Categorization of Anomalies in Smart Manufacturing Systems to Support the Selection of Detection Mechanisms

Felipe Lopez[1], Miguel Saez[1], Yuru Shao[2], Efe Balta[1], James Moyne[1], Z. Morley Mao[2], Kira Barton[1], and Dawn Tilbury[1]

***Abstract*—An important issue in anomaly detection in smart manufacturing systems is the lack of consistency in the formal definitions of anomalies, faults, and attacks. The term anomaly is used to cover a wide range of situations that are addressed by different types of solutions. In this paper, we categorize anomalies in machines, controllers, and networks along with their detection mechanisms, and unify them under a common framework to aid in the identification of potential solutions. The main contribution of the proposed categorization is that it allows the identification of gaps in anomaly detection in smart manufacturing systems.**

***Index Terms*—Intelligent and Flexible Manufacturing, Factory Automation**

I. Introduction

A new trend has emerged in the last decade under the names of Smart Manufacturing (SM) in the United States and Industry 4.0 in Europe. The goal of SM is to optimize manufacturing by connecting the different stages of the production lifecycle, gathering data from every stage and using it to dynamically adapt the system to variations in production demands and operating conditions [1]. SM systems are typically large. Various machines and material handling devices are connected by large networks and supervised by several controllers. The increased connectivity in SM is expected to improve decision making, but it also enables undesired events to propagate and affect multiple components. Although the manufacturing community is optimistic that the overall impact of SM will be positive [2], it is important to have a clear understanding of its vulnerabilities [3], [4].

Different groups working with manufacturing anomalies often focus and develop solutions that are tailored only for a subset of system problem types. Mechanical engineers focus on prognostics and health management of machines, while control engineers target controller faults, network specialists work with network faults, and cybersecurity experts develop strategies to protect production systems from attacks. A current barrier for the unified study of anomalies in SM is the lack of a common nomenclature to aid in the specification of the challenges and solutions.

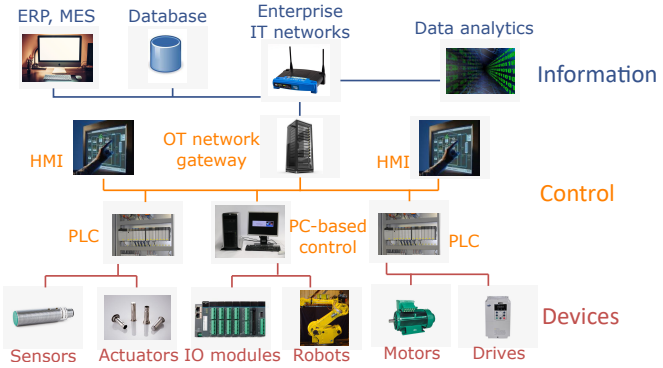

Fig. 1. Integrated landscape of smart manufacturing systems connecting enterprise and control systems. Manufacturing data is made available to the company's Operational Technology (OT) and Information Technology (IT) networks to provide visibility of the plant floor operation at higher levels of the enterprise.

In an effort to aid the study of anomalies in SM from a cyber-physical perspective, we provide a review of anomalies as studied in different disciplines and unify them under a common framework. Although SM covers different aspects of manufacturing operation (e.g., machine operation, supply chain, and finances), we limit our scope to studying anomalies in machines, controllers, and communication networks, illustrated in the device and control layers of Fig. 1. Moreover, the discussion presented in this paper is focused on discrete manufacturing applications, in which parts move across different stations where machines (e.g., CNC[1] machines, robots) perform operations as coordinated by logic controllers. Communication between the multiple machines, sensors, and controllers is supported by industrial networks.

A previous taxonomy of vulnerabilities in SM systems focused on cyber attacks, neglecting other sources of anomalies that could impact production in similar manners [5]. In this paper, we analyze manufacturing anomalies regardless of their origin and match them with suitable anomaly detection mech-

Manuscript received: February, 15, 2017; Revised May, 3, 2017; Accepted May, 31, 2017.

This paper was recommended for publication by Editor Jingshan Li upon evaluation of the Associate Editor and Reviewers' comments. This work was supported in part by the National Science Foundation (NSF) under award number CSR 1544678.

[1]Felipe Lopez, Miguel Saez, Efe Balta, James Moyne, Kira Barton and Dawn Tilbury are with the Department of Mechanical Engineering, University of Michigan, Ann Arbor, MI 48109, USA {lopezfe,migsae,baltaefe,moyne,bartonkl,tilbury}@umich.edu

[2]Yuru Shao and Z. Morley Mao are with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109, USA {yurushao,zmao}@umich.edu

Digital Object Identifier (DOI): see top of this page.

[1]Computer Numerical Control

anisms. The main contribution of the proposed categorization is that it allows the identification of gaps in anomaly detection in SM systems that should be addressed in future studies. We identified that most existing anomaly detection approaches were developed for manufacturing plants that are not as closely integrated as current manufacturing enterprise systems. As a result, these approaches are not suitable for the interconnected systems currently used in SM, and an opportunity exists for the development of new anomaly detection methods.

The rest of the paper is organized as follows. In Section II, we propose definitions for anomalies, faults, and attacks in SM systems. In Section III, we introduce five types of anomalies based on how they first manifest in the manufacturing system. In Section IV, we identify seven types of anomaly detection mechanisms based on their predictive capabilities and knowledge requirements. Section V maps the identified types of anomalies to suitable types of anomaly detection methods. Finally, we conclude this paper in Section VI.

II. Definitions

In this study, we specify the production system as the complete set of hardware and software involved in the fabrication of a specified part. This includes machines, robots, material handling systems, controllers, and networks. Suppliers, human operators and end-users of the manufactured goods are considered external to the system. Some of the terms used to describe unexpected occurrences in these systems are *anomaly, fault, and attack*. We propose the following definitions to distinguish them.

Definition 1 (Anomaly): *An anomaly is an occurrence that is different from what is standard, normal, or expected.*

Definition 2 (Fault): *A fault is an anomaly that is related to an unwanted situation and may be associated with failure, malfunction, or quality degradation.*

Definition 3 (Attack): *An attack is a purposeful action by an element external to the system that results in anomalous operation.*

Definition 4 (Anomaly detection): *Anomaly detection is the process of identifying anomalous behavior.*

The following conclusions can be obtained from the aforementioned definitions:

- Anomaly is the superclass of interest in our study. Faults and attacks are subsets of anomalies.
- The study of anomalies requires knowledge of normal or expected behavior.
- A fault is a type of anomaly. Therefore, all faults are anomalies but not all anomalies are faults. For example, overheating of an electric motor may be an anomaly, but if the temperature stays within admissible bounds it may not be a fault. On the other hand, if temperature exceeds the upper permissible limit and interrupts the motor operation, then it could be classified as a fault [6].
- The outcome of an anomaly or fault is not strictly dependent on the initial intent. For example, an anomaly or fault may be accidental or intentional, and yet the impact on production could be the same.
- Attacks require intent to cause an action, but not necessarily intent to cause harm; i.e., there are malicious and non-malicious attacks. For example, a non-malicious attack may occur when an operator, considered external to the SM system but able to act upon it, uploads a controller version that is incompatible with the current system configuration.
- Due to the cyber-physical nature of SM systems, attacks can originate from the cyber domain or the physical domain, and may impact both domains [7]. We can further classify attacks into: cyber attacks (e.g., virus infection, SQL injection) and physical attacks (e.g., breaking a physical connection). Cyber attacks may also be of the kinetic cyber type [5], [8], which are cyber attacks that can cause physical damage or injury (e.g., Stuxnet malware [9]).

Fig. 2 illustrates that the terms anomalies, faults, and attacks are not equivalent in the scope of our study.

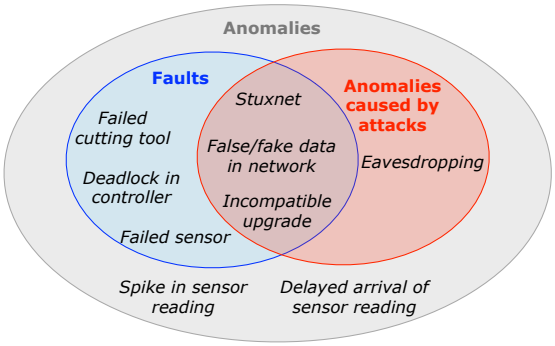

Fig. 2. Venn diagram used to illustrate examples of anomalies, faults, and attacks in SM.

III. Categorization of Anomalies in Smart Manufacturing

Studies of anomalies in SM have traditionally been restricted to a specific domain (cyber or physical) and to a specific component (e.g., network, CNC machine). This domain-specific approach creates unnatural divisions in an integrated system. In this section, we organize anomalies in SM based on how they first manifest in the manufacturing system. Some of these anomalies, if allowed to evolve and propagate in the system, may transform into or cause anomalies of other types.

A. Dimensions of Anomalies

A set of dimensions is used to identify characteristics that can distinguish between different types of anomalies. Most of the existing discussions in the literature are focused on the *temporality* aspect. We identify two additional dimensions, *domain* and *multiplicity*. The domain dimension is useful for studying cross-domain interactions in SM systems. The multiplicity dimension differentiates between anomalies that are observed on a single component and those that manifest in multiple components at once.

Temporality. Anomalies may be classified depending on whether they occur in a snapshot in time or over a time interval.

(a) Snapshot: Anomalies that manifest in instantaneous observations, without the need to consider their temporal behavior.
(b) Dynamic: Anomalies that have a temporal attribute; i.e., they evolve over time as in a trend. Dynamic anomalies may also manifest in snapshots in some instances, e.g., if a degradation trend is not addressed and the system drifts into a region where a snapshot observation reveals an anomaly.

Domain. As stated in Section I, anomalies may manifest in either cyber or physical components.

(a) Physical: Physical assets that are usually controlled and monitored by computer-based algorithms, supported by cyber components.
(b) Cyber: Computing and network components that support functions such as diagnostics, control and communication in SM.

Multiplicity. We partition anomalies based on the size of the subset of components where they first manifest.

(a) Single component: Anomalies that manifest only in single component of the system (e.g., a sensor, actuator, controller, robot), while the rest of the components continue to work normally.
(b) Multiple components: Anomalies that manifest in a subset of components of the system. The anomaly may have originated in one component, but the effect is not apparent until a subset of components is affected (e.g., a faulty sensor leading a controller into instability). Alternatively, the anomalous behavior may originate from two or more components acting normally as independent units, while resulting in anomalous behavior due to the combined interactions. For example, a CNC program may be modified without the correct tool change, resulting in individually correct behaviors that produce the wrong part.

B. Types of Anomalies

Anomalies can be described with respect to the aforementioned dimensions. Here we identify five types of anomalies, shown in Table I, and indicate the attributes of these anomalies with respect to the dimensions identified in section III-A. It should be noted that an anomaly may belong to one or more type at the same time, e.g., a sudden loss of communication would be both an instantaneous anomaly and a communication anomaly. While this is not an exhaustive list of anomalies in SM, the anomalies used in this study demonstrate the categorization process proposed in this manuscript.

Instantaneous anomalies: Anomalies that manifest in the system without any prior indication. The anomaly could be observed in one variable (e.g., a spike in a temperature trace) or multiple variables (e.g., step changes in voltage and current where individually both measurements are within bounds, but from a multivariate perspective their collective values suggest an anomaly). Observations may originate from physical (e.g., power consumption) or cyber (e.g., unusually large data packet) domains. The concept of time associated with instantaneous anomalies does not necessarily mean that they are detected in real time. For example, the average value of pressure could be anomalous as reported at the end of a stage.

Evolving anomalies: Anomalies that manifest in the evolution of process observations. The anomaly could originate from single (e.g., current consumption unexpectedly ramping up) or multiple sources (e.g., changes in current and temperature in a welding process where individually both signals show normal trends, but their multivariate dynamics conflict with expectations because one variable increases while the other decreases). Observations may come from physical or cyber domains.

Communication anomalies: Anomalies that appear in the communication network. These could include lack of communication, arrival of faulty data packets, unexpected traffic, and cyber attacks. They may be observed in a single component of the network or in several components at the same time. Anomalies may appear in a snapshot of time or be detectable only through the evolution of observations (e.g., denial of service).

Event-based controller anomalies: Anomalies that manifest as the unexpected occurrence of an event or as the missing of an expected event. Event-based anomalies may manifest in single (e.g., an actuator missed a part) or multiple (e.g., deadlock blocking several resources) components. Although these anomalies often appear in the cyber domain, they may be the result of faults in logic controllers or problems with the hardware connected to them (sensors, actuators, and wiring). Event-based anomalies are detectable only through dynamic observations (i.e., comparison of the environment before and after a moment in time), which may be untimed (i.e., describing only what happened) or timed (i.e., describing both what and when it happened).

Integration anomalies: Anomalies that manifest in a system where components seem to function normally but the final outcome is anomalous. Examples of this type of anomaly are found in incompatible upgrades, when a component is changed but the rest of the system is not adjusted accordingly (e.g.,

TABLE I
CATEGORIZATION OF SM ANOMALIES FOLLOWING IDENTIFIED DIMENSIONS.

Anomaly type	Component multiplicity		Domain		Temporality	
	Single	Multiple	Cyber	Physical	Snapshot	Dynamic
Instantaneous anomalies	✓	✓	✓	✓	✓	
Evolving anomalies	✓	✓	✓	✓		✓
Communication anomalies	✓	✓	✓		✓	✓
Event-based controller anomalies	✓	✓	✓			✓
Integration anomalies		✓	✓	✓	✓	✓

changing the program of a robot without updating the PLC); and more recently, in kinetic cyber attacks, where instead of targeting individual machines or a network, an attacker may focus on the communication interfaces. Since integration anomalies appear in systems, they often involve both cyber and physical domains. If not addressed quickly, integration anomalies may evolve and become detectable as other types of anomalies.

IV. Categorization of anomaly detection mechanisms

Numerous methods have been proposed to detect anomalies in manufacturing systems. Although originally proposed for different types of components (e.g., machine, controller), several similarities can be identified among the various anomaly detection mechanisms.

A. Dimensions of Anomaly Detection Mechanisms

Dimensions were chosen to make distinctions in detection mechanisms based on predictive capabilities and knowledge requirements for the data and the system. Four dimensions were chosen: *incorporation of system dynamics*, *prediction level*, *level of supervision*, and *incorporation of system knowledge*.

Incorporation of system dynamics. Approaches may differ depending on whether the analysis looks only at instantaneous observations or considers past observations:

(a) Static: This approach considers only instantaneous observations.
(b) Dynamic: Dynamic detection mechanisms use observations taken at different time instances (e.g., time-series models) to monitor system dynamics. In simple cases, system dynamics may be used to adjust attributes within the static observation approach; e.g., adjusting limits based on recent data. In elaborate cases, the use of system dynamics may include a sequence of behavior; e.g., a progression of states leading to a failure mode.

Prediction level. Anomaly detection methods may differ depending on their ability to forecast the occurrence of anomalies:

(a) Reactive: Reactive methods require an anomaly to occur in order to be detected. This method does not utilize prediction.
(b) Trend analysis: A trend analysis considers current and previous observations to evaluate trends or patterns in data that may lead to an anomaly.
(c) Predictive: Predictive methods use current and previous observations to forecast when abnormal values of specific variables are expected. Predictions are often reported as estimates of time-to-failure (TTF) or remaining-useful-life (RUL), and a prediction confidence or interval.

Level of supervision. Often, process, product or equipment quality or health data is used to indicate the occurrence of a fault. For example, metrology or yield data can indicate a fault related to product scrap or quality degradation, while maintenance event data can indicate a fault leading to equipment failure. This information may be passed to the anomaly detection method to enhance the identification of certain classes of anomalies [10]. The level of information that is used within a given detection method can be classified as:

(a) Supervised anomaly detection: These methods use labeled data sets that include known anomalous scenarios to aid in the identification and classification of anomalies and faults.
(b) Semi-supervised anomaly detection: Semi-supervised methods use normal data sets to train models of normal behavior, and label any observations that deviate significantly from those models as anomalies.
(c) Unsupervised anomaly detection: Unsupervised methods trade flexibility for reliability. This type of method does not require labels for the anomalies, nor does it makes distinctions between training and test data. Rather, unsupervised methods often use norms and probability densities of training data to estimate normal and anomalous regions. These techniques generally result in a larger percentage of false or missed alarms.

Incorporation of system knowledge. The tendency in anomaly detection solutions is to rely on historical data to develop purely statistical, empirically-based models. Unfortunately, system knowledge or subject matter expertise (SME) is often neglected in favor of "one-size-fits-all" statistical techniques that result in higher levels of false and missed alarms. Based on the level of incorporation of system knowledge, detection mechanisms can be categorized in this dimension as:

(a) Statistical: System knowledge is not used in the anomaly detection mechanism if it is purely statistical or data driven. There are a large number of purely statistical techniques including Statistical Process Control (SPC) for fault detection [11], Principal Components Analysis (PCA), and Deep Learning in big data systems [12]. While some of these techniques can find patterns that can be related to cyber and physical phenomena, system knowledge is not incorporated into the detection mechanism at the outset [13].
(b) Phenomenological: SME is combined with statistical methods in the detection mechanisms. For example, model forms may be used to capture basic system knowledge and/or relationships between variables, and then statistical data is used for tuning to account for intricacies not covered in the basic model. An example might be a physical equation for the torque of a motor delivering power to a conveyor system, given the voltage, current and temperature of the motor, with statistical tuning to account for motor wear and inefficiencies not covered in the basic equation for power delivery. Another example can be found in cognitive computing, where a human could aid in the selection and ranking of variables to be monitored in an anomaly detection configuration. Model tuning can occur only during the model training phase, or be employed during operation to capture changes in system dynamics.

(c) Cyber-physical models: These anomaly detection methods use models that are constructed with purely cyber-physical information about the system. An example might be a model based entirely on first principles physics. Statistical data is not used to tune the model. Note that the model does not have to be static, but any dynamics would be captured by incorporating cyber-physical knowledge. An example might be a model of a logic controller, where the model and the anomaly detection solution would be based solely on the control logic.

B. Types of anomaly detection mechanisms

Various anomaly detection mechanisms have been grouped into the seven types shown in Table II and described below. Anomaly detection mechanisms may be used in isolation (e.g., limit checking) or in conjunction with other mechanisms (e.g., clustering followed by limit checking with limits set differently in each cluster), resulting in solutions that can be mapped to one or more of the identified types at the same time. The list we are presenting is not exhaustive and other anomaly detection categories may be identified following the dimensions introduced in Section IV-A.

Feature extraction with limit checking: Limit checking is the most basic and frequently-used method for anomaly detection. This method consists of checking when numeric signal traces or some features within those traces (e.g., spikes, ramps, step changes) lie outside a user-defined region of normal operation (e.g., average value of trace violating high or low limits, spike height greater than a threshold) [14], [15]. Limit checking methods may be performed with binary, fuzzy, or adaptive thresholds [6]. This type of method works in reactive mode or with trend analysis, where limits are set to capture a drift value before it results in a fault. Limit checking may be performed with limits that are explicitly defined, tuned from training data of normal operations, or identified with data-driven methods; making it supervised, semi-supervised, or unsupervised, respectively. The definition of limits may be driven only by data, be based on cyber-physical models, or follow a phenomenological approach.

Signal models: This type of anomaly detection covers methods of anomaly detection for measured process signals that show oscillations that are harmonic or stochastic in nature, e.g., measurements from rotating machinery. Mathematical models use dynamic observations to calculate features (e.g., amplitudes, phases, and spectrum frequencies) that are then used to identify changes from normal behavior (semi-supervised) or specific faults (supervised) [6]. In the area of vibration analysis of machines, time-domain, frequency-domain and time-frequency domain analysis are used to detect faults (reactive mode), to aid condition based maintenance (trend analysis), and to predict remaining useful life (predictive mode) [16], [17]. Anomaly detection mechanisms based on signal models may be statistical, phenomenological or based on cyber-physical models.

Knowledge-based methods: In knowledge-based methods, static or dynamic measurements are checked against predefined rules or fault patterns. Some examples of knowledge-based methods are expert systems, rule-based, ontology-based, logic-based, and state-transition analysis [18]. Anomaly detection methods can be semi-supervised, when the state of the system and the onset of anomalies are identified based on a set of rules (e.g., check for protocol-dependent features in data packet, verify occurrence of expected events) [19], or supervised, when specific process faults or network attacks are included in the model using expressive logic structure (e.g., detecting network anomalies by identifying illegitimate behavioral patterns with a sequence of states and transitions that can model network protocols) [18], [20]. Knowledge-based methods can be used in conjunction with other detection mechanisms. For instance, a set of rules could be used to provide context to the limits of a limit-based system. Knowledge-based methods may be either phenomenological or purely cyber-physical based with no reliance on data for model formulation.

Regression: Regression is a type of anomaly detection in which a relationship is identified between predictors and a dependent variable [22]. Some common methods for regression are Generalized Linear Models (GLM), Partial Least Squares (PLS), Support Vector Regression (SVR), Gaussian Process Regression (GPR), Artificial Neural Networks (ANN), decision trees, and ensemble methods [46]–[51]. Depending on the temporal nature of the predictors, regression can work either with static (e.g., linear regression) or dynamic (e.g., ARMA models) data. Regression models can be used to detect anomalies after their occurrence (reactive), evaluate trends that may lead to anomalies (trend analysis), or predict when they are most likely to occur (predictive). Regression can be used in conjunction with other types of anomaly detection to trigger alarms when the dependent variable leaves user-defined limits, for example. Regression may be used with data from cyber,

TABLE II
CATEGORIZATION OF ANOMALY DETECTION MECHANISMS FOLLOWING IDENTIFIED DIMENSIONS. SOME LABELS ARE ABBREVIATED: SUPERVISED (SUP.), SEMI-SUPERVISED (SEMI-SUP), UNSUPERVISED (UNSUP.), STATISTICAL (STAT.), PHENOMENOLOGICAL (PHENOM.), AND PHYSICAL (PHYS.).

Detection mechanism	System dynamics		Prediction			Supervision			System knowledge		
	Static	Dynamic	Reactive	Trend	Predictive	Sup.	Semi-sup.	Unsup.	Stat.	Phenom.	Cyber-phys.
Limit checking	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Signal models		✓	✓	✓	✓	✓	✓		✓	✓	✓
Knowledge-based method	✓	✓	✓	✓		✓	✓			✓	✓
Regression	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
State estimation		✓	✓	✓	✓	✓	✓		✓	✓	✓
Clustering	✓		✓			✓	✓	✓	✓	✓	
Classification	✓		✓			✓			✓	✓	

physical, or both domains. The models used for regression can be purely statistical or phenomenological (statistically tuned). Regression models may be semi-supervised or supervised, when incorporating some sort of system knowledge, or unsupervised, when relying only on statistical analysis. Unsupervised solutions, while commonly used, may lead to higher occurrences of false and missed alarms, are susceptible to noise, and are unable to correlate anomalies to faults.

State estimation: State estimation includes methods of semi-supervised or supervised anomaly detection for state-determined dynamical systems, where the structure and model parameters are known. In these methods, a set of state variables are sequentially estimated based on their previous values and available measurements of input and output variables. Similar to regression, these methods can be used with other types of anomaly detection to set warnings when estimates leave a region of normal operation or detect specific faults based on the estimates [6], [39]. State estimates may be used to warn about anomalies based on their current values (reactive), to avoid anomalies based on the current trend (trend analysis), or to predict their onset (predictive, if health or quality degradation is accounted for in the state vector). Estimation is performed in cyber or physical domains, depending on the model that is adopted. If the model includes the interaction between cyber and physical components, it could also be used with cyber-physical systems. The models used for state estimation may be data-driven, phenomenological, or based on cyber-physical knowledge of the system.

Clustering: Clustering is a type of anomaly detection where process observations that are similar in some user-defined metric are assigned to the same group (cluster). Clustering works in reactive mode with snapshot data. Clustering often works in unsupervised mode but it may also be used in semi-supervised and supervised approaches, if the identified clusters are mapped to a set of predefined classes. Multiple forms of clustering are available based on distribution, density, connectivity (hierarchical clustering), following centroids (k-means algorithms), among other methods [10]. Clustering methods may be purely statistical or phenomenological (if system knowledge is used to organize the identified clusters).

Classification: Classification methods identify to which set of predefined categories (classes) a new observation belongs on the basis of training data. The categories may be predefined utilizing phenomenological approaches (e.g., machine fault modes) or statistical mechanisms (e.g., pattern recognition in Deep Learning systems [12]). One of the major benefits of using classification methods is that fault detection and diagnosis are performed at the same step [6]. Similar to clustering, these methods work in reactive mode with snapshot data. Classification can only be performed in supervised approaches.

V. Mapping smart manufacturing anomalies to detection mechanisms

Most of the detection mechanisms identified in section IV can be applied to various types of anomalies. Table III matches the types of anomalies with suitable detection mechanisms identified in the literature.

Instantaneous anomalies: This type of anomaly can be identified with various techniques, such as feature extraction with limit checking, rules from knowledge-based methods, regression, estimation, clustering, and classification. This type of anomaly is the most studied in the literature.

Evolving anomalies: The identification of anomalies in the dynamics of the observations can be performed with limit checking for dynamic features, signal models, knowledge-based systems, regression, state estimation, clustering, and classification.

Communication anomalies: Communication anomalies can be detected with various methods, including limit checking in the form of statistical testing, knowledge-based methods, clustering, and classification.

Event-based anomalies: This type of anomaly has traditionally been addressed with knowledge-based methods, and more specifically, with logic-based methods. Formal models of the logic controllers may be used for their formal verification of liveness, safety, and reversibility at the discrete-event level; and to assure correctness of the event-based behavior of the control system.

Integration anomalies: The challenge for the identification of integration anomalies is that it requires an integrated view of the system as opposed to having dedicated anomaly detection methods for the individual components. Integration anomalies could potentially be identified by incorporating the multiple components of the production system in a large knowledge-base, which could take into account the discrete-event behavior of the logic controller and the way it interacts with the various machines and material handling devices; or with state estimation, accounting for the state of the entire system. The identification of integration anomalies requires the use of elaborate models of the production system and has been studied only in a handful of academic exercises [40], [41]. Integrated approaches may also be used for rapid fault diagnosis in interconnected systems [34], in order to reduce the number of consecutive and redundant alarms, and to rapidly

TABLE III
Mapping types of anomalies to candidate detection mechanisms

Detection mechanism	Instantaneous	Evolving	Communication	Event-based	Integration
Limit checking	[6], [15], [21], [22]	[6], [22], [23]	[18], [24], [25]		
Signal models		[6], [21], [26]	[27]		
Knowledge-based	[21], [28]	[6], [28], [29]	[18], [20], [25], [30], [31]	[19], [32], [33]	[9], [34]
Regression	[6], [10], [12], [35]	[6], [12], [26], [35]–[37]	[35]		
State estimation	[6], [29], [38], [39]	[6], [29], [38], [39]			[40], [41]
Clustering	[10], [35]		[18], [25], [35], [42]–[44]		
Classification	[6], [10], [35]	[29], [35]	[18], [25], [31], [35], [45]		

isolate the root cause with Failure Mode and Effect Analysis (FMEA) [52] and Fault Tree Analysis (FTA) [53], as well as to assess cyber-physical vulnerabilities [54].

VI. Concluding remarks

In this paper, we have explored the various anomalous behaviors that may appear in SM. Definitions were provided for the terms used to refer to anomalous scenarios in manufacturing. Various categories of anomalies were identified. In our categorization, we have unified all cyber- and physical anomalies in a common framework to respond to the ever-increasing connectivity in SM systems.

Anomaly detection methods in the literature were evaluated with respect to their capability to respond to the challenges brought by the advent of SM. Although static solutions are well developed and widely used in current manufacturing facilities, solutions that incorporate or track system dynamics are more accurate and should be considered as enhancements in future studies. Using a similar argument, current snapshot methods should evolve to methods that monitor system dynamics and state progression, and reactive methods should evolve to include trend analysis and predictive methods. Further improvements can be obtained with prescriptive methods, which rely on process data to warn about potential risks and take preventive actions. More importantly, due to the complexity of SM systems, the incorporation of system knowledge and SME in solution development should be considered (when available) over purely statistical methods.

We identified the different methods of anomaly detection that could be applied in SM and categorized them. The categories of SM anomalies were matched with the categories of detection methods that could potentially be used to identify them. It should be kept in mind that, in practice, multiple methods for anomaly detection are often used together to improve capability. There are multiple methods to identify some well-known categories of anomalies (instantaneous, evolving, communications, and discrete events). However, since most anomaly detection mechanisms were not tailored for closely-integrated system, most methods do not support cross-domain, multivariate, multi-component analysis of SM systems. Although some anomaly detection mechanisms would be able to work with an integrated model of the entire manufacturing system, their application for the detection of integration anomalies is currently uncommon.

The study and detection of integration anomalies will require the development of new methods, which are not expected to substitute but to complement anomaly detection methods at the component level. Future work in this area will focus on the development of cyber-physical models of SM systems for use in cross-domain, multi-component anomaly detection methods tailored for interconnected SM systems. Cyber-physical models may be used to verify expected relationships between the cyber and physical components of the SM system and to provide knowledge of the system-level state to improve anomaly detection at the component level.

References

[1] J. Davis, T. Edgar, J. Porter, J. Bernaden, and M. Sarli, "Smart manufacturing, manufacturing intelligence and demand-dynamic performance," *Computers & Chemical Engineering*, vol. 47, pp. 145–156, 2012.

[2] B. A. Weiss, G. W. Vogl, M. Helu, G. Qiao, J. Pellegrino, M. Justiniano, and A. Raghunathan, "Measurement science for prognostics and health management for smart manufacturing systems: key findings from a roadmapping workshop," in *Annual conference of the prognostics and health management society*, 2015.

[3] Z. DeSmit, A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "Cyber-physical vulnerability assessment in manufacturing systems," *Procedia Manufacturing*, vol. 5, pp. 1060–1074, 2016.

[4] L. J. Wells, J. A. Camelio, C. B. Williams, and J. White, "Cyber-physical security challenges in manufacturing systems," *Manufacturing Letters*, vol. 2, no. 2, pp. 74–77, 2014.

[5] Y. Pan, J. White, D. C. Schmidt, A. Elhabashy, L. Sturm, J. Camelio, and C. Williams, "Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems." *International Journal of Interactive Multimedia & Artificial Intelligence*, vol. 4, no. 3, 2017.

[6] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer Science & Business Media, 2006.

[7] S. R. Chhetri, J. Wan, and M. A. Al Faruque, "Cross-domain security of cyber-physical systems," in *Design Automation Conference (ASP-DAC), 2017 22nd Asia and South Pacific*. IEEE, 2017, pp. 200–205.

[8] S. D. Applegate, "The dawn of kinetic cyber," in *Cyber Conflict (CyCon), 2013 5th International Conference on*. IEEE, 2013, pp. 1–15.

[9] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[10] M. Goldstein and S. Uchida, "A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data," *PloS one*, vol. 11, no. 4, 2016.

[11] M. Thomson, P. Twigg, B. Majeed, and N. Ruck, "Statistical process control based fault detection of CHP units," *Control Engineering Practice*, vol. 8, no. 1, pp. 13–20, 2000.

[12] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[13] V. J. Hodge and J. Austin, "A survey of outlier detection methodologies," *Artificial intelligence review*, vol. 22, no. 2, pp. 85–126, 2004.

[14] R. Olszewski, "Generalized feature extraction for structural pattern recognition in time-series data," Ph.D. dissertation, Carnegie Mellon University, 2001.

[15] C. Jin, J. Moyne, J. Iskandar, H. Hao, B. Schulze, M. Armacost, and J. Lee, "Pattern recognition-agumented feature extraction for semiconductor manufacturing processes," in *APC Conference XXVIII*, 2016.

[16] Z. Peng and F. Chu, "Application of the wavelet transform in machine condition monitoring and fault diagnostics: a review with bibliography," *Mechanical systems and signal processing*, vol. 18, no. 2, pp. 199–221, 2004.

[17] A. K. Jardine, D. Lin, and D. Banjevic, "A review on machinery diagnostics and prognostics implementing condition-based maintenance," *Mechanical systems and signal processing*, vol. 20, no. 7, pp. 1483–1510, 2006.

[18] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: methods, systems and tools," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 303–336, 2014.

[19] B. Berthomieu and M. Diaz, "Modeling and verification of time dependent systems using time Petri nets," *IEEE transactions on software engineering*, vol. 17, no. 3, p. 259, 1991.

[20] J. M. Estevez-Tapiador, P. Garcia-Teodoro, and J. E. Diaz-Verdejo, "Stochastic protocol modeling for anomaly based network intrusion detection," in *Information Assurance, 2003. IWIAS 2003. Proceedings. First IEEE International Workshop on*. IEEE, 2003, pp. 3–12.

[21] R. Kothamasu, S. H. Huang, and W. H. VerDuin, "System health monitoring and prognostics–a review of current paradigms and practices," in *Handbook of Maintenance Management and Engineering*. Springer, 2009, pp. 337–362.

[22] B. Abraham and A. Chuang, "Outlier detection and time series modeling," *Technometrics*, vol. 31, no. 2, pp. 241–248, 1989.

[23] A. Ray, "Symbolic dynamic analysis of complex systems for anomaly detection," *Signal Processing*, vol. 84, no. 7, pp. 1115–1130, 2004.

[24] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang, and S. Zhou, "Specification-based anomaly detection: a new approach for detecting network intrusions," in *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 2002, pp. 265–274.

[25] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers & security*, vol. 28, no. 1, pp. 18–28, 2009.
[26] G. W. Vogl and M. A. Donmez, "A defect-driven diagnostic method for machine tool spindles," *CIRP Annals-Manufacturing Technology*, vol. 64, no. 1, pp. 377–380, 2015.
[27] V. Alarcon-Aquino and J. A. Barria, "Anomaly detection in communication networks using wavelets," *IEE Proceedings-Communications*, vol. 148, no. 6, pp. 355–362, 2001.
[28] R. Wirth, B. Berthold, A. Krämer, and G. Peter, "Knowledge-based support of system analysis for the analysis of failure modes and effects," *Engineering Applications of Artificial Intelligence*, vol. 9, no. 3, pp. 219–229, 1996.
[29] P. M. Frank, "Fault diagnosis in dynamic systems using analytical and knowledge-based redundancy: A survey and some new results," *Automatica*, vol. 26, no. 3, pp. 459–474, 1990.
[30] T. F. Lunt, R. Jagannathan, R. Lee, A. Whitehurst, and S. Listgarten, "Knowledge-based intrusion detection," in *AI Systems in Government Conference, 1989., Proceedings of the Annual*. IEEE, 1989, pp. 102–107.
[31] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," *Expert Systems with Applications*, vol. 41, no. 4, pp. 1690–1700, 2014.
[32] W. M. Van der Aalst, "The application of Petri nets to workflow management," *Journal of circuits, systems, and computers*, vol. 8, no. 01, pp. 21–66, 1998.
[33] M. P. Cabasino, A. Giua, and C. Seatzu, "Fault detection for discrete event systems using Petri nets with unobservable transitions," *Automatica*, vol. 46, no. 9, pp. 1531–1539, 2010.
[34] M. Melik-Merkumians, T. Moser, A. Schatten, A. Zoitl, and S. Biffl, "Knowledge-based runtime failure detection for industrial automation systems," in *Workshop Models@ run. time*, 2010, pp. 108–119.
[35] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM computing surveys (CSUR)*, vol. 41, no. 3, p. 15, 2009.
[36] W. Q. Wang, M. F. Golnaraghi, and F. Ismail, "Prognosis of machine health condition using neuro-fuzzy systems," *Mechanical Systems and Signal Processing*, vol. 18, no. 4, pp. 813–831, 2004.
[37] D. Friedlander, I. Chattopadhyay, A. Ray, S. Phoha, and N. Jacobson, "Anomaly prediction in mechanical systems using symbolic dynamics," in *American Control Conference, 2003. Proceedings of the 2003*, vol. 5. IEEE, 2003, pp. 4275–4280.
[38] R. K. Mehra and J. Peschon, "An innovations approach to fault detection and diagnosis in dynamic systems," *Automatica*, vol. 7, no. 5, pp. 637–640, 1971.
[39] Z. Wang, D. Anand, J. Moyne, and D. Tilbury, "Improved sensor fault detection, isolation, and mitigation using multiple observers approach," *Systems Science & Control Engineering*, vol. 5, no. 1, pp. 70–96, 2017.
[40] S. Windmann and O. Niggemann, "Efficient fault detection for industrial automation processes with observable process variables," in *2015 IEEE 13th International Conference on Industrial Informatics (INDIN)*. IEEE, 2015, pp. 121–126.
[41] O. Graeser, B. Kumar, O. Niggemann, N. Moriz, and A. Maier, "AutomationML as a shared model for offline-and realtime-simulation of production plants and for anomaly detection," in *Informatics in Control, Automation and Robotics*. Springer, 2013, pp. 195–209.
[42] G. C. Tjhai, S. M. Furnell, M. Papadaki, and N. L. Clarke, "A preliminary two-stage alarm correlation and filtering system using SOM neural network and k-means algorithm," *Computers & Security*, vol. 29, no. 6, pp. 712–723, 2010.
[43] L. Portnoy, E. Eskin, and S. Stolfo, "Intrusion detection with unlabeled data using clustering," in *In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001*, 2001.
[44] C. Manikopoulos and S. Papavassiliou, "Network intrusion and fault detection: a statistical anomaly approach," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 76–82, 2002.
[45] D. Barbará, J. Couto, S. Jajodia, and N. Wu, "Adam: a testbed for exploring the use of data mining in intrusion detection," *ACM Sigmod Record*, vol. 30, no. 4, pp. 15–24, 2001.
[46] D. C. Montgomery, E. A. Peck, and G. G. Vining, *Introduction to linear regression analysis*. John Wiley & Sons, 2015.
[47] S. Seo, M. Wallat, T. Graepel, and K. Obermayer, "Gaussian process regression: Active data selection and test point rejection," in *Neural Networks, 2000. IJCNN 2000, Proceedings of the IEEE-INNS-ENNS International Joint Conference on*, vol. 3. IEEE, 2000, pp. 241–246.
[48] C. E. McCulloch, "Generalized linear models," *Journal of the American Statistical Association*, vol. 95, no. 452, pp. 1320–1324, 2000.
[49] I. Helland, "Partial least squares regression," *Encyclopedia of statistical sciences*, 2006.
[50] D. Basak, S. Pal, and D. C. Patranabis, "Support vector regression," *Neural Information Processing-Letters and Reviews*, vol. 11, no. 10, pp. 203–224, 2007.
[51] C. Fyfe, "Artificial neural networks," in *Do Smart Adaptive Systems Exist?* Springer, 2005, pp. 57–79.
[52] D. H. Stamatis, *Failure mode and effect analysis: FMEA from theory to execution*. ASQ Quality Press, 2003.
[53] C. A. Ericson and C. Ll, "Fault tree analysis," in *System Safety Conference, Orlando, Florida*, 1999, pp. 1–9.
[54] Z. DeSmit, A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems," *Journal of Manufacturing Systems*, 2017.