Integrated Cyber Physical Assessment and Response for Improved Resiliency

P. Sivils[1], C. Rieger[2], K. Amarasinghe[1], M. Manic[1]

1 Introduction

Cyber-physical systems (CPS) are commonly used architectures for critical infrastructure applications such as smart urban environments. The Internet-of-Things (IoT) is a network based architecture in which physical devices, sensors, embedded electronics, software, vehicles, etc. can communicate and transfer data with each other over an internet connection. IoT technology is a subset of CPS in which physical procedures are controlled and affected by computational processes while the computations are simultaneously altered based on the physical system state. In expansive CPS designs, such as those required for IoT enabled urban ecosystem applications, expansive networks are implemented to collect, transfer, monitor, and analyze data. This data is processed for automated control applications, generate predictive models, and provide enhanced understanding for operators and consumers. [39]

For cyber-physical systems, as in control systems and critical infrastructure, ensuring the resilience of a system is critical to its long-term efficiency and security. CPS uses many automated systems to perform tasks and handle anomalies. These systems can be very complex, have different methods of integration, and involve varying levels of human interaction. Resilience is a multi-disciplinary effort that ensures changes and anomalies experienced by a system are tolerated by the system design. Resilient control systems maintain system monitoring, awareness, cybersecurity, and decision making at an acceptable level of operation to facilitate normal and necessary functions.

Ensuring the trustworthiness of data coming from the various devices, sensors and network traffic should be one of the top priorities in designing any cyber-physical system (CPS). Trustworthy sources ensures that the available data is being used efficiently and the outputs are accurate. This is especially important in smart city

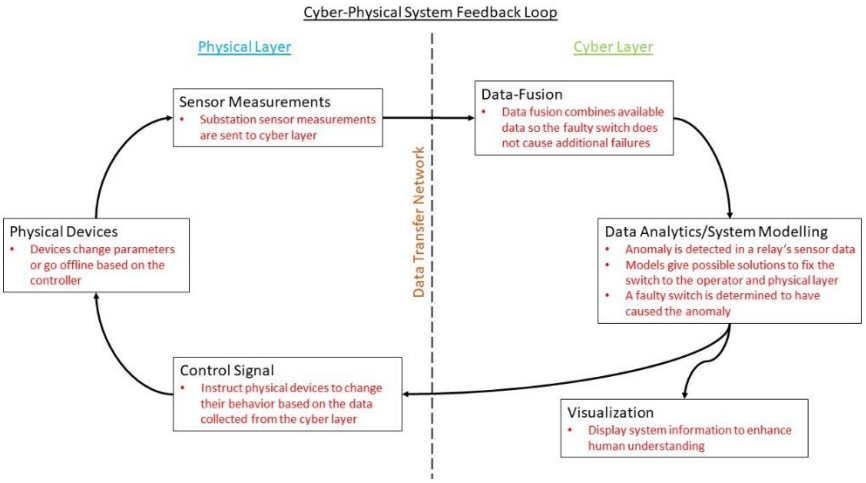
[1] Virginia Commonwealth University
[2] Idaho National Laboratory

infrastructure where outputs and decisions affect people's daily lives. Untrustworthy data can lead to poor automated system control, difficulty in decision making, and frustrating end-user experiences. This data is very often very large in scale and comes from heterogeneous sources. Moreover, information technology (IT) and operation technology (OT) operators who now find themselves responsible for cybersecurity come from a variety of backgrounds, differing decision support requirements, and knowledge capabilities. To effectively abstract the complexity of cybersecurity and simultaneously address the variety of roles, knowledge, and need, a design is needed that performs much of the required analysis for the user and presents only relevant information in a consistent way. IoT infrastructure on a city-wide scale requires many different data nodes in the form of devices and sensors to perform specific, individualized tasks. This means that the datasets created from a city-wide IoT system will be high-dimensional and heterogeneous.

This chapter provides a summary and analysis of crucial concepts in understanding cyber-physical degradation assessment, heterogeneous data-fusion, and visualization under a smart city IoT architecture. These concepts will provide a basis for enhancing the effectiveness of human response to physical and cyber-events within the scope of smart city infrastructure. It is important to understand that CPS degradation analytics provide the source information that a data-fusion engine will use to tailor context awareness to the human. Visualization presents this information to ensure a reproducible response for each operational role regardless of background (e.g., cyber, operational, scientific, etc.) or level of performance or the humans involved at any particular time.

1.1 What are Cyber-Physical Systems?

Cyber-physical systems are usually used to monitor and control critical infrastructures. Examples include smart grids, autonomous vehicles, and smart buildings. CPS combines physical components and computer-controlled algorithms for monitoring and process control. CPS integration is achieved through the implementation of feedback loops in which both the cyber and physical aspects of a system affect each other. The physical processes are monitored and controlled by the computational algorithms embedded in the cyber aspects of a CPS, and computations are simultaneously altered by the physical state of the CPS. This is accomplished through data analysis, system modelling, both data-driven and physical, and data fusion to enhance knowledge discovery from heterogeneous sources of cyber-physical data. In general, OT systems are one type of CPS. Processing heterogeneous, high-dimensional data from acquisition through data-fusion is a critical task that must ensure capability and scalability in CPS. [5, 7]



The IoT is a subset of CPS. IoT architectures establish communication networks between multiple decentralized, heterogeneous CPS. In this sense, the IoT is the second layer of CPS that enables digital integration and communication. IoT applications are often provided by embedding sensors, software, devices for computational or networking applications, etc. into existing objects within CPS architectures. These are usually physical objects that are not usually designed for computational tasks (appliances, toys, vehicles, etc.). The communication and data-transfer between the various IoT devices takes advantage of pre-existing network infrastructure such as the internet, reducing overhead for large-scale distributed system applications. [39]

1.2 Challenges in CPS

Concern over cyber-attacks has led to the thoughtless proliferation of tools focused on addressing pressing cybersecurity needs without long-term considerations. Much of what has been developed originates in the IT sector, and has been inherited with little customization by the control systems world. As a result, control systems professionals who have not been traditionally responsible for security, now have a role in the cybersecurity of OT systems, and they lack tools customized to the OT environment. Therefore, it is safe to assume that various roles exist within the security equation, and a different level of expertise is required for the many individuals working in these complex systems. Even within IT, the diversity of manufacturers, number of cyber security appliances installed, and sheer number of parameters monitored can create data overload in the most adept user. This overload situation can grow as an increasing number of security solutions are fielded to protect the system,

each with its own stream of monitoring data. The resulting data deluge likely produces many false negatives because humans cannot examine all the data that has become available. Additionally, the common use of overly conservative alarm thresholds produces numerous false positives that human controllers learn to ignore since the majority are frivolous.

Based upon cyber, physical, and interacting cyber-physical characterizations of both host and network patterns, CPS models can be used to distinguish conditions and behaviors indicative of a cyber-attack from benign, unintended actions or physical failures. As a feedback loop to recognize performance, latency and integrity will provide the fundamental attributes that will be correlated by measurable cyber-physical parameters [3], [4], [5]. Through the use of leveraged and data-driven models, cyber-physical parameters specific to use cases can be evaluated to correlate performance impact. That is, given a change (normal or abnormal) in the cyber-physical environment, unacceptable variations will be evaluated and codified. The resulting process will establish a network performance baseline, a direct measurement of resilience, and a diverse approach to recognizing distributed threats across the interwoven layers of the OT/IT architecture.

Computer networks remain the primary vector for cyber-attacks, and yet detecting cyber-attacks over computer networks remains limited—"misuse-based intrusion detection" [1], which relies on static "signatures" of "known bad" activity, has significant value, but also remains blind to unknown attacks, and frequently even to slight variations on attacks. "Anomaly-based intrusion detection" [1], which analyzes statistical variations from "normal," helps to address some of these issues [2], but is limited by the massive imbalance in "good" data to "bad" data in-training sets, the high cost of false positives to human operators, the so-called "semantic gap" between flagging anomalous events and understanding the cause of those events, and the raw diversity of network attacks [2]. Moreover, the extremely high and diverse types of network traffic and computing environments present in IoT infrastructure makes these problems even worse. Indeed, many commercial solutions are ineffective since these are often either not capable of performing on networks with bandwidths as high as those on IoT networks, or not tuned for such environments. A basic misapplication of the anomaly-detection approach is to assume that all anomalous behaviors are necessarily suspicious. The terms, "anomalous," "errant," and "malicious" all have different meanings, but "malicious" carries a value judgment with it. Normal activities may vary significantly with software upgrades and network changes.

Combining multiple heterogeneous data sources can introduce multiple challenges for data-fusion, system-modeling, and visualization applications. The collected datasets may contain information with varying resolutions, is incomplete or uncertain, or is unsynchronized due to various offsets in the measurement devices. Every node in a CPS, whether it is recording data or providing an end-user interface, will have its own method of recording and saving data. So within a large-scale IoT system, the vast amounts of available data sources can provide their data in many different formats that must be combined so that an analytics model can make sense

of it. Additionally, the available data is a mix of cyber-data, e.g. network traffic, and physical data, e.g. temperature readings. Both types of data are part of the same system and should be looked at as a whole, rather than separate entities with their own architecture. Data-fusion techniques combine heterogeneous sources of data into a new representation by exploiting existing interdependencies in the dataset. These techniques are used to help improve the performance, scalability, and reliability of the control and monitoring analytics systems that implement these datasets.

2 Cyber-Physical Analytics for Resilience and Assessment

This section outlines the anomaly detection analytics to be used in combination with high-fidelity models to recognize and mitigate cyber-attacks and enhance system resilience. Providing complete, reliable, and actionable information is essential for system resiliency and decision-making within an IoT system. In order to ensure the trustworthiness of available sensors in an IoT system design, analytics that ascertain accurate health measurements of sensors is essential. Failures within highly interdependent and complex environments can lead to cascading adverse consequences. As the digital footprint of these environments has continued to evolve, the potential ramifications of conjoined CPS failures has not been considered and has instead become more obscure. If recognized and characterized quickly and consistently at the source, however, the adverse effects can be localized and cascading failures prevented. With this focus in mind, methodologies should be implemented to characterize a diverse range of behaviors found on OT/IT networks and classify them according to their degree of normality. Application of these methodologies will lead directly to measurable improvements in system resilience.

A cyber-physical approach towards IoT infrastructure will notably ascertain degradation—both cyber and physical—to distinguish cyber-attack from physical failure. Information on blended security attacks (both cyber and physical) should also be characterized. Analytics systems should remain robust under various degradation scenarios resulting in partial or unreliable information. IoT enabled sensors and devices, as well as the networks between them are susceptible to malicious tampering, unforeseen failures, and accidents; as well as degradation that arises naturally from normal operations. Robust cyber-physical analytics designs should enhance the response of decision-makers by identifying and providing actionable information about how and where degradation is occurring.

Computer networks within a system are often the primary vector for cyber-attacks on IoT infrastructure. However, established intrusion detection system (IDS) methodologies are limited when it comes to distinguishing between anomalous and malicious network behavior. “Misuse-based intrusion detection” requires a priori knowledge of network traffic patterns that indicate malicious activities. This type of network monitoring, while useful, is unable to detect unknown, or sometimes

slightly altered, cyber-attacks. Another IDS scheme, "anomaly-based intrusion detection," implements various statistical metrics to determine how far off network traffic is from baseline activity. Statistical analysis is useful for mitigating the problems inherent in misuse-based IDS, but it introduces another problem with differentiating between non-malicious anomalous traffic patterns from cyber-attacks identified by the IDS. Due to vast diversity of network traffic patterns, which is further exacerbated by the vast diversity of cyber-attacks and the large amounts of traffic inherent in a city-wide IoT system, many anomalous patterns can emerge that are not malicious in nature. Since the simple approach of assuming all anomalous network traffic is malicious is impractical at scale, false-positives flagged by an IDS requires some human analysis to understand the causes of the events and to provide the necessary response. This presents a further problem as backgrounds, knowledge, and physical capabilities vary among individuals. As such, wide-scale IDS systems for IoT applications should aim to provide as few, if any, false positives as possible. These systems should be able distinguish degradation arising from cyber-attacks and physical failures. Additionally, a design focus on quickly identifying and localizing failures enables fast and accurate response times for human operators. A design focused on localization can also help mitigate cascading failures. As IoT systems grow larger and more interconnected, the potentiality of one failure leading to other, possibly unforeseen, failures in multiple other areas increases.

2.1 State Awareness and Anomaly Detection

Developing an accurate state awareness system with robust anomaly detection techniques is crucial to providing users with the relevant information and models needed to recognize threats and coordinate effective responses. These systems are typically implemented either through data-driven or physics-based models. Data driven models encompass computational intelligence (CI) and statistical models. These designs use collected data to generate models that represent the system as it should be when fully-functional. These state estimations can be compared to current system states which can help identify when and where system anomalies are occurring and predict how a system will behave in the future given the current state. Additionally, there are data-driven models that use 'online' learning algorithms. These algorithms continue to refine their initial models using new data collected after deployment. These algorithms allow the models to be further refined over time to better handle new or unforeseen challenges/attacks. While data-driven system models are powerful tools for IoT analysis applications, there are some potential issues that should be kept in mind during the design process. Data-driven approaches use some form of pattern matching to build their models and therefore require large datasets describing the systems activity, with data on multiple safe/unsafe scenarios often being required. Not having enough training data can result in a model with poor performance leading to unsatisfactory results. This means that designing useful

models can require extensive, potentially cost-prohibitive, data collection. The pattern matching nature of data-driven models means they are also susceptible to overfitting, where the trained model too closely resembles the training data. Overfitting can cause the model to have very little room for error, meaning normal data patterns that were missing from the training data could be flagged as abnormal resulting in many false positives. Additionally, pattern matching schemes are susceptible to spoofing. Spoofing is when an attacker reverse engineers the model allowing them to know what inputs are needed to create a desired output. In CI applications, most CI models are 'black-box' algorithms. This means that observers can only know the inputs and outputs of the model but cannot get information about the model's inner workings. This makes understanding and explaining the behavior of a model extremely difficult, if not impossible.

Computational intelligence (CI) and machine-learning methods have been used to provide anomaly detection systems for a variety of applications. Artificial neural networks (ANNs), such as multilayer perceptron (MLP), are a popular machine-learning technique that have been shown to provide excellent results in anomaly detection applications. In cybersecurity, ANNs have been used in anomaly-based network intrusion detection systems that can handle a large variety of cyber-attacks [8]. Designs were presented in literature that were able to achieve very high detection rates (~99%) [9] [10] [11] [12] on various datasets. Additionally, [13] [10] presented ANN designs that can not only achieve high-detection rates, but also report very few false positives and false negatives (~0.1%). Recently, [12] presented an improvement to standard MLP anomaly detection in medical CPS by reducing the detection process to multiple 2-class classifications to improve accuracy and reduce false reports. ANNs used for anomaly detection systems in control system architectures, such as smart grids, have been presented with relatively high detection rates [14] [15] [16], though the reported false alarm rates are often high as well. Integrity attacks can compromise a system by spoofing system data so that it appears to an operator that the system is in a safe-state, while an attacker gains access to critical resources. An ensemble modeling design, where multiple models are aggregated to increase accuracy, was presented in [17] for these types of anomalies that performed better than other prior MLP methods with a small percentage of false reports (~2%).

Another area of CI that has shown promise in CPS anomaly detection is fuzzy logic. Fuzzy logic systems (FLSs) embed human understanding and knowledge into a system in the form of 'if-then' rules. These rules are then converted into crisp values, which can then be used for decision-making tasks. Traditionally, the rule base for a FLS is derived from expert knowledge of the system, though since some CPSs can be extremely complex, various publications have explored adaptive fuzzy architectures that can generate their own rules [18] or allow them to be dynamically altered [19]. FLSs are grey-box algorithms, where some inner workings of the system can be known but other aspects remain unknowable. This is an improvement over other CI algorithms in terms of understandability and system awareness.

Recently, deep-learning neural network algorithms, such as convolutional and recurrent neural networks, have emerged as the state-of-the-art in machine-learning

due to their ability to produce more robust models than standard ANN architectures. Literature has presented deep learning algorithms for cyber-attack anomaly detection, showing robust detection against a variety of attacks on CPSs [20] [21]. Additionally, a simple convolutional neural network design was presented in [22] to monitor motor conditions in real-time with a high accuracy when tested on real-world motor datasets.

Classical CI algorithms are still in use, though in recent research they are mostly used for comparison and validation of newer CI methods. These include K-Nearest Neighbor (KNN) [23], Support Vector Machine (SVM) [23] [24], and Self-Organizing Map (SOM) [25] [26].

Various other statistical modeling algorithms have been explored for enhancing anomaly detection applications. These algorithms do not necessarily fall under the CI category, though they are similarly data-driven, and are often used alongside CI classifiers to enhance performance. [27] and [24] present a detailed comparison of multiple statistical modeling methods. Multiple experiments were run using Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Principal Component Analysis (PCA), S-Transform, and Shapelet algorithms on Phasor Measurement Unit (PMU) fault and generation-loss datasets. Each method was verified using various KNN and SVM classifiers. The authors show that the more recent Shapelet methods outperformed all other compared methods. Interestingly, the authors also note that feeding raw data into the classifiers often outperformed classic statistical methods. PMU data was also used in [23] to test a kernel principle component analysis (kPCA) method for anomaly detection in high-resolution micro-PMUs. The kPCA was combined with a novel 'partially hidden structured' SVM to classify the type of anomaly detected. The authors showed the combined algorithms outperformed standard decision algorithms such as Ada Boost and Decision Trees.

These methods have also been explored for the detection of cyber-anomalies. A Reduction of Quality (RoQ) attack detection method is presented in [28]. Since a quality drop in network traffic does not always imply that a system is under attack, a more robust algorithm is needed to detect anomalies, as well as identify that the anomalies are malicious. The two-stage design uses wavelet analysis to detect abrupt changes in quality in the first step. Autocorrelation analysis is then used to identify attack characteristics in the local network traffic. The proposed design achieved a 3% false negative rate with 0% false positives. A Chi-square statistics algorithm was proposed by [29] for tiered intrusion detection applications with multiple alarms. The Chi-square algorithm achieved detection rates of 71-100%, depending on various conditions, with no false positives.

Physics-based models implement prior expert knowledge to exploit known relationships in the available data to detect when an anomaly has impacted the system. Their advantage over data-driven models is that they are white-box by nature, allowing users to have access to all of the information of the inputs, outputs, and inner-workings of the model. Another advantage of physics-based models is that

they do not rely on data for training meaning no data collection is necessary. However, the required expert knowledge needed to design an adequate model may not always be readily available. Physics-based models can also miss useful intricacies in a system that data-driven models can exploit. Hybrid models that incorporate aspects of both data-driven and physics-based models can help alleviate the weaknesses found in both modeling schemes.

Physics-based modelling techniques can be seen in [30] and [24] where the authors presented a physics-based method that uses energy information from PMUs to reconstruct a model of the system as a whole that can then be used to detect anomalies present in the system. A physics-of-failure mechanism is presented in [31] using particle-filtering, a probability density algorithm, to detect anomalies in brushless DC motors. A different model-based anomaly detection method is proposed in [32]. This method uses 'gaps' between data points to define and detect anomalies in the data. This approach does not require any prior knowledge of the system and uses only a local subset of data points. The authors detail its potential for anomaly detection in big data and data stream applications due to its computational efficiency.

2.2 Distributed Systems

The distributed nature of IoT systems for city infrastructure applications adds its own challenges in the development of data analytics systems. The many devices and sensors in a city-wide IoT system can be spread out across large distances, and all of this data needs to be collected, analyzed, and acted upon quickly. Classic distributed system architectures implemented a central data-fusion center where all data is funneled to a single location, analyzed, and output analytics are sent back out to the system and users. While this approach is 'efficient' in that only one location has to be built, maintained, and protected, there are some downsides that become more problematic on large-scale distributed architectures. First, data transfers take time. In a city-wide IoT, emergency decision making requires all relevant information be provided as quickly as possible. This means that data transfers need to be as fast as possible to enable real-time analysis and system monitoring. Second, central data-fusion centers inherently create single-points-of-failure across the system. This increases the chance of crippling security risks and makes localizing degradation difficult. Lastly, not all data may be necessary for global degradation analysis. Certain data-streams from devices and sensors in the network may only be relevant to the health of their respective device or subsystem meaning including them in a global degradation analysis design may be unnecessarily increasing the computational overhead of the system.

A common design method used to alleviate these issues is to decentralize the system such that multiple localized subsystems perform their degradation analysis as independently as possible. Using decentralized subsystems allows for shorter

data transfers as each subsystem data center should be local to the data sources fed into it. Subsystems reduce single points of failure as each subsystem can continue to run independently if another subsystem is shut down. Subsystem analytics could also help identify the source and cause of the degradation. The computational overhead inherent in high-dimensional heterogeneous data sets can be reduced since each subsystem only uses the data it needs. Additionally, if a central data-fusion center is needed for global degradation analytics, subsystems can report device and sensor information as needed, or only provide a subsystem overview reducing the amount of network traffic and necessary computational overhead and the central location. However, it should be kept in mind that in any complex system like smart city IoT infrastructure, crucial interdependencies may exist across all data sources. In a system where degradation in one area can have huge impacts on other aspects of the system and/or the wellbeing of city residents, care must be taken to ensure the communication of the interdependencies between subsystems is not lost in the architecture design or within the implementation of knowledge- and data-fusion techniques.

A fully decentralized CPS design is proposed in [35] that uses relay-assisted sensor networks. Their design makes accurate estimations by only exchanging information between neighboring sensors, using relay nodes to transmit information to the rest of the network. The authors show their design scheme can handle sensor failures, fading channels, and noisy data without making assumptions about the communication topology, which further enhances resilience. Another design for a decentralized resilient monitoring system is presented in [36]. The system quantifies the trustworthiness, or data quality, of the sensors by comparing readings to a known trustworthy source. The system is divided into subsystems through process-variable probabilistic-mass-function adaptations to alleviate the high-dimensionality of data is CPS, and knowledge fusion techniques are incorporated to ensure important interconnected information between subsystems is not lost. Distributed CPS designs also have a layer of communication that must be taken into account. When parts of a CPS are separated, potentially by large distances, reliable communication is just as important as the control algorithms. [37] introduced a joint optimization framework for control and communication. It proposes a simulated annealing-based optimization approach to minimize the number of control tasks sent, with the sub-objective of minimizing energy consumption across devices during communications, and was successfully implemented on a heating, ventilating, and air conditioning (HVAC) dataset.

The increasing interconnectedness of information and communication technologies in CPS make in-depth design analysis crucial to ensure that both physical safety and cybersecurity requirements are met. [38] presented a formal methodology to integrate safety and security analysis into a single framework. Their method, System-Theoretic Accident Model for Safety and Security (STPA-SafeSec), offers a top-down approach to analyze and identify constraints in both areas of cyber-physical systems simultaneously. STPA-SafeSec focuses on the desired outcomes of a system, rather than using existing threats as the basis for security requirements.

The framework was applied to various scenarios in micro-grid systems and was shown to help system analysts identify critical system components along with safety and security impacts arising from specific vulnerabilities.

2.3 Resilient Monitoring

In CPS, particularly critical infrastructure, safeguards must be taken to keep the system stable despite device degradation from malicious attacks or natural damage/degradation. Resilient system-state awareness, estimation, and anomaly detection methods are crucial for system monitoring and decision-making under highly dynamic conditions. Additionally, CPS can encompass large numbers of distributed networks. These networks can contain different data types and may span large distances, increasing both the computational and temporal overhead needed to perform analysis. Many CPS use a central data-fusion center to perform tasks, though this can create a single-point-of-failure for the entire system.

As with anomaly detection, CI techniques have been a promising area for resilience in state-of-the-art CPS architectures. [18] presented a fuzzy-neural data-fusion engine to model systems to create resilient state awareness. The design implements an ANN that models current and future system states based on historical data to enhance state awareness when system data is unreliable or unavailable. This was implemented alongside standard threshold-based alarms and a fuzzy logic-based anomaly detection system to further enhance the state awareness architecture. Similarly, an adaptive neuro-fuzzy controller is presented in [19] for use in a nuclear power plant and was shown to be highly tolerant to faults in a variety of control tests.

A model-based state estimation method using Satisfiability Modulo Theory (SMT) is presented in [33]. SMT uses first-order logic to create and verify models. The proposed design models a CPS using Boolean and convex constraints; then, the authors' Imhotep-SMT uses the constraints to estimate the state and identify which sensors are under threat. This method was verified using simulated data, as well as successfully controlling an unmanned ground vehicle under adversarial attacks and noisy sensor data.

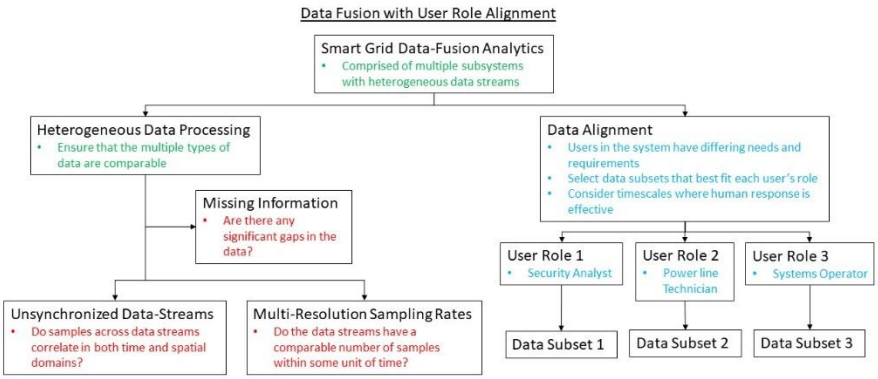
CPS resilience can also be improved through the design choices made. [34] described a theoretical framework for secure state estimation in CPS. This work discusses two ideas for system design towards state estimation: (1) system-states cannot be accurately reconstructed if more than half of the sensors are under attack, and (2) if a system can be stabilized in the presence of sensor attacks, then its state can be accurately estimated as well. The authors use this framework to show the importance of designing resilient controllers that can be used for secure state estimation, rather than separately implementing secure controllers and secure estimators.

3 Data-Fusion and Data Alignment

This section provides an overview of challenges and possible solutions for data-fusion in the domains of IoT and CPS. Data-fusion is the process of combining the available data streams into new, less unwieldy representations by exploiting existing interdependencies in the dataset [18]. These representations are then used to increase the reliability and consistency of state awareness, control, modeling, and predictions for a CPS. Datasets generated by large scale CPS are usually high-dimensional (data is collected from multiple sources) and heterogeneous (data of different types and modalities is collected and reported). Furthermore, the collected data can have low or multiple resolutions, report events out of sync with other data sources, or just be missing

Human effectiveness is a challenge in all contexts of human interface with information technology (IT) and operation technology (OT), including cybersecurity. Even within common role and responsibility area, the backgrounds, best methods of learning/comprehension, and physical performance vary among individuals. In moving towards a repeatable and low latency response to cyber-attacks, both human and automated response actions to cyber-events must be considered. This includes consideration of the most resilient effectiveness that can be achieved by adding human influence within an OT system. The human aspect of OT systems requires an extension of research and evaluation of the fusion and presentation of cyber-physical analytics that characterize the cyber-posture. Considering the importance of the cognitive and social environment, multidisciplinary exercises are planned to characterize the performance of research solutions. To this end, data-fusion designs should be created with a focus on delivering appropriate representations of information to the operator/consumer.

An extensive survey on recent data-fusion techniques and applications can be found in [39].



3.1 Multi-Modal Data

Multi-modal data describes data that is collected from multiple sources under varying conditions, such as data acquisition techniques in CPS. System modeling and decision-making tasks often rely on high-frequency data to achieve sufficiently accurate results. Data sources can have different resolutions, or sampling rates, meaning that one sensor may record data at 100 times per second, while another sensor records data only once a second. This is detrimental to the performance of the system as the analytics system will be forced to compare 99 fresh data points from the first sensor to the same static data point collected from the second sensor. Any important concurrent changes or interdependencies between the two sensors is completely lost within that second until the second sensor makes its next measurement. It is often too expensive and/or time consuming to ensure that all devices meet the same standards, even more so if part of the infrastructure is already implemented. As technology improves, newer devices may be introduced to the system that outperform the old ones and not every device can, or even needs to, be consistently upgraded to keep up. Therefore it is necessary to have a software solution to handle low/multiple sample rates to ensure that there exists enough data points from each sensor to generate accurate analytics as often as needed.

A method using ANNs is presented in [40] to increase state awareness by increasing the spatial resolution of data. The authors' method implemented data downscaling to gain increased spatial resolution, and they validated their algorithms on real-world CO2-concentration datasets. Similarly, [41] presented an online ANN method that can predict high-resolution temporal data using lower resolution sensors. The authors validated their algorithm on a real-world building energy management dataset, showing their method was more accurate than classical predictive models and that it could adapt to changes in building behavior. Another solution to the problem of data-fusion for multi-resolution data is presented in [42]. The proposed surface modeling algorithm combined features with varying resolutions through surface reconstruction and registration using Gaussian Process (GP)-modeling. The algorithm was validated on simulated and measured multi-surface data, and was significantly faster than the commonly used weighted least squares data-fusion (WLSDF).

Due to the heterogeneous nature of IoT data, it is important to keep the various data streams synchronized. Since system input is often collected from heterogeneous sources, synchronization of the data streams is important for state awareness and control. The potentially large number of heterogeneous data sources allows for singular events to be observed by multiple devices at once. These data sources can have varying latencies due to sample rates, transmission times, and missing data/noise. Multiple sensors monitoring the same object can end up with unsynchronized measurements, whether temporally or spatially. The sensors will all record the same event, but the multiple data streams will report the event happening at

different times. Unsynchronized data can be caused by inherent device measurement latencies, physical distance from what is being monitored, transmission times, network issues, etc. Using data that is not synchronized can increase the difficulty of system-modeling and prediction tasks by introducing conflicting information about the system's status and potentially malicious activity.

Unsynchronized sensor data can lead to conflicting information in decision-making and modeling tasks. [43] proposed a method for data alignment in sensor networks without the use of extra hardware or software in the sensors. The algorithm uses distinguishable points in the datasets to create a link between physical events and time. The authors showed their method successfully reduces the temporal offset between sensors, though testing was done with only two measurement devices. Another method for synchronizing the constant spatiotemporal offsets in measurement devices is shown in [44]. The authors presented an offline method to calculate the offsets using continuous state representation using a single estimator rather than the two-stage designs of previously established methods. This was shown to generate highly accurate offset estimations on several combinations of heterogeneous sensors.

Data-streams can also be incomplete or uncertain. Data sources can be compromised, temporarily disabled, or physically broken causing uncertainty in the IoT control systems. Trust metrics should be implemented so when conflicting data is presented to the system, determining which data sources can be trusted and which sources should be discarded can be done quickly to avoid unwanted consequences on the control side. Incomplete data should notify operators so that measures can be taken to restore the data source to its operational state, and safeguards should be in place to adjust the control and state awareness models in the presence of the missing data, or at the least notify users of a potential decrease in operational accuracy so any necessary risk assessments can be properly made before any actions are taken.

To help analysis on incomplete data, [45] presented a framework for rapid knowledge discovery from potentially incomplete datasets called structured data-fusion (SDF). SDF implements multidimensional arrays (tensors) so that users can quickly create and change libraries of processing methods, or factorizations. This allows users to work towards finding solutions from incomplete data faster and with reduced overhead.

When multiple sources provide conflicting data about an event, a method for choosing which sources to trust and which to disregard needs to be in place. [46] presented an algorithm for conflict resolution in heterogeneous datasets through "source-reliability estimation." The authors implemented an optimization model where source trust weights are continuously updated for each source based on their distance from known truths derived from confirmed reliable sources in the system. The optimization problem was tested on multiple real-world and simulated multi-source datasets and was shown to outperform other popular conflict resolution methods, such as the Gaussian Truth Model. A multi-sensor data-fusion approach to fall classification is presented in [47]. The authors presented a novel approach for daily activity and fall detection for individuals using accelerometer and gyroscope

data collected from a smartphone, along with user-specific measurements (i.e., height, weight, etc.). The authors combined the available data using Receiver Operating Characteristic (ROC) theory and then input the combined data into a threshold classification algorithm.

A fast-growing field that relies on cyber-physical data-fusion is autonomous vehicles. These systems require fast and accurate data-fusion to make life-and-death decisions in real-time. The unique challenges presented by autonomous vehicles may produce solutions and provide insight into problems faced by other control systems. [48] proposed a data-fusion method to increase performance from incomplete multi-sensor systems, specifically for auto traffic in urban areas. The authors used Multiple Linear Regression (MLR) models with historical taxi global positioning system (GPS) data to extract spatiotemporal traffic-state correlations. This information is used to fill in data gaps to increase the accuracy of other sensors. Historical data correlations could be implemented to make predictions in case of sensor failure, enabling other devices to make accurate decisions without ignoring the information of the failed device. Authors also noted the use of data-centric parallelization for handling large multisensory datasets, but no specifics were noted. [49] proposed a new model for describing moving objects using meta-information from multiple sources and global relationships to other objects to reduce measurement and sampling errors present in existing models. The authors used this model to develop a new map-matching algorithm, IF-Matching (Information Fusion Matching). This algorithm outperformed Spatio-Temporal Matching and performed as well as the ACM Geographic Information Systems Cup 2012 winner on city-wide trajectory data.

3.2 Data Alignment/Tailoring

Because of the potentially large scale of CPS data, displaying all of the information that is available can be overwhelming and unnecessary for the consumer. Finding and reporting only the information that is relevant to the consumer and the current/predicted system state may help improve decision-making response-time, accuracy, and reproducibility.

Since CPSs often contain large amounts of data from multiple sources, feature selection is a crucial component in anti-system architecture. Selecting the most relevant data and sources can improve both the accuracy and speed of decision-making tasks, as well as enhance understanding and system awareness. [50] showed a factor analysis method for feature selection using probabilistic kernels that outperformed common factor analysis methods for physical degradation monitoring. The selected feature sets were verified using support vector regression. A unique feature selection paradigm is model predictive control (MPC), which is a commonly used and effective technique for process control in industry. This technique models the dynamics of a plant to optimize input data based on predictions of future behavior. A

MPC algorithm for modeling non-linear systems using neural networks is proposed by [51]. The authors use feed-forward neural networks to create a parameter-varying MPC for use in tracking a system with partially unknown dynamics over a set of operating points. The algorithm was validated on simulated tank and tubular reactor systems.

In critical infrastructure systems, the final decision is left to a human operator. The operator must look at the data and possible countermeasures supplied by the system and make a choice on how best to deal with the situation. Often, all countermeasures are given equal weight regardless of the situation. [52] proposed a method using the analytic hierarchy process to suggest alternate recovery options to the operator based on specific criteria (e.g., economic, security, social, environmental). This method was then applied to an intrusion detection system that could suggest alternative actions based on the input criteria.

In large-scale CPSs, end-users require efficient access to the available data. A data management system for healthcare applications that focuses on data accessibility is presented in [53]. The proposed cyber-physical patient-centric healthcare system incorporates cloud and big-data analytics for data collection, management, and application service layers in the system. The data-collection layer combines heterogeneous data nodes with adapters to give nodes access to the system and vice-versa. The data-management layer incorporates a distributed file-storage system with a distributed parallel computing framework to ensure efficient data storage and retrieval, along with real-time and offline data analysis of the data. Finally, the application service layer supplies operational resources for developers and end-users, such as data access and visualizations, testbeds, security management, etc.

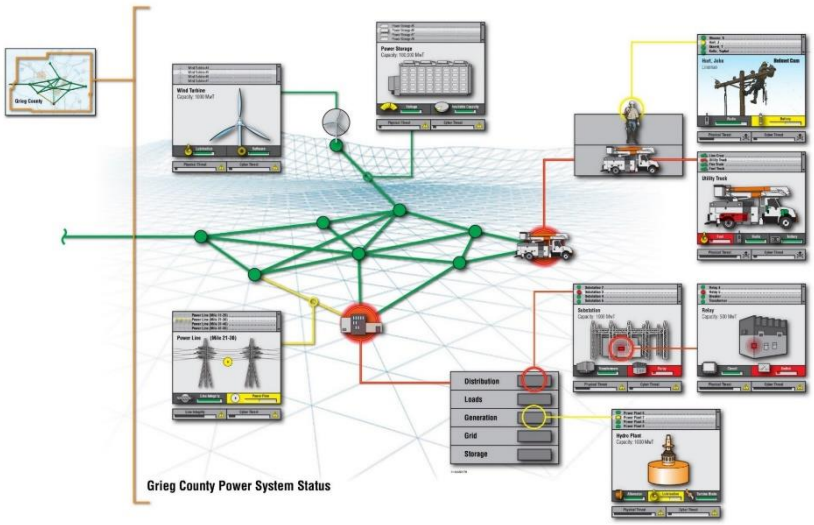
4 Data Visualization

This section provides a brief review of recent research conducted in visualization, with a focus on data-fusion for cyber-physical systems. Accurate visual representations of information is essential for any large scale system. Visualizations inform operators and consumers of how the system is running, health metrics, and can identify problem areas. Intuitive visualizations aid and simplify human-machine interaction by making relationships in the data more apparent and facilitating efficient decision making. The large size of the datasets available in a city-wide IoT application makes visualization a difficult task. It is not realistic to present all of the data in a single interface because the interface will be cluttered and unintuitive. While data-fusion reduces and exploits correlations among huge data streams, visualization plays a critical role in human understanding of this data. Visualization simplifies human-machine interaction. Accurate visualization of information can make previously unknown relationships apparent and facilitate faster, better decision-making.

4.1 Dynamic Visualization

Dynamic visualizations change how the data is represented in real time which allows users to quickly understand where changes in the system are happening and if they have cause cascading failures. Dynamic data visualization allows for visual representations of data that can be altered as the represented data changes. This can allow for quick and intuitive understanding of changes in the system as size, color, length, etc., is altered. in an IoT design, devices can be connected to and communicate with each other over a network. This can allow for an efficient peer-to-peer resource sharing system to be implemented across the system. Resource sharing adds an additional layer to visualization by allowing local visual implementations to change dynamically based on global data as well. It is also important that different visualization nodes are consistent in their presentation to users. This helps users learn how the display layout implemented by the system works, and ensures users won't have to relearn the basic navigation when introduced to a new display.

Of course, any visualization system that emphasizes some data over others is deciding on behalf of the user. Although it may do so according to user-stated preferences, this decision can also form a filter bubble [54], where important information may be suppressed because the user has not deemed it important. Filter bubbles become a self-perpetuating confirmation bias that may blind rather than reveal. Visualization developers implicitly trust their creations, but for critical tasks such as cybersecurity, operators tend to distrust decisions and simplifications made by visualization [55]. Thus, all visualization research should take user-trust into account and enable users to understand what is being hidden by the things that are being emphasized.



One method for dynamically optimizing the area of relevant images on a display is shown by [56]. The authors propose an optimization algorithm that will display a set of objects using the entire display area, but sizing images based on the relevance of information contained in each based on a user-defined context. The proposed Cyber-Physical Directory Framework was implemented and tested using mobile devices. Individual users could select their preferences (e.g., favorite foods/movie genres), and the display would resize information according to the user-defined data when the device was pointed at it (see Figure 1). A more robust version of the algorithm is shown by [57], where cloud data is included to incorporate more user-specific data than the previous work. This technique could employ different metrics to dynamically resize system information as certain data streams become more relevant to system stability.

4.2 Top-Down Visualization

In a smart urban environment application, the system infrastructure will be spread out widely with many small components. This is a difficult system to visualize as operators and consumers may need access to very low level system information, but not all of the data can be shown at one. A potential visualization scheme to alleviate this problem is a high level, top-down design with an information 'drill-down' to access lower level data representations. An initial visualization may only show a map of the city with the major areas or landmarks marked. Users could then select an area to open a new visualization with more detailed information about the selected domain. This tiered design can continue for as many layers as are needed, though too many layers can be counter-productive.

A visualization scheme that could incorporate the top-down design previously discussed as well as incorporate dynamic data representations is presented in [59]. The authors presented a study of several techniques that can be used to visualize entity interoperability in cyber-physical systems, specifically the Node-Link Diagram (NLD) and corresponding balloon layout. An NLD is a tree-like graph structure with nodes being entities in the tool chain and links being relationships between the tools. Each node and link can be resized and color coded to represent different qualitative and quantitative information. However, the authors note that an NLD could become unwieldy and ambiguous as the size of the represented system increases. To alleviate this problem, the balloon layout is suggested. This layout clusters tools into smaller NLDs contained in parent nodes (see Figure 2), and the parent nodes create a higher level NLD.

4.3 Visualization Techniques

A visualization design that is directly applicable to CPS is shown in [60]. The authors proposed a visual analytics concept to better handle the problems of critical infrastructure monitoring, cascading effects in infrastructure, and crisis response management. Their method proposes various visualization techniques to combine data from multiple infrastructures into a unified overview to assist operators in decision-making. Specifically, the authors' method aims to highlight important events, portray crisis events towards understanding in interdisciplinary teams, and present system details and controls when needed. The presented design was tested on a real power grid with an interconnected digital communication grid, and was shown to consistently highlight current and future events in the tested infrastructures (see Figure 3).

Certain applications may require end-users to visualize data directly rather than relying on a high-level system representation. A method for visualizing and exploring patterns in temporal multivariate data is presented by [61]. The authors create temporal multidimensional scaling (MDS) plots that consider temporal-event information from the multivariate data to create sequences of one-dimensional similarity mappings. In the MDS plots, the x-axis is time and the y-axis is a similarity metric which visually groups similar events together over time. Furthermore, the multivariate nature of the data is visualized through a sequenced diversity matrix shown underneath the temporal MDS plots as a heat map (see Figure 4). The colors of the matrix elements represent the diversity metrics, with black representing low diversity and white high diversity, to show the correlations between features. This visualization, coupled with a clustering algorithm to assist in event detection, allows users to find, analyze, and define reoccurring patterns in the data.

A newer area in visualization technology are 3D visualizations. Using 3D technology, more information can be kept within the reduced dataset while maintaining an accessible form for human visualization and intuition. 3D technology can also allow users to 'step into' and immerse themselves in the data. However, 3D visualizations also induce occlusion, hiding artifacts behind one another.

Visualizing self-organizing maps (SOMs) in a 3D environment was presented in [62] by using an immersive visualization technology called the Cave Automatic Virtual Environment (CAVE). SOMs are typically used for dimensionality reduction and feature selection to transform high-dimensional data into lower spaces that can be easier for humans to understand. The CAVE technology uses motion tracking to allow users to fully immerse themselves in the data (see Figure 5). The virtual environment is updated as users move around and interact with the data using a wand tool. CAVEs excel at collaborative visualization where multiple users simultaneously explore a dataset, but they have practical limitations. Often, direct manipulation of CAVE objects is difficult or impossible, and they are not yet considered practical for use in other than exploratory and academic environments where there is no time sensitivity. It remains to be seen whether the technology can make the

leap to operational usability. The authors tested the CAVE-SOM method on several benchmark datasets and a wind-power dataset.

[63] presented a project aiming to provide end-users with effective use of quantitative and qualitative 3D visualization and 2D analysis for big data applications. This work implements and improves upon a visualization method called Particle Base Volume Rendering (PBVR) for parallel volume rendering. PBVR and its improvements can run on a Graphics Processing Unit architecture, allowing for interactive use without having to pause to reload information. Other visualizations include contour maps and multidimensional transfer functions. A 4D cross-correlation, volume-data environment is in development.

5 Conclusions

This chapter outlined several challenges identified in cyber-physical system design, with potential solutions from recent publications. Discussions for establishing resilient CPS architectures that leverage IoT devices were outlined. Providing complete, reliable, and useful information is essential for the systems and operator's understanding and decision-making. Developing an accurate state awareness system, along with robust anomaly detection techniques, is crucial to providing users with the relevant information and models needed to recognize threats and coordinate effective responses. Data-driven CI algorithms have shown promising solutions for state awareness and prediction, attack detection, and decision-making with compromised data. Many of these algorithms are 'online,' meaning they can continue to learn after deployment to potentially adapt to new anomalies in the system, and provide information that is most relevant to the system and/or the decision-makers' needs. However, the pattern-matching nature of data-driven algorithms are subject to problems, such as spoofing, limited data-sets, and overfitting. Additionally, the black-box nature of CI designs do not allow for in-explanations or in-depth analysis of why the system behaves a certain way. Model-based and physics-based designs are other commonly used methodologies. These systems do not rely on data for generation and are white-box, which allows end-users and analysts to understand the inner workings of the system. However, creating these models require expert knowledge of how the system operates, and they won't be able to capture potential intricacies in the data that data-driven pattern matching methods can. These two approaches to modelling could be used together in a hybrid-modelling approach so that each methods strengths can cover the others weaknesses, though to the best of the authors' knowledge, no work has been presented on this topic.

Managing large-scale CPS provides its own challenges. Many architectures rely on a central data-fusion center that collects data from distant locations, makes decisions, and sends data back out. These data transfers take time and create single-

points-of-failure across the network. A common solution in many large-scale systems is decentralizing the system into multiple, localized subsystems that collect and analyze data independently. Allowing the subsystems to make calculations and decisions from local data can reduce the computational overhead inherent in high-dimensional heterogeneous datasets and would require only essential information be sent to a system controller/operator on an as-needed basis. It also allows for multiple, subsystem specific algorithms to be implemented, though steps should be taken to ensure important interdependencies between subsystems are not lost by implementing knowledge-fusion or other techniques.

CPS datasets are usually high-dimensional, heterogeneous datasets that may have low/multi-resolutions, temporally unsynchronized features, etc. Because of the large amounts of data needed for system-modeling and prediction, it is crucial that the information be consistent and synced temporally. Machine-learning approaches have promising applications for datasets containing low or varying sample rates. Artificial neural networks in particular were shown to be able to increase both temporal and spatial resolutions on building sensor data. Another statistical machine-learning method, Gaussian Process Modeling, was used to combine multiple features with different resolutions. Due to varying transmission times and device latencies, CPS devices may report measurements as being recorded simultaneously, though in reality are not matched temporally.

Though CPS can provide a lot of data, not all of it may be relevant to a consumer. Recognizing and reporting the most relevant system information can increase the speed and reproducibility of the decision-making and analysis process. An algorithm to improve prediction quality for human-in-the-loop control systems was shown for emergency response applications. Using the analytic hierarchy process, the algorithm can suggest a hierarchy of recovery options derived from user-defined metrics indicating how important different criteria are (e.g., economic, security, environmental) for that system. These metrics can be defined for the needs of an individual, plant, or company to help ensure design-specific requirements are met in critical decision-making. Displaying user-relevant information is also an important aspect in visualization. Too much data can clutter a screen and make it difficult to locate what the consumer needs, but too little information will not provide robust system representation. However, the information needs to be sourced from the system globally and not be too focused on local activity. Visualization designs throughout a system should be consistent in their presentation to help users navigate all displays without having to relearn basic navigation of a display.

References

[1] D. E. Denning, “An intrusion-detection model,” *IEEE Trans Softw Eng*, vol. 13, no. 2, pp. 222–232, Feb. 1987.

[2] R. Sommer and V. Paxson, “Outside the closed world: On using machine learning for network intrusion detection,” in *2010 IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.
[3] D. Wijayasekara, M. Manic, and C. Rieger, “Fuzzy linguistic knowledge-based behavior extraction for building energy management systems,” in *2013 6th International Symposium on Resilient Control Systems (ISRCS)*, 2013, pp. 80–85.
[4] T. Vollmer, M. Manic, and O. Linda, “Autonomic intelligent cyber-sensor to support industrial control network awareness,” *IEEE Trans. Ind. Inform.*, vol. 10, no. 2, pp. 1647–1658, May 2014.
[5] T. Vollmer and M. Manic, “Cyber-physical system security with deceptive virtual hosts for industrial control networks,” *IEEE Trans. Ind. Inform.*, vol. 10, no. 2, pp. 1337–1347, May 2014.
[6] G. Rueff, B. Wheeler, T. Vollmer, and T. McJunkin, “INL Control System Situational Awareness Technology Final Report,” INL, Idaho Falls, ID, EXT-11-23408, Jan. 2013.
[7] O. Linda, D. Wijayasekara, M. Manic, and C. Rieger, “Computational intelligence-based anomaly detection for building energy management systems,” in *2012 5th International Symposium on Resilient Control Systems*, 2012, pp. 77–82.
[8] N. Ádám, B. Madoš, A. Baláž, and T. Pavlik, “Artificial neural network-based IDS,” in *2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, 2017, pp. 000159–000164.
[9] N. Sen, R. Sen, and M. Chattopadhyay, “An effective back propagation neural network architecture for the development of an efficient anomaly-based intrusion detection system,” in *2014 International Conference on Computational Intelligence and Communication Networks*, 2014, pp. 1052–1056.
[10] J. Esmaily, R. Moradinezhad, and J. Ghasemi, “Intrusion detection system based on multi-layer perceptron neural networks and decision tree,” in *2015 7th Conference on Information and Knowledge Technology (IKT)*, 2015, pp. 1–5.
[11] Z. Jadidi, V. Muthukkumarasamy, E. Sithirasenan, and M. Sheikhan, “Flow-based anomaly detection using neural network optimized with GSA algorithm,” in *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops*, 2013, pp. 76–81.
[12] N. Mowla, I. Doh, and K. Chae, “Evolving neural network intrusion detection system for MCPS,” in *2017 19th International Conference on Advanced Communication Technology (ICACT)*, 2017, pp. 183–187.
[13] C. Callegari, S. Giordano, and M. Pagano, “Neural network-based anomaly detection,” in *2014 IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2014, pp. 310–314.
[14] A. M. Kosek, “Contextual anomaly detection for cyber-physical security in smart grids based on an artificial neural network model,” in *2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*, 2016, pp. 1–6.
[15] M. Ghanbari, W. Kinsner, and K. Ferens, “Anomaly detection in a smart grid using wavelet transform, variance fractal dimension and an artificial neural network,” in *2016 IEEE Electrical Power and Energy Conference (EPEC)*, 2016, pp. 1–6.
[16] V. Ford, A. Siraj, and W. Eberle, “Smart-grid energy fraud detection using artificial neural networks,” in *2014 IEEE Symposium on Computational Intelligence Applications in Smart Grid (CIASG)*, 2014, pp. 1–6.
[17] S. Ntalampiras, “Detection of integrity attacks in cyber-physical critical infrastructures using ensemble modeling,” *IEEE Trans. Ind. Inform.*, vol. 11, no. 1, pp. 104–111, Feb. 2015.
[18] D. Wijayasekara, O. Linda, M. Manic, and C. Rieger, “FN-DFE: Fuzzy-neural data-fusion engine for enhanced resilient state-awareness of hybrid energy systems,” *IEEE Trans. Cybern.*, vol. 44, no. 11, pp. 2065–2075, Nov. 2014.
[19] E. Hatami, N. Vosoughi, and H. Salarieh, “Design of a fault tolerated intelligent control system for load following operation in a nuclear power plant,” *Int. J. Electr. Power Energy Syst.*, vol. 78, pp. 864–872, Jun. 2016.

[20] J. Goh, S. Adepu, M. Tan, and Z. S. Lee, "Anomaly detection in cyber-physical systems using recurrent neural networks," in *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*, 2017, pp. 140–145.

[21] C. G. Cordero, S. Hauke, M. Mühlhäuser, and M. Fischer, "Analyzing flow-based anomaly intrusion detection using replicator neural networks," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, 2016, pp. 317–324.

[22] T. Ince, S. Kiranyaz, L. Eren, M. Askar, and M. Gabbouj, "Real-time motor fault detection by 1-D convolutional neural networks," *IEEE Trans. Ind. Electron.*, vol. 63, no. 11, pp. 7067–7075, Nov. 2016.

[23] Y. Zhou, R. Arghandeh, I. Konstantakopoulos, S. Abdullah, A. von Meier, and C. J. Spanos, "Abnormal event detection with high resolution micro-PMU data," in *2016 Power Systems Computation Conference (PSCC)*, 2016, pp. 1–7.

[24] S. Brahma, R. Kavasseri, H. Cao, N. R. Chaudhuri, T. Alexopoulos, and Y. Cui, "Real-time identification of dynamic events in power systems using PMU data, and potential applications #8212: Models, promises, and challenges," *IEEE Trans. Power Deliv.*, vol. 32, no. 1, pp. 294–301, Feb. 2017.

[25] S. Y. Huang and Y. N. Huang, "Network traffic anomaly detection based on growing hierarchical SOM," in *2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2013, pp. 1–2.

[26] M. Du, S. Ma, and Q. He, "A SCADA data-based anomaly detection method for wind turbines," in *2016 China International Conference on Electricity Distribution (CICED)*, 2016, pp. 1–6.

[27] M. Biswal, Y. Hao, P. Chen, S. Brahma, H. Cao, and P. D. Leon, "Signal features for classification of power system disturbances using PMU data," in *2016 Power Systems Computation Conference (PSCC)*, 2016, pp. 1–7.

[28] K. Wen, J. Yang, F. Cheng, C. Li, Z. Wang, and H. Yin, "Two-stage detection algorithm for RoQ attack based on localized periodicity analysis of traffic anomaly," in *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*, 2014, pp. 1–6.

[29] M. Gu, "The algorithm of information system anomaly detection," in *2013 3rd International Conference on Consumer Electronics, Communications and Networks*, 2013, pp. 653–657.

[30] R. G. Kavasseri, Y. Cui, and S. M. Brahma, "A new approach for event detection based on energy functions," in *2014 IEEE PES General Meeting | Conference Exposition*, 2014, pp. 1–5.

[31] M. Balchanos, D. Mavris, D. W. Brown, G. Georgoulas, and G. Vachtsevanos, "Incipient failure detection: A particle filtering approach with application to actuator systems," in *2017 13th IEEE International Conference on Control Automation (ICCA)*, 2017, pp. 64–69.

[32] P. Angelov, "Anomaly detection based on eccentricity analysis," in *2014 IEEE Symposium on Evolving and Autonomous Learning Systems (EALS)*, 2014, pp. 1–8.

[33] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, "Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach," *IEEE Trans. Autom. Control*, vol. PP, no. 99, pp. 1–1, 2017.

[34] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[35] S. Zhu, Y. C. Soh, and L. Xie, "Distributed inference for relay-assisted sensor networks with intermittent measurements over fading channels," *IEEE Trans. Signal Process.*, vol. 64, no. 3, pp. 742–756, Feb. 2016.

[36] H. E. Garcia, S. M. Meerkov, and M. T. Ravichandran, "Resilient plant monitoring systems: Techniques, analysis, design, and performance evaluation," *J. Process Control*, vol. 32, pp. 51–63, Aug. 2015.

[37] X. Cao, P. Cheng, J. Chen, and Y. Sun, "An online optimization approach for control and communication co-design in networked cyber-physical systems," *IEEE Trans. Ind. Inform.*, vol. 9, no. 1, pp. 439–450, Feb. 2013.
[38] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, "STPA-SafeSec: Safety and security analysis for cyber-physical systems," *J. Inf. Secur. Appl.*
[39] F. Alam, R. Mehmood, I. Katib, N. N. Albogami, and A. Albeshri, "Data-fusion and IoT for smart ubiquitous environments: A survey," *IEEE Access*, vol. 5, pp. 9533–9554, 2017.
[40] K. Amarasinghe, D. Wijayasekara, and M. Manic, "Neural network-based downscaling of building energy management system data," in *2014 IEEE 23rd International Symposium on Industrial Electronics (ISIE)*, 2014, pp. 2670–2675.
[41] D. Wijayasekara and M. Manic, "Data-fusion for increasing temporal resolution of building energy management system data," in *IECON 2015 - 41st Annual Conference of the IEEE Industrial Electronics Society*, 2015, pp. 004550–004555.
[42] M. J. Ren, L. J. Sun, M. Y. Liu, C. F. Cheung, and Y. H. Yin, "A reconstruction-registration integrated data-fusion method for measurement of multi-scaled complex surfaces," *IEEE Trans. Instrum. Meas.*, vol. 66, no. 3, pp. 414–423, Mar. 2017.
[43] T. R. Bennett, N. Gans, and R. Jafari, "A data-driven synchronization technique for cyber-physical systems," in *Proceedings of the Second International Workshop on the Swarm at the Edge of the Cloud*, New York, NY, USA, 2015, pp. 49–54.
[44] J. Rehder, R. Siegwart, and P. Furgale, "A general approach to spatiotemporal calibration in multi-sensor systems," *IEEE Trans. Robot.*, vol. 32, no. 2, pp. 383–398, Apr. 2016.
[45] L. Sorber, M. V. Barel, and L. D. Lathauwer, "Structured data-fusion," *IEEE J. Sel. Top. Signal Process.*, vol. 9, no. 4, pp. 586–600, Jun. 2015.
[46] Y. Li *et al.*, "Conflicts to Harmony: A framework for resolving conflicts in heterogeneous data by truth discovery," *IEEE Trans. Knowl. Data Eng.*, vol. 28, no. 8, pp. 1986–1999, Aug. 2016.
[47] B. Andò, S. Baglio, C. O. Lombardo, and V. Marletta, "A multi-sensor data-fusion approach for ADL and fall classification," *IEEE Trans. Instrum. Meas.*, vol. 65, no. 9, pp. 1960–1967, Sep. 2016.
[48] Z. Shan, Y. Xia, P. Hou, and J. He, "Fusing incomplete multi-sensor heterogeneous data to estimate urban traffic," *IEEE Multimed.*, vol. 23, no. 3, pp. 56–63, Jul. 2016.
[49] J. Hu and A. V. Vasilakos, "Energy big data analytics and security: Challenges and opportunities," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2423–2436, Sep. 2016.
[50] J. Wang, J. Xie, R. Zhao, K. Mao, and L. Zhang, "A new probabilistic kernel factor analysis for multisensory data-fusion: Application to tool condition monitoring," *IEEE Trans. Instrum. Meas.*, vol. 65, no. 11, pp. 2527–2537, Nov. 2016.
[51] A. Gautam and Y. C. Soh, "Stabilizing model predictive control using parameter-dependent dynamic policy for nonlinear systems modeled with neural networks," *J. Process Control*, vol. 36, pp. 11–21, Dec. 2015.
[52] G. Bernieri, S. Damiani, F. D. Moro, L. Faramondi, F. Pascucci, and F. Tambone, "A multiple-criteria decision-making method as support for critical infrastructure protection and intrusion detection system," in *IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society*, 2016, pp. 4871–4876.
[53] Y. Zhang, M. Qiu, C. W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: Healthcare cyber-physical system assisted by cloud and big data," *IEEE Syst. J.*, vol. 11, no. 1, pp. 88–95, Mar. 2017.
[54] E. Pariser, *The filter bubble: What the Internet is hiding from you*. Penguin UK, 2011.
[55] G. A. Fink, C. L. North, A. Endert, and S. Rose, "Visualizing cybersecurity: Usable workspaces," in *2009 6th International Workshop on Visualization for Cyber Security*, 2009, pp. 45–56.
[56] J. L. Lamothe, J. She, and M. Cheung, "Cyber-physical directory: A dynamic visualization of social media data," in *2013 IEEE International Conference on Green Computing and*

Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, 2013, pp. 2007–2012.

[57] M. Cheung, J. She, and S. Park, "Analytics-driven visualization on digital directory via screen-smart device interactions," *IEEE Trans. Multimed.*, vol. 18, no. 11, pp. 2303–2314, Nov. 2016.

[58] J. L. Lamothe, J. She, and X. Tan, "Cyber-physical directory with optimized visualization," in *2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing*, 2014, pp. 271–276.

[59] D. Gürdür, J. El-Khoury, T. Seceleanu, and L. Lednicki, "Making interoperability visible: Data visualization of cyber-physical systems development tool chains," *J. Ind. Inf. Integr.*, vol. 4, pp. 26–34, Dec. 2016.

[60] S. Mittelstaedt, D. Spretke, D. Sacha, D. A. Keim, B. Heyder, and J. Kopp, "Visual analytics for critical infrastructures," in *International ETG-Congress 2013; Symposium 1: Security in Critical Infrastructures Today*, 2013, pp. 1–8.

[61] D. Jäckle, F. Fischer, T. Schreck, and D. A. Keim, "Temporal MDS plots for analysis of multivariate data," *IEEE Trans. Vis. Comput. Graph.*, vol. 22, no. 1, pp. 141–150, Jan. 2016.

[62] D. Wijayasekara, O. Linda, and M. Manic, "CAVE-SOM: Immersive visual data mining using 3D self-organizing maps," in *The 2011 International Joint Conference on Neural Networks*, 2011, pp. 2471–2478.

[63] H. Miyachi, K. Koyamada, D. Matsuoka, and I. Kuroki, "Fusion visualization system as an open science foundation," in *2016 19th International Conference on Network-Based Information Systems (NBiS)*, 2016, pp. 401–404.