IEEE Open Journal of the
Industrial Electronics Society

Received 27 February 2022; revised 10 April 2022; accepted 19 May 2022. Date of publication 30 May 2022;
date of current version 9 June 2022. The review of this paper was arranged by Associate Editor Milos Manic.

Digital Object Identifier 10.1109/OJIES.2022.3178834

Unified IT&OT Modeling for Cybersecurity Analysis of Cyber-Physical Systems

AIDA AKBARZADEH AND SOKRATIS KATSIKAS

Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 2802 Gjovik, Norway

CORRESPONDING AUTHOR: AIDA AKBARZADEH (e-mail: aida.akbarzadeh@ntnu.no).

This work was supported in part by the Research Council of Norway under Project 280617 in the Cyber-Physical Security in Energy Infrastructure of Smart Cities and in part under Project 310105 in the Norwegian Centre for Cybersecurity in Critical Sectors.

ABSTRACT Cyber-Physical Systems (CPSs) engineering profoundly relies on modeling methods to represent the system and study the operation and cybersecurity of CPSs. The operation of a CPS is the result of the collaboration between Information Technology (IT) and Operational Technology (OT) components. While OT focuses on the system's process physics, the emphasis of IT is on information flow. Consequently, different system models are utilized to study various aspects of CPSs, which may infer different views of the same system. The increasing complexity of CPSs and the high number of cyberattacks against Industrial Control Systems (ICSs) and CPSs in recent years have highlighted the necessity of considering these interrelations based on a unified model to analyze cybersecurity of CPSs. However, the diversity of engineering fields and implicit relations and dependencies between them have made it difficult to integrate the modeling methods towards a unified IT&OT model of CPSs.In this paper, we propose a comprehensive method, based on bond graphs, to model CPS and analyze their cybersecurity. Unlike existing methods, modeling the cyber layer along with the physical layer based on the system flow provides a holistic graphical representation of a CPS, which facilitates collaboration between IT and OT experts.

INDEX TERMS Bond graph, cyber physical system, cybersecurity, industrial control system, safety.

I. INTRODUCTION

Cyber-Physical Systems (CPSs) are systems that integrate computation, communication, and controlling capabilities of Information and Communication Technology (ICT), with the traditional infrastructures. This integration facilitates the monitoring and controlling of objects in the physical world as one of the essential requirements of different Critical Infrastructures (CIs), such as manufacturing, healthcare, transportation and the energy sector, to name a few [1], [2]. However, this integration has significantly increased the number of connections among the system components, and this in turn has expanded the attack surface of CIs and has led to making possible complex cyber, and cyber-physical attacks such as Stuxnet and the attacks against the Ukraine's power grid [3]. Cyber-physical attacks have highly increased in recent years in numbers and intensity. For instance, compromising a water treatment facility to poison its community with a ransomware attack against a pipeline operator that disrupted gas supplies to the southeastern United States made the headlines in 2021 [4].

Interactions within a CPS can be classified to cyber–physical, physical–cyber, cyber–cyber, and physical–physical; this also implies that different types of dependency exist in CPSs [5].

As a result, one may attack a CPS in a variety of ways. Nevertheless, not all aspects of cybersecurity in CPSs have received equal attention; the focus has mainly been on information security, protecting access, and ensuring secure delivery of packets, rather than on securing process operations [6], [7].

Bolshev *et al.* argued that following typical security assessments for different CPSs without addressing the cyber–physical/physical–cyber interactions and recognizing the environment in which the system is used will lead to a false sense of security [7]. Recently Krotofil *et al.* showed that a physical process can be leveraged by attackers as a communication medium to deliver malicious payloads between devices that belong to one process in cyber-physical systems, even though these devices are segregated electronically [8].

Their work highlighted the significance of expanding the security scope to cover the physical process layer. Therefore, the analysis of the cybersecurity of a CPS requires an analysis of the cyber components, the physical components, and particularly the interactions between the system components [9]. The authors in [10] provided a list of current research challenges in CPSs and concluded that the essential idea to tackle those challenges is to develop a unified model to capture communication patterns in a high-level that collects the detailed behavior of individual nodes, with respect to different physics and their associate logic. Wang *et al.* also pointed out the importance of understanding the dynamics of various subsystems and their interactions for system designers to develop better CPSs [11].

On the other hand, the diversity of interactions within CPSs also reveals the necessity of collaboration between research communities from different backgrounds, including control theory, power systems, and cyber security, to study associated engineering principles related to the integration of cyber and physical elements of a CPS [12]. In this regard, the IEEE Systems Council established the IEEE Technical Committee on Cyber-Physical Systems in 2017 to promote interdisciplinary research in the design, implementation and operation of CPSs which require the consideration of multiple aspects such as security, reliability, fault tolerance, flexibility and extensibility [13].

Therefore, the security of a CPS highly depends on the collaboration within a cross-functional cybersecurity team that consists of members as suggested in the NIST framework [14]. However, the authors in [15] mentioned that the convergence between Information Technology (IT) and Operational Technology (OT) causes operators to lose a comprehensive understanding of functions and interdependencies within a CPS, and this may lead to incomplete risk assessment. Moreover, IT and OT experts normally utilize different system models, which may infer different views of the same system.

To tackle this challenge, it is required to develop a generic, yet easy to understand model to represent physical and logical facets as well as the interactions within the system components. This will enable both IT and OT experts, and in general members of a cybersecurity team with different backgrounds, to work on the same model and will allow them to identify and predict new complex cyber-physical attacks.

In order to fulfill the aforementioned requirements and to include infrastructures of diverse nature, in this paper we use bond graphs (BGs) to create unified IT&OT models of CPSs. Bond graph is a homogeneous and multi domain modeling approach which has found wide application in the modeling and simulation of physical dynamic systems, due to the physics-based equations derived from it. However, to model a CPS based on the BG approach, it is required to expand the approach to include cyber aspects of CPSs as well. This paper proposes a method that provides a holistic model to study the cybersecurity of CPSs, based on the BG approach. In summary, bond graphs help us to

- Develop a generic and easy to understand multi-domain model of CPSs that represents physical and logical facets as well as the interactions within the system components;
- Achieve a comprehensive understanding of functions and interdependencies within a CPS for both IT and OT experts;
- Facilitate the collaboration within a cross-functional cybersecurity team with people from different backgrounds to analyze the security of CPSs based on the proposed unified IT&OT model.

The rest of this paper is organized as follows: we review the related work on modeling CPSs in Section II. Section III provides the necessary knowledge background of BGs. In Section IV we describe the proposed approach and a case study is leveraged in Section V to demonstrate the application of the method. Finally, Section VI concludes the paper and indicates directions for future work.

II. RELATED WORK

Due to the inherent and ever-growing complexities of CPS, modeling methods are essential to facilitate the representation and analysis of such systems [16]. Indeed, modeling methods simplify the detection of design defects, capturing the evolution of a system, and extracting formal properties, such as determinism, that can be proved later [17].

A complete model of a CPS should indicate a coupling of physical processes, computations and the environment in which the system resides [18]. However, recent literature mainly concentrates on system entities either from the cyber or the physical facets, not of their integration. For instance, Modelica is a multi-domain language for component-oriented modeling of CPSs, which has mainly been developed to model physical systems. Accordingly, although this language has some advantages in modeling the behavior of systems, it cannot accurately cover the interactions between the physical and cyber components within a CPS. Besides, it is hard to understand by a non-expert [19]. The Architecture Analysis & Design Language (AADL) is another modeling language that has been proposed for embedded software systems, which unfortunately cannot support the dynamic physical behavior of the systems [20].

A large number of researchers apply formal methods such as pi-calculus, Petri-net, timed automata and hybrid automata to model CPSs. Formal methods describe the behavior of a system based on the usage of the mathematical specification language. Notwithstanding the capacity of the formal methods to model the physical behavior of complex systems, these methods suffer from high complexity in specifying non-functional properties and providing a visual representation of a system. The authors in [21] stated that formal modeling of CPSs is a complicated and not efficiently executable approach as it includes the double challenge of combined discrete-continuous dynamics and concurrent behavior.

Seiger *et al.* [22] proposed a process-based framework based on Business Process Model and Notation (BPMN). This work shed light on the urgent necessity of representing flows

of data within CPS processes from a high-level perspective to assist in understanding the complex behavior of a CPS.

A critical review of different modeling techniques to represent CPSs was conducted in [19]. The authors reviewed 62 papers and stated that, despite the efforts dedicated to modeling CPSs, there are still remarkable open challenges. They concluded that new CPS modeling methods should be developed to a) provide an intuitive and easy to understand multi-domain modeling approach that represents the system processes and targets technical and non-technical stakeholders; b) cover both physical and cyber parts, communication between cyber and physical parts and their corresponding functionalities to portray the behavior of a CPS as a collection of functionalities in the cyber, physical or control part of the system.

Another survey on methods and applications of design and modeling CPSs is provided in [23]. The authors argued that as the development of CPSs deals with challenges from different domains such as mechanics, electronics, engineering, control and computation, it is required to develop transdisciplinary models and conceptual frameworks to integrate them.

Villar *et al.* reviewed different methods and concluded that Model-Driven Engineering is a powerful means to address the increasing complexity of real-time and embedded systems [24]. The authors reached the conclusion that a practical modeling method should be easy to grasp and be applied to different domains and suggested that the number of fundamental modeling primitives should be limited.

Among different graphical modeling methods to represent the physical process of a system, a BG is a description formalism that can be applied in the multidisciplinary dynamic engineering systems from different energy domains such as the mechanical, the electrical, the thermal, and the hydraulic domain [25]. BGs were first used as a modeling tool, and have gradually been extended to solve various challenges, including fault detection and isolation, observability and controllability [26]. Kumar *et al.* [27] presented a method based on the BG modeling approach for modeling a system of systems (SoS). They argued that the causal and structural properties of the BG can be applied to model the control and supervision of a system. Reference [28] utilized the BG model to show the energy interactions throughout a microgrid as a cyber physical system. To verify the accuracy and correctness of the BG model, the author performed a simulation of the microgrid in PLECS and compared it with the BG model. According to this comparison, the author stated that the BG model is a viable approach to model CPSs and to represent their interdisciplinary nature; this approach can be applied in further studies to develop system protection software against cyber attacks. Acknowledging their effort, the main focus of this work is on the energy interactions throughout a microgrid without considering the cyber layer. Zerdazi *et al.* [29] described an approach to model deception attacks on supervisory control and data acquisition (SCADA) systems using BG modeling. The authors argued that an attack on the control signal or sensor measurements can be represented on the BG model by either an additional effort source or flow source.

Considering the previous works, BG is a promising approach to model CPSs, that should expand to cover the cyber layer and the interaction between the cyber and physical components within a CPSs. Expanding the BG model can also contribute to the analysis of different cyber and cyber-physical attacks on CPSs.

Therefore, in this paper, we attempt to a) present a unified IT&OT modeling approach based on the bond graph to capture both physical and cyber characteristics of CPSs to provide better insight; and b) investigate possible faults and cyberattacks by developing a six-step method to enhance the security of CPSs.

III. BACKGROUND

A BG is a graphical representation of a physical dynamic system in the form of a directed graph [30]. A BG is composed of *bonds (edges)* and *elements*. BG modeling is based on the power transfer principle between the different components of a system, since in each energy domain, the amount of power transferred is equal to the product of two physical quantities, i.e, Power = Effort × Flow [31]. Therefore, the physical interaction among components of a system is done by the allocation of Effort (e) and Flow (f) variables on them. Table 1 shows BG variables used in different domains [25].

In a BG, each bond represents the power exchange between the connected elements. In other words, bonds represent the bilateral signal flow of the power-conjugate variables *effort* and *flow*. The symbol of the effort is commonly written above or to the left of a bond and the symbol of the flow below or to the right of that. In BG representation any energetic process can be modeled using the following elements:

- Two *active* elements, sources of effort S_e and flow S_f, which provide input power to the system.
- Three generalized *passive* elements (I, C, and R) of which the R- element represents passive energy dissipation phenomena, while the I- and C- elements represent passive energy storage elements.
- Four *power conserving* elements, namely *transformer (TF)*, *gyrator (GY)*, *flow conservation junction '0'* (is used to regroup BG elements which share the same effort) and *effort conservation junction '1'* (is used to regroup BG elements which share the same flow).
- *Modulated* elements (actuators) whose values depend on some other variables, such as *modulated sources of effort (MSe)* and *modulated sources of flow (MSf)*.
- Two *detectors (sensors)*, namely *detector of effort (De)* and *detector of flow (Df)*, which can measure effort and flow in a system.

For instance, consider an ideal physical model of a simple circuit shown in Fig. 1(a). Here, the circuit is producing power at the voltage source (Ge) and consuming power at the load resistor (R). To model this simple circuit using the BG, we model the voltage source (G_e) and the load resistor (R) with the source of effort *Se* and the R- element, respectively. Since

TABLE 1. Bond Graph Variables in Different Domains [25]

Domain name	Energy	Electronic	Hydraulic	Thermodynamic	Mechanics
First variable	Effort (e)	Voltage (V)	Total pressure (P)	Temperature (T)	Force (F)
Second variable	Flow (f)	Current (I)	Volume flow (Q)	Entropy flow (S')	Velocity (V)

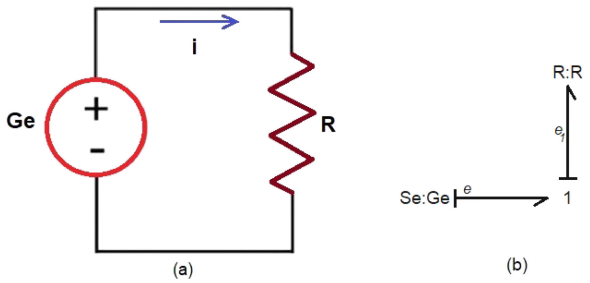

FIGURE 1. (a) A simple circuit with one source and one load. (b) The corresponding BG of the simple circuit.

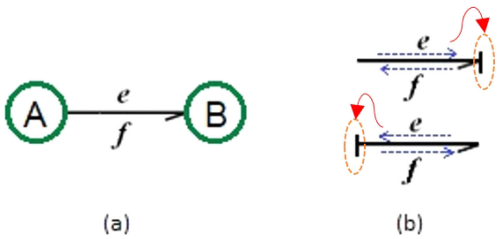

FIGURE 2. (a) The half arrow indicates the direction of the bond, and (b) the causal strokes represent the direction of the effort variable.

G_e is connected in series with R in the circuit, which implies that the same current i flows through both components, we utilize a 1-junction to regroup G_e and R in the BG model, as shown in Fig. 1(b).

A. CAUSAL STROKE

In a BG, a short line perpendicular to the bond at one of its ends is used to represent the (computational) direction of the effort variable *causal stroke*. The causal stroke can lie at either the tip or tail of the half arrow, depending on the causality. The position of the causal stroke is independent of the half arrow that indicates the direction of the bond.

Fig. 2 represents an example of BG modeling in which A and B are two physical elements, and the half-headed arrow is a power bond. The half-arrow, labeled by two unified power variables named effort (e) and flow (f), indicates the exchanged power between A and B. The direction of power flow in a bond is indicated by putting a stroke on the arrow as shown in Fig. 2(b).

Elements in a BG follow different types of causality. S_e and S_f have fixed causality, which means that under any circumstances, only one of the two element variables is allowed to be the outgoing variable. An effort source S_e always supplies effort into the system and has the causal stroke outwards, while a flow source S_f has the dual form of S_e and supplies flow as an input to the system. The C and I elements have a preferred causality, while the R element has an indifferent causality.

Port Element	Type of Causality	Causality
Effort Source (Se)	Fixed causality	Se ⊣
Flow Source (Sf)		S_f ⊢
C-element	preferred causality	C ⊣
I-element		I ⊢
R-element	Indifferent causality	R ⊣ or R ⊢
0-junctions	Constrained causality	⊢ 0 ⊣
1-junctions		⊣ 1 ⊣
Transformer		⊢ TF ⊢ or ⊣ TF ⊣
Gyrator		⊢ GY ⊣ or ⊣ GY ⊢

FIGURE 3. Bond graph port elements and their corresponding causality [28].

TF, GY, 0- and 1-junctions have causal constraints relations. Bonds connected to a 0-junction share common effort, and only one bond (i.e., the effort-deciding bond), must bring in the effort. This implies that 0-junctions always have exactly one causal stroke at the side of the junction belonging to the effort-deciding bond. The causal condition at a 1-junction is the dual form of the 0-junction. At a 1-junction, where all flows are the same, only one bond will bring in the flow and has the causal stroke away from the junction. Fig. 3 demonstrates elements and their corresponding causality in a BG.

B. CAUSALITY ASSIGNMENT AND STATE EQUATIONS

Causality assignment or *causal augmentation* is an algorithmic procedure of assigning causality on a BG based on the properties of elements. This process begins with the elements that pose the strongest causality constraints and continues until all elements get their causality assigned. The steps of the process are as follows:

1) Choose an unassigned port with a *fixed causality*, assign its causality, and propagate this assignment through the graph using the causal constraints. Continue this step until all ports with fixed causality are assigned.
2) Choose a not yet causal port with a *preferred causality* (i.e, C- and I-elements), assign the causality, and propagate this assignment through the graph using the causal constraints. Repeat this step until all ports with preferred causality obtain their causalities.
3) Choose a not yet causal port with a *constrained causality*, assign its causality, and propagate this assignment through the graph. Continue this step for all ports with constrained causality.
4) Choose a not yet causal port with an *indifferent causality*, assign its causality, and propagate this assignment

through the graph using the causal constraints. Ensure all ports with indifferent causality received their causality strokes by the end of this step.

A BG model with a correct causality implies that one can extract the set of state equations of the system and compute the unknown variables.

Once the causal strokes are assigned, a BG contains all information necessary to derive the set of state equations describing the system. Depending on the system, the equations are either a set of first-order differential equations (ODEs) or differential-algebraic equations (DAEs). To write the equations, first, each bond on the BG should be labelled to create unique variables. Then, the set of equations will be extracted considering the variable determining the junctions, and unknown variables replaced with the system variables. Notice that BG software like 20-sim [1] automates this process, and there is no need to generate the equations by hand. Nevertheless, we explain how to write equations with an example in Section V. We refer readers to [25], [32] for a detailed description of BG theory and related elements.

IV. THE PROPOSED METHOD

CPSs are governed by various effects of different engineering disciplines and technological components, such as sensors and actuators. Besides, different interactions exist among components within a CPS. For example, the interactions between the cyber part and the physical part in a typical power system [33] are as follows. First, local measurements on a power system sample the voltage magnitudes (or the reactive power outputs of the generators) and convert them into analog or digital signals (physical–cyber interaction). Next, by means of communication networks, this data will be transferred to the control center (cyber–cyber interaction). In the control system, to keep the system in the desired state, pertinent computation will be conducted based on the received data, and appropriate control commands will be sent to the related actuators. Then, these actuators will take proper action based on the received control commands (cyber–physical interaction). Finally, the physical states of the power system will gradually reach the desired point as a consequence of the changes that have been made by actuators (physical–physical interaction). Accordingly, one can understand that the purpose of adding the cyber layer (ICT) to traditional systems is to improve system control and monitoring to ensure that the primary objective of the system, which is delivering a service or commodity to the consumers (end-users), is properly met.

Therefore, we need two types of flow to model CPSs, namely *commodity flow* and *information flow*. Fig. 4 demonstrates the flows and interactions within a CPS.

In the sequel we utilize the flows to describe the physical layer and the cyber layer in CPSs.

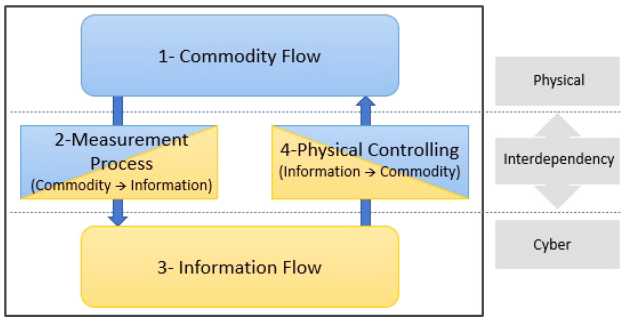

FIGURE 4. Concept model of interactions within a CPS.

A. PHYSICAL LAYER

The commodity flow in a CPS refers to the main objective of the system, i.e. delivering a commodity or service such as electricity, gas, water and oil to the end users. A commodity flow moves from the generator (the initial point) towards the end users of the system and the process physics and the causality of the system could be studied based on that.

As explained in Section I, it was recently shown that attackers might be able to utilize the commodity flow in a CPS as a communication medium to transfer malicious payloads to their target component to affect a system component or disrupt the functionality of the entire system. To this end, the physical layer of CPSs also should be taken into consideration for security analysis. Therefore, we model the physical layer of a CPS based on its objective, main stream of the system, by leveraging the elements of the BG discussed in Section III. This will be further explained with a case study in Section V.

B. CYBER LAYER

In our model, an information flow passes through the cyber components and indicates the interaction among the communication and control parts of the CPSs, i.e. the cyber layer. To address software components as well as other types of low-power devices such as sensors and actuators in the modeling approach, it is necessary to extend our view of the modeling elements presented in the physical layer to include *signals*. In the cyber layer, sensors and actuators are necessary to measure and control the system response and states. Sensors convert a non-electrical signal into an electrical one while actuators perform the opposite. The amount of power that sensors and actuators take out of the system is very small and can be neglected. Therefore, based on the description of energy and effort in the BG approach, the energy transferred by the information flow (electrical signal) is negligible compared to the energy exchanged between the physical components. In the BG approach, information flow is shown as a full arrow on the bond and mainly used to represent the signal transmitted by components such as sensors, actuators and controllers. These system components are said to be *active components* and are represented by a block diagram.

To the best of our knowledge, the information exchange between the active components has been only used to show

[1] https://www.20sim.com/

FIGURE 5. Bond graph modeling of: (a) data flow, (b) command signal,(c) data flow with protected channel and (d) command signal with protected channel.

how system components are connected in a BG, and the mathematical aspect of information flow is neglected insofar it is not related to the physics of the problem. However, information flow in a BG model can be used to study the security of CPSs and turn the BG to a proper approach to conduct a holistic cyber-physical analysis. To this end, we classify the information flow to 1) *data flow*, represented by a full arrow and 2) the *command signal*, represented with a hollow arrow on the bond (see Fig. 5). This will further facilitate the detection of different types of attacks and the investigation of security properties such as the CIA triad, (i.e., Confidentiality, Integrity and Availability) in a CPS. Moreover, channels connecting components in the cyber layer also play a significant role in providing or defeating security. As a result, we expand the BG model to demonstrate the properties of a channel. If a communication channel between two components is protected, this will be indicated with a dashed line, otherwise, it will be represented by a solid line (see Fig. 5). In Fig. 5, *A* and *B* are any systems or elements which exchange only information (data or command), and there is no exchange of energy between them. This information bond carries either effort information (effort activated bond with zero flow) or flow information (flow activated bond with zero effort).

C. FAULT AND CYBER ATTACK MODELING

The main focus of OT is on providing the operational safety of the process engineering systems; this is essentially based on fault detection and isolation procedures. These procedures mainly begin with fault modeling, as the most important step, and continue with comparing the actual behavior of the system with the reference behavior. Bond graph is a well known approach to detect faults mainly in the physical layer and has been applied in different domains [26], [34]. In this approach, a fault is modeled as an additional effort source (MSe for 1-junctions) or flow source (MSf for 0-junctions) and added to the same junction where the target element is placed. However, from the cybersecurity perspective, IT is more concerned about the root causes of a fault that occurs in a system, as it might be the consequence of a cyber-attack. Recently, Zerdazi *et al.* [35] used a BG approach to detect deception attacks. Besides, the *Anomaly Detection* methods developed in the cyber domain follow the same approach as for the fault detection in the physical layer. These methods are designed to detect anomalous behavior in a system, based on

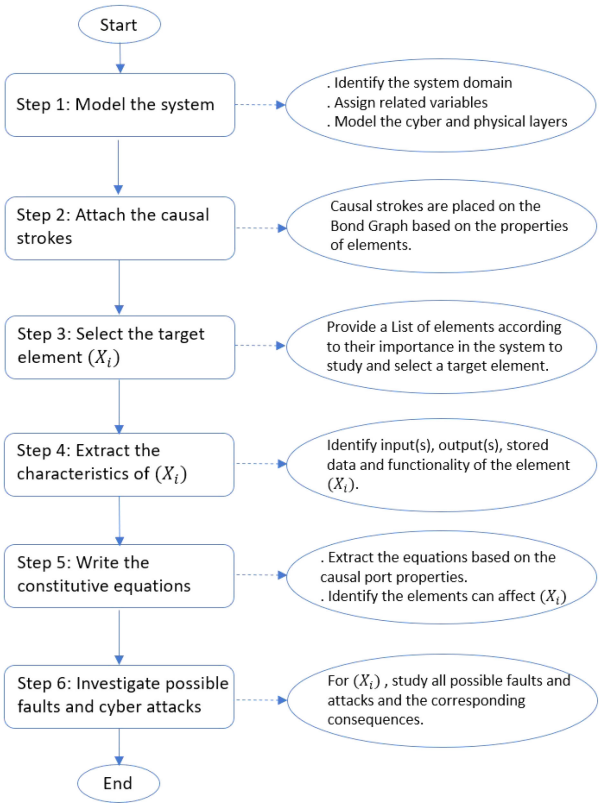

FIGURE 6. The flow chart of the proposed method.

the premise that unexpected behavior could be the result of an attack [36]. Considering these two aspects, one can argue that any deviation from the normal values in a CPS is considered a fault; this fault either appears due to influencing the cybersecurity properties (at the cyber layer) or the physical processes (at the physical layer). As a result, utilizing a common model can assist in modeling faults and detecting pertinent causes in CPSs. This can provide better insight and reduce possible conflicts. Therefore, we propose a six-step method based on the BG approach to model a CPS and study possible faults and cyber-attacks. The method is described in the next subsection.

D. METHOD

As shown in Fig. 6, the proposed method consists of the following steps:

Step 1: *Model the system.*

The first step is to identify the domain of the system and the related variables. For example, Fig. 1 shows an electronic circuit, for which we should utilize the pertinent variables *voltage* and *current* (see Table 1). Then, the physical layer of the system and the commodity flow path can be modeled based on the elements presented in Section III. To show the cyber layer, we consider the information flow and model cyber elements and corresponding command and data flows that pass through the system. Notice that properties of the connecting link should also be represented based on the symbols proposed in Fig. 5.

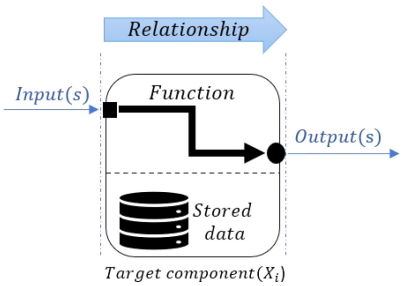

FIGURE 7. Graphical representation of the characteristics of a target element.

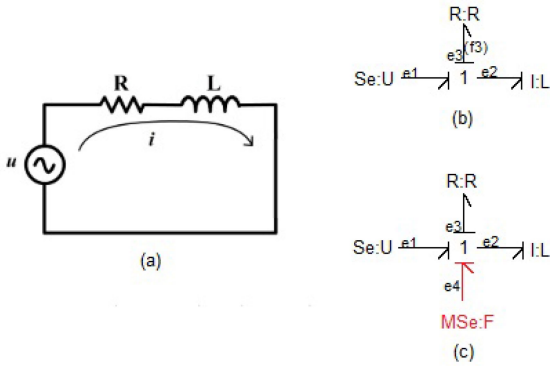

FIGURE 8. (a) A simple RL circuit; (b) the BG model of the RL circuit with the healthy resistance R; and (c) the BG model with faulty resistance, represented by a modulated energy source.

Step 2: *Attach the causal strokes.*

As explained earlier, causal strokes represent the direction of the effort variable, and are required to extract the system equations. Considering the causality assignment procedure described in Section III, the causal strokes should be placed on bonds connected to port elements following this order: first effort and flow sources, then I- and C-elements, followed by transformers and gyrators, and lastly junctions and R-elements. The causality of the rest of the port elements is determined afterwards as they have flexibility in the placement.

Step 3: *Select the target element* (X_i).

Select the system component the analyst is interested in, to investigate possible faults and cyber-attacks. One can provide a list of target elements to check, preferably based on the importance of components in a system. Recently, the authors in [37] proposed a method to rank the criticality of components in CPSs by leveraging the characteristics of system components and their connected links based on the graph metrics, which can be applied here to extract the list of target elements.

Step 4: *Extract the characteristics of the target element.*

This step facilitates the identification of the attack surface for each target element. We enumerate the input(s) and output(s) of the element with respect to their connection properties and extract the functionality of the element. Some elements have stored data like a set point or threshold values to compare with the input; in this case, the stored data also should be considered. Fig. 7 shows the relationship between the input(s) and output(s) of a target element.

Step 5: *Write the constitutive equations.*

For each target element, we write the related constitutive equations based on the causal port properties and substitute the unknown variables as functions of the known variables [38]. Once the equation is derived, we investigate whether variables that appear in the equation can affect the target element in case of the fault occurring, or not. This fault can for example occur due to (accidental) additive noise. For instance, consider the RL circuit shown in Fig. 8. Here, we know that the I-element stores energy and its voltage (e_2) is described by the following equation:

$$e_2 = e_1 - e_3 = U - Rf_3; \quad (e_2 \propto R) \tag{1}$$

As e_2 is proportional to R, a fault on R affects the voltage of the I-element as well. As explained earlier, a fault on R-element can be modeled by a modulated effort source on the 1-junction as depicted in Fig. 8(c) and it changes the value of e_2 by F as (2) shows:

$$e_2 = e_1 + (MSe - e_3) = U + (F - Rf_3); \tag{2}$$

Following the same approach will assist in the identification of values and parameters that can influence the target element, even those elements that are not directly connected to the target element. In the following section, we will discuss this in more detail.

Step 6: *Investigate possible combinations of faults and cyber-attacks.*

Finally, considering the characteristics of the target element explained in step 4 and the identified faults in step 5, we study all possible combinations of faults and attacks for each target element and investigate the corresponding consequences.

V. CASE STUDY: APPLICATION OF PROPOSED METHOD

In this section, we will apply the proposed methodology to detect cyber physical attacks in a typical power system.

Our case study is developed based on the realistic network infrastructures proposed by Pan *et al.* [39]. This system consists of two network zones: a field network, and a control network to control the system. The field network illustrated in Fig. 9 is a three-bus two-line transmission system that is a modified version of the IEEE nine-bus three-generator system [39] and includes several components. G1 and G2 are power generators, L1 and L2 are transmission lines, BR1 through BR4 are circuit breakers and R1 through R4 are relays. Each relay includes integrated phasor measurement unit (PMU) functionality and is able to trip and open the related breaker when a fault occurs on a transmission line. Operators are also able to manually issue commands to each relay to trip and close the corresponding breaker. Fig. 9 also depicts potential locations for the presence of an insider attacker in the system.

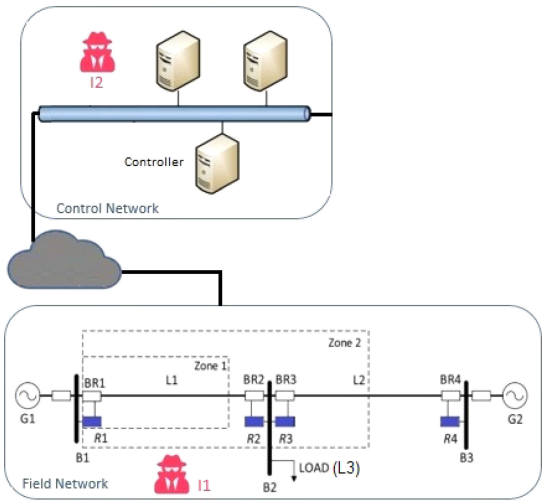

FIGURE 9. Graphical representation of the case study.

To investigate possible cyber physical attacks on the power system, we follow the steps proposed in Section IV.

Step 1: To construct the BG model of the case study shown in Fig. 10, we need to determine the appropriate port element of each component in Fig. 9, as explained in Section III. After that, the identified port elements need to be connected using proper port junctions considering the circuit configuration; 1-junction for elements in series and 0-junction for elements in parallel.

Notice that in Fig. 10 the field network is represented in detail to understand the system process; however, for simplicity the controlling part is portrayed in an element called *controller*.

A circuit breaker, which is an electrical switch designed to protect an electrical circuit from damage caused by overcurrent or short circuit, is shown by 1s-junction in the BG model. The 1s-junction represents flow switching and flow will be active at mutually exclusive instants of time. Boolean variables U and $\overline{U}$, are associated with the related bond to model the switching act. For theoretical details, the interested reader may refer to [40]. Fig. 10 shows four 1s-junction with two flow-deciding bonds. As an example, for $1S_1$, when U_1 is 1, flow ($f4$) passes through bond 4 and when $\overline{U_1}$ is 1, $f4$ is 0.

Relays in electrical circuits sense electrical flow and trigger circuit breakers. Accordingly, R1, R2, R3 and R4 in the system are modeled as flow detectors Df (which sense the flow) and modulated source flow MSf (to trigger related circuit breakers). Power generators G1 and G2 are modeled as effort source Se, while load L3 is shown as an R-element. Moreover, the dissipation phenomena on the transmission lines L1 and L2 are modeled by impedance R:L1 and R:L2 in Fig. 10, respectively.

Note that in Fig. 9, elements {G1, BR1, L1, BR2} from the left side and elements {G2, BR4, L2, BR3} from the right side are connected to B2 (Bus2) and are parallel with Load (L3). Therefore, to clearly show these connected components to B2 (Bus2) from both sides and facilitate writing the equations in Step 5, two 1-junctions labelled as $B2$ and $B2'$ are used in the BG model.

Step 2: According to the order of adding causal strokes discussed in Section III-B, we first assign causality to the source elements G1 and G2. Then, we assign the indifferent causality of R-elements {L1, L2, L3}, followed by the constrained causality of the 1-junctions and 1S-junctions. Fig. 10 shows the causal BG of the case study.

Step 3: Here we select R1 as the target element to study its corresponding properties.

Step 4: We extract the characteristics of relay R1 as the target element. A relay (such as R1 in our example) can measure the current that passes through line (L1), and based on the predefined threshold (set-point) or received commands from a controller, controls the associated circuit breaker. Therefore, without loss of generality we can assume that relay R1 is composed of two elements of the BG, one sensor to measure the current and one actuator to trigger the corresponding circuit breakers. It is also possible to model a relay as one mechanical or electrical element based on the BG. However, that would not help us to study the security-related issues in a CPS. It should be noted that the main focus here is to model each element of a CPS in a way that facilitates the analysis of characteristics of the system components and their interactions with other system components, from the cybersecurity perspective. In Fig. 10, Df:R1 denotes the flow detector (sensor), and MSf:T1 refers to the modulated source of flow (actuator).

As shown in Fig. 10, the communication between R1 and its connected elements (circuit breaker and controller) is not protected as there is no protected channel. This is not surprising for communication among elements placed in the field network and the control network in industrial systems.

Therefore, by considering inputs and output of the relay R1, adversaries may inject or replay commands into the relay to change the threshold T1 (i.e., stored data), they may alter or replay sensor measurements (Df) to cause upstream algorithms to take incorrect control actions (controller MQ or R1), or they may alter or replay control commands (from MSf to the breaker) to directly cause incorrect system actions. This can be summarized as follows:

For MSf:T1

Changing the value of T1 via Q12 or manually;
Altering Q12, which consequently will affect the breaker;
Q12:1 Open the breaker (BR1);
Q12:0 Close the breaker (BR1)
Altering Q11 directly;
If $Q11 = 0 \Rightarrow U_1 = 1, \overline{U_1} = 0$ (BR1:Off)
If $Q11 = 1 \Rightarrow U_1 = 0, \overline{U_1} = 1$ (BR1:On)

For Df:R1

Physical attack (fault);
Changing the measured flow value (I_{19});
If $I_{19} < T1 \quad [T1 = Threshold(R1)] \Rightarrow U_1 = 1, \quad \overline{U_1} = 0$ (BR1:Off)
If $I_{19} > T1 \quad [T1 = Threshold(R1)] \Rightarrow U_1 = 0, \quad \overline{U_1} = 1$ (BR1:On)

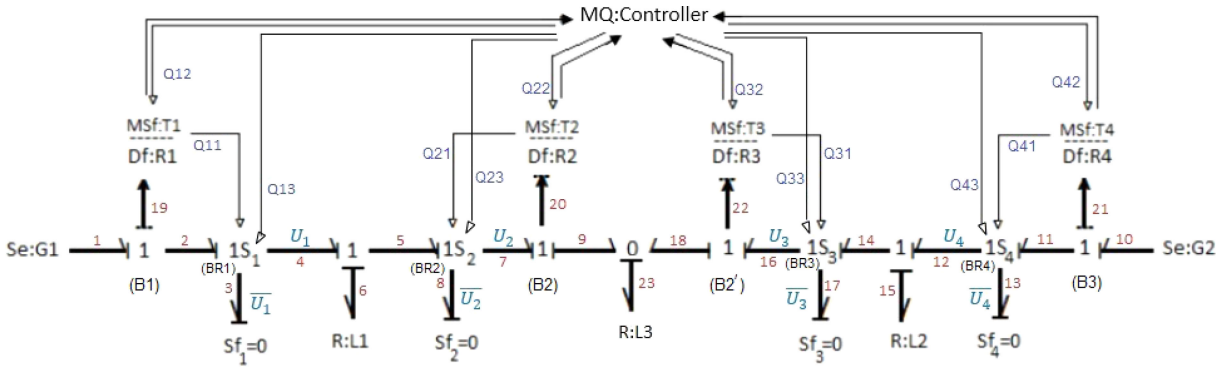

FIGURE 10. **BG model of the case study.**

Step 5: According to the causality shown in Fig. 10 we can write the constitutive equation corresponding to the target element R1. Here, we first extract the equations of all junctions to better understand the system. Considering the rules of the 1-junction in which bonds connected to 1-junction share common flow and the summation of efforts of all bond is zero, we have:

$$f_1 = f_2 = f_{19}, \quad e_1 + e_2 + e_{19} = 0 \tag{3}$$

$$f_4 = f_5 = f_6, \quad e_4 + e_5 + e_6 = 0 \tag{4}$$

$$f_7 = f_9 = f_{20}, \quad e_7 + e_9 + e_{20} = 0 \tag{5}$$

$$f_{16} = f_{22} = f_{18}, \quad e_{16} + e_{22} + e_{18} = 0 \tag{6}$$

$$f_{12} = f_{14} = f_{15}, \quad e_{12} + e_{15} + e_{14} = 0 \tag{7}$$

$$f_{10} = f_{11} = f_{21}, \quad e_{10} + e_{11} + e_{21} = 0 \tag{8}$$

For 1s-junctions we have:

$$f_2 = U_1 f_4 + \overline{U_1} f_3, \quad e_4 = U_1(e_2), \quad e_3 = \overline{U_1}(e_2) \tag{9}$$

$$f_5 = U_2 f_7 + \overline{U_2} f_8, \quad e_7 = U_2(e_5), \quad e_8 = \overline{U_2}(e_5) \tag{10}$$

$$f_{14} = U_3 f_{16} + \overline{U_3} f_{17}, \quad e_{16} = U_3(e_{14}), \quad e_{17} = \overline{U_3}(e_{14}) \tag{11}$$

$$f_{11} = U_4 f_{12} + \overline{U_4} f_{13}, \quad e_{12} = U_4(e_{11}), \quad e_{13} = \overline{U_4}(e_{11}) \tag{12}$$

0-junction is dual of 1-junction. Therefore, we have:

$$e_{18} = e_9 = e_{23}, \quad f_{18} + f_9 + f_{23} = 0 \tag{13}$$

Considering the characteristics of a flow sensor, here e_{19}, e_{20}, e_{22} and e_{21} are equal to zero. Besides, there are two power generators $e1 = G1$ and $e2 = G2$ in the system. For the three resistors {L1, L2, L3} in the system, we have:

$$e_6 = f_6.L1, \quad e_{15} = f_{15}.L2, \quad e_{23} = f_{23}.L3 \tag{14}$$

because, due to Ohm's Law, the current through a resistor (R) is directly proportional to the voltage across the resistor which is represented as $e = f.R$ in the BG.

Now, for the target element R1, we extract the related equation based on (1) to (12) and the causality shown in Fig. 10. Note that the flow measured by the Df:R1 element is I_{19} and $e_{19} = 0$. Therefore, based on the (3) we have:

$$I_{19} = f_2 = f_1; \quad e_2 = -G1 \tag{15}$$

Since f_1 and f_2 are unknown flow variables we should substitute them.

Based on the (9) we have:

$$I_{19} = f_1 = f_2 = f_4 \quad \text{and,} \quad e_4 = e_2 = -G1 \quad (\text{If} \quad U_1 = 1) \tag{16}$$

$$I_{19} = f_1 = f_2 = f_3 \quad \text{and,} \quad e_3 = e_2 = -G1 \quad (\text{If} \quad \overline{U_1} = 1) \tag{17}$$

This approach will be continued until I_{19} can be represented based on known parameters of the system as follows:

$$I_{19} = \frac{G1}{L1 + L3} \quad \text{if} \quad (U_1 = 1 \& U_2 = 1 \& U_3 = 0 \& U_4 = 0) \tag{18}$$

$$I_{19} = \frac{G1}{L1 + L3} \quad \text{if} \quad (U_1 = 1 \& U_2 = 1 \& U_3 = 0 \& U_4 = 1) \tag{19}$$

$$I_{19} = \frac{G1}{L1 + L3} \quad \text{if} \quad (U_1 = 1 \& U_2 = 1 \& U_3 = 1 \& U_4 = 0) \tag{20}$$

$$I_{19} = \frac{G1 - I_{21}.L3}{L1 + L3} = \frac{G1}{L1 + L3} + \frac{I_{21}.L3}{L1 + L3} \tag{21}$$

if $(U_1 = 1 \& U_2 = 1 \& U_3 = 1 \& U_4 = 1)$.

For I_{21} we have:

$$I_{21} = \frac{G - I_{19}.L3}{L2 + L3} \tag{22}$$

Therefore, substituting (22) into (21) results in:

$$\begin{aligned} I_{19} &= \frac{G1}{L1 + L3} - \frac{L3}{L1 + L3}\left(\frac{G2 - I_{19}.L3}{L2 + L3}\right) \\ &= \frac{G1(L2 + L3) - L3G2}{(L1 + L3)(L2 + L3) - L3^2} \end{aligned} \tag{23}$$

if $(U_1 = 1 \& U_2 = 1 \& U_3 = 1 \& U_4 = 1)$.

TABLE 2. Relation Between I_{19} and Boolean Variables U

I_{19}	U_1	U_2	U_3	U_4
$I_{19} = \frac{G1}{L1+L3}$	1	1	0	0
$I_{19} = \frac{G1}{L1+L3}$	1	1	0	1
$I_{19} = \frac{G1}{L1+L3}$	1	1	1	0
$I_{19} = \frac{G1(L2+L3)-L3G2}{(L1+L3)(L2+L3)-L3^2}$	1	1	1	1

Equation (23) reveals that the value of I_{19} is dependent on components {L1, L2, L3, G1 and G2} and any change (or fault) of these components directly affects the value of I_{19}. Note that some of these components have a remarkable topological distance from the target element R1.

Step 6: By taking into account the results of step 4 and step 5, here we can investigate different attack scenarios on the target element R1.

In general, relays are placed in the power system to trip the circuit breakers in the case of a fault and overcurrent, to protect transmission lines. Overcurrent protection is critical for personal and system safety from different hazardous conditions that can result from materials igniting. Therefore, it is important to ensure that I_{19} is measured and reported accurately by R1. From step 5, (16), (17), (18) and (21) reveal that the value of I_{19} depends on the Boolean variables U. As a result, an attacker may take advantage of this dependency to attack relay R1 and the system. Table 2 summarizes the relation between I_{19} and the corresponding Boolean variables.

Moreover, the result of step 4 contributes to discovering the following attack scenarios:

- **Trip command injection attacks:** An attacker sends an unexpected relay trip command to relay R1 to open associated breakers. Here, we assume that the attacker aims to trip the breaker BR1 at the ends of transmission line L1 to force L2 to carry more power flow and put the system under stress.
- **Data Injection Attack (or 1LG fault):** In this case, an attacker imitates a valid fault, such as a single line to ground (1LG) fault, by altering the value of (I_{19}). This attack leads to loss of view and may cause an operator to take invalid actions.
- **Relay Disabled Attack**: An attacker changes the settings of relay R1 to disable its operation. As a result, R1 will not trip breakers even in the presence of the pertaining stimulus.
- **Relay setting change Attack**: To disturb the functionality of R1, an attacker changes the stored value of T1 in relay R1 to $T1 + \Delta f$. If $T1 + \Delta f$ is greater than $T1$, then the transmission line L1 experiences over current, which can damage the system and cause safety issues. Likewise, decreasing the threshold (i.e., $T1 + \Delta f < T1$) can cause degradation of service and affect the system performance. However, discovering the latter one is more challenging, and this attack may remain unknown for a while.

To identify more complex attacks, it is required to study both the security properties and the operation of the system in more detail. As an example, consider the Aurora attack in which adversaries send opening and closing commands at a very fast pace to relay R1, to cause the breaker R1 to open and close periodically. This will force the generator G1 to lose synchronization with the transmission line L1 and damage G1 due to stress generated by torque variation.

When an attacker sends the opening command to R1, R1 will trigger BR1, and G1 will be isolated from the grid. The attacker knows that because of the slow governor action, the generator can not stop immediately and its frequency will keep increasing. This leads to a frequency difference between the grid and the generator G1. Therefore, the attacker leverages this vulnerability and sends a closing command to R1 at a very fast pace (before 15 cycles) to connect G1 to the grid with "out-of-sync" conditions. This causes large electrical and mechanical transients, damage to G1, and even blackout. It is clear that discovering and conducting the Aurora attack, as an example of a complex attack in CPSs, mainly depends on proper knowledge of the process physics of the system.

Notice that, due to the nature of a power conserving description of a system in the BG, one can model the generator G1 based on its electromechanical properties to investigate the effect of improper synchronization in this example. Indeed, this implies the *reusability* of modeling CPSs based on the BG, which is a valuable advantage in modeling the systems that cover several physical domains, and those systems might need to be expanded/modified later [24].

As the last point, this approach can also contribute to sensitivity analysis of the interactions and system components in case of faults and attacks. For instance, a closer look at (16), (17) and (18) shows that I_{19} is equal to $\frac{G1}{L1+L3}$ if at least one of the $U3$ and $U4$ is zero. This implies that not all deviations and parameter changes have an equal impact on the system.

VI. CONCLUSION

In this paper, we showed that modeling the cyber layer along with the physical layer based on the system flow, as the initial target of a CPS, can provide a holistic view of a CPS and allow to evaluate how adversaries might perturb the cyber part and ultimately the physical part of the system. To the best of our knowledge, none of the available methods reviewed in section II provides this. Accordingly, we proposed a comprehensive and domain-agnostic method, based on the BG approach. According to the proposed six-step method, one can follow the sequence of interactions based on the topological parts of the model and utilize corresponding equations to investigate dependencies and relations between the components of a CPS to extract potential fault points, attack surfaces, and the consequences of attacks. Considering the numerous components of large-scale CPSs, this investigation begins with the most critical components ranked in the list of target components that contribute to the optimization of the analysis. Modeling a CPS based on its fundamental object that represents the process physics of the system along with the cyber layer will help operators and the security team to discover potential complex attacks. As stated in [17], modeling methods simplify the detection of design defects; this can also assist system designers and operators to examine what-if design scenarios

and enhance the security and fault tolerance of CPSs by applying proper countermeasures at early stages. Additionally, in modeling large systems, reusability is a critical feature; as shown in the case study, the proposed approach has this capability for different physical domains. Therefore, in case of any changes in the system, its model can be easily modified. Developing software tools for supporting the full application of the proposed method and demonstrating its applicability and usefulness in further realistic examples of a larger scale is among our future research plans.

REFERENCES

[1] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: Analysis, challenges and solutions," *Comput. Secur.*, vol. 68, pp. 81–97, 2017.

[2] T. Tagarev, N. Stoianov, and G. Sharkov, "Integrative approach to understand vulnerabilities and enhance the security of cyber-bio-cognitive-physical systems," in *Proc. Eur. Conf. Cyber Warfare Secur.*, 2019, pp. 492–XIX.

[3] A. Cardenas and S. Cruz, "Cyber-physical systems security knowledge area," in *Proc. Cyber Secur. Body Knowl.*, pp. 3–9, 2019.

[4] DRAGOS, "ICS/OT cybersecurity year in review 2021," pp. 4–5, 2022. [Online]. Available: https://hub.dragos.com/report/2021-year-in-review

[5] A. Akbarzadeh and S. Katsikas, "Identifying and analyzing dependencies in and among complex cyber physical systems," *Sensors*, vol. 21, no. 5, 2021, Art. no. 1685.

[6] C. Bodei, P. Degano, G.-L. Ferrari, and L. Galletta, "Tracing where IoT data are collected and aggregated," *Log. Methods Comput. Sci.*, vol. 13, no. 3, Jul. 2017, doi: 10.23638/LMCS-13(3:5)2017.

[7] A. Bolshev, J. Larsen, M. Krotofil, and R. Wightman, "A rising tide: Design exploits in industrial control systems," in *Proc. 10th USENIX Workshop Offensive Technol.*, 2016, pp. 178–188.

[8] M. Krotofil, K. Kursawe, and D. Gollmann, "Securing industrial control systems," in *Security and Privacy Trends in the Industrial Internet of Things*. Berlin, Germany: Springer, 2019, pp. 3–27.

[9] R. Akella, H. Tang, and B. M. McMillin, "Analysis of information flow security in cyber–physical systems," *Int. J. Crit. Infrastructure Protection*, vol. 3, no. 3/4, pp. 157–173, 2010.

[10] P. Sobhrajan, S. Y. Nikam, D. Pimpri, and P. D. Pimpri, "Comparative study of abstraction in cyber physical system," *Int. J. Comput. Sci. Inf. Technol*, vol. 5, no. 1, pp. 466–469, 2014.

[11] Q. Wang, G. Zhang, and F. Wen, "A survey on policies, modelling and security of cyber-physical systems in smart grids," *Energy Convers. Econ.*, vol. 2, pp. 197–211, 2021.

[12] J. Butts, M. Rice, and S. Shenoi, "Modeling control system failures and attacks–the Waterloo campaign to oil pipelines," in *Proc. Int. Conf. Crit. Infrastructure Protection*, 2010, pp. 43–62.

[13] S. Hu and A. Y. Zomaya, *IEEE Tech. Committee Cyber-Physical Syst. (CPS)*, [Online]. Available: https://ieeesystemscouncil.org/cyber-physical-systems-technical-committee

[14] K. Stouffer *et al.*, "Guide to industrial control systems (ICS) security," *NIST Special Publication*, vol. 800, no. 82, pp. 16–16, 2011.

[15] B. Green, M. Krotofil, and D. Hutchison, "Achieving ICS resilience and security through granular data flow management," in *Proc. 2nd ACM Workshop Cyber- Phys. Syst. Secur. Privacy*, 2016, pp. 93–101.

[16] S. J. Oks, M. Jalowski, A. Fritzsche, and K. M. Möslein, "Cyber-physical modeling and simulation: A reference architecture for designing demonstrators for industrial cyber-physical systems," *Procedia CIRP*, vol. 84, pp. 257–264, 2019.

[17] P. Derler, E. A. Lee, and A. S. Vincentelli, "Modeling cyber–physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 13–28, Jan. 2012.

[18] J. C. Jensen, D. H. Chang, and E. A. Lee, "A model-based design methodology for cyber-physical systems," in *Proc. 7th Int. Wireless Commun. Mobile Comput. Conf.*, 2011, pp. 1666–1671.

[19] I. Graja, S. Kallel, N. Guermouche, S. Cheikhrouhou, and A. Hadj Kacem, "A comprehensive survey on modeling of cyber-physical systems," *Concurrency Comput.: Pract. Experience*, vol. 32, no. 15, 2020, Art. no. e4850.

[20] Z. Yu, D. Yunwei, Z. Fan, and Z. Yunfeng, "Research on modeling and analysis of CPS," in *Proc. Int. Conf. Auton. Trusted Comput.*, 2011, pp. 92–105.

[21] E. Kamburjan, S. Mitsch, M. Kettenbach, and R. Hähnle, "Modeling and verifying cyber-physical systems with hybrid active objects," Jun. 2019, *arXiv:1906.05704*.

[22] R. Seiger, S. Huber, and T. Schlegel, "Toward an execution system for self-healing workflows in cyber-physical systems," *Softw. Syst. Model.*, vol. 17, no. 2, pp. 551–572, 2018.

[23] P. Hehenberger, B. Vogel-Heuser, D. Bradley, B. Eynard, T. Tomiyama, and S. Achiche, "Design, modelling, simulation and integration of cyber physical systems: Methods and applications," *Comput. Ind.*, vol. 82, pp. 273–289, 2016.

[24] E. Villar, J. Merino, H. Posadas, R. Henia, and L. Rioux, "Mega-modeling of complex, distributed, heterogeneous CPS systems," *Microprocessors Microsystems*, vol. 78, 2020, Art. no. 103244.

[25] W. Borutzky, *Bond Graph Methodology: Development and Analysis of Multidisciplinary Dynamic System Models*. Berlin, Germany: Springer, 2009.

[26] S. Benmoussa, B. O. Bouamama, and R. Merzouki, "Bond graph approach for plant fault detection and isolation: Application to intelligent autonomous vehicle," *IEEE Trans. Automat. Sci. Eng.*, vol. 11, no. 2, pp. 585–593, Apr. 2014.

[27] P. Kumar, R. Merzouki, B. O. Bouamama, and A. Koubeissi, "Bond graph modeling of a class of system of systems," in *Proc. 10th Syst. Syst. Eng. Conf.*, 2015, pp. 280–285.

[28] M. J. White, "Bond graph modeling of critical infrastructures for cyber-physical security implementation," Ph.D. dissertation, Dept. Elect., Missouri Univ. Sci. Technol, Rolla, MO, USA, 2021.

[29] I. Zerdazi and M. Fezari, "Scada attack modeling using bond graph," in *Proc. Int. Conf. Inf. Commun. Technol. Disaster Manage.*, 2019, pp. 1–2.

[30] W. Borutzky, *Bond Graph Modelling of Engineering Systems*, vol. 103. Berlin, Germany: Springer, 2011.

[31] P. Carreira, V. Amaral, and H. Vangheluwe, *Foundations of Multi-Paradigm Modelling for Cyber-Physical Systems*. Berlin, Germany: Springer Nature, 2020.

[32] R. Merzouki, A. K. Samantaray, P. M. Pathak, and B. O. Bouamama, *Intelligent Mechatronic Systems: Modeling, Control and Diagnosis*. Berlin, Germany: Springer Science & Business Media, 2012.

[33] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2375–2385, Sep. 2015.

[34] M. Yu, C. Xiao, W. Jiang, S. Yang, and H. Wang, "Fault diagnosis for electromechanical system via extended analytical redundancy relations," *IEEE Trans. Ind. Inform.*, vol. 14, no. 12, pp. 5233–5244, Dec. 2018.

[35] I. Zerdazi, M. Fezari, and M. Ouziala, "Detection of deception attacks in supervisory control systems using bond graph," *Autom. Control Comput. Sci.*, vol. 54, no. 2, pp. 156–167, 2020.

[36] E. D. Knapp and J. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*. Amsterdam, Netherlands: Syngress, 2014.

[37] A. Akbarzadeh and S. Katsikas, "Identifying critical components in large scale cyber physical systems," in *Proc. IEEE/ACM 42nd Int. Conf. Softw. Eng. Workshops*, 2020, pp. 230–236.

[38] B. O. Bouamama, A. Samantaray, K. Medjaher, M. Staroswiecki, and G. Dauphin-Tanguy, "Model builder using functional and bond graph tools for FDI design," *Control Eng. Pract.*, vol. 13, no. 7, pp. 875–891, 2005.

[39] S. Pan, T. Morris, and U. Adhikari, "Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data," *IEEE Trans. Ind. Inform.*, vol. 11, no. 3, pp. 650–662, Jun. 2015.

[40] A. C. Umarikar and L. Umanand, "Modelling of switching systems in bond graphs using the concept of switched power junctions," *J. Franklin Inst.*, vol. 342, no. 2, pp. 131–147, Mar. 2005.