International Journal of Ambient Computing and Intelligence
Volume 15 • Issue 1

Threat Attribution and Reasoning for Industrial Control System Asset

Shuqin Zhang, Zhongyuan University of Technology, China
Peiyu Shi, School of Computer Science, Zhongyuan University of Technology, China*
Tianhui Du, Zhongyuan University of Technology, China
Xinyu Su, Zhongyuan University of Technology, China
Yunfei Han, Zhongyuan University of Technology, China

ABSTRACT

Due to the widespread use of the industrial internet of things, the industrial control system has steadily transformed into an intelligent and informational one. To increase the industrial control system's security, based on industrial control system assets, this paper provides a method of threat modeling, attributing, and reasoning. First, this method characterizes the asset threat of an industrial control system by constructing an asset security ontology based on the asset structure. Second, this approach makes use of machine learning to identify assets and attribute the attacker's attack path. Subsequently, inference rules are devised to replicate the attacker's attack path, thereby reducing the response time of security personnel to threats and strengthening the semantic relationship between asset security within industrial control systems. Finally, the process is used in the simulation environment and real case scenario based on the power grid, where the assets and attacks are mapped. The actual attack path is deduced, and it demonstrates the approach's effectiveness.

KEYWORDS

Assets, Attribution, Industrial Control System, Reasoning, Threat Modeling

1. INTRODUCTION

With the popularization of industrial Internet of Things and the development of industrial network intelligence (Tsuchiya et al., 2018), the operation and production mode of traditional industries—such as key manufacturing (Chen, 2020), chemical industry, electric power etc. (Alaba et al., 2017)—is gradually updating itself to be more intelligent and informational (Sasaki et al., 2022). Industrial Control System (ICS) is an asset control system used in industrial manufacturing that integrates computer equipment and industrial process control components. The ICS breaks down the notion of isolation inherent in traditional industry and external access (Kumar et al., 2022). The traditional industry did not take security, especially system security, as part of the main design criterion at the beginning (Mi et al., 2021). As the development of ICS networking and information technology (Cruz et al., 2016) are developing, many security protection measures created by network isolation

DOI: 10.4018/IJACI.333853 *Corresponding Author

are increasingly being connected to the network, which may create the risk of exposing ICS security vulnerabilities to hackers (Babu et al., 2017), causing severe economic losses and negative social impact. Threats to asset security in ICS increase along with the level of asset complexity. ICS is involved in almost all aspects of industrial production (AlMedires et al., 2021), and any asset issue could affect the manufacturing and production businesses' ability to continue operations (Zhang et al., 2021), thus causing risks that are out of control. Therefore, how to deal with the behavior of hackers and how to attribute the source of the hacker attacks are the difficulties of today's research. Because of the natural inequality between attack and defense (Su et al., 2022), we must comprehend the asset type and its functions in ICS and take into account all potential threats and attacks in combination with security, so as to judge the impact of the attack on ICS, speculate the attack path of hackers, and ultimately anticipate and respond to hacks in a proactive manner.

Related researchers mainly use three ways to determine ICS security: intrusion detection, security assessment, and system configuration. Intrusion detection is mainly used to achieve prevention by detecting network attacks to avoid being attacked. Bhamare et al. (2020) investigates the applicability of machine learning for anomaly and intrusion detection in ICS but does not take into account the impact on the entire ICS when it is attacked. Security assessment focuses on evaluating system vulnerability prioritization and thus satisfying system security. Qassim et al. (2019) examines the entire network system to ensure system security by identifying a vulnerability assessment methodology in ICS that ensures system security only in terms of vulnerabilities. System configuration focuses on configuring the system for security. AlgoSec (2018) focuses on evaluating cybersecurity policies related to cloud access and implementing them where necessary. This approach focuses more on local security policies. None of the above three approaches consider the impact of a cyberattack on the ICS, and do not consider the diversity of system impacts after being attacked.

In the ICS, the ever-changing ecological environment (Zhang et al., 2019) makes attackers feel in their element. For example, manufacturers often update their software systems for the convenience purpose of users and human-computer interaction ability, but these operations may lead to new vulnerabilities (Knapp et al., 2014), especially those that lack security considerations when considering the initial design (Kriaa et al., 2015). Moreover, the attacker's method and routes are constantly updated, while the defender cannot keep abreast of the latest attack technology and vulnerability information. Therefore, simple intrusion detection, attack attribution and attack prediction cannot perfectly analyze the attack behavior. We need to design a new method to detect and analyze the complex ecological environment of the ICS in time to enhance our knowledge of the threat attack.

Considering the above issues, this paper suggests an ICS threat attribution and reasoning method. Because of the importance of assets in the ICS (Li et al., 2017), this method uses the Purdue model, MITER ATT&CK etc., to describe the asset, and divides the assets into several asset types according to the actual situation of the ICS, thus constructing the ICS's asset type. Then, we use machine learning to analyze the power system attack data set (Koay et al., 2022), which can attribute the source of related attack threats and achieve good results. In this way, it can be learned which part of the ICS has been attacked. Finally, this paper simulates the scenario of the power system attack data set and the real scenario of the attacks on the Ukrainian power grid case (Sullivan et al., 2017). It automatically adds the impact of the ICS or the impact that will be caused after the attack by the attacker through reasoning rules, and finally maps it, which can show the attack path of the attacker.

This paper mainly makes the following contributions:

1. According to the actual situation of ICS, a threat model is constructed, which takes detection, threat, asset, and reality into consideration. And it describes the ICS from the perspective of assets, combines the Purdue model and the actual situation of ICS, puts forward a new concept of asset architecture, constructs an ontology model applicable to the security, and designs six kinds of common inference rules so that it can automatically reason about the system state.

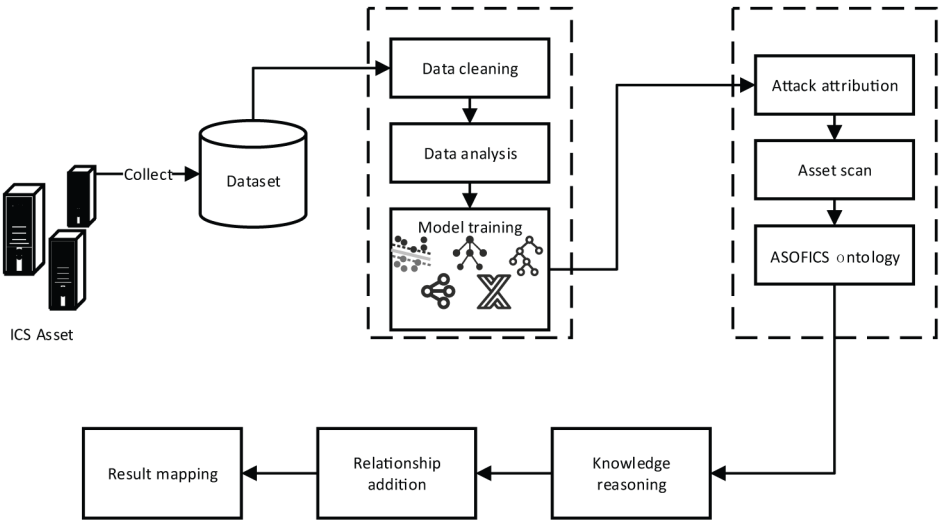
2. The problem of uneven data distribution of power system attack dataset is solved, and the attribution analysis of power system attack data using machine learning can detect the anomalies in the power system after being attacked, and in the comparative experiments. Better results are obtained and the first component that receives the impact of the attack is obtained.
3. Using reasoning rules to analyze the scenarios of the power system attack dataset and the case of the Ukrainian power grid hacking. By reasoning and analyzing the behavior of the attacker, new relationships can be automatically added to obtain the attack path of the attacker, which is finally mapped it, thus the comprehensive picture of ICS will be presented to the relevant personnel.

In this paper, Section 1 introduces the pertinent context and key contributions; Section 2 introduces related work; a new ICS asset threat model is suggested in Section 3; Section 4 attributes the source of ICS attacks; Section 5 develops the industrial control system's asset security ontology and provides the pertinent reasoning guidelines; Section 6 analyzes the attribution results, and verifies the effectiveness of the method in this paper by combining the power system attack data set scenario and a real case, and maps it to the knowledge map; in the end, we summarize the entire paper and propose some future works. Figure 1 represents the overall process of this article.

2. RELATED WORK

At present, the field of ICS has drawn the attention of researchers, and preliminary work on ICS security has been done. Kumar et al. (2022) used the attack tree as the common language and modelled three prominent APT attacks in the ICS. The attack tree modeling language was used to organize and systematically characterize each attack. The method was then verified by the attack scenario of the industrial oil pipeline. Mou et al. (2020) used the knowledge map to construct the map of the process manufacturing of the ICS to ensure the safety of the assets. This method only considered the internal relationship of the assets but lacked the consideration of the impact of external factors on the internal relationship of the assets. Samanis et al. (2022) evaluated 28 indicators in 18 free ICS asset scanning programs, considering the exclusive protocol in ICS. In a word, security experts had conducted exploratory research on a number of ICS related topics, but in the area of ICS security, there was no specialized threat modeling technique. The stability of the entire environment will be

Figure 1. Overall framework of this article



determined by the ICS assets. The relationship between assets and security in ICS was not taken into account in the above research. Therefore, this research suggests a novel ICS threat modeling scheme from the viewpoint of ICS assets. This framework may equip security workers with a broad spectrum of security awareness and can effectively express the relationship among assets, threats, and realities.

There are two ways to detect network attacks, one is to simply detect the attack, and the other is to attribute the source of the attack. Network attack detection can only identify the status of the current environment, such as normal status, attack status, etc., and cannot obtain more information. Mokhtari et al. (2021) summed up the intrusion detection of industrial control systems as the detection of abnormal activities. Based on the measurement data of SCADA, a MIDS intrusion detection system was proposed, and a hard-ware-in-the-loop test platform was built to detect abnormal activities. An anomaly detection technique based on state recognition was proposed by Hurley et al. (2012), which identified the normal and critical state of the system through data-driven clustering method and detected attacks in ICS. Network attack attribution is mainly divided into four levels: host attribution, control host attribution, attacker attribution, and attack organization attribution. These four kinds of attribution can be summarized into two types: component attribution and organization attribution. Both host attribution and control host attribution are component attribution, mainly for specific components in the attacked environment. Organization attribution mainly refers to the attribution of various information of the attacker, such as the identity, organization, and region of the attacker.

Huang et al. (2021) used the clue data and threat intelligence in the network attack event to extract relevant information, built the network attack event attribution relationship diagram according to the network attack event attribution ontology, learned the relevant path through the graph embedding algorithm, and finally realized the organization attribution through the classifier. Li et al. (2021) trained a multi-classification model of SMOTE-RF, which could better deal with the multi-classification problem of data imbalance. This method obtained the behavior characteristics of APT from the devices in the Internet of Things and used real dynamic data to complete the organization tracing behind the APT attack. Jahromi et al. (2021) proposed an attack detection traceback framework for ICS, which used decision tree and representation learning model to detect attacks in ICS and uses deep integrated neural network to organize traceback for attacks. In the ICS, due to the diversity of components in the environment and the complexity of interconnection (Ooi et al., 2023), it is difficult for researchers to attribute component of network attacks in ICS. At the same time, the development of IoT (Internet of Things), smart devices and other technologies also provide attackers with more attack objects and use of springboard (Zhang et al., 2013), which increases the difficulty of the component attribution process. This paper uses the power system attack data set and classifies it using the machine learning method to attribute the source of the components in the environment, find the attack source of the attacker, and realize the component attribution.

By describing information items, ontology is used to exchange domain knowledge and enhance the semantic link between information objects. Ontology modeling has made some progress recently according to security researchers in the security field. A network security ontology created by Kotzanikolaou et al. (2022) had two layers of data regarding the threats and physical environment and could combine risk assessment. By using this ontology to create a malware knowledge map and extract the hidden information from it, Rastogi et al. (2020) created a malware ontology called MALONT. A security ontology for risk monitoring was proposed by Merah et al. (2021) using Cyber Threat Intelligence (CTI), highlighting the interdependence of risk concepts that could expand the use of Structured Threat Information Expression (STIX). Zhang et al. (2021) proposed a RIoTSCO Internet of Things security ontology integrating multi-source heterogeneous data. This ontology built a million-level heterogeneous database by combining intelligence. However, none of the aforementioned studies considered the specific circumstances surrounding ICS security. In order to give security personnel a comprehensive understanding of the internal workings of ICS assets, this paper suggests an ontology for security built on ICS assets that seeks to strengthen the relationships between ICS assets and assets, assets and threats, and threats and consequences by using inference rules.

3. NEW ICS ASSET THREAT MODEL

3.1 Basic Definition

From the standpoint of the assets, this paper describes the concepts of assets in ICS, as follows:

Definition 1 - Asset: Assets are the components in ICS that have a direct or indirect impact on industrial production.

Definition 2 - Component: Components include not only physical components in ICS, but also some protocols or systems used in ICS, that is, all computer equipment and industrial control process components in ICS belong to the category of components.

Definition 3 - Effect: The effect of this article mainly represents two meanings, one is the relationship between assets and assets, and the other is the change of an asset after an attack.

Definition 4 - Asset type: A part of assets with similar characteristics or functions belongs to the same asset type.

Definition 5 - Attack source: In this article, the attack source mainly refers to the first affected component after being attacked by the attacker, that is, if the attacker uses Component A as a springboard to attack other components in ICS, Component A is the attack source of this attack.

Definition 6 - Attribution: Attribution in this article indicates the determination of the attack source after being attacked.

Assume that the asset security domain in ICS is AICS_ ASSET, the component in the ICS is MICS_ ASSET, the part is PAICS_ ASSET, the protocol is POICS_ ASSET, the system is SICS_ ASSET, record the asset category as ACICS_ ASSET, then the formula is as follows:

$$PA_{ICS\_ASSET}, PO_{ICS\_ASSET}, S_{ICS\_ASSET} \in M_{ICS\_ASSET} \tag{1}$$

$$M_{ICS\_ASSET} \in A_{ICS\_ASSET} \tag{2}$$

$$AC_{ICS\_ASSET} \in A_{ICS\_ASSET} \tag{3}$$

The above shows the relationship between some terms in this article. Among them, assets include all components, and asset category is a part of the assets with similar functions. Both the visible components of the entity and the virtual network protocol or system belong to components.

3.2 ICS Asset Structure

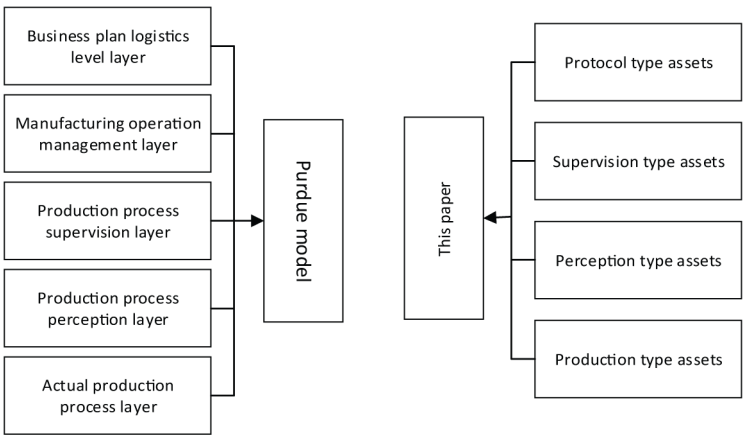
Purdue model divides the ICS into five layers through the interdependencies among the components of the industrial control system: the actual production process layer, the production process perception layer, the production process supervision layer, the manufacturing operation management layer, and the business plan and the logistics layer. To be specific, the actual production process layer mainly describes the actual manufacturing or production process; the production process perception layer mainly describes the operation and perception process of the actual production process; the production process supervision layer is mainly responsible for the monitoring and management of the production process; manufacturing operation management refers to the business process of producing target products; and the business plan and logistics layer mainly represents the relevant activities of a manufacturing organization. It can be found that the first three layers of Purdue model mainly aim at the actual production of ICS and focus on the production process. The latter two layers mainly

describe the production plan of the ICS, with human factors in the majority. We research the assets in the production process of the ICS, which corresponds to the first three layers of the Purdue model.

The biggest difference between ICS and ordinary IT network is the difference in protocol. Due to the physical isolation and other characteristics of ICS protocol, security issues were not considered at the beginning of design. With the development of intelligent ICS, which is increasingly connected to the Internet, the security features of physical isolation no longer exist in front of hackers. The security of the ICS protocol was thoroughly studied by Fang et al. (2022), who concentrated on the ICS's protocol vulnerabilities. They explained the significance of the ICS protocol from three perspectives: the protocol's vulnerability, the attacker's attack strategy, and the attack's consequences. In the incident where the Ukrainian power grid was compromised, the attacker intruded into the SSH back door by using phishing mail, thus intruded into the servers of the Ukrainian power grid, caused during a significant power outage. In this event, the attacker obtains the authority of the Ukrainian power grid by attacking the SSH protocol vulnerability, thus implementing the attack. Purdue model cannot well describe the important role of protocol in this event. Therefore, this paper builds the ICS asset structure by using the protocol as part of the ICS asset.

After research, we found that attackers often attack the ICS from the monitoring and management system to affect the underlying equipment of the ICS for their own purposes. Stuxnet (Masood et al., 2021), for example, is a combination of malicious code attack and zero-day vulnerability, which destroys the field equipment level centrifuge to halt Iran's progress toward nuclear weapons. In this event, the attacker obtained some permissions of the computer through malicious code, thus completing the main attack on the device layer at the attack site. To sum up, we divide the assets of ICS into four parts: production type assets PRDICS, perception type assets ADICS, supervision type assets SDICS and protocol type assets PTDICS. Figure 2 shows the difference between Purdue model and asset division in this paper. Among them, production type assets mainly represent the actual production process of the ICS; perceived type assets mainly describe the perception process of the actual production process; supervision type assets are mainly aimed at the monitoring and management of the production process in the industrial control system; and protocol type assets mainly represent protocols in ICS. Among the four types of assets, the sequence of asset grade from high to low is: regulatory assets, perception assets, and production assets, while the asset grade of protocol assets cannot be determined because they exist in the other three types of assets. Based on the above, we can have a good description of ICS assets.

Figure 2. Comparison between purdue model and the asset structure of this paper



The ICS asset, AICS, is indicated as follows:

$$\{PRD_{ICS}, AD_{ICS}, SD_{ICS}, PTD_{ICS}\} \in A_{ICS} \quad (4)$$

3.3 ICS Asset Threat Model

Through the ICS asset structure's split, we propose an ICS asset threat model, as shown in Figure 3.

Figure 3 mainly shows the primary framework for the threat of ICS assets. In this paper, threats and consequences are added based on the four parts of ICS assets. Among them, protocol type assets, supervision type assets, perception type assets, and production type assets are collectively referred to as assets. Threat is mainly used for describing the threat to the ICS, including the attacker's organization, the tools, the time or means of the attack, etc. The consequence indicates the possible results of the ICS assets after being attacked. Attackers need to research and plan various information in the assets, and then devise one or more attack strategies that can lead to specific effects, and finally act on the relevant assets. In the same way, the consequences of related assets will also react on assets. Through the analysis of ICS asset security presented above, we can gain a more comprehensive understanding of the internal ecological environment of ICS, as well as the security circumstances surrounding all ICS assets.

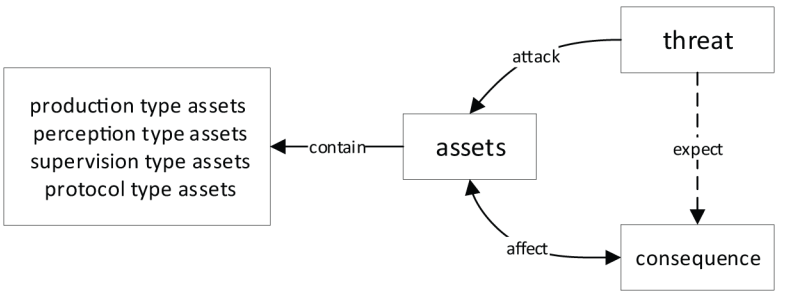
4. ICS ATTACK ATTRIBUTION METHOD

4.1 Power System Attack Data Set

Through the analysis and model construction in the previous section, we can already make a detailed description of the asset attacks in ICS. However, for the unique structure and assets in the ICS environment, how to attribute the source of attacks is also a very important link, that is, to detect the source of attacks. In ICS, assets are often interrelated. Once one of the assets is threatened, the entire asset environment will be affected, and even cause the collapse of the entire environment. Therefore, in ICS, we need not only to detect attacks, but also to attribute the source of attacks. In this way, we can keep track of slight changes to components in the ICS assets and grasp the situation perception in ICS in real time from point to surface.

In response to the above problems, this paper uses the power system attack data set collected by Mississippi State University and Oak Ridge National Laboratory (2014) to verify the model method in this paper. The data set is mainly divided into three modules: dual metadata set, triple metadata set, and multiple metadata set. The dual metadata set is mainly used to distinguish attack events and natural events; three data types of attack events, natural events, and non-events collected by triple metadata set; and the multiple data sets mainly mark 37 scenarios, including all aspects of the threat to the power system. Threats are classified into natural threats and attack threats. For example,

Figure 3. ICS asset threat model



short circuit fault and line maintenance caused by natural events are natural threats, that is, there are no human factors. Scenarios such as remote trip command injection and relay setting change are mainly caused by human operation, which is an attack threat. The following table makes a statistical comparison of the above data sets.

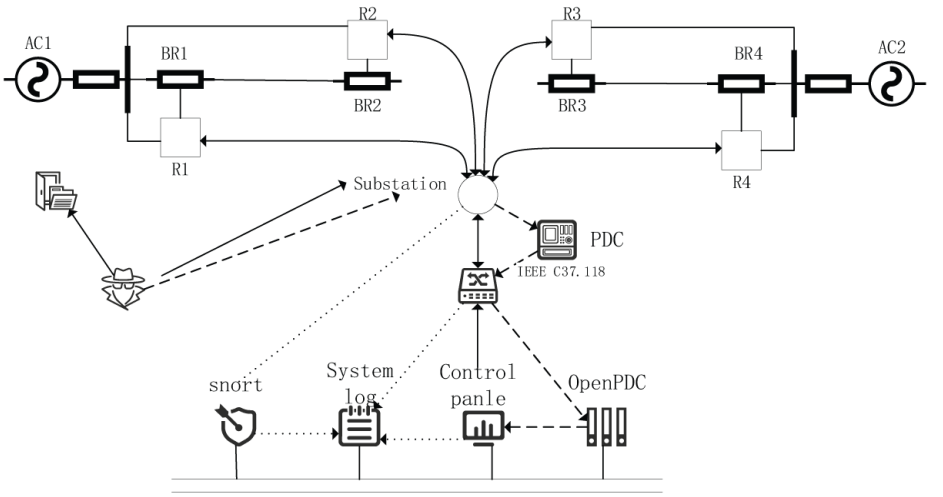
For the data sets shown in Table 1, especially the multivariate data sets, each event is marked, and each event is subdivided into components that occur to the tag, thus marking 37 scenarios. If the remote trip command injection attack is used to attack component A and component B respectively, and the relay setting change is used to attack component C, these are three scenarios. We learn and analyse the above situation via machine learning to sense the upcoming attack, attribute, and find the attack source. We then use the reasoning method mentioned in the next section to have a global grasp of ICS assets, that is, when a component is attacked, its impact on the entire ICS asset environment can be understood in detail.

The power system attack data set collected by Mississippi State University and Oak Ridge National Laboratory is shown in Figure 4 below, where AC represents the power supply, BR mainly represents the circuit breaker, and R represents the intelligent equipment that controls BR. R contains relays, and Rn controls BRn. The four intelligent devices are controlled by the substation. The data of the substation can be handed over to the switch by the PDC (Phasor Data Concentrator), or directly interact with the switch. The switch is managed by the control panel. The openPDC obtains data

Table 1. Dataset scenario comparison

Data Type	Dataset Contains Scenarios
Binary metadata set	Attack events, natural events (such as sudden tripping and other natural events, not man-made events)
Triple metadata set	Attack event, natural event, no event (event under normal operation of power system)
Multiple data set	Natural event (including short circuit or line maintenance of different components), no event, attack event (including remote trip command attack of different components, data injection attack, relay setting change, etc.)

Figure 4. Power system attack imitation scenario



from the HMI and feeds it back to the control panel. The control panel generates system logs. The entire environment is detected by the snort system, which can also be regarded as a defense device in the environment. The relay is controlled by Modbus/TCP protocol, and the phasor data concentrator (PDC) mainly uses IEEE C37.118 (2013) protocol to transmit data.

Through the above environment, a simple power system can be imitated. The power system data set is composed of a 128-dimensional data set by measuring the current, voltage, voltage phase angle, radio wave, and other data of the above parts, simulating attacks by destroying a component and recording the damaged component and measurement data. Through this data set, we can use machine learning method to classify the data set and speculate the impact of an attack on a component through the fluctuation of the measured value, then complete the attribution.

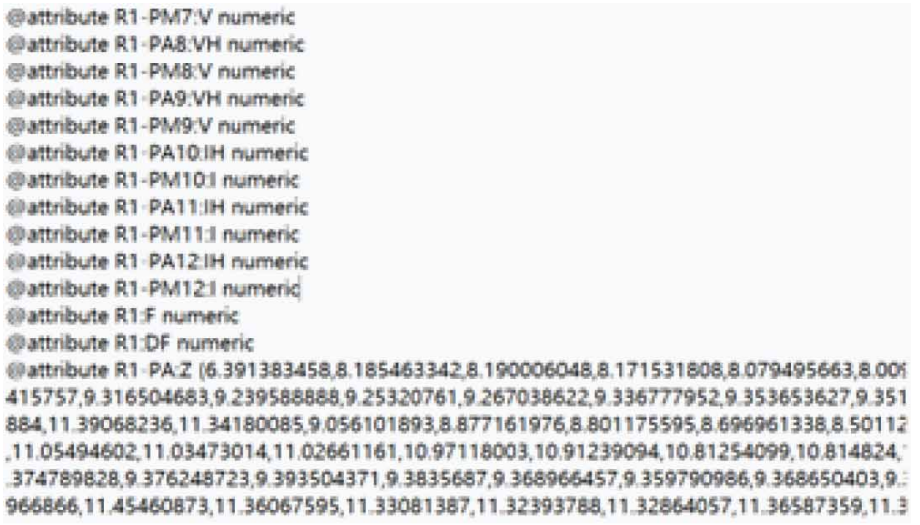
Figure 5 shows the raw data of the power system attack dataset, such as R1-PM7:V represents the voltage phase magnitude about PM7 measured by R1; R1-PA8:VH represents the voltage phase angle of PA8 measured by R1; R1-PA10:IH represents the current phase angle about PA10 measured by R1; R1-PM10:I represents the voltage phase magnitude about PM10 measured by R1, containing a total of 24000 data.

4.2 Related Models

This paper mainly compares five machine learning models: SVM (Jakkula, 2006), decision tree (Song & Ying, 2015), random forest (Cutler et al., 2012), XGBoost (Chen et al., 2015), and KNN (Guo et al., 2003) to classify the above data sets so as to verify the accuracy and effectiveness of this experiment.

SVM is a supervised learning classifier for binary or multivariate classification of data. The goal is to solve the hyperplane of the maximum edge distance between the decision boundary and the learning sample. In order to solve it, a convex quadratic programming problem is created. Little sample data categorization issues can be resolved with SVM, especially if the sample data is not more than 10000. SVM can also solve the dimension disaster and nonlinear separable classification problem through the kernel function method. Since SVM has the problem of solving the hyperplane of the maximum margin between the decision boundary and the learning sample, the computational complexity of SVM depends on the number of support vectors of the learning sample rather than the dimension of the learning sample.

Figure 5. Raw data showing of power system attack dataset



Decision tree is a supervised learning model that can be selected according to certain conditions to achieve the goal. The node of the decision tree represents the feature, and the edge represents the direction. Through the feature and direction selection, the leaf node is finally obtained, which is the classification result. In addition to not supporting missing values, the decision tree does not require any data preprocessing, and can handle both numerical variables and classification variables. However, the decision tree is not a stable model. If the sample data is not balanced before training, the decision tree will create a biased tree.

Several decision trees are combined in the integrated learning algorithm known as random forest. By voting the split results of multiple decision trees, the output result is determined by the category with the highest votes. Random forest can solve the problem of weak generalization ability of decision tree by random feature selection and random sample selection. Training can be highly parallelized and faster under large sample data. Random forest is not sensitive to some missing features because of randomly selected features. However, in noisy data sets, random forest can easily fall into over-fitting.

XGBoost is an algorithm toolkit based on the Boosting framework, an optimized distributed gradient lifting library, and a strong classifier that integrates many weak classifiers. The algorithm continuously uses feature splitting to grow additional trees. Each additional tree learns a new function, fits the residual of the last prediction by the new function, and finally adds the scores of the trained trees to get the final prediction value. XGBoost uses Taylor expansion to speed up the gradient descent. It can optimize the calculation of leaf splitting only by relying on input data. In essence, it increases the applicability of XGBoost by separating the selection of the loss function from the optimization of the model algorithm.

KNN calculates the distance from the test data to each object in the training data, sorts it according to the distance, and selects the K training data closest to the current test data as the neighbor of the current test data. Finally, it determines the category of the test category by counting the category frequency of the K training data.

5. ICS ASSET THREAT ONTOLOGY AND REASONING

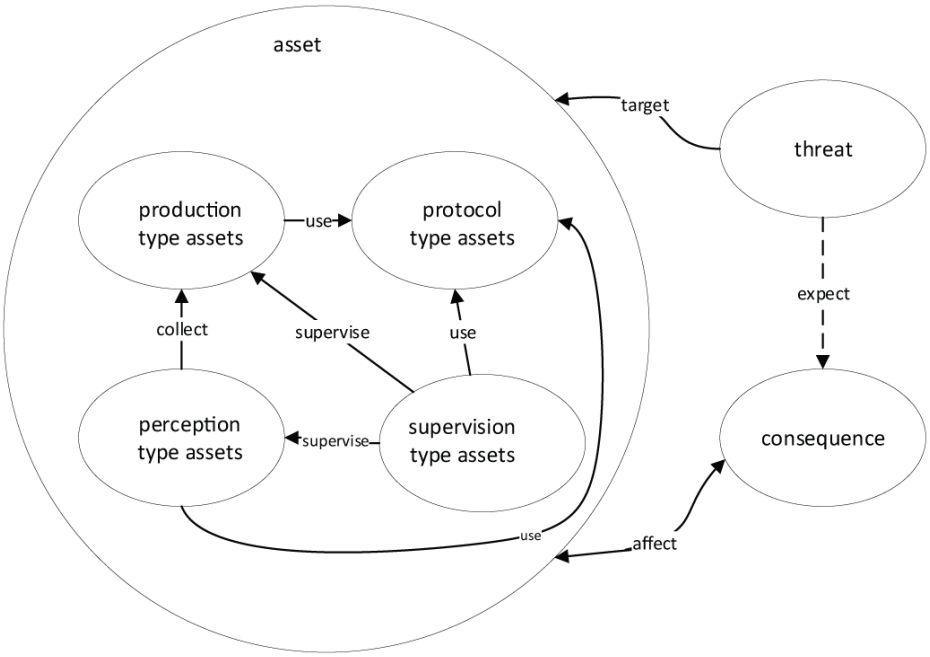
As a continuation of the attack attribution in the previous section, we can attribute the source of the attack on ICS assets once it has been attacked. In Section 3, although we have established the link between the threats of ICS assets and supplied a threat model for security, attacking real ICS assets remains a challenge. Through the formal description of specific domain knowledge, the ontology proposes the Asset Safety Ontology for Industrial Control Systems (ASOFICS), which solves the semantic heterogeneity problem among ICS asset, threat, and consequence (Xu et al., 2017; Lee et al., 2017), and plays an important role in the construction of the three-in-one ICS ecosystem of ICS asset, threat, and consequence.

The ontology for ICS asset threat in this section is inspired by multiple ontologies (Zhang et al., 2021; Li et al., 2021; Rastogi et al., 2020; Merah et al., 2021). After being combined with some concepts and adjusted by a number of details, the ontology here is more suitable for the description of assets and their environment in ICS. The ontology model to be discussed in this section considers the concepts necessary for ICS asset, threat, and consequence. These interrelated sources of knowledge are not involved in the referenced ontology. This section uses OWL language to build a unified formal description, in which concepts are equivalent to classes and relationships are equivalent to properties. In the second half of this section, the semantic Web rule language is used to design inference rules and to display the implicit information in the ontology.

5.1 ICS Asset Ontology's Class and Property

Six top level classes are present in the ASOFICS ontology that is suggested in this section: production type assets, perception type assets, supervision type assets, protocol type assets, threat, and consequence. Figure 6 illustrates the connections between the six top-level classes.

Figure 6. The interrelationship among the six top classes



The attack target of the attacker, the interplay of various assets, threats, and consequences, among other things, are described in this article through properties, as illustrated in Table 2.

As indicated in Table 2, this research presents 13 relationship properties grouped into three groups. The ICS asset structure, which is primarily used to specify properties between assets in the ICS structure, is the subject of the first group, such as ActOn and FeedbackTo, used to 'act on' and 'feedback on' separately. For example, HMI will act on production type assets, and perception assets often feedback their perception information to HMI. This is how we can define the relationship between the ICS asset components. BelongTo describes that one component is contained in another component. For instance, relays in ICS assets often exist in intelligent devices, thus Relays and intelligent devices are BelongTo properties. Control refers the control and management function of

Table 2. Property description among assets

Property	Type
ActOn (Asset: x; Asset: y) FeedbackTo (Asset: x; Asset: y) BelongTo (Asset: x; Asset: y) Measure (Asset: x; Asset: y) Control (Asset: x; Asset: y)	Description of the relationship among assets
Attack (Threat: t; Asset: x) AttackAffect (Threat: t; Asset: x) Infiltrate (Threat: t; Asset: x) MayControl (Threat: t; Asset: x) HaveThreat (Asset: x; Threat: t) UseAttack (Threat: t; Threat: th)	Description of the relationship between asset and threat
MayCause (Threat: t; Conse: co) AssetAffect (Asset: x; Asset: y, Conse: co)	Description of the relationship between asset and consequence

regulatory assets on other assets, such as the control of production type assets in HMI; the measurement is expressed by Measure. Several sensors exist in the sensing assets to measure a range of values in the ICS manufacturing process, such as thermometer and flowmeters in chemical production as well as the current value of the ammeter in the power plant. HaveThreat indicates the threat of one asset.

The second group describes the properties of attackers, including Attack, AttackAffect, Infiltrate, MayControl, and UseAttack. Specifically, Attack describes the attack properties of attackers against assets. AttackAffect describes the impact of an attack on other associated components. Infiltrate means intrusion, expressing intrusion phenomenon of the attacker rather than a direct attack on the intrusion device, which represents an indirect relationship and an implicit attack that bypasses the alarm device (defense measures). MayControl means that the attacker has the potential to take control of both high-level and low-level resources. We are aware of the tools or attack technologies the attacker is using because the term UseAttack refers to the use of an attack. All attacks can be described by Attack, whereas UseAttack relates to the known attack techniques. Both of these terms directly define the attack. On the contrary, AttackAffect, Infiltrate, and MayControl describe the indirect impact caused by the attack.

The consequence layer's properties fall under the last group, which are MayCause and AssetAffect. MayCause is used to describe the possible consequences caused by attackers, and AssetAffect refers to the consequences caused by certain assets.

5.2 Reasoning Rule Design

The inference rule connection strategy stated below not only serves the description of the ontology model, but also serves the description of actual assets in ICS. After meeting the specified connection strategy, it can automatically connect to form a new relationship. Note that RICS-asset is the inference rule set in the ICS asset security domain, and KIICS-asset is the knowledge base in the ICS security domain, thus the inference rule set is defined as follows:

$$R_{ICS-asset} = \left\{R_1, R_2, R_3, \ldots, R_n \mid R \in KI_{ICS-asset}\right\}, n > 0 \tag{5}$$

It should be noted that R represents the specified inference rule. Only if the condition of the inference rule (the left half) is true can the conclusion on the right be deduced, thus, as to add a new relationship.

The relationship between conditions (C) and new relationships (N) is expressed as follows and described using SWRL:

$$\left\{\exists C_1 \cap C_2 \cap C_3 \cap \ldots \cap (C_{n-i} \mid \ldots \mid C_n) \rightarrow N_1, N_2, \ldots, N_n\right\}, n \geq i > 0 \tag{6}$$

In logical rules, use "and" and "or" to indicate '∩' and 'l'. Three definitions apply to C and N, where C (a) denotes a member of Class C; P (x, y) denotes that certain properties are shared by x and y; and a numerical type or instance is represented by (x, y).

To facilitate the following rule design, we mark the set of classes in the area of ICS asset security as $\text{Class}_{\text{ICS-asset}}$, the set of properties in the area of ICS asset security as $\text{Property}_{\text{ICS-asset}}$, and the set of instances in the area of ICS asset security as $\text{Individual}_{\text{ICS-asset}}$:

$$Class_{ICS-asset} = \left\{Class_1, Class_2, \ldots, Class_n\right\}, n \geq 0 \tag{7}$$

$$Property_{ICS-asset} = \left\{Property_1, Property_2, \ldots, Property_n\right\}, n \geq 0 \tag{8}$$

$$Individual_{ICS-asset} = \left\{Individual_1, Individual_2, \ldots, Individual_n\right\}, n \geq 0 \tag{9}$$

$$Individual \in Class_{ICS-asset} \tag{10}$$

$$\{Class^n \cap Property^n \cap Individual^n \rightarrow Property^m, Individual^m\}, n \geq m > 0 \tag{11}$$

Class ^{n} mainly indicates that there are n classes in Class $_{ICS\text{-}asset}$.

In the area of ICS asset security, we have developed six different types of reasoning rules based on the aforementioned explanation, where '⋀' means 'and', as shown in Table 3.

Rule 1: If component a act on component b and the two are connected, we can assume that component b will be impacted by an attack on component a, thus if the attacker attacks component a or the attack has an influence on component a, then component b is affected by the attack. For instance, if a server is attacked by an attacker and the server is connected to the communication system, the server attack will have an impact on the communication system.

Rule 2: If a component of the attack has an impact on an asset and that impact has consequences, we can deduce that the attacker may also have consequences. For instance, a server is attacked by an attacker; the server and the communication system are connected, so that the attacker can affect the communication system. Meanwhile, the communication system assets will affect the

Table 3. Formal inference rule table

Order Number	Rule
Rule1	(Attack(?attacker, ?element_a) or (UseAttack(?attacker, ?tool) or AttackAffect(?attacker,?element_a))) ⋀ (ActOn(?element_a, ?element_b) or BelongTo(?element_b, ?element_a)) -> AttackAffect(?attacker, ?element_b)
Rule2	(AttackAffect(?attacker, ?element_a) or Attack(?attacker, ?element_a) or Infiltrate(?attacker, ?element_b)) ⋀ AssetAffect(?element_a, ?asset)) ⋀ Consequence(?asset) -> MayCause(?attacker, ?asset)
Rule3	FeedbackTo(?element_a, ?element_b) ⋀ ActOn(?element_a, ?element_b) ⋀ AttackAffect(?attack, ?element_a) ⋀ (sub-regulator(?element_a) or sub-protocol(?element_a))-> Infiltrate(?element_a, ?element_b)
Rule4	Control(?element_a, ?element_b) ⋀ Control(?element_c, ?element_b) ⋀ AttackAffect(?attacker, ?element_a)⋀AttackAffect(?attacker, ?element_c)-> Infiltrate(?element_a, ?element_b) ⋀ MayControl(?attacker, ?element_b)
Rule5	Infiltrate(?element_a, ?element_b) ⋀BelongTo(?element_b, ?element_c)⋀ ActOn(?element_b, ?element_c) -> AttackAffect(?element_a, ?element_c)
Rule6	UseAttack(?attacker, ?tool) ⋀ Threat(?tool) ⋀ (Attack(?tool, ?element_a) or AttackAffect(?tool, ?element_a) or MayControl(?attacker, ?element_a))⋀ AssetAffect(?element_a, ?event) ⋀ Consequence(?event) -> MayCause(?attacker, ?event)

occurrence of "loss of connection" and other real events, thus the attack that affects the switch could result in "loss of connection" events.

Rule 3: Component a may influence component b and information from component a is accessible to component b. Component a in the regulator type assets (or protocol type assets) may breach component b during an attack on component a. Since the majority of production type assets and perception type assets are manually operated and lack intelligence, attackers will typically avoid operating on the components in these two types directly in favor of attacking regulator type assets and protocol type assets, which will have an indirect impact on production type assets and perception type assets. For instance, the two-way communication between the scheduling workstation and SSH enables the scheduling workstation to both influence SSH and give scheduling workstation input. As a result, when an attacker attacks the scheduling workstation, the likelihood that he will hack SSH through it rises.

Rule 4: Both component a and c have control over component b. It can be assumed that the attacker may want to seize control of component b if the attack simultaneously affects both component a and c. For instance, the attacker wants to obtain the management authority of the server through the control center and then bypasses snort to intrude the server. Therefore, the purpose of the attacker is to obtain the corresponding authority to control the server, so as to facilitate the subsequent attack.

Rule 5: When an assault spreads from component a to b, component b is a part of and affects component c, we can assume that component c is the object of b's attack. For instance, SSH is used for remote calls, therefore if an attack manages to bypass the backdoor, the attack probably will have an effect on the communication server as well.

Rule 6: An attacker is employing a menacing and threat-type tool. We can assume that the attacker may have consequences if the attacks (or attack effect) component a and the assets of component a result in a consequence event. For instance, we are unable to identify the attack trace if a hacker uses killdisk to hide his trace (log file).

6. EXAMPLE AND EVALUATION

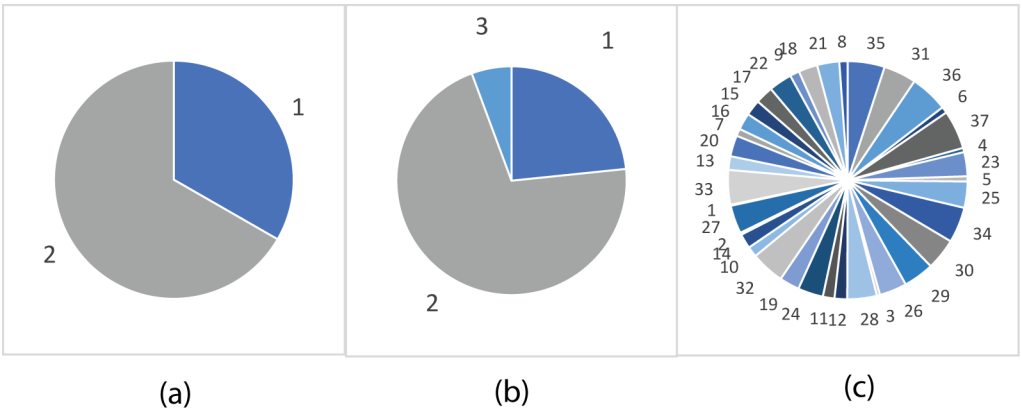
This section is mainly composed of three parts. The first part attributes the threat attack source of ICS and obtains the attack source through five machine learning classification models to verify the effectiveness and accuracy of the experiment. In the second part, the power system attack data set is used as the background to simulate two kinds of network attacks, and the inference rules are used to conduct security inference on ICS assets. The third part simulates the case of Ukraine power grid intrusion, which enables us to predict the threat attack and comprehensively grasp the asset security in ICS environment.

6.1 Comparison of Results

We first need to analyze the data distribution of the dataset. As shown below, Figure 7(a) represents the data distribution of the binary dataset, Figure 7(b) represents the data distribution of the ternary dataset, and Figure 7(c) represents the distribution of the multivariate dataset, with the numbers in the figure representing the scene labels. The scenario 1 in Figure 7(a) is twice as different from scenario 2, scenario 2 in Figure 7(b) is 10 times as different from scenario 3, and the most numerous scenario in Figure 7(c) is 40 times as different from the least numerous scenario.

Due to the fact that this dataset is in ARFF format, it is necessary to clean this dataset and convert it to the CSV format that we are familiar with. Through analysis we can find that the first 127 dimensions of data all have an impact on the final traceability results. In this dataset, there are 160,000 data for attack events and only 80,000 data for no events; it is obvious that the data is not balanced, so it is necessary to use the BorderlineSMOTE function to deal with the data imbalance

Figure 7. Data distribution within the power system attack dataset



mentioned above. After the processing of the data, they all obtain the same percentage. Finally, setting 20% of the test set for testing the above model gives the following results.

In this section, five commonly used machine learning classification methods—SVM, random forest, decision tree, XGBoost, and KNN—are compared to analyze the attribute of the attack source of the power grid system attack data set on Mississippi State University and Oak Ridge National Laboratory. This paper classifies three groups of power grid system attack data sets. The classification performance is shown in Figure 8.

As shown in Figure 8, A stands for accuracy, P stands for precision, R stands for recall rate, and F stands for F1 value. Additionally, B stands for binary dataset, T stands for ternary dataset, and M stands for multivariate dataset.

Accuracy represents how many samples in the prediction results are correct. It can be seen from Figure 6 that the accuracy of the SVC-RBF model is relatively low, especially in the face of multiple classification problems. On the contrary, the functionality of random forest algorithm is superior to the other four methods in the classification of dual metadata set, triple metadata set, and multiple metadata set. The specific accuracy is shown in Table 4.

Figure 8. Comparison of results

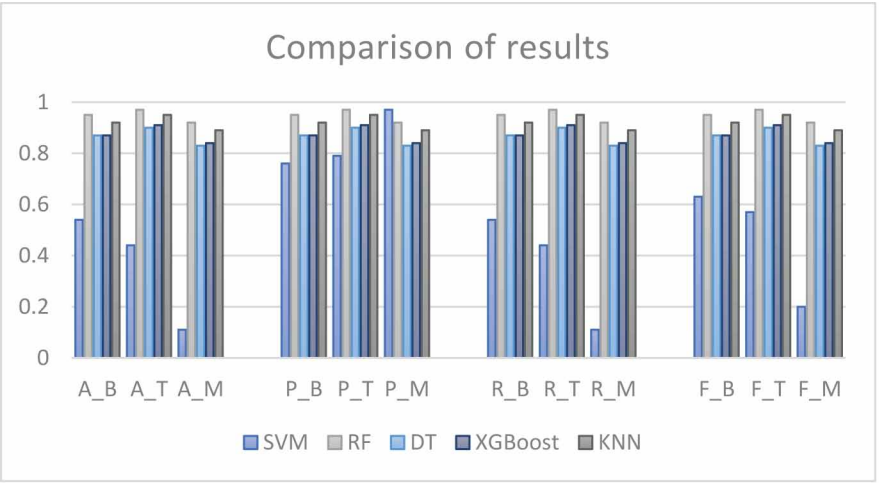


Table 4. Specific accuracy value of each algorithm

Model	Binary	Ternary	Multivariate
SVM	0.54	0.44	0.11
RF	0.95	0.97	0.92
DT	0.87	0.90	0.83
XGBoost	0.87	0.91	0.84
KNN	0.92	0.95	0.89

Precision is commonly known as P value. In this indicator, the function of SVM is better than that of accuracy. This indicator indicates how many of the samples that are predicted to be positive are true positive samples, indicating that SVM can predict the true positive samples correctly in the classification problem. However, the function is still not as good as the other four models, which may be related to the fact that SVM is only suitable for processing small sample data. Among other algorithms, random forest still shows the highest performance in three data sets, and the function of KNN is second only to random forest. The specific precision is shown in Table 5.

In the index of recall rate, the function of SVM is not ideal, that is, it cannot predict correctly compared with the original sample SVM. Random forest still shows the best performance in the index of recall rate, and KNN is also second only to random forest. The specific recall rate is shown in Table 6.

SVM does not perform well in F1-value because of the large difference in precision and recall. The other four models are stable, as shown in Table 7.

As shown in Table 8, Wang et al. (2019) also uses the power system attack dataset and adds 16 new features by using PMU to measure the physical significance of the features, combining the features by weight voting and achieves better results on SVM. In this paper, the unbalanced dataset

Table 5. Specific P value of each algorithm

Model	Binary	Ternary	Multivariate
SVM	0.76	0.79	0.97
RF	0.95	0.97	0.92
DT	0.87	0.90	0.83
XGBoost	0.87	0.91	0.84
KNN	0.92	0.95	0.89

Table 6. Specific recall rate of each algorithm

Model	Binary	Ternary	Multivariate
SVM	0.54	0.44	0.11
RF	0.95	0.97	0.92
DT	0.87	0.90	0.83
XGBoost	0.87	0.91	0.84
KNN	0.92	0.95	0.89

Table 7. Specific F1-value of each algorithm

Model	Binary	Ternary	Multivariate
SVM	0.63	0.57	0.20
RF	0.95	0.97	0.92
DT	0.87	0.90	0.83
XGBoost	0.87	0.91	0.84
KNN	0.92	0.95	0.89

is equalized by data equalization and significantly improved on Random Forest, Decision Tree, and KNN. Especially regarding KNN, the dataset is improved by 10 percentage points and much better than the way of feature combination in the original paper. The importance of data equalization for model learning training can be seen in Table 8.

In the experiments shown in Table 8, SVC-RBF classification is mainly adopted by SVM. Due to its unsatisfactory effect on large sample data, the effect of SVM in Figure 4 is unstable and the training time is too long. The other four models all have ideal functions; however, the training speed of XGBoost is slower than the other three models because of its requirements of integrated learning. Compared with the other four models, the function of random forest is highly desirable and stable. This is because random forest is composed of a group of decision trees, which is superior to decision trees in function. Moreover, random forest can solve the problem of weak generalization ability of the decision tree through random feature selection and random sample selection.

The above analysis allows us to attributively measure the threat attack. When the ICS is attacked, its traffic data can be obtained which is classified and attributes through machine learning, and then the source component of the ICS attack can be output. To sum up, we recommend using random forest, KNN, and XGBoost to classify the source of attacks in turn.

6.2 Scenario Simulation

Here, the above dataset scenario is imitated to verify the effectiveness of the threat attribution reasoning method of ICS assets proposed in this paper. Two attack scenarios are simulated in this dataset scenario that are remote trip command injection and relay settings change, both of which are described and analyzed in detail below.

6.2.1 Remote Trip Command Injection

Based on the above description, we have a general idea of the data set framework. Through the scenario description of the data set, the entities in the data set are identified and extracted, the asset structure of the power grid system is constructed, and the asset threat model of ICS is used to divide its assets. Through the attribution classification mentioned in the previous section, we can capture the first component of the attack on the power grid control system at the time the attack occurs. The single relay command injection attack on intelligent device R1 is simulated during the remote command injection attack, and the outcomes are then presented.

Table 8. Comparison of the average accuracy of this paper with other

Comparison	SVM	RF	DT	XGBoost	KNN
Wang et al.(2019)	0.89	0.91	0.82	0.90	0.82
Average	0.36	**0.95**	**0.87**	0.88	**0.92**

As shown in Figure 9, the PDC receives the synchronization vector data and feeds it back to openPDC through the switch. After being attacked in the system, the source of attack can be obtained in time through the above-mentioned attributing method. When attacking the remote trip command injection, the attacker first needs to evade the snort defense system. After bypassing the defense alarm system, the attacker can intrude the master control of ICS, affect the switch, and then control the substation followed by injecting the trip command into the relay in R1 through the remote command injection, and making the BR1 circuit breaker corresponding to R1 open, resulting in tripping and power failure.

Remote trip command injection attack is a compound attack that utilizes both remote services and command line interface technologies. MITER ATT&CK (2021) describes exploitation of remote services as the abuse of remote services by using the errors of the system itself, thus causing intrusion. The command line interface is used by attackers to execute related commands interactively with the system, thereby causing attacks. Pan et al. (2015) believed that the remote trip was because the remote trip receiving side had received the trip command. Therefore, if an attacker wants to complete the remote trip command injection attack, he needs to evade the alarm device in the system, invade the system server to obtain the corresponding permissions, and finally achieve the attack through the trip command injection. By comparison, it is found that the reasoning rules in this paper can perfectly display the above logical order.

6.2.2 Relay Setting Change

This paper imitates the relay setting change attack in the power system attack dataset scenario as well, in which the relay has two states: enabled and disabled. The relay setting change attack is an attack by changing the state of the relay.

As shown in Figure 10, to prevent the attack from being detected, the attacker needs to bypass the snort alarm device, then attack the control center to gain access, and subsequently intrude the switch which can also control the substation. Since the substation controls four intelligent devices from R1 to R4, the change of the substation state will affect the intelligent device R1, and eventually change the state of the relay R1r contained in R1.

Figure 9. Mapping of remote tripping command injection attack

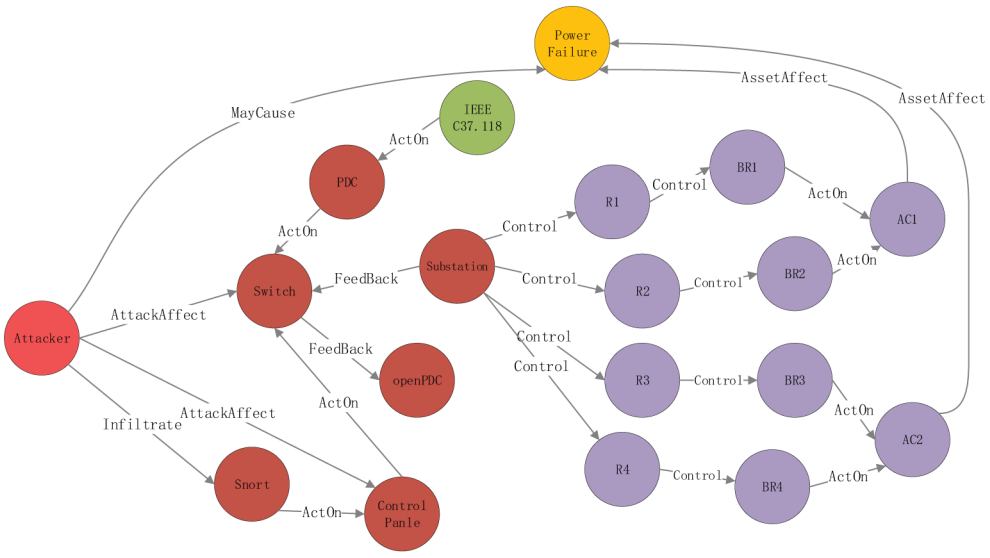
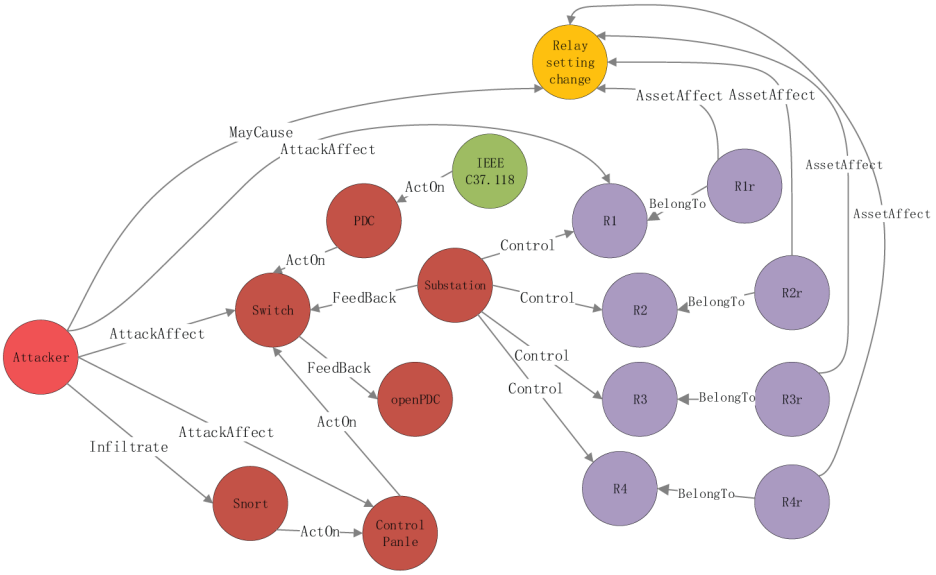


Figure 10. Mapping of relay setting change attack



The relay setting change attack uses the change operating mode technology in MITER ATT&CK. This technology changes the operation mode of the controller to obtain additional access rights. In this circumstance, the attacker first needs to evade the snort alarm system, then obtains the control authority, subsequently affecting the intelligent equipment in the substation through the switch, and finally completes the setting change of the relay in the intelligent equipment. After research, the logic used in this work is congruent with how an actual attack would be conducted.

Figure 10 clearly demonstrates each step of the attacker's penetration into the power grid system, allowing us to foresee the attacker's potential outcomes and prepare to defend any assets that may be impacted.

This method is proved effective by our research. This report also uncovers the information that was concealed inside the power grid system's assets following an attack. This study associates asset-threat-consequence and maps it, which demonstrates that the model technique in this paper is more thorough when combined with the inference rules.

6.3 Real Case

In order to verify the effectiveness of this method, the Ukrainian power grid intrusion case is used as an example in this section to support the proposed threat attribution and technique of reasoning for ICS assets. Based on our study and the research report on ANTIY (2016), this paper makes statistics on the internal assets of the Ukrainian power grid, as shown in Table 9.

Table 9. Asset statistics in Ukrainian power grid

Asset Type	Related Asset
Production type assets	Generator, transformer, circuit breaker, disconnector, transmission line, vacuum arc extinguishing chamber, switch cabinet, ring-network cabinet, lightning arrester, etc.
perception type assets	Monitoring and measuring instruments, voltage transformers, current transformers, relay protection devices, etc.
supervision type assets	DCS, SCADA, monitoring device, communication server, telephone system, MES, PLC, HMI, ERP
protocol type assets	IEC 60870-5, SSH, CIP, EtherNet/IP

Millions of people's daily lives have been impacted by the Ukrainian power grid intrusion. In this instance, the switch action of seven substations was mostly responsible for the 80,000 customers who lost power for 3 to 6 hours. Due to management incompetence, a malicious email sent by the attacker was read, and the infected email immediately downloaded malicious software, disconnecting the Ukrainian Electric Power Company's primary control from the substation, wiping out all evidence of the attack. The attacker also prevented residential customers who had lost power from communicating with the outside world by interfering with the communication system, which allowed them to eventually realize the coordinated attack, as seen in Figure 11.

The general mechanism of the Ukrainian power grid penetration is already clear based on the example described above. Next, we will take this case as an example to conduct knowledge reasoning and obtain the subsequent intrusion procedure.

Step 1: When an attacker is seen attempting to assault the dispatch center, which manages the main HMI and monitoring system, using blackenergy, it can be speculated that the attack will affect the above components and the attacker may control them.

Step 2: Attackers can breach SSH horizontally because the dispatch center uses SSH for communication.

Step 3: SSH is a method of getting access to the communication server. It also has a connection to the master HMI. The master HMI, which is controlled by the dispatching center, directly manages the transformer's switch operation, giving the attacker the potential to start a power outage. The first three steps are shown in Figure 12.

Step 4: Because the attacker oversees the dispatch center's monitoring system, the monitoring system may be turned off, leading to blind monitoring.

Step 5: The attack trail will be deleted by the killdisk once the attacker launches it through blackenergy, which also clears the attack trace, making it even more difficult for the staff to identify the attack's origin in time.

Step 6: After the attacker attacks the phone system with DDOS, residents are unable to feedback the outage event to the customer service via a malfunctioning which further prolong the power outage time. The latter three steps are shown in Figure 13.

Through the above discussion, we are aware of the basic strategy used in the Ukrainian power grid breach event. The knowledge map can be used to generate the following results by linking the aforementioned technique to it.

Figure 11. Invasion case of the Ukrainian power grid

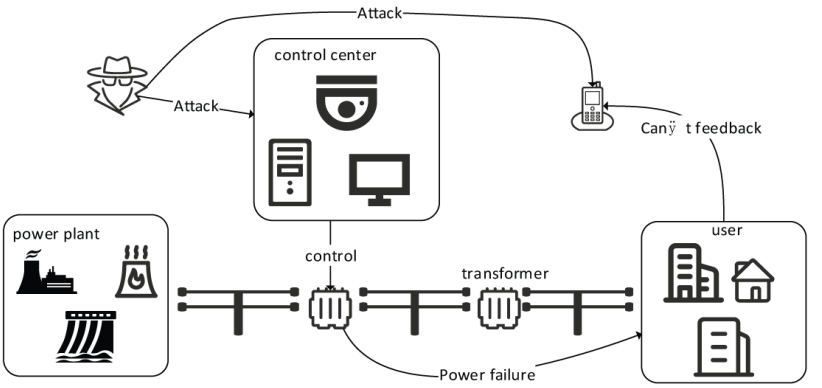


Figure 12. The first three steps of reasoning

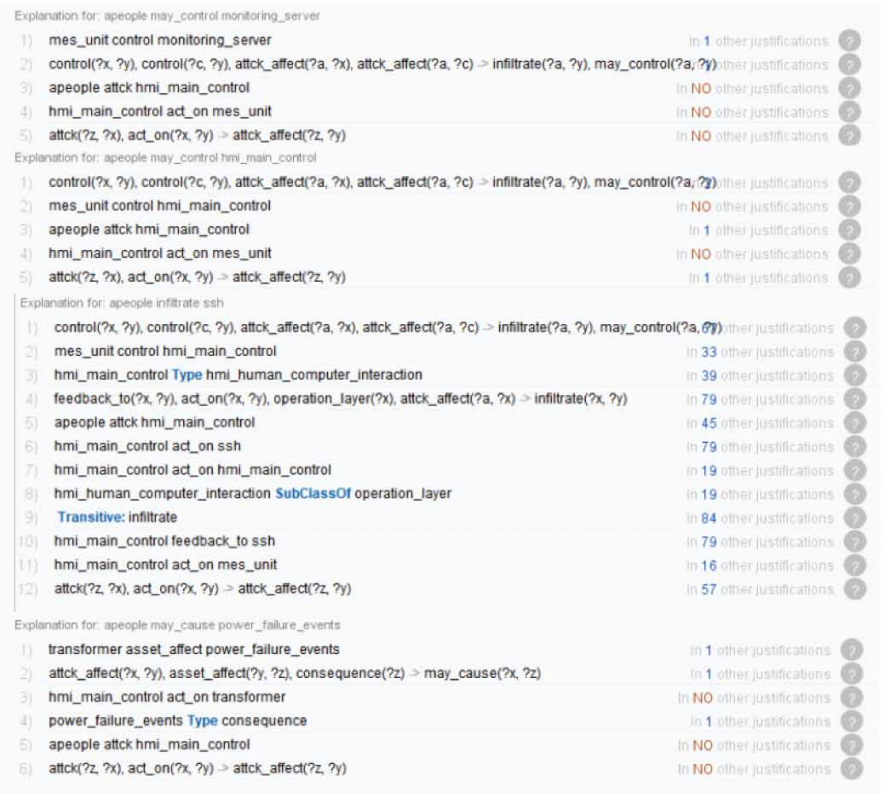


Figure 13. The last three steps of reasoning

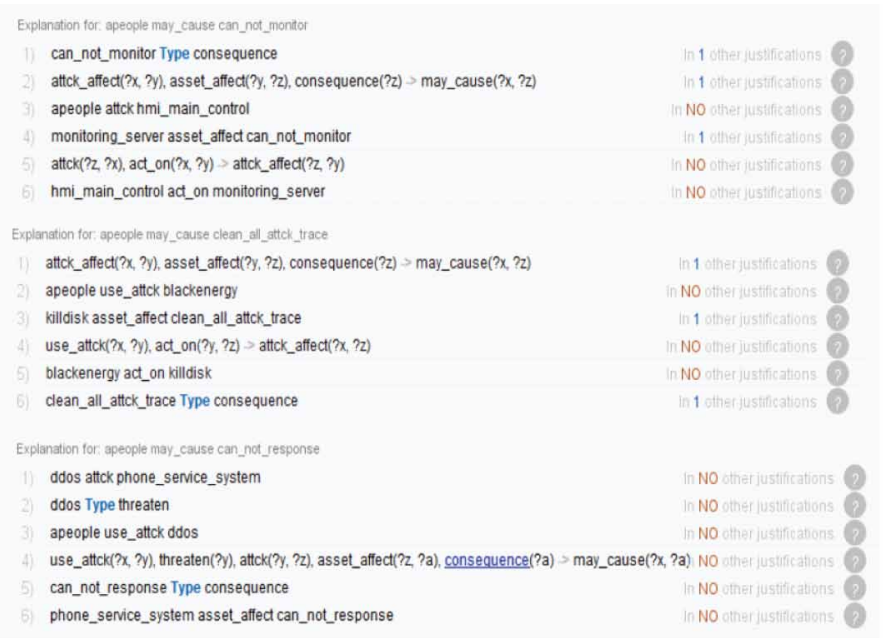
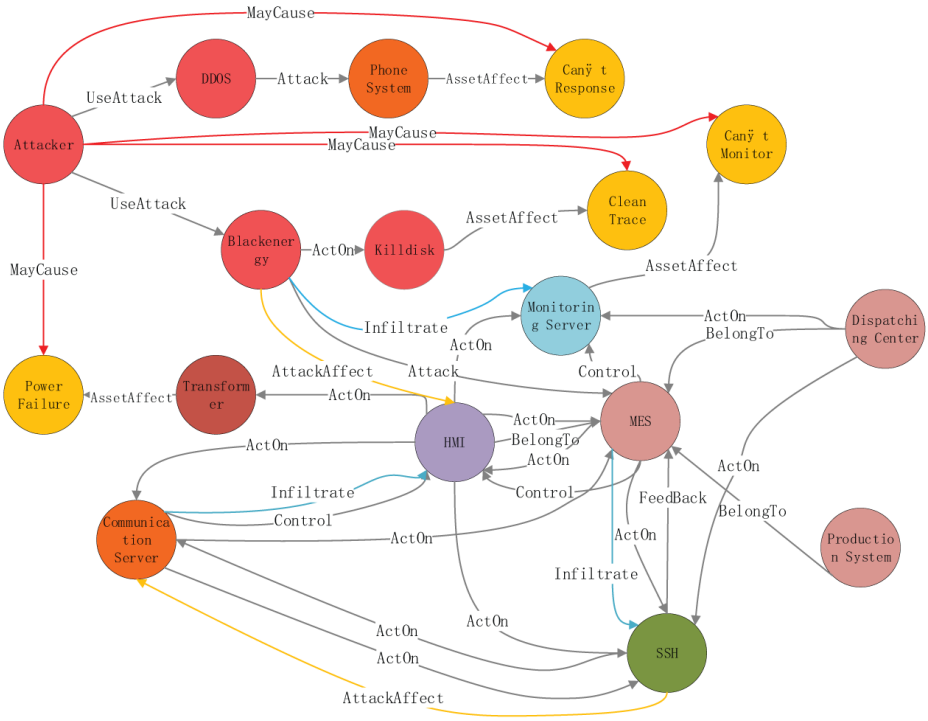


Figure 14. The three aspects of asset-threat-consequence are mapped to the knowledge map



The red node indicates a threat, the red line indicates possible damage the attacker and its tools could cause, the yellow line indicates potential impact on assets, and the blue line indicates the attacker's penetration attack.

Through the above illustration, each step taken by the attacker to breach the Ukrainian power infrastructure is easily understood. We may make a pre-decision beforehand based on the potential effects of the attacker, and we can protect the assets that might be impacted in advance.

This method's analytical results are contrasted with power grid intrusion case report for Ukraine, and the results are shown in Table 10.

On the other hand, it turns out that the step of the Ukrainian power grid intrusion scenario that this methodology ultimately recreates is compatible with the actual intrusion process, and the reasoning conclusions in this study are more in-depth, which suggests that this method is effective. The fact that

Table 10. Report on Ukraine power grid intrusion cases and results comparison

Analysis Report	Results of This Paper
Attackers use blackenergy to penetrate horizontally	Use blackenergy to attack the dispatch center and intrude on the server
Capture monitoring/device area host	Control the primary monitoring and control system, causing a power outage and blindness
Clear system log erase attack trace	To erase attack traces, use killdisk
Prevent users through the DDoS from contacting customer service	DDoS assaults can be used to block users from calling customer support

this research uses the asset-threat-consequence correlation, knowledge mapping, and combination of reasoning rules to derive the concealed information within the Ukrainian power grid assets following an attacker attack demonstrates how complete the model method used in this paper is.

7. CONCLUSION

The threat model proposed in this paper bridges the gap in the field of ICS asset security. The following table compares the coverage of the threat model in this paper with other models as a way to demonstrate the range of scenarios expressed by the current model in the ICS security domain.

From Table 11, it can be seen that in the field of ICS security, most of the studies only consider the threat itself. In ICS, threat, reality, and asset are interrelated, and considering only one-sided factors cannot really solve the security problems, but should be considered from the aspects of detection, threat, asset, and reality, all while obtaining the state of the system after an attack through reasoning.

In this research, a threat attribution and reasoning mechanism based on ICS assets is proposed. By looking at the problem from the perspective of the assets, this strategy suggests a new ICS threat model. This model also considers that the protocol was part of assets, thus relevant personnel can better manage the hazard posed by ICS assets. On this basis, the power system attack data set is used for attributing classification training. Through attributing classification, the attack source can be found, and good results have been achieved. Then the ontology for ICS asset security is constructed, and six inference rules are proposed. Due to the fact that machine learning and rule-based mechanisms can operate in a predictable manner, this paper uses machine learning for attribution analysis of power system attack datasets. In the face of data imbalance in the power system attack dataset, the problem is solved using relevant algorithms and good results are achieved on Random Forest, Decision Tree, and KNN, where KNN improves by 10 percentage points. Finally, the power system attack dataset scenario and the Ukrainian power grid intrusion case are simulated. The findings of the experiments demonstrate the effectiveness of the threat attribution and reasoning approach based on ICS that is suggested in this paper in solving the security issue of ICS assets and assisting security professionals in maintaining security conditions inside the ICS assets.

However, our work did not take into account the corresponding defensive measures. Subsequently, we will also add mitigation measures to the ontology model. When the system is attacked, the mitigation measures can be direct feedback. In this way, it can not only build the security status of the system, but also timely feedback the defense plan. In addition, due to the uncertainty of cyber-attacks and the complexity of ICS, our work does not consider the impact of probabilistic factors, that is, the probability of a certain consequence for the whole system after being subjected to a certain attack.

Table 11. Comparison of the ICS asset security model in this paper with others

Citation	Detection	Threat	Asset	Reality	Reasoning	Mitigation
Pedro, A. et al. (2022)		√		√		
Alanen, J. et al. (2022)		√	√	√		
Li, Z. et al. (2022)	√	√			√	
Zhang,S. et al.(2021)		√			√	√
Mauri, L. et al.(2022)		√	√			
Firoozjaei, M. et al.(2022)		√		√		
Pu, H. et al.(2022)		√				√
This Paper	√	√	√	√	√	

In the future, we will not only include mitigation measures, but also consider probabilistic factors, which will lead to a more comprehensive ICS threat model. At the same time, we will also study more cases to turn the above semi-automated operations into automated steps.

AUTHOR CONTRIBUTIONS

Conceptualization, S.Z., P.S., T.D., X.S. and Y.H.; methodology, S.Z. and P.S.; software, P.S.; validation, S.Z., P.S., T.D. and X.S.; formal analysis, P.S.; investigation, S.Z. and P.S.; resources, P.S. and T.D.; data curation, P.S. and T.D.; writing-original draft preparation, P.S.; writing-review and editing, S.Z., P.S., T.D., X.S. and Y.H.; visualization, P.S.; supervision, S.Z.; project administration, S.Z. and P.S. All authors have read and agreed to the published version of the manuscript.

FUNDING STATEMENTS

This research was funded by the Key Program Research Fund of Higher Education of Henan, China, grant number No. 21A520053.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10–28. doi:10.1016/j.jnca.2017.04.002

Alanen, J., Linnosmaa, J., Malm, T., Papakonstantinou, N., Ahonen, T., Heikkilä, E., & Tiusanen, R. (2022). Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. *Reliability Engineering & System Safety*, *220*, 108270. doi:10.1016/j.ress.2021.108270

AlgoSec. (2018). *AlgoSec Security Policy Management Solution*. https://www.algosec.com/

AlMedires, M., & AlMaiah, M. (2021, July). Cybersecurity in Industrial Control System (ICS). In *2021 International Conference on Information Technology (ICIT)* (pp. 640-647). IEEE. doi:10.1109/ICIT52682.2021.9491741

Babu, B., Ijyas, T., Muneer, P., & Varghese, J. (2017, March). Security issues in SCADA based industrial control systems. In *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)* (pp. 47-51). IEEE. doi:10.1109/Anti-Cybercrime.2017.7905261

Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., & Meskin, N. (2020). Cybersecurity for industrial control systems: A survey. *Computers & Security*, *89*, 101677.

C37. 244-2013 - IEEE. (2013). *Guide for Phasor Data Concentrator Requirements for Power System Protection, Control, and Monitoring*. https://ieeexplore.ieee.org/document/6514039

Chen, K. S. (2020). Fuzzy testing decision-making model for intelligent manufacturing process with Taguchi capability index. *Journal of Intelligent & Fuzzy Systems*, *38*(2), 2129–2139. doi:10.3233/JIFS-190865

Chen, T., He, T., Benesty, M., Khotilovich, V., Tang, Y., Cho, H., ... & Zhou, T. (2015). Xgboost: Extreme gradient boosting. *R Package Version 0.4-2, 1*(4), 1-4.

Cruz, T., Queiroz, R., Simões, P., & Monteiro, E. (2016, June). Security implications of SCADA ICS virtualization: Survey and future trends. In *Proceedings 15th European Conference Cyber Warfare Security (ECCWS)* (pp. 74-83). Academic Press.

Cutler, A., Cutler, D. R., & Stevens, J. R. (2012). Random forests. *Ensemble Machine Learning: Methods and Applications*, 157-175.

Fang, D., Liu, P., Qin, C., Song, Z., Sun, Y., Shi, Z., & Sun, L. (2022). Survey of protocol security of industrial control system. *Journal of Computer Research and Development*, *5*, 978–993.

Firoozjaei, M. D., Mahmoudyar, N., Baseri, Y., & Ghorbani, A. A. (2022). An evaluation framework for industrial control system cyber incidents. *International Journal of Critical Infrastructure Protection*, *36*, 100487. doi:10.1016/j.ijcip.2021.100487

Guo, G., Wang, H., Bell, D., Bi, Y., & Greer, K. (2003). KNN model-based approach in classification. In *On the Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE: OTM Confederated International Conferences, CoopIS, DOA, and ODBASE 2003, Catania, Sicily, Italy, November 3-7.* Proceedings (pp. 986-996). Springer Berlin Heidelberg. doi:10.1007/978-3-540-39964-3_62

Harbin ANTIY Technology. (2016). *Comprehensive analysis report on attacks on Ukraine's power system*. www.antiy.cn/research/notice&report/research_report/20160323.html

Huang, K. Z., Lian, Y. F., Feng, D. G., Zhang, H. X., Wu, D., & Ma, X. L. (2021). Method of cyber attack attribution based on graph model. *Journal of Software*, *33*(2), 683–698.

Hurley, J., Munoz, A., & Sezer, S. (2012, June). ITACA: Flexible, scalable network analysis. In *2012 IEEE International Conference on Communications (ICC)* (pp. 1069-1073). IEEE. doi:10.1109/ICC.2012.6363995

Jahromi, A. N., Karimipour, H., Dehghantanha, A., & Choo, K. K. R. (2021). Toward detection and attribution of cyber-attacks in IoT-enabled cyber–physical systems. *IEEE Internet of Things Journal*, *8*(17), 13712–13722. doi:10.1109/JIOT.2021.3067667

Jakkula, V. (2006). Tutorial on support vector machine (svm). School of EECS, Washington State University.

Knapp, E. D., & Langill, J. T. (2014). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress.

Koay, A. M., Ko, R. K. L., Hettema, H., & Radke, K. (2022). Machine learning in industrial control system (ICS) security: Current landscape, opportunities and challenges. *Journal of Intelligent Information Systems*, 1–29.

Kotzanikolaou, P. (2022, February). A cybersecurity ontology to support risk information gathering in cyber-physical systems. In *Computer Security. ESORICS 2021 International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, Germany, October 4–8, 2021, Revised Selected Papers* (Vol. 13106, p. 23). Springer Nature.

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety*, *139*, 156–178. doi:10.1016/j.ress.2015.02.008

Kumar, R., Kela, R., Singh, S., & Trujillo-Rasua, R. (2022). APT attacks on industrial control systems: A tale of three incidents. *International Journal of Critical Infrastructure Protection*, *37*, 100521. doi:10.1016/j.ijcip.2022.100521

Lee, O. J., Nguyen, H. L., Jung, J. E., Um, T. W., & Lee, H. W. (2017). Towards ontological approach on trust-aware ambient services. *IEEE Access : Practical Innovations, Open Solutions*, *5*, 1589–1599. doi:10.1109/ACCESS.2017.2663407

Li, S., Zhang, Q., Wu, X., Han, W., & Tian, Z. (2021). Attribution classification method of APT malware in IoT using machine learning techniques. *Security and Communication Networks*, *2021*, 1–12. doi:10.1155/2021/9396141

Li, X., Zhou, C., Tian, Y. C., Xiong, N., & Qin, Y. (2017). Asset-based dynamic impact assessment of cyberattacks for risk analysis in industrial control systems. *IEEE Transactions on Industrial Informatics*, *14*(2), 608–618. doi:10.1109/TII.2017.2740571

Li, Z., Song, B., & Li, D. (2022). Safety risk recognition method based on abnormal scenarios. *Buildings*, *12*(5), 562. doi:10.3390/buildings12050562

Masood, Z., Raja, M. A. Z., Chaudhary, N. I., Cheema, K. M., & Milyani, A. H. (2021). Fractional dynamics of stuxnet virus propagation in industrial control systems. *Mathematics*, *9*(17), 2160. doi:10.3390/math9172160

Mauri, L., & Damiani, E. (2022). Modeling threats to AI-ML systems using STRIDE. *Sensors (Basel)*, *22*(17), 6662. doi:10.3390/s22176662 PMID:36081121

Merah, Y., & Kenaza, T. (2021, August). Ontology-based cyber risk monitoring using cyber threat intelligence. In *Proceedings of the 16th International Conference on Availability, Reliability and Security* (pp. 1-8). doi:10.1145/3465481.3470024

Mi, J., Huang, W., Chen, M., & Zhang, W. (2021). A method of entropy weight quantitative risk assessment for the safety and security integration of a typical industrial control system. *IEEE Access : Practical Innovations, Open Solutions*, *9*, 90919–90932. doi:10.1109/ACCESS.2021.3091136

Mississippi State University and Oak Ridge National Laboratory. (2014). *Power system attack data set* [Data set]. http://ece.uah.edu/~thm0009/icsdatasets/PowerSystem_Dataset_README.pdf

MITRE ATT&CK. (2021). *Matrix for ICS*. https://attack.mitre.org/

Mokhtari, S., Abbaspour, A., Yen, K. K., & Sargolzaei, A. (2021). A machine learning approach for anomaly detection in industrial control systems based on measurement data. *Electronics (Basel)*, *10*(4), 407. doi:10.3390/electronics10040407

Mou, T. H., & Li, S. Y. (2022). Knowledge graph construction for control systems in process industry. *Chinese Journal of Intelligent Science and Technology*, *4*(01), 129–141.

Ooi, S. E., Beuran, R., Kuroda, T., Kuwahara, T., Hotchi, R., Fujita, N., & Tan, Y. (2023). Intent-driven secure system design: Methodology and implementation. *Computers & Security*, *124*, 102955. doi:10.1016/j.cose.2022.102955

Pan, S., Morris, T., & Adhikari, U. (2015). Developing a hybrid intrusion detection system using data mining for power systems. *IEEE Transactions on Smart Grid*, *6*(6), 3104–3113. doi:10.1109/TSG.2015.2409775

Pedro, A., Pham-Hang, A. T., Nguyen, P. T., & Pham, H. C. (2022). Data-driven construction safety information sharing system based on linked data, ontologies, and knowledge graph technologies. *International Journal of Environmental Research and Public Health*, *19*(2), 794. doi:10.3390/ijerph19020794 PMID:35055616

Pu, H., He, L., Cheng, P., Sun, M., & Chen, J. (2022). Security of industrial robots: Vulnerabilities, attacks, and mitigations. *IEEE Network*.

Qassim, Q. S., Jamil, N., Daud, M., Patel, A., & Ja'affar, N. (2019). A review of security assessment methodologies in in-dustrial control systems. *Information and Computer Security*, *27*(1), 47–61. doi:10.1108/ICS-04-2018-0048

Rastogi, N., Dutta, S., Zaki, M. J., Gittens, A., & Aggarwal, C. (2020, August). Malont: An ontology for malware threat intelligence. In *International workshop on deployable machine learning for security defense* (pp. 28-44). Cham: Springer International Publishing. doi:10.1007/978-3-030-59621-7_2

Samanis, E., Gardiner, J., & Rashid, A. (2022, August). SoK: A taxonomy for contrasting industrial control systems asset discovery tools. In *Proceedings of the 17th International Conference on Availability, Reliability and Security* (pp. 1-12). doi:10.1145/3538969.3538979

Sasaki, T., Fujita, A., Ganán, C. H., van Eeten, M., Yoshioka, K., & Matsumoto, T. (2022, May). Exposed infrastructures: Discovery, attacks and remediation of insecure ics remote management devices. In *2022 IEEE Symposium on Security and Privacy (SP)* (pp. 2379-2396). IEEE. doi:10.1109/SP46214.2022.9833730

Song, Y. Y., & Ying, L. U. (2015). Decision tree methods: Applications for classification and prediction. *Shanghai Jingshen Yixue*, *27*(2), 130. PMID:26120265

Su, Q., Wang, H., Sun, C., Li, B., & Li, J. (2022). Cyber-attacks against cyber-physical power systems security: State estimation, attacks reconstruction and defense strategy. *Applied Mathematics and Computation*, *413*, 126639. doi:10.1016/j.amc.2021.126639

Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the US power grid. *The Electricity Journal*, *30*(3), 30–35. doi:10.1016/j.tej.2017.02.006

Tsuchiya, A., Fraile, F., Koshijima, I., Ortiz, A., & Poler, R. (2018). Software defined networking firewall for industry 4.0 manufacturing systems. *Journal of Industrial Engineering and Management*, *11*(2), 318–333. doi:10.3926/jiem.2534

Wang, D., Wang, X., Zhang, Y., & Jin, L. (2019). Detection of power grid disturbances and cyber-attacks based on machine learning. *Journal of Information Security and Applications*, *46*, 42–52. doi:10.1016/j.jisa.2019.02.008

Xu, G., Cao, Y., Ren, Y., Li, X., & Feng, Z. (2017). Network security situation awareness based on semantic ontology and user-defined rules for Internet of Things. *IEEE Access : Practical Innovations, Open Solutions*, *5*, 21046–21056. doi:10.1109/ACCESS.2017.2734681

Zhang, C., Wei, T., Chen, Z., Duan, L., Szekeres, L., McCamant, S., & Zou, W. (2013). Practical control flow integrity and randomization for binary executables. In *2013 IEEE Symposium on Security and Privacy*. (pp. 559-573). IEEE. doi:10.1109/SP.2013.44

Zhang, F., Kodituwakku, H. A. D. E., Hines, J. W., & Coble, J. (2019). Multilayer data-driven cyber-attack detection system for industrial control systems based on network, system, and process data. *IEEE Transactions on Industrial Informatics*, *15*(7), 4362–4369. doi:10.1109/TII.2019.2891261

Zhang, S., Bai, G., Li, H., Liu, P., Zhang, M., & Li, S. (2021). Multi-source knowledge reasoning for data-driven IoT security. *Sensors (Basel)*, *21*(22), 7579. doi:10.3390/s21227579 PMID:34833653

Shuqin Zhang, Professor. Dr., graduated from Harbin Engineering University in 2005. Worked in Zhongyuan University of Technology. His research interests include IoT security, data mining, network attack and defense, and wireless network.

Peiyu Shi, Student. Master, graduated from Zhongyuan University of Technology in 2017. Worked in Zhongyuan University of Technology. His research interests include ICS security.

Tianhui Du, Student. Master, graduated from Zhengzhou University of Aviation Industry Management in 2017. Worked in Zhongyuan University of Technology. His research interests include Intrusion detection.

Xinyu Su, Student. Master, graduated from Zhongyuan University of Technology in 2016. Worked in Zhongyuan University of Technology. Her research interests include Knowledge graph.

Yunfei Han, Student. Master, graduated from Zhongyuan University of Technology in 2014. Worked in Zhongyuan University of Technology. Her research interests include IoT.