International Journal of Innovation in Enterprise System, Volume 3, Issue 02, July 2019, pp 31-41

An Insider Threat Categorization Framework for Automated Manufacturing Execution System

Nur Ameera Natasha Mohammad[1], Warusia Mohamed Yassin[2], Rabiah Ahmad[3], Aslinda Hassan[4], and Mohammed Nasser Ahmed Al Mhiqani[5]

[1,2,3,4,5]Center for Advanced Computing Technology, Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka

ameeramohamad88@gmail.com, s.m.warusia@utem.edu.my, rabiah@utem.edu.my, aslindahassan@utem.edu.my, almohaiqny@gmail.com

Corresponding author: Nur Ameera Natasha Mohammad
Received: 15 September 2018, Accepted: 17 January 2019, Published: 13 July 2019

***Abstract*—**Insider threats become one of the most dangerous threats in the cyber world as compared to outsider as the insiders have knowledge of assets. In addition, the threats itself considered in-visible and no one can predict what, when and how exactly the threat launched. Based on conducting literature, threat in Automated Manufacturing Execution Systems (AMESs) can be divided into three principle factors. Moreover, there is no standard framework to be referring which exist nowadays to categorize such factors in order to identify insider threats possible features. Therefore, from the conducted literature a standard theoretical categorization of insider threats framework for AMESs has been proposed. Hence, three principle factors, i.e. Human, Systems and Machine have considered as major categorization of insider threats. Consequently, the possible features for each factor identified based on previous researcher recommendations. Therefore, via identifying possible features and categorize it into principle factors or groups, a standard framework could be derived. These frameworks will contribute more benefit specifically in the manufacturing field as a reference to mitigate an insider threat.

***Keywords*—**automated manufacturing execution systems insider threats, factors and features, insider threat categorization framework.

I. INTRODUCTION

An insider threats can be defined as a possible harm which launch against assets of an organization which usually this kind of activity could be divide into intentional and unintentional, based on several participation of people such as current or former employee, supplier, contractor and business partner [1].

Moreover, as contrast to human participation, there is also some participation from an-other contributor such as in unintentional threat contains malfunction of equipment and outsource operation downfall [2]. The malfunction of equipment defined as the unexpected abnormal operation of hardware or devices which directly affect the capability of a system to control and keep the private information safely due to loss of data loss instantaneous. In addition, outsource operation downfall defined as failure to protect the security element in outsourcing operation which resulting in loss of information capability, availability and integrity [2]. Hence, those mentioned participation contributor can become as threats within organization as these will affect the image or reputation of an organization.

Along with the participation from above contributor, [3] has divided the aim of the insider threats into three categories, namely motive, opportunity and capability. The first element called as motive which explained as motivations or encouragement of insider attacker to perform threat. In addition, the next element so called as an opportunity defined as the objective of insider to perform threat using the knowledge about an organization that insider has gathered. Moreover, the third element called as a capability defined as the power of an insider has to launch the threat through the accessibility obtained. For example, previously proposed model called Capability Means Opportunity (CMO) estimates a person, social, and administrative or organizational factor for insider threat detection. Moreover, for an effective insider threat case to happen, an insider requires the ability to compel a threat, the motive to do so, and the opportunity to compel the crime [4], [5], [6], [3] For better understanding, the abovementioned CMO model has illustrated in Fig. 1.

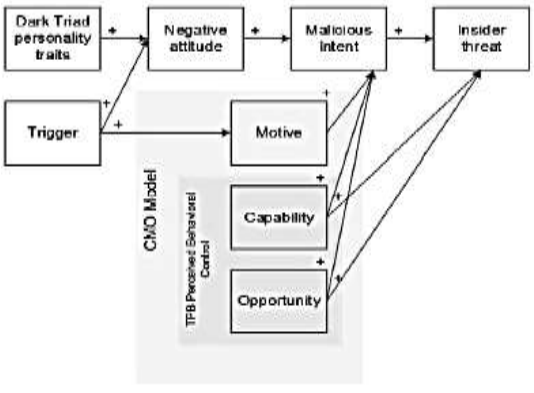

Fig. 1 CMO Model for insider threat detection (adapted from [3])

Based on the Fig. 1, motive explained as predicated of evidential circumstances of external circumstances that can incite the emotion such as a motive for financial and personal gain, revenge, thrill and competitive advantage [7], [4], [8]. Besides the element of motive, the capability (also can be referred as power) of an insider (also can be referred as human) has defined as sophistication dimensions of insider threats which having right and knowledge about how the organizational system works to pass the access which may facilitate to launch threat. Other than that, opportunity refers as the insider's ability to exploit the weakness or vulnerabilities of organizational systems [4]. Therefore, with the knowledge of organizational weaknesses such as unclear, outdated or nonexistence security policies and poor access control configurations on systems can lead insiders to launch the attack/harm without doubt using this opportunity [4]. Besides that, author [9] has defined trigger as unexpected negative events that happened around the insiders which can motivate themselves to behaving negatively. Some example of negative events is losing control, does not receive any rewards and promotion. With those negative events listed, author [3] reported that the insider can generate a negative attitude towards an organization and can either create or intensify a motive.

From these two elements of insider threat contributor, an insider can directly perform a malicious intention towards an organization supported with opportunity and capability an insider has. However, without capability and opportunity element, an insider obstructed from performing threat because of not having knowledge about an organization and the power to access inside the organization. In contrast, the situation of insider that have the knowledge and power to pass through access of an organization can be different. As illustrated in the proposed CMO model above, those three main elements need to be fulfilled by an insider to completed insider threats. On the other side of view, the element of insider threat contributor from illustrated model can be applied by the outsider who might have motive and capability to launch any threats toward the organization. With a motive to harm the organization as encouragement and capability to access into an organization, an outsider can perform threat easily. Unfortunately, an outsider might have possibility to get caught as he/she does not know the right place or vulnerabilities (opportunity) that suitable for the threat. Therefore, for an outsider to perform threat without being recognized within an organization will be difficult because each of the elements have their own contribution to completed insider threat performance.

Besides the studies on motive, opportunity and capability of insider threats by author [3] above, author [10] has proposed the insider threat taxonomy with various terminologies that categorized by combining a few related terms of insider threat, including access, motivation or inspiration of threats, the indicator used by insiders, types and activities performed, user profile categorization, methods used and some detection techniques proposed to mitigate insider threats. For better understanding, the abovementioned of insider threat taxonomy has illustrated in Fig. 2 below.

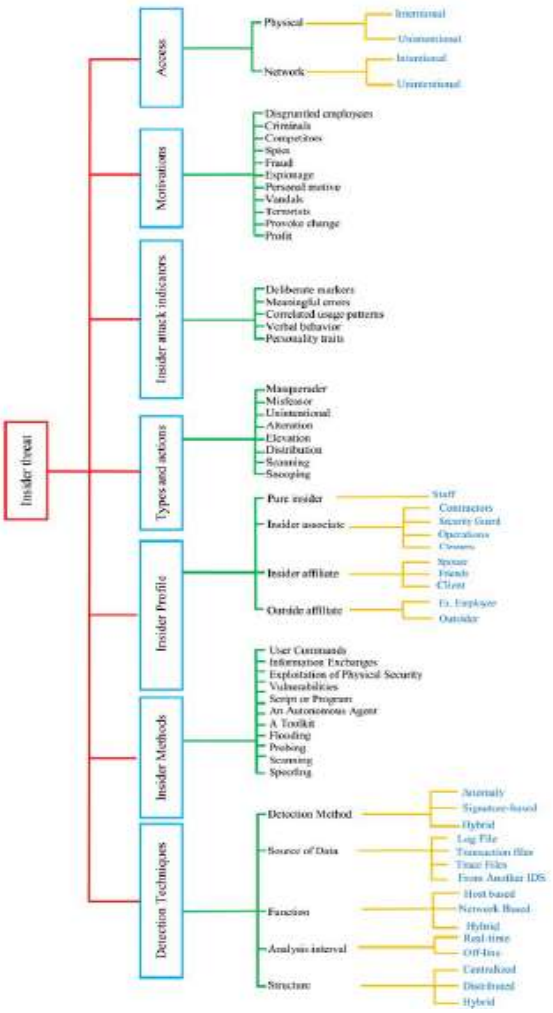

Fig. 2 The taxonomy of insider threat (adapted from [10])

The element in an access category includes whether the insider intentionally or unintentionally get physical access or network access to be inside the organization before launch any harm or threat. Other than that, in motivation category, each of the motivation are different as it depends on the type of insider. For example, the motivation of disgruntled employees, mostly because of the unsatisfied feelings towards organization which led them to hold grudges and at last performed threat that gives bad impact to

the performance of the organization. While for fraud threat, the employee usually used the access provided to distract the financial sources of organizations for their own benefits.

In addition, [10] also highlighted some of insider threat indicators, including personality traits, verbal behavior, deliberate markers, meaningful errors and correlated of usage patterns. Moreover, the types and activities performed by insider have been categorized into masquerader, alteration, the traitor, the elevation, snooping type of insiders, distributed threats and unintentional. Those types of insider performed different kind of threats activities which also has a relation to their motive of threats towards the organizations or target. Other than that, author [10] also has categorized some of insider profiles, which are pure insider, associate insider, affiliate insider and affiliate outsider. In addition, for the methods used by insider has been divided into user commands which insider used some programming commands, information exchange where the insider decide to obtain some information using any kind of tricks, make use of organizations vulnerabilities and develop kind of program such as a logic bomb to be released in network anytime.

Along with the studies carried out by authors [3] and [10] above, [11] stated that many companies still depend on the preserved management and production systems, resulting in a dramatic increase in the requirement of critical industrial protection systems and manufacturing outlines from cyber security threats that may include threat from inside. Other than that, [12] reported the system in industrial manufacturing claim a constant collaboration with different networked computing nodules, devices and human operatives. Therefore, the most effective approach is critical in order to guarantee the quality of production of an organization and the efficient work from every employee at each of the shop floor level as long as these employees do not have any insider threat characteristic that will harm the organization. Besides authors above, [13] also stated the important for the industry to grow into more well-organized, modernize methods and mature innovative of products and services with satisfied quality. Unfortunately, there are many challenges need to face by an organization, including manufacturing in implementing these technologies such as the need to emphasize skills/knowledge among employee. This situation of pressure from the organization to the employee can also contribute to the development of insider motivation within employee themselves as not all of them can accept the changes made. Therefore, this motivates us to carry out the studies within the scope of protecting critical industrial system based on a few reviewed undertaken as mentioned above. Along with the studies, there is no standard framework that is available. Therefore, we proposed our framework based on insider threat categorization that stated by other researchers.

Hence, this model can give a clear view on how encourages this capable insider to launch insider threat in an organization. Moreover, in viewing such components from the previous model, a researcher may obtain knowledge or ideas on how to design a framework for the categorization of insider threats in several groups as well as features. Furthermore, the researcher can use any identified insider threat model as CMO model above as a reference or guideline to produce with a framework for the future and better understanding in insider threat mitigation in any fields of work such as in manufacturing automated execution field. Therefore, this paper applies the studies on some insider threats features gathered from different factors that categorize as human factor, system factor and machine factor. A number of reviewed articles which fall under the abovementioned factor categories as one of insider threat contributor being highlighted systematically. Moreover, each factor has a variety of strategies in reviewing the probability of insider threats in order to produce a solution based on the studies undertaken. The features identified will be applied in creating a standard framework to give a general idea of where those insider threat features of factor can happen in manufacturing execution system. Moreover, the manufacturing execution system defined by author [14] as huge quality of data that coming from system and converted into useful information about the production of scheduling, material handling and quality samples. Unfortunately, there is no general framework that can be referenced for researchers to conduct future research based on automation manufacturing execution system related to insider threats involving the mentioned factors above. By taking note on how difficult to produce generalize the framework in such fields, the implementation of those factors in the proposed framework can be the guidelines in future study.

II. RELATED WORKS

This section will discuss on some factor that containing features that lead to insider threats known as human factors, system factors and machine factors. Each factor has a multiples kind of schemes in reviewing the possibility of insider threats in order to produce a solution based on the carried out studies.

2.1.Insider Threats Cause by Human Factor

The human factor can be defined as a human behavior that behaves abnormally, which contribute to an insider threats actions. For instance, according to [15] insider threats has been referred to as an action to harm by trusted individual to the organization. Some of the researcher relates psychology and motivation for human to make this kind of threat shows that, the fact remains as it was difficult to predict who will perform or commit securities fraud [16] and severe employment crises contributed to exhibited signs of dissatisfaction and serious personnel problems months aforementioned to a threat [17]. The aim of this research is to assess an employee's behavior associated with the risk of insider abuse with the use of prototype psychological model [15]. The advantages of this research area can provide clues or leads for officers to take action in advance of actual crimes, and also provide framework be considered for further analysis in the insider threat model.

In addition to above author, [18] approaches the scope of insider threats into unintentional insider threats which define as a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, through action or inaction without malicious intent, unwittingly causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's resources or assets, including information, information systems, or financial systems. The unintentional factors have few categorizations into organizational factor, i.e. work were set embrace inadequate properties and poor management systems [19] while lack of knowledge and memory failures and stress fall into human factors [20]. In addition, personality predispositions and demographic (age, gender) fall into psychosocial and demographic factors [15].

Moreover, another researcher has derived on how the analyst proposed a relationship between Dark Triad personality traits, related constructs and external process experiences that derived from past collected works using formal modelling methodology that can determine the retrospective detection probability and viability of behavioral model [3]. From the previous research by [21] have resulted in the development of the Five-Factor Model (FFM) from a structure of personality and has comprehensive acceptance between personality researchers, including extraversion, agreeableness, conscientiousness, neuroticism, and openness to experience [21]. The Dark Side is considered as a socially violent personality and are categorized as Machiavellianism, narcissism and psychopathy which common personalities include socially vindictive character, self-promotion, emotional indifference, unfaithfulness and violence have ability to exploit others [22].

Besides author above, [23] has proposed the taxonomies analysis can contribute to the association and the disambiguation of insider threat incidents as the protection solution used against them. The objective of their approach is to systems the knowledge gathered in insider threat research, but at the same time leveraging current stranded theory method for severe literature review. The proposed categorization follows workflow, including incidents and data sets, investigation of attackers, simulations or reproductions and defense solutions. There are few related research involves taxonomies such as the technique used by [24] is illustrated workflow between categories, proposed a structured taxonomy of insider threat incidents. The advantages of this paper are a unique fundamental taxonomy that subsidies to orthogonal taxonomy of incidents and defining the possibility of defense solutions employed against them and an updated outline of widely available data sets that can be used to examine detection resolutions against other works. Table 1 below shows variety of human factors containing features that discovered.

2.2.Insider Threats Cause by System Factor

Besides the human factor that has been reviewed, there are also some researches focused on system factor that can lead to insider threats such as system failure or errors, operational activities or sequences, and so forth. There are various researchers have concerns about this factor and proposed different detection approach under the anomaly detection such as time-based, threshold-based and deviation-based against insider threats.

As proposed by the author in [25] PRODIGAL has been configured to explore methods for unsupervised and semi-supervised anomaly detection to identify users who are possible to permit further investigation by discovering users who frequently perform near the upper of the anomaly recognition score list on multiple days. It has three levels of explanation need to be considered to support the analyst such as consists of pre-computed single feature detection scores which available for examination, a collection of features or sets of features contributed to anomaly score from an individual detector for individual users and combinations of the contribution from different type of detectors that are incorporated into the ensemble computation of overall anomaly scores. From the level of explanation and approachable methods, PRODIGAL can give sureness to detect recognized, assumed insider threat situations,

variations and the combination of situation [26].

TABLE 1
UNITS FOR MAGNETIC PROPERTIES

Author	Category of Features	Proposed Solution	Example of Features
[15]	Employee's behaviour	Used predictions of a Bayesian model and a linear regression model to assess an employee's behaviour	Disgruntlement, anger management issues, disregard for authority, stress, personal issues and lack of dependability
[24]	Unintentional insider Threats	Review of unintentional insider threats and divided into a few Factors	Accidental disclosure of private and sensitive information, accidental loss of physical records and devices also reveal of information from social engineering
[3]	User Personality	Dark Traits personality traits	Socially mean character, self-promotion, emotional sensitivity, betrayal and aggressiveness which this behaviour due to lack of guilt, lack of understanding and empathy have intention to exploit others.
[23]	Insider threat incidents	High profile of data leakage and unintentional insider	Individual and political gain, ignorant, revenge, lack of training, excessive workload, personal problems which include type of malicious insider such as traitors and masquerades.

Moreover, [27] proposed Corporate Insider Threat Detection (CITD) system which is capable of gaining a general feature set that characterizes the user's current activity in the organization at former time steps and amongst several users. The comparison between extensive ranges of different metrics is to evaluate the amount of anomaly that was displayed through each of them. Notifications are produced for the researcher based on different taxonomy structures of the anomaly metrics plus with both threshold and deviation-based assessments. Other than that, this approach produces response circle to reconfigure the increments connected with different anomaly metrics which was based on the anticipated conclusions of the analyst [27].

In addition, another author [28] has proposed the probabilistic modelling structure for examining malicious occasions performing in interdependent critical organizations as latter critical infrastructures (CI). Even though the effort on ensuring these critical infrastructures operate smoothly, the possibility of possible threat, including an insider threat to happen is still possible due to exposure to threat such as faults or system failures. The threat to interrupt with CI also given a huge measure of outages or even loss of control in the case of a cooperated manufacturing control system [29]. Because of that, [28] has proposed a model with the relation between data streams that focused on the programmed handling of quick detection using hidden Markov Model (HMM) considerations of linear time in variant (LTI) models to estimate the interactions. The system is also capable to recognize whether there is unfairness in the prototype or not since it depends on the possibilities of the group of models implement in the proposed method.

Other than that, [30] has proposed the method that is based on finding the possible failure threats and define the effect of each error on the Physical Protection System (PPS) effectiveness. Along with that, the features used was at the source of Estimate of Adversary Sequence Interruption (EASI) technique, the technique of Estimate and Prevention of the Insider Threats (EPIT) recommended for the best approximation of insider threats. By modifying the EASI approach through the addition of a risk rate of the management that based on the outcomes of the computable investigation of insider threats, a practical staff organization system is required to control the performances of the employee. Table 2 below shows variety of system factors containing features that discovered.

2.3.Insider Threats Cause by Machine Factor

Apart from human and system factors, author [31] has reported some of technical attempt by an insider to disable monitoring machine in some organization which might be related to manufacturing fields. This is because technical control such as a keyboard or mouse devices that attached to certain main machine in an operation is usually exposed to someone who can reboot the host computer that the hypervisor is running on an and insider easily gets the opportunity to alter some of the security settings for the hypervisor. In that case, insider who basically has potential ability can disable defense tools first before being able to disrupt or shut down or undertaking the machine used on their workstation [31]. Therefore, the author (Crawford & Peterson 2013) proposed a technique to determine whether insider threat.

TABLE 2
FEATURES ON SYSTEM FACTOR

Author	Detection Approach	Category of Features	Proposed Solution	Example of Features
[26]	Data processing behavior	Repeated improper behavior	Data processing and anomaly detection components	Communications patterns
[27]	Threshold based and deviation based	Operational procedure	Assessment of observations at time steps and processes	Server operation, capability of logging user activity includes what resources accessed and at what time of the access, threshold and deviation-based anomalies
[28]	Time based	Disruption between incoming data	Estimate between the precise nodes over repeated time frames.	Denial of services, false positive rate, false negative rate and detection relay, electrical power systems, disruptions of sensors and actuators.
[30]	Risk based	Failure of proper production	Organized documentation for the specific estimation of insider adversary behaviors among protective devices	The threat of adversary and the vulnerability of defense devices

detection can be performed on a Windows guest virtual machine (VM) through virtual machine introspection (VMI). An introspection tool or machines called as Virtual Machine Introspection (VMI) are a tool or machine that remains transparent and difficult to notice by the guest and are extremely difficult to subvert. With VMI, even users with full authorization or permission are unconscious or unaware of the monitoring abilities of the VMI tool and are not able to compromise them.

Besides that, author [32] has proposed the defense mechanism the front end of line (FEOL) integrated circuit and back end of line (BEOL) implementation in the equipment to ensure the improve proposal has a high error rate and the output close by considering cell organization, directionality of connections to regulate the FEOL data from the BEOL data. FEOL was used in untrusted platform and BEOL in a trusted platform and both connected in a thread called as proximity threat to recover leak connection between them. The threat has made the component of physical proximity FEOL exploited [33]. The experiment started by launching FEOL threats by an untrusted BEOL platform. Next, comparable looking FEOL mechanisms were designed for defense against the projected threat which next improves defense procedure to lessen interruption overhead and capitalize on security. The defense mechanisms used are naïve defense, delay aware defense and secure aware defense [32].

There are also some of the researchers that look into the case of threats that happened in some organizations which use Supervision Control and Data Acquisition (SCADA) approach. Accordingly, [34] has divided the insider threats into two parts which unresolved alarms threat defines as the minute of operator has no intent of eliminating the inbound alarms by means of interruption or delay of threat and incorrect or incomplete threat and misconfiguration threat defines as when the worker attempts to produce misconfiguration or alarms through overload threat, outage threat and incorrect setting threat. Overload threat happened when wrong modification of topology and load transmission, which possibly will be the reason of overload or a power disaster in a huge area, outage threat as when insider opens the output feeders and incorrect setting threat reported as inappropriate equipment settings that can be a reason to equipment improper operation. Due to the previous analysis on what this kind of threat capability to do through a machine, [35] has proposed method called statistical anomaly detection method (SADM) in electric power of the SCADA system by doing simulation using substations level and transmission organism scenario. Table 3 below shows variety of machine factors containing features that discovered.

Other than author above, author [36] has explained split manufacturing is a reliable technique to preserve against threats in manufacturing based mischievous activities such as IP piracy, overbuilding, and insertion of hardware Trojans which also can be helpful to faces insider threats. In fact, there are many losses in finances due to IP piracy, which also have become one of the concerns in both commercial and military fields [37]. Therefore, author [36] has aimed to produce the premiere level of security while ensuring acquires the highest outline in the clouds. The method used for the proposed approach by providing the theoretical structure for computing the outline level flexibility against any closeness prompted information outflow through the centric placement techniques targeting to make split

manufacturing protected against any nearness threat despite the fact of certifying practicality. Different from previous approaches, the analyst presented two real world outline techniques towards secure split manufacturing, which coloring graph of gate-level and clustering the same type of the gates contribute to accomplishing particularly improved trade-offs for outline rate and security [36]. Table 3 below shows variety of machine factors containing features that discovered.

TABLE 3
FEATURES ON MACHINE FACTOR

Authors	Category of Features	Proposed Solution	Example of features
[47]	Technical impact against machine	Determination on insider threat detection	Disable monitoring machine before being able to disrupt or shut down or undertaking the machine used on their workstation
[32]	Old security features and network prototype	Improve defense procedure	Exploitation of physical attack and IP theft
[35]	Unresolved alarms threat and misconfiguration threat	Simulation on two scenarios of insider threats.	Unresolved alarm (delay attack and incorrect or incomplete attack) and misconfiguration attacks (overload attack, outage attack and incorrect setting attack)
[36]	Theoretical structure for computing in the machine	The latter theoretical structure for computing the outline level flexibility against any closeness prompted information outflow from inside	Intellectual property piracy or theft

III. FRAMEWORK OF AUTOMATED MANUFACTURING EXECUTION SYSTEM

In this section we will create an illustrated standard framework involves in the automated manufacturing execution system and relate the framework with contributing factors. In addition, the study of contributing factors of possible insider threats that can be relate in manufacturing fields has been divided into human factors, system factors, and machine factors accordingly. The example of scenario created is as shown in Fig. 3 below.

The framework designed below called as automated manufacturing execution system control consisting two major phases which is tracking and ordering system in which the data inserted into the server before proceeding to car production system. As illustrated on the left side of the figure, the admin will release the related data throughout the system which have a connection that link to the database.

Next, the database server will feed in the data to the application server, once the instruction from human (admin) via the system application is received. The application server will analyze and deliver the related data to related production shop such as engine, stamping, welding, painting or trimming throughout the switch.

The switch normally employed to send the data to the related destination as there is several productions Master Programmable Logic Control (MPLC) geographically distributed. A bunch of data will be stored into MPLC register known as buffering as storage medium. The data will be delivered to the rightful machine in an order of first-in-first-out (FIFO) manner. The buffer will be updated with new data from the server frequently, which based on n-1 concept. For example, if the buffer consisting 10 data of N, whenever the data reduce to 9 (10-1), the MPLC will request new data from the server.

The data delivered by the switch in string form unable to understand by the machine. Therefore, this information will be translated by the MPLC into readable form, i.e. 0 and 1 which next orders the machine to conduct the production.

Upon completion of production of the machine, there must be cycled to notify/feedback shows the job has made as well as requests for new data. As such, the machine will send completion signal to the MPLC and at the same time request for new data. The completed task feedback will further escalate to the DB Server from the MPLC through the Switch and Application Server. The admin can check these complete of the activity for tracking purpose throughout the tracking system as shows above.

Moreover, in this illustrated framework also has shown some of the involvement of contributing factors that contain some features of insider threats within illustrated standard framework involves in AMES will be explained for better understanding of where those possible threat can happen. Other than that, the illustrated standard framework also can be as a reference to another researcher on insider threats study. The three main factors have been divided into A (human factor), B (system factor) and C (machine factor) accordingly as shown in Fig. 3 below.

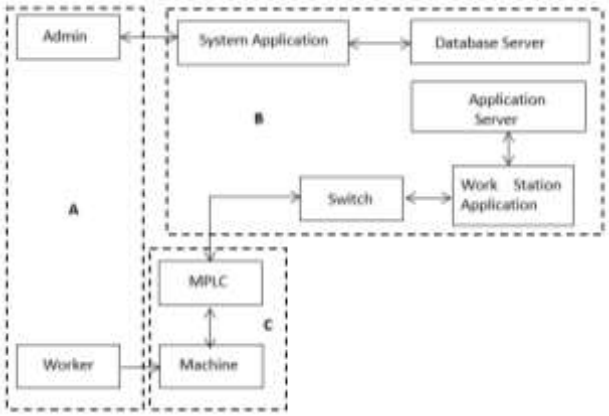

Fig. 3 Standard framework involves in Automated Manufacturing Execution System (AMES).

In contact with human features in phase A, the effort of any organization or even in the manufacturing itself have put their employee to apply the best practice, impactful yet systematic work environment, but an important component that can assume as a major factor in the peaceful working environment is the human or employee emotion [38]. For example, as to relate to above framework, the employee, i.e. admin or line worker could be feeling stressed [15] as a consequence of their fault or mistakes in production activity by their higher management. Therefore, the employee can perform threats (Admin) to take revenge against their employer by disrupting the smoothness of process in manufacturing production systems.

Other than that, the performance and judgment of the employee can be affected by physical conditions that have a connection to emotional impact due to exhaustion or sleepiness which can raise the chances of human inaccuracy [39]. For example, if the worker does not have enough sleep or rest, he/she can be emotionally sensitive [3] and can be less effective during work performance, which then lead to make mistakes. The situation can become worse when employees cannot tolerate with working pressure [23] in manufacturing production fields that provide a worker with low financial support or monthly payment. These kinds of situations can fire up insider passion or greed to perform threat for their own benefits [40] and [3] such as accidentally expose private information [24] i.e. the technical process of car production to competitors as he/she think that they can gain more in terms of finances.

On the other view, drugs and alcohol also are might be reasons behind the threats launch from an individual and clearly it gives bad impact on employee work performance as it affects memory, focus, calculation, intellection, visuospatial talents and capability to follow composite understanding. Due to the increasing of dopamine levels also can affect the quantity of risk that people might take (Park 2008). For example, the unintentional insert wrong data into the server (A) can cause wrong data uploaded to the application server (B) and MPLC (C) and finally result in wrong production or machine error. Therefore, from scenario shown above, those human factors that have been summarized can be expected to happen from the A to the C.

Beside human factor explained above, the study also has been conducted on some features of system factor such as repeated improper behavior [26] which can be described as what consequences of system failure that contribute to the reputation of an organizational or production fields. Other than that, author [41] reported one of the contributing factors of system failure when employee frequently gives respond to any phishing email. For example, from the review of research papers above, we can relate to the framework as an employee might have conceptualizing problem on how the production works which involve operational procedure [42] with the system and next resulting in the documentation or production failure [43] because employee give respond to the malicious email.

Other than that, the organization or company plays a big part in training their employees, especially on defensive strategies to any possible threat which might contribute harm to the organization [44]. For example, if the system used in production cycle faces some technical problem such as unexpected of wrong sequences [45] of information delivery, which supposedly from the database to the application server (B) but the data jump or skip application server and go directly to MPLC (C). This show how the data reached at the MPLC (C) from the server without analyzed by the application server (B) before being distributed to the related shop.

Besides of human and system factors above, some literature review of machine factors also has been reviewed. According to [32], an organization or companies in manufacturing need to use updated and the latest version of a machine to produce more secure and effective working environment because if any, working fields, including manufacturing do not use the latest version of a machine with the latest security features, the chances or probability for the insider to have full knowledge of the machine' vulnerabilities is huge. This kind of situation can be considered as must grab opportunity over the power of insiders have to perform threats easily. For example, from framework above, insider launches their threat to the old security features and network prototype used as he or she already acknowledges

vulnerability of machine used [32]. This threat can cause data flow or delivery of data from each stage have some disruption [46] and give wrong output from production system and also give effect to the performance of the company to their clients. From the explanation on how the tracking and ordering system starts from insertion of data by human (admin) to the respondent or a feedback cycle back to the database (A), the employee or can be named as insider can interrupt that process so the right data will not be delivered back to the server. This situation can directly affect the performance and reputation of the company.

In addition, some of the related insider threats such as an unresolved alarms threat, misconfiguration threat and incorrect setting threat [35] also can be the cause to interruption between the machines itself [46]. Additionally, insiders also might technically attempt to disable monitoring machine before being able to disrupt or shut down or undertaking the machine used on their workstation [47]. For example, the insider wants to take over a machine that containing binary information from MPLC (C). Therefore, he/she shut down the monitoring first before taking over the machine (C) as he/she can exchange the converted information before proceeding to the next phase. Other than that, during the study also we can assume some of the accidents of failure of machines, such as power outages might also happen during the production system.

IV. Conclusion

From the review above has shown that there is no standard framework of the automated manufacturing execution system to classify the three factors into one main framework. There are a few reviews on manufacturing execution systems such as by [48] and [14] but not generalize in the automated manufacturing execution system. There are some effects from automated manufacturing execution system failure that can be assumed, such as downtime, production loss and productivity decrease. Unfortunately, these effects do not have any reference, including a standard framework to conduct future research. Therefore, the illustrated framework can be used as reference by other researcher to come out with a better solution that might have implementation of the internet of things (IoT) and cloud usage.

Acknowledgment

This research founded by Ministry of Education through trans discipline TRGS/1/2016/FTMK-CACT/01/D00006 and conducted at Universiti Teknikal Malaysia Melaka (UTeM).

References

[1] N. Elmrabit, S. Yang, and L. Yang, “Insider threats in information security,” *21st International Conference on Automation and Computing (ICAC)*, pp.1–6, 2015.

[2] M. E. Whitman, and H. J. Mattord, “Threats to information security revisited 1”, vol. 8, pp. 311-332, 2012.

[3] M. Maasberg, J. Warren, and N. L. Beebe, “The dark side of the insider: Detecting the insider threat through examination of dark triad personality traits,” in *2015 48th Hawaii International Conference on System Sciences (HICSS)*, pp. 3518-3526, 2015, IEEE.

[4] K. R. Sarkar, “Assessing insider threats to information security using technical, behavioural and organisational measures,” *Information Security Technical Report*, *vol.* 15, no. 3, pp.112–133, 2010, [Online]: Available at: http://dx.doi.org/10.1016/j.istr.2010.11.002.

[5] S. L. Pfleeger, J. B. Predd, J. Hunker, and C. Bulford, “Insiders Behaving Badly: Addressing Bad Actors and Their Actions,” *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 169–179, Mar. 2010.

[6] C. Xiaojun, S. Jinqiao, P. Yiguo, and Z. Haoliang, “An Intent-Driven Masquerader Detection Framework Based on Data Fusion,” *Trustworthy Computing and Services Communications in Computer and Information Science*, pp. 450–457, 2013.

[7] T. Walker, “Practical management of malicious insider threat - An enterprise CSIRT perspective,” *Information Security Technical Report*, *vol.* 13, no. 4, pp. 225–234. 2008, Available at: http://dx.doi.org/10.1016/j.istr.2008.10.013.

[8] A. Cummings, T. Lewellen, D. Mcintire, A. P. Moore, and R. Trzeciak, “Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector,” Jul. 2012.

[9] C. Posey, R. J. Bennett, and T. L. Roberts, “Understanding the mindset of the abusive insider: An examination of insiders’ causal reasoning following internal security changes,” *Computers and Security*, vol. 30, no. 6-7, pp. 486–497, 2011, Available at: http://dx.doi.org/10.1016/j.cose.2011.05.002.

[10] A. N. Mohammad, N. L. Clarke, A. Hassan, W. Yassin, Z. Z. Abidin, M. N. A. Mhiqani, and R. Ahmad, “A New Taxonomy of Insider Threats; An Initial Step in Understanding Authorized Attack,” *International Journal of Information Systems and Management*, vol. 1, no. 1, p. 1, 2018.

[11] Joaquim G. Antunes, António Pinto, Pedro Reis, and Carla Henriques, “INDUSTRY 4.0: A CHALLENGE OF COMPETITION,” *INDUSTRY 4.0: A CHALLENGE OF COMPETITION*, pp. 1–9, Jan. 2018.

[12] B. R. Ferrer, W. M. Mohammed, J. L. M. Lastra, A. Villalonga, G. Beruvides, F. Castaño, and R. E. Haber, “Towards the Adoption of Cyber-Physical Systems of Systems Paradigm in Smart Manufacturing Environments,” *2018 IEEE 16th International*

Conference on Industrial Informatics (INDIN), pp. 792–799, 2018, Available at: https://ieeexplore.ieee.org/document/8472061/.

[13] F. Fernández-Armesto, "Industry 4.0 Challenge and Motivation," vol. 2, no.6, pp. 89–97, 2018.

[14] R. Soto, "Validation of Manufacturing Execution System (MES)," *Dados*, vol. 200 pp. 172–200, 2017.

[15] F. L. Greitzer, L. J. Kangas, C. F. Noonan, A. C. Dalton, and R. E. Hohimer, "Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats," *2012 45th Hawaii International Conference on System Sciences*, 2012.

[16] L. A. Kramer, R. J. Heuer, and K. S. Crawford, "Technological, Social, and Economic Trends are Increasing U.S. Vulnerability to Insider Espionage," *PsycEXTRA Dataset*, 2005.

[17] E. D. Shaw and L. F. Fischer, "Ten Tales of Betrayal: The Threat to Corporate Infrastructure by Information Technology Insiders Analysis and Observations," 2005.

[18] A. Azaria, A. Richardson, S. Kraus, and V. S. Subrahmanian, "Behavioral Analysis of Insider Threat: A Survey and Bootstrapped Prediction in Imbalanced Data," *IEEE Transactions on Computational Social Systems*, vol. 1, no. 2, pp. 135–155, 2014.

[19] F. L. Greitzer, D. M. Rice, S. L. Eaton, and M. C. Perkins, "Learning to Pull the Thread: Application of Guided Discovery Principles to the Inquiry Process," *Learning to Pull the Thread: Application of Guided Discovery Principles to the Inquiry Process*, pp. 1–11, 2005.

[20] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," *Proceedings of the SIGCHI conference on Human Factors in computing systems - CHI 06*, 2006.

[21] T. A. Judge, and J. E. Bono, "Five-Factor Model of Personality and Transformational Leadership," vol. 85, no. 5, pp. 751–765, 2000.

[22] D. L. Paulhus, and K. M. Williams, K.M., "The dark triad of personality: Narcissism, machiavellianism, and psychopathy, vol. 36, pp. 556–563.

[23] Ivan Homoliak, Flavio Toffalini, Juan Guarnizo, Yuval Elovici, and MARTÍN OCHOA, "Insight into Insiders: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures," 2018.

[24] May, C.R. et al., 2017. "Insight into Insiders: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures."

[25] T. E. Senator, "Multi-Stage Classification," 2005.

[26] H. G. Goldberg, W. T. Young, A. Memory, and T. E. Senator, "Explaining and Aggregating Anomalies to Detect Insider Threats," *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 2016.

[27] P. A. Legg, O. Buckley, M. Goldsmith, and S. Creese, "Caught in the act of an insider attack: detection and assessment of insider threat," *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, 2015.

[28] S. Ntalampiras, Y. Soupionis, and G. Giannopoulos, "A fault diagnosis system for interdependent critical infrastructures based on HMMs," *Reliability Engineering and System Safety*, vol. 138, pp. 73–81. 2015, Available at: http://dx.doi.org/10.1016/j.ress.2015.01.024.

[29] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998–1010, 2012.

[30] Bowen Zou, Ming Yang, Jia Guo, Junbo Wang, E. R. Benjamin, Hang Liu, and Wei Li, "Insider threats of Physical Protection Systems in nuclear power plants: Prevention and evaluation," *Insider threats of Physical Protection Systems in nuclear power plants: Prevention and evaluation*, pp. 1–8, 2017.

[31] K. Scarfone, and P. Hoffman, "Guide to Security for Full Virtualization Technologies Recommendations of the National Institute of Standards and Technology," *National Institute of Standards and Technology Special Publication*, no. 800–125, pp. 1–35. 2011, Available at: http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf.

[32] Yujie Wang, Trio Cao, Jiang Hu, and J. V. Rajendran, "Front-End-of-Line Attacks in Split Manufacturing," pp. 1–8, 2016.

[33] J. Rajendran, O. Sinanoglu, and R. Karri, "Is Split Manufacturing Secure?," *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013*, 2013.

[34] R. R. Rantala, "Bureau of Justice Statistics Special Report," *Cybercrime against Businesses, 2005*, pp. 1–20, Sep. 2008.

[35] P. M. Nasr and A. Y. Varjani, "Alarm based anomaly detection of insider attacks in SCADA system," *2014 Smart Grid Conference (SGC)*, 2014.

[36] A. Sengupta, S. Patnaik, J. Knechtel, M. Ashraf, S. Garg, and O. Sinanoglu, "Rethinking split manufacturing: An information-theoretic approach with secure layout techniques," *2017 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2017.

[37] SEMI, "IP Challenges for the Semiconductor Equipment and Materials Industry," Jun. 2012.

[38] J. R. Nurse, O. Buckley, P. A. Legg, M. Goldsmith, S. Creese, G. R. Wright, and M. Whitty, "Understanding insider threat: A framework for characterising attacks," *in Security and Privacy Workshops (SPW)*, pp. 214-228, 2014, IEEE.

[39] A. S. Høvdanum, O. C. Jensen, G. Petursdóttir, and I. M. Holmen, "A review of fatigue in fishermen: a complicated and under prioritised area of research," *International Maritime Health*, vol. 65, no.3), pp. 166-172, 2014.

[40] W. R. Claycomb, and A. Nicoll, "Insider threats to cloud computing: Directions for new research challenges," in *Computer Software and Applications Conference (COMPSAC)*, 2012 IEEE 36th Annual, pp. 387-394, 2012, IEEE.

[41] N. Viswanathan, C. J. Alpert, C. Sze, Z. Li, G.-J. Nam, and J. A. Roy, "The ISPD-2011 routability-driven placement contest and benchmark suite," *Proceedings of the 2011 international symposium on Physical design - ISPD 11*, 2011.

[42] P. A. Legg, Oliver Buckley, Michael Goldsmith, and Sadie Creese, "Automated Insider Threat Detection System Using User and Role-Based Profile Assessment," *Automated Insider Threat Detection System Using User and Role-Based Profile Assessment*, pp. 1–10, May 2015.

[43] B. Zou, M. Yang, J. Guo, J. Wang, E.-R. Benjamin, H. Liu, and W. Li, "Insider threats of Physical Protection Systems in nuclear power plants: Prevention and evaluation," *Progress in Nuclear Energy*, vol. 104, pp. 8–15, 2018.

[44] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?," *Proceedings of the 28th international conference on Human factors in computing systems - CHI 10*, Apr. 2010.

[45] B. X. Zhu, "Resilient control and intrusion detection for SCADA systems," (No. UCB/EECS-2014-34). California Univ Berkeley Dept of Electrical Engineering and Computer Sciences, 2014.

[46] B. Zhu, and S. Sastry, "SCADA-specific Intrusion Detection / Prevention Systems: A Survey and Taxonomy," pp.1–16, 2010

[47] M. Crawford, and G. Peterson, "Insider threat detection using virtual machine introspection, *2013 46th Hawaii International Conference on System Sciences*, pp. 1821–1830. 2013, Available at: http://ieeexplore.ieee.org/document/6480061/.

[48] A. Bradley, "Manufacturing Execution Systems for Sustainable Production," *Manufacturing Execution Systems for Sustainable Production*, pp. 1–10, May 2009.