 111, 2004.

[14] 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.

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

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

[17] 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.

[18] 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.

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

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

[21] C. Wueest, Targeted Attacks Against the Energy Sector, Symantec Corp., pp. 129, 2014.

[22] U. H. R. Nayak, Intrusion Detection and Prevention Systems, Springer, p. pp 225-243, 2014.