frontiers | Frontiers in Energy Research

TYPE Methods
PUBLISHED 06 January 2023
DOI 10.3389/fenrg.2022.1022231

OPEN ACCESS

EDITED BY
Hao Yu,
Tianjin University, China

REVIEWED BY
Xinjian Huang,
NARI Technology Co., Ltd., China
Lefeng Cheng,
Guangzhou University, China

*CORRESPONDENCE
Bo Wen,
wenbo1@hb.sgcc.com.cn

SPECIALTY SECTION
This article was submitted to Smart Grids,
a section of the journal
Frontiers in Energy Research

RECEIVED 18 August 2022
ACCEPTED 09 September 2022
PUBLISHED 06 January 2023

CITATION
Wen B, Li H, Zhang J, Han Q and Ding Z (2023), An intelligent analysis method of security and stability control strategy based on the knowledge graph. *Front. Energy Res.* 10:1022231. doi: 10.3389/fenrg.2022.1022231

An intelligent analysis method of security and stability control strategy based on the knowledge graph

Bo Wen[1]*, Hengxuan Li[1], Junhao Zhang[2], Qingqing Han[3] and Zehua Ding[3]

[1]State Grid Hubei Electric Power Company, Electric Power Research Institute, Wuhan, China, [2]School of Electrical Engineering, Southeast University, Nanjing, China, [3]Nanjing Dongbo Smart Energy Research Institute, Nanjing, China

The security and stability control system is the guarantee of the security and stability operation of the power grid. With the increasing scale of distributed new energy access to the power grid, the security and stability control strategy of the power grid is becoming more complex, and it is becoming increasingly important to correctly analyze and implement the security and stability control strategy. In order to ensure the correctness of the security and stability control strategy implemented by the security and stability control device, it is necessary to analyze the security and stability control strategy in detail. Therefore, this article proposes an intelligent analysis method of the security and stability control strategy based on the knowledge graph. First, this article introduces the ontology design method of the security and stability control strategy based on the knowledge graph, combines the characteristics and applications of the knowledge graph, analyzes the relationship between the elements of the strategy, and designs a clear-structured knowledge network. Second, this article analyzes the automatic construction technology of the graph, constructs the six-element ontology model of the security and stability control strategy, and realizes the human–computer interaction functions such as auxiliary decision making, strategy reasoning, and intelligent search based on the knowledge graph. Using artificial intelligence technology, this article takes the security and stability control strategy of a certain area's security and stability control system as an example to model and manage. The results show that it can assist the tester to quickly retrieve the strategy, effectively improve the detection efficiency of the security and stability control strategy, avoid the omission and ambiguity caused by the manual understanding of the strategy, and ensure the accuracy and comprehensiveness of the security and stability control strategy detection.

KEYWORDS

security and stability control strategy, knowledge graph, ontology design, security and stability control device detection technology, knowledge graph construction technology

Introduction

The security and stability control system is an important defense line to ensure the security and stability operation of a large power grid (Li et al., 2021), in which the security and stability control strategy is the core of the security and stability control device and system. The correct implementation of the security and stability control strategy is of great significance to ensure the security and stability of the power system.

Due to the regional differences in China's power grid, the security and stability control system and security and stability control devices are customized equipment, so there are differences in the language expression of the security and stability control strategy table in different regions. In recent years, with the expansion of complex AC and DC power grids, the grid connection of large-scale new energy, and the trend of power electronization of the power system, the interaction between power electronic devices in an increasing proportion will have a serious impact on the system (Cheng et al., 2018). The variable operation mode of the power grid leads to higher dimensions of the security and stability control strategy table, a large difference between the system operation condition and the ideal situation, and the mismatch of the security and stability control strategy is more likely to occur, and it is extremely difficult to manage and apply the strategy table manually.

At present, there are few research studies on the security and stability control detection technology, mainly focusing on the automation of the test process, the standardization of the strategy text, and the assistance of the decision-making system. Aiming at the shortcomings of traditional security and stability control testing methods, a set of intelligent debugging systems for security and stability control strategy has been developed, which can avoid the operation errors of the inspectors (Xiao et al., 2020). To improve the readability of the security and stability control strategy table, some standardized ideas are proposed by analyzing the detaiedl deviation of the security and stability control strategy text (Zhao and Gu, 2014). To provide reference for staff to take control measures in a timely manner, a power grid operation analysis system based on security and stability control strategy rules has been developed (Wang et al., 2018).

In order to cope with the increasingly complex power grid operation mode in the future, it is necessary to use intelligent means to analyze the security and stability control strategy to enrich the strategy retrieval means, so that testers can quickly and comprehensively obtain the strategy information and provide better assistance for the detection of security and stability control devices. To build a knowledge graph in the field of security and stability control strategy and better manage and represent the key information in the strategy can effectively improve the efficiency of testers when searching for strategies.

The new generation of artificial intelligence (AI), called AI 2.0, has recently become a research focus. Data-driven AI 2.0 will accelerate the development of smart energy and electric power systems (Smart EEPSs). In AI 2.0, machine learning (ML) forms a typical representative algorithm category used to achieve predictions and judgements by analyzing and learning from massive amounts of historical and synthetic data to help people make optimal decisions. ML has preliminarily been applied to the Smart Grid (SG) and Energy Internet (EI) fields, which are important Smart EEPS representatives (Cheng and Yu, 2019a). In order to solve the multi-energy scheduling optimization problem, the concept of intelligent scheduling based on parallel scheduling is proposed, which is called the parallel scheduling robot (PDR), and is used to realize intelligent scheduling robots based on intelligent artificial society (SAS) modeling (Cheng and Yu, 2019b). In order to better describe the evolution law of group behavior and predict individual decision-making behavior, the evolutionary equilibrium nature of the medium and long-term strategic bidding problem in the deregulated homogeneous and heterogeneous generation side market (PGM) under different market clearing mechanisms is studied. Based on the assumption of limited rationality and limited information, a general two-population n-strategy evolutionary game is proposed (Cheng et al., 2022).

Applying artificial intelligence to the field of security and stability control strategy, building a knowledge graph of security and stability control strategy, and better managing and expressing key information in the strategy can effectively improve the efficiency of testers when searching for strategies.

The construction of Chinese knowledge graphs has important research and application value for the processing and storage of Chinese information. It can change the existing information retrieval methods. On the one hand, it can realize concept retrieval through reasoning; on the other hand, the classified structured knowledge is displayed graphically (Liu et al., 2016).

The graph database in the knowledge graph has the advantages of storage and query, which is consistent with the requirements of security and stability control system strategy retrieval.

1) Storage: a graph database has flexible design patterns, and a knowledge graph can store different types of massive data. When the operation mode change strategy needs to be updated, the information can be updated based on the graph data.
2) Query: the application of graph databases strengthens the relational expressions and enables efficient relational queries. With the help of the relationship between nodes and node attributes, the security and stability control strategy information can be searched more conveniently and efficiently.

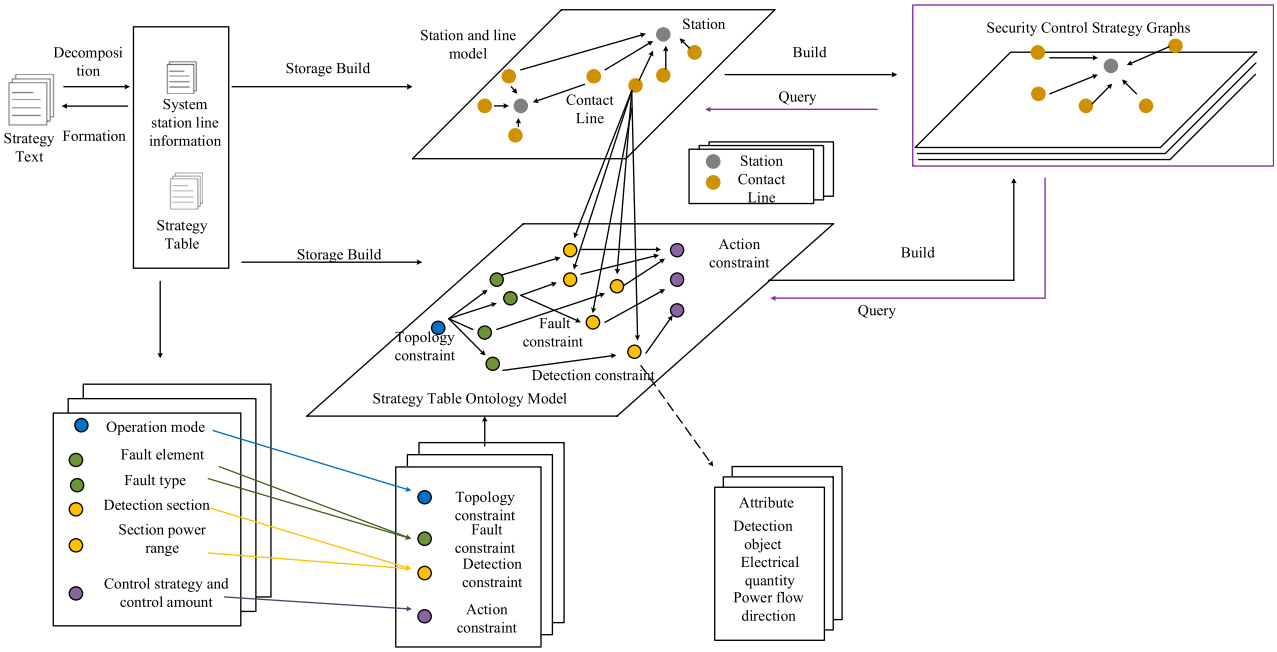

FIGURE 1
Modeling framework of security and stability control strategy based on the knowledge graph.

At present, no scholars have applied the knowledge graph to the field of security and stability control strategy. In this article, a domain knowledge graph is designed based on the low efficiency problem of security and stability control device detection. The purpose is to condense the logic in the actual query strategy, form an effective knowledge graph combined with the analysis of the strategy itself, and make intelligent decision making through the knowledge query.

Modeling of the security and stability control strategy based on the knowledge graph

The strategy retrieval of the security and stability control system needs to be queried in the corresponding system operation regulations. A strategy retrieval of the security and stability control system needs to obtain the specific strategy of the corresponding station in the device function requirements where the strategy is issued according to the fault tripping information and the corresponding cutting command. There are various forms of strategy description, including the description of collected information, strategy descriptions, and some fault-detailed strategy descriptions. The strategy description must cooperate with the corresponding strategy table. When searching, it is necessary to jump to the strategy table, which seriously affects the smoothness of the search. In some complex cases, it is necessary to rely on the notes in the remarks to find other information. In the actual test process, it is inefficient to retrieve strategies only by using the security and stability operation specification.

As the memory of the knowledge graph, the graph database can intelligently manage a large amount of information and construct a large-scale knowledge base so as to solve the low efficiency of security and stability control strategy retrieval.

Therefore, under the premise of understanding the security and stability control strategy retrieval problem and the performance of the knowledge graph, this article proposes a security and stability control strategy modeling framework based on the knowledge graph. As shown in Figure 1, first, the security and stability control strategy text is analyzed, and the relationship between its various elements is expounded. Second, the complete strategy is divided into two parts: the strategy table and the station and line information, and their ontology model are designed, respectively. Finally, a complete knowledge graph of security and stability control strategy is realized by combining the two contents and constructing a six-element ontology model of stability control strategy. All the key elements of the policy table can be visually displayed during policy retrieval, which improves the efficiency of policy retrieval for testers.

Strategy table text analysis

Before designing the knowledge graph ontology, analyze the text information of the strategy first.

TABLE 1 Strategy table for section composition of Yuanhuan I, II lines, Shibo line, and Boyuan line.

Topological constraint	Steady-state frequency (Hz)	Detect constraint		Action constraint		
Operation mode	**Fault component**	**Fault type**	**Inspection section**	**Section power range**	**Control measure and quantity**	**Strategy supplement**
Normal mode	Any one of Yuanhuan I, II lines	Interphase faults	Gushanjiahe	≥475	150 (R3)	Maximum output of a single machine in Gushanjiahe does not exceed 35 MW
				≥560	300 (R3)	
	Lijiayuan #2 bus	Single-phase permanent faults and no fault	Yuanhuan I, II lines	≥560	300 (R1)	
				≥630	450 (R1)	
		Busbar tripping	Yuanyun line	≥475	150 (R3)	
				≥560	300 (R3)	

The presentation of the security and stability control strategy table of the power system in various regions of China is different, but there is a correlation between the constituent elements of the strategy table. The strategy table is mainly composed of non-representational elements such as operation mode, fault element, fault type, detection section, section power range, control measures, and control quantity, remarks. This article analyzes the document "Shiyan security and stability control system security and stability operation regulations" issued by a regional power company; that is, the security and stability control strategy table described in the document. Take one of the strategies as an example. As shown in Table 1, the strategy table is composed of the sections of Yuanhuan I, II lines, Shibo line, and Boyuan line.

1) Operation mode: the division of the strategy table is based on the section formed by the transmission lines. A security and stability operation regulation contains several strategy tables, including all possible system operation modes in the security and stability control system. The operation mode here refers to the operation condition of a certain line, such as the normal operation mode, the shutdown of a certain line, and the shutdown of any double-circuit line. The operation mode is the basis of the operation mode.
2) Fault components: the fault elements in the strategy table follow the operation mode, but the content is not closely related to the operation mode. The lines in the fault components are related to the lines that constitute the current section strategy table. Some complex strategies include bus faults. For example, if the fault component is "any bus in the East Ring Road," this information needs to be queried in the operation regulations, "bus wiring requirements of some substations," and cannot be obtained from the title of the strategy table.
3) Fault type: fault types can be roughly divided into line faults, including interphase faults, single-phase permanent faults, and transformer faults such as bus tripping. A complete fault logic includes the information of fault components and fault types. For different fault components, the fault types are different, so the fault types and fault components are in parallel in the actual strategy.
4) Inspection section: the power flow situation is reflected here, and the complex power flow situation has different judgement basis and specific constraints. Some detection sections are annotated with upper corner marks, which are generally strong constraints that restrict whether this strategy is enabled, thus affecting the judgement of the whole strategy. The detection section is not directly related to the operation mode, fault element, and fault type, it presents a parallel relationship.
5) Section power range: as the most divided part of the strategy table, the existence of a section power range makes the whole strategy table into a complex causal network.
6) Control measures and quantities: as the last component elements in the strategy table, control measures, and control quantities are the end of each specific strategy. All specific strategies begin with the operation mode and end in the control action. Its text content has control quantity and control sequence number, and the specific control measures must find the corresponding cutting sequence.
7) Strategy supplement: from the aforementioned analysis, it is clear that the constituent elements in the strategy table have different meanings and are intricately connected with each other. The complicated conditions lead to a large number of parallel relationships among the elements in the strategy table, and these parallel relationships must be processed to achieve intuitive strategy retrieval.

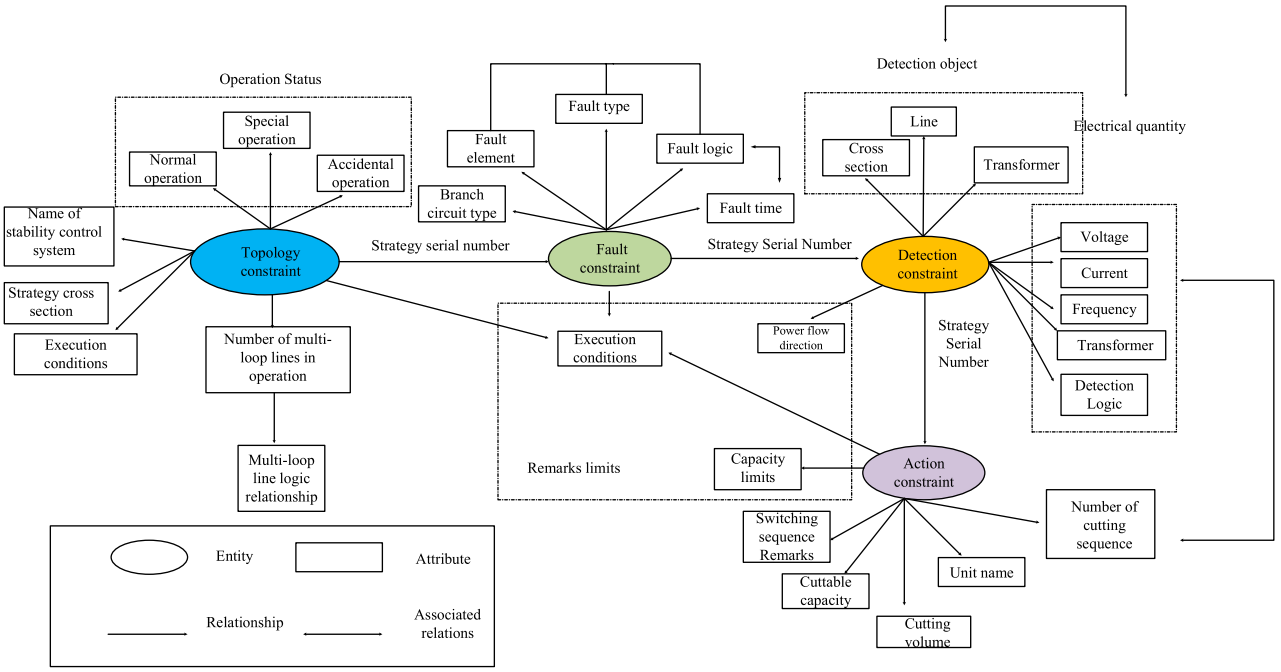

FIGURE 2
Four-element ontology model for control strategy.

Ontology model design for policy-oriented tables

In this article, we propose an ontology model with the policy serial number as the connecting relationship. The key elements of the whole strategy table can be shown intuitively by searching only the relationship name, i.e., the strategy number, which is the key information for the testers to retrieve the strategy, and the elements of the strategy table can be arranged in the form of a line, which is suitable for the human way of thinking. In addition to the fusion of the elements, if the aforementioned seven types of elements are used individually as nodes and connected, the large number of parallel relationships within them will inevitably lead to interleaved connections. By compressing the seven types of data into four categories, the interlacing of connection lines is greatly reduced, and an intuitive and logical retrieval strategy is achieved.

In this article, an ontology model for policy-oriented tables is designed based on the representation of RDF triples, and the entities, attributes, and entity relationships in the triples are set in detail, as shown in Figure 2.

In this quadratic ontology model, topological constraints are used as the starting point. Since the strategy serial number has been defined as an entity relationship, testers can retrieve the whole strategy by simply looking up by entity relationship. To optimize the layout design of the whole knowledge graph, the specific security and stability control system name and the line section to which it belongs are set in the topological constraint as attributes reflecting the strategy title. According to the different system states, the topological constraints have three attributes, according to which the state types can be quickly determined, which are normal operation, special operation, and accident operation. For example, normal operation refers to normal plan; special operation refers to the maintenance of trunk lines, interconnection transformers and other equipment. In addition, the attribute also contains the number of multiple circuits in operation and logical relationships.

The fault constraint is the combination of faulty components and fault types, which can uniquely identify the relevant fault information and cover all fault conditions under the policy. Its attributes are branch type, fault line, fault type, the number of branches contained in the section, and the time of failure. In some complex strategies, two or more faults can occur at the same time, so it is also necessary to construct an attribute characterizing the logical relationship to determine the successive faults of the line as well as the logic of the time interval between different faults, such as “with” and “or”.

The monitoring constraint node is a combination of the detection section and the section power range, which is used to describe the range of electrical quantities detected by the strategy object. The entity attributes have two kinds of detection objects: electrical quantities and the detection objects include sections, lines, transformers, etc. The electrical quantities are traditional voltage, current, frequency, power flow, etc. The power flow

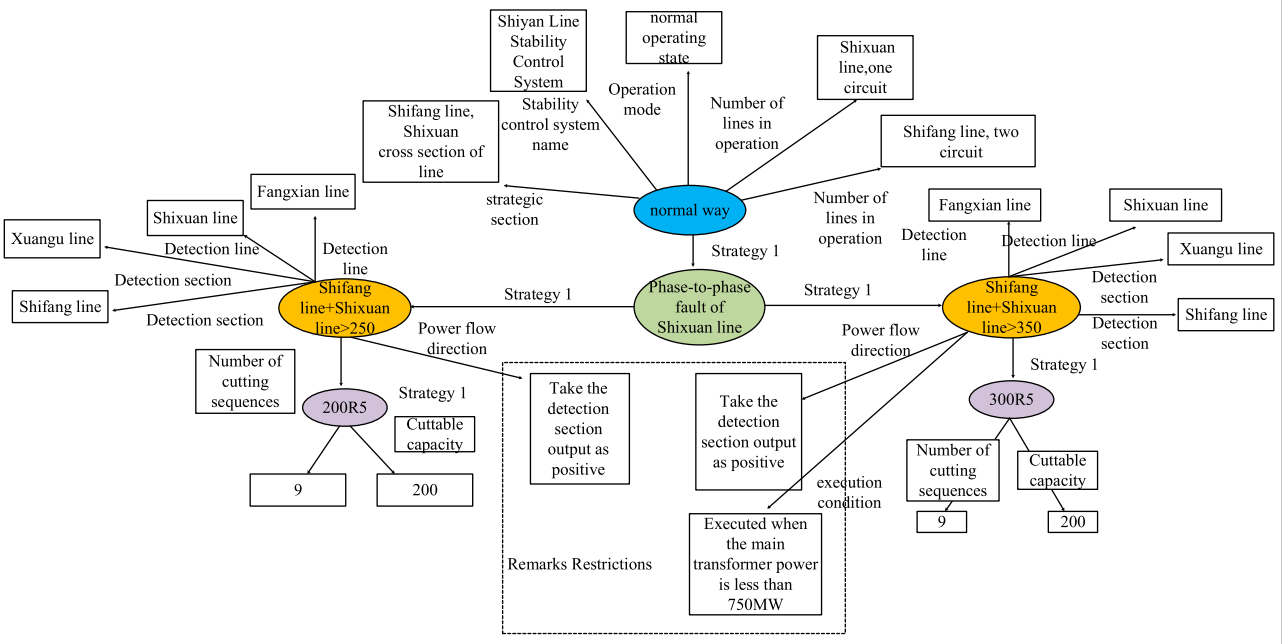

FIGURE 3
Example of the security and stability control system strategy.

direction is generally judged based on the comments in the remarks. Similar to the fault constraint, part of the strategy executes the corresponding control measures based on the tide of multiple transport cross sections, and the detection logic term should be added to the properties of the detection constraint.

The action constraint is the control measure and control quantity in the policy table, and the focus here is on the generator tripping quantity and generator tripping sequence. The generator tripping quantity is characterized by numbers, while the specific information of the generator tripping sequence is used as the attribute of the action constraint node, which mainly contains the number of generator tripping sequences, unit name, generator tripping capacity, and generator tripping sequence remarks.

The remarks in the strategy table can be summarized as power flow direction, execution conditions, output limits, etc. Power flow direction and output limit can be used as additional attributes of detection constraints and action constraints respectively, while the execution condition is more complicated, and the amount of cut machine in the action constraint must be limited according to the topology constraint and fault constraint in special cases, so the three nodes of topology constraint, fault constraint, and action constraint still need the additional attribute of execution condition.

Taking a certain strategy in a regional security and stability control system as an example, first, the nodes are established according to the four constraints of the quaternion ontology model. The relationship between each node is connected by the strategy name. When retrieving the strategy, only the entity relationship "strategy 1" is searched, which can achieve the effect shown in Figure 3. Different constraints are colored differently so that their types can be quickly determined. The properties of each node are designed according to the aforementioned quaternion ontology model, and the remarks contain restrictions on the detection section direction and the execution conditions in a certain case, which are added to the respective "detection constraints" nodes as additional properties of "tide direction" and "execution conditions," respectively.

Ontology model design for security and stability control system-oriented policy

In the query strategy, the inspector not only needs the key information in the strategy table, but also needs to quickly locate the monitoring line of the station. In the previous section, all the information in the strategy table can be presented by the quaternion ontology model and only need to establish the relationship between station, contact line, and detection section to complete the model design of the whole safety control strategy.

In addition to the important elements in the strategy table, the complete strategy should also include the information of system stations and monitoring lines. Therefore, it is necessary to add two entities, "stations" and "contact lines". The "stations"

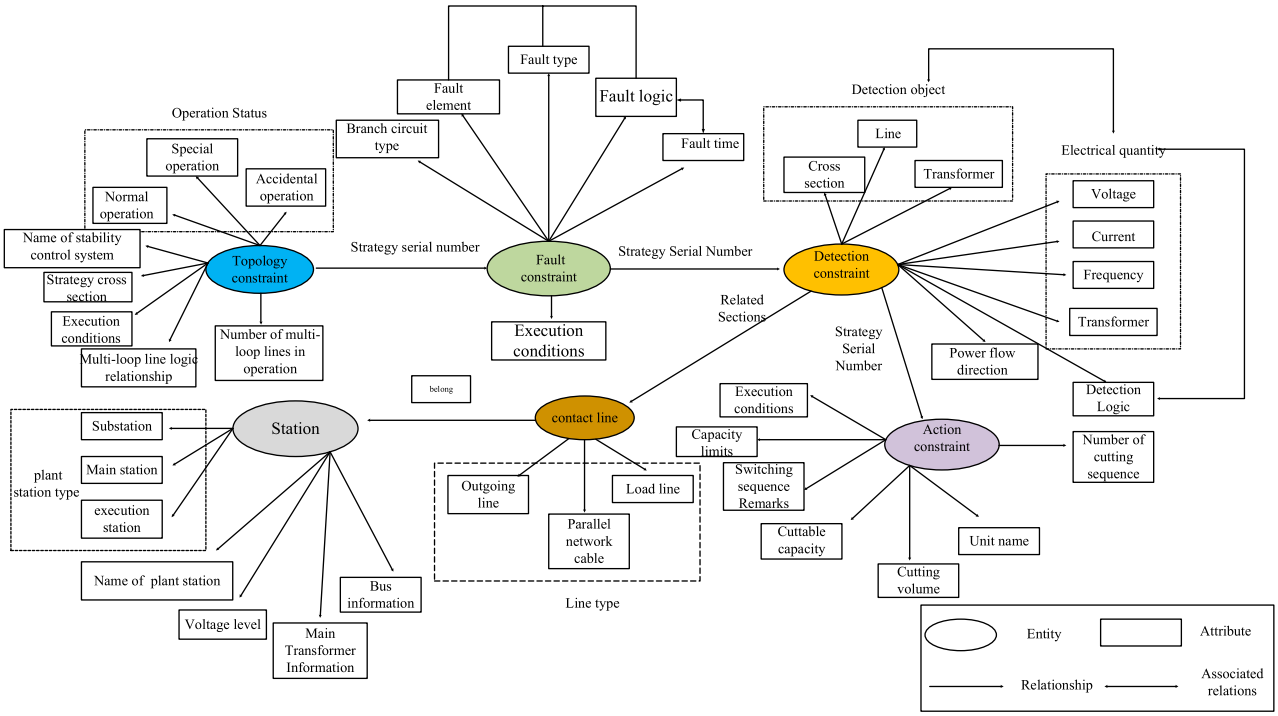

FIGURE 4
Six-element ontology model for the control strategy.

node has four attributes to describe a complete station layout: station name, voltage level, main substation, busbar, wiring, and station type. The "contact line" acts as a node connected to the monitoring stations but also connects to its relevant test section.

The two new entities, station and contact line, are connected to the previous quaternion ontology model to establish the connection of station–contact line–detection cross section–fault information to achieve the strategy information modeled. So far, the complete strategy information can be completely represented by the knowledge graph, and the specific model is shown in Figure 4. The six-element ontology model for security control strategy includes six entities: topology constraint, fault constraint, detection constraint, action constraint, station, and contact line, and each entity has its own related relationship and attributes.

Automatic construction technology of the security and stability control strategy knowledge graph

Since most of the data in the strategy table is structured, the policy entity graph can be constructed on the basis of the original structured database, and for unstructured data such as strategy descriptions and strategy table notes, natural language processing (NLP) related techniques are used. By means of knowledge extraction, entities, relationships, attributes, and other elements are extracted from the text to form useful information by disambiguation, and further integrated and refined by knowledge processing. Event extraction performs knowledge extraction and representation of strategy descriptions. The knowledge update updates the knowledge graph when the strategy table format is changed and new strategies are added

Ontology model design for policy-oriented tables

Knowledge extraction is a technical means to convert semi/unstructured data into structured data, mainly including the extraction of entity, relationship, and attribute knowledge elements (Cheng et al., 2022). Among the automatically constructed means, machine learning-based knowledge extraction methods are widely used.

Entity extraction, named entity recognition (NER) technology. In the field of safety and control policy, entity extraction is required to identify and mark the information elements in the policy table, policy description, and security and stability control technical specifications such as classification

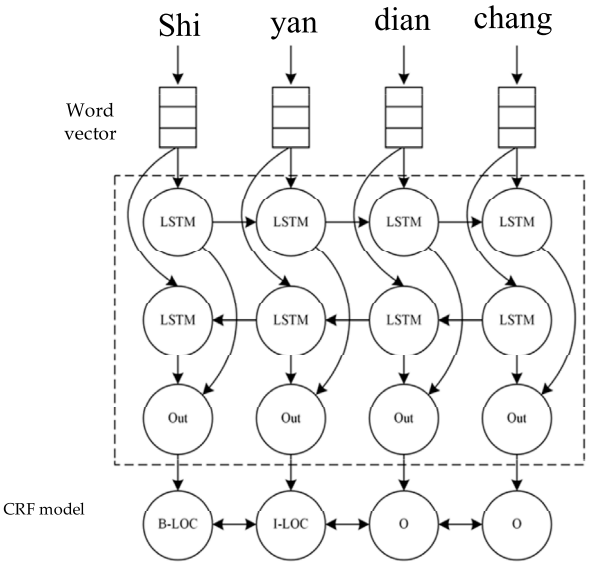

FIGURE 5
Bidirectional LSTM and CRF model for entity recognition.

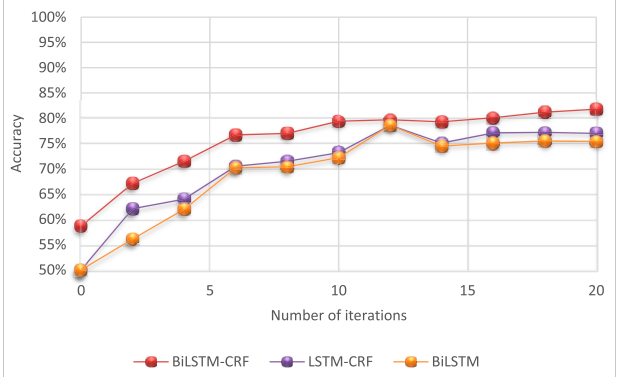

FIGURE 6
Accuracy of intelligent algorithm in processing long texts information and overlapping texts information.

operation status, fault information, detection section information, station name, and line name. Entity extraction generally uses neural network model. The neural network model will automatically capture effective features from the text. The mainstream models include hidden Markov model (Cen et al., 2008), conditional random field (Liu and Wang, 2018), and BiLSTM model (Thomas and Sangeetha, 2019). At present, the same effect as that of the traditional rule extraction method BiLSTM can greatly reduce the computation. Second, the deep neural network is a feature-progressive learning algorithm, and shallow neurons directly learn some low-level simple features from the input data, such as edges and textures. While deep features continue to learn higher-level features based on the learned shallow features and learn deep semantic information from the perspective of computers. The increase of hidden layers means that the number of nested layers of nonlinear transformation brought by the activation function is more, so that more complex mapping relationships can be constructed and richer data features can be extracted. The BiLSTM in this article processes all the texts of the security and stability control strategy. The use of deep neural networks has become the mainstream. Taking the most commonly used BiLSTM + CRF model as an example, Figure 5 shows that the four Chinese characters of "Shiyan dian chang" are transformed into word vectors that can be recognized by the computer. The word vector is then fed as input into the LSTM feature extractor to obtain a feature representation of the sequence, and the BiLSTM is able to improve the feature extraction capability of the model by being able to use the sequence information after that moment when extracting features at a certain moment. Finally, the CRF conditional random field model is used as a decoding tool to transform the output of the previous layer into NER labeled sequences, and the two characters of "Shiyan" are successfully labeled as toponymic entities. The advantage of CRF is that it can predict the hidden state sequence by observing the sequence. We also compared the accuracy of processing long text information and overlapping text information by BiLSTM-CRF with that of BiLSTM and LSTM-CRF methods, as shown in Figure 6. The accuracy of BiLSTM-CRF is obviously superior to other methods.

Relationship extraction: after the entity extraction of strategy text, a series of discrete named entities are obtained, and then the semantic information is obtained through relationship extraction to link the strategy entities before a web-like knowledge structure can be formed. There are two main difficulties concerning the relationship extraction of strategy text: relationship overlap and long-text information.

1) Overlapping relationships: there are complex relationships among the key information in the security and stability control strategy. 1) Single-entity overlap (SEO): in the strategy table, the text content of both the fault element and the detection section is "Shibai line," so the fault constraint and "Shibai line" and the detection constraint and "Shibai line," the two triads, have the entity "Shibai line," resulting in a single entity overlap problem. 2) Entity pair overlap (EPO): strategy 1 and strategy 2 have the same operation mode and fault element information, but the operation mode and the fault element have both "strategy 1" and "strategy 2" entity relationships; that is, there are multiple relationships between an entity pair. 3) Subject–object overlap (SOO), such as: "Shixuan line" and "Shiyan station" have a subordinate relationship; "Shixuan line" is the object of "Shiyan station," and "Shixuan line" is the

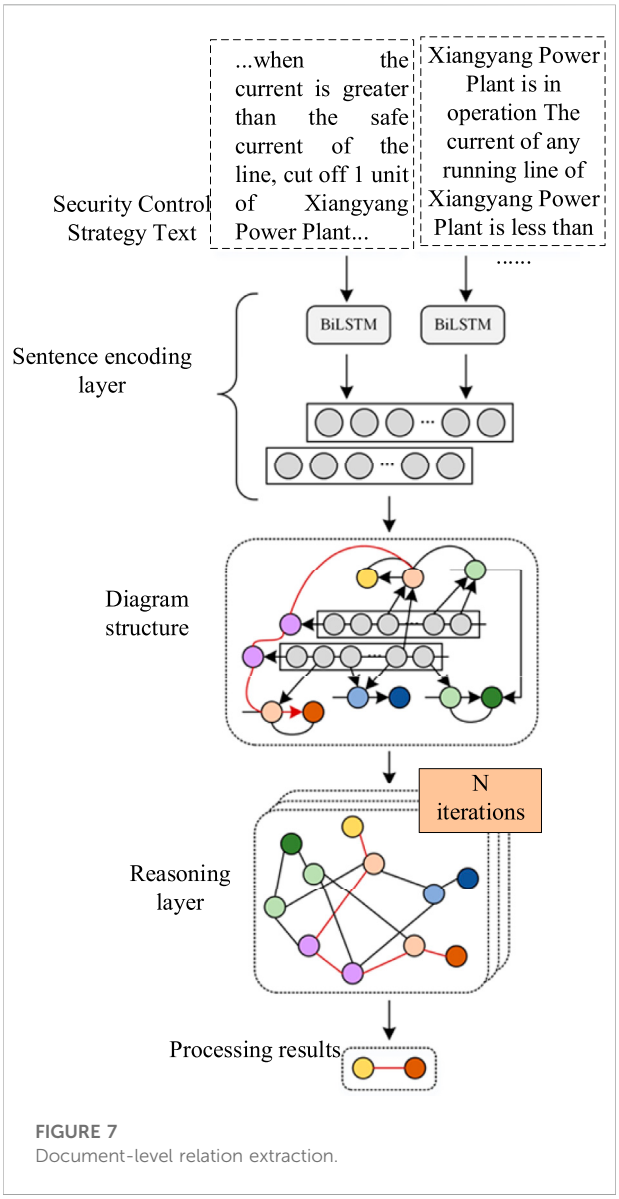

FIGURE 7
Document-level relation extraction.

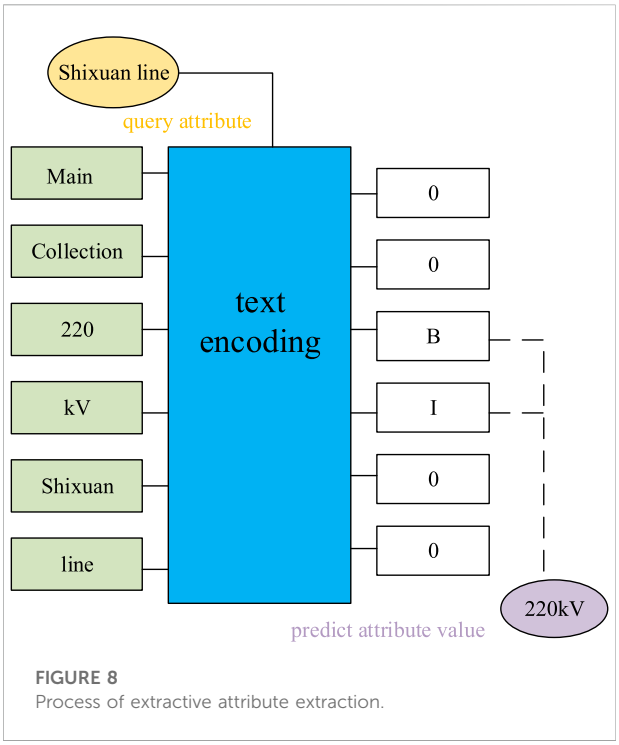

FIGURE 8
Process of extractive attribute extraction.

subject of "detection constraints," there will be a phenomenon that an entity is both subject and object of the phenomenon.

2) Long text or document-level information: in a strategy description, each sentence is basically composed of two entities. In order to obtain the station information, line information, and other entities and their relationships from the technical specification, it is necessary to use relationship extraction at the level of both long text and document. Compared with other types of documents, the complexity of security and stability control policy information is higher, which is mainly reflected in serious ambiguity problems, more information jumping phenomena between paragraphs, and difficult to identify professional terms. Moreover, there are often a large number of simplified terms in long documents, which cannot be identified by non-specialists. The document graph-based approach is more suitable for relationship extraction of security and stability control policies, as it has more advantages for handling the complex logic of security and stability control policies. A heuristic approach to construct graph structure is proposed (Christopoulou et al., 2019), as shown in Figure 7, to train a path, connecting two entities and iteratively weighing the information on that path several times, thus passing the information on the path to reasoning effect.

Attribute extraction [12] is the extraction of attributes and attribute-value pairs (AVP), which in turn complements the complete information of the entity. For example, as shown in Figure 8, the input information is "mainly collecting 220 kV Shixuan line". By extracting the words in the input text, the predicted attribute value is composed, and finally, the attribute value is 220 kV. For such highly structured texts as security and stability control strategy tables, the regular information in them can be directly extracted from the entity corresponding attribute names and attribute values (Huang et al., 2019). For highly structured text, such as security and stability control strategy tables, the attribute name and attribute value corresponding to the entity can be directly extracted from the regular information. For the technical specifications with different forms, semi-structured policy descriptions and unstructured long texts, it is more stable to use data mining methods. The relationship patterns

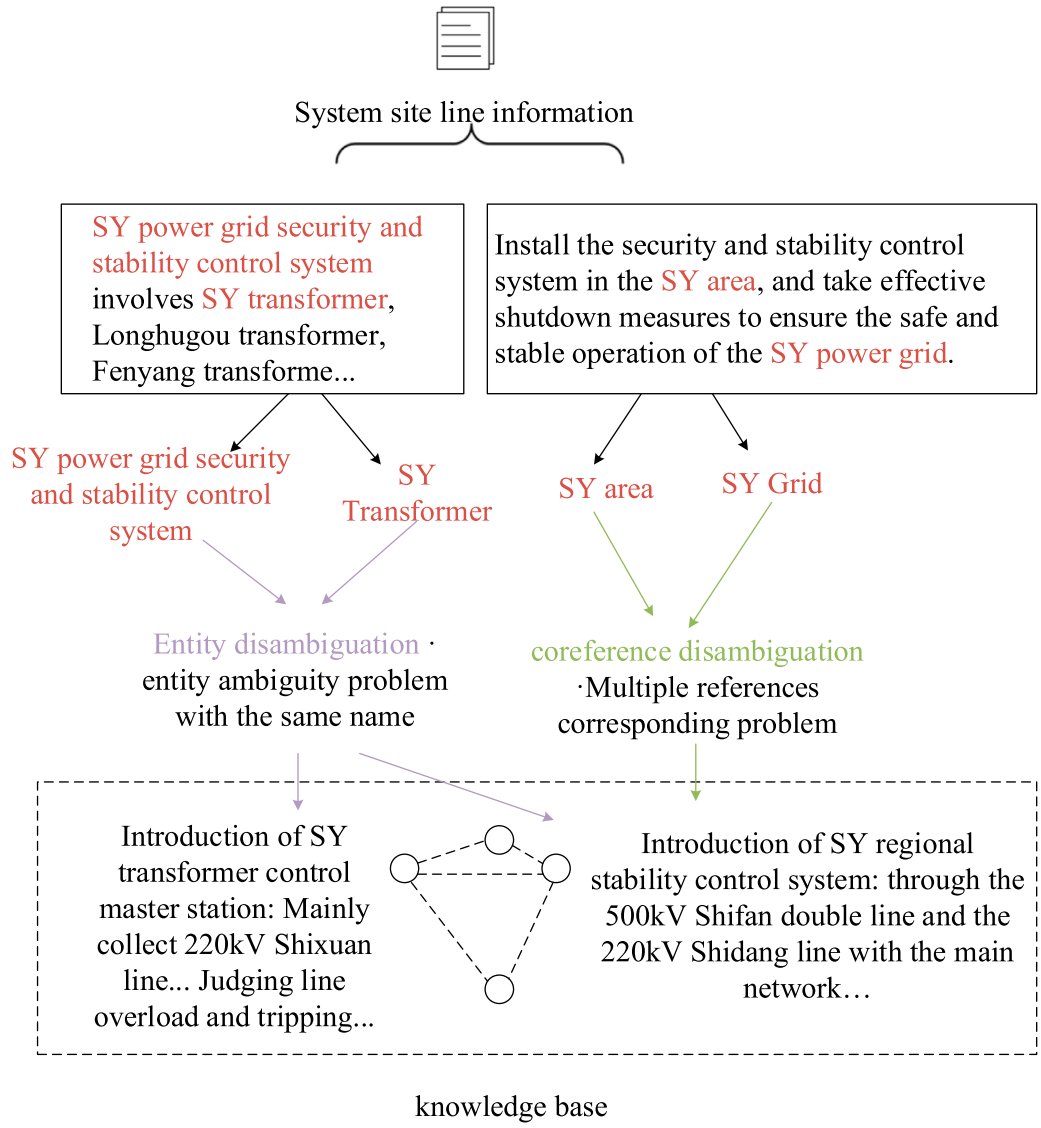

FIGURE 9
Entity link diagram.

between entity attributes and attribute values are directly mined from these texts, so as to complete the positioning of attribute names and attribute values. In the actual security and stability control strategy text, many attribute values have attribute names near them to constrain their meaning, such as "the voltage level of the Shixuan line is 220 kV," where "kV" is the attribute name of "voltage level" and "220″ is the attribute value of "voltage level", which are often called famous attributes in NLP technology, so these keywords can be used to locate the attribute values of famous attributes (Wang et al., 2010).

The knowledge graph for security and stability control strategy belongs to the professional domain graph, and it has high requirements on information quality and the error tolerance rate of information noise compared with the more widely used common sense knowledge graph.

Knowledge fusion

In the complex knowledge sources of security and stability control strategy, there are problems such as knowledge duplication of different data sources, fuzzy correlation between knowledge, and poor extraction quality (Lin et al., 2017). So, it is necessary to integrate, disambiguate, and process the security and stability control strategy

knowledge with multi-source heterogeneity, semantic diversity, and serious ambiguity problems. After obtaining entities, relationships, and attributes from the data of various types of structures through information extraction, the results often contain a large amount of redundant and erroneous information, and the relationships between the data lack hierarchy and logic. Knowledge fusion mainly includes entity linking and knowledge fusion, through which knowledge fusion can eliminate ambiguity and thus ensure the quality of knowledge.

In order to be able to establish the semantic linkage existing between entities, it is necessary to use the co-linear relationship of entities and link multiple synonymous entities to the knowledge base at the same time to complete the collective entity linking. The process of entity linking is as follows: 1) entity recognition is used to extract entity items from strategic text; 2) conduct entity disambiguation and coreference resolution to judge whether entities with different names have the same meaning; 3) after defining the entity object, link to the corresponding entity in the knowledge base, as shown in Figure 9.

1) Entity disambiguation: entity disambiguation is a technology used to solve the entity ambiguity problem of the same name. For example, the referent "SY" can correspond to the name of the security and stability control system "SY grid security and stability control system" in a certain region, or it can refer to the name of a substation "SY substation. " By entity disambiguation, it is possible to link the semantics of the context and establish entity links accurately, and the key lies in how to define the similarity between entity objects and referent items, and the commonly used methods are social network models (Wang H. et al., 2013), spatial vector models (Pedersen et al., 2005), and semantic models (Riesbeck and Schank, 2013). Entity disambiguation techniques can also help intelligent search applications better understand the user's search intent and improve search quality. Entity disambiguation is important for knowledge graphs in terms of search applications in the field of security and stability control strategy.
2) Entity resolution: entity resolution technology is mainly used to solve the problem ofmultiple referents corresponding to the same entity object. For example, in the technical specification, "Fangxian substation," "Fangxian main substation," and "Fangxian 1# main substation" all point to the same entity, and the pronouns in them, such as the term "its" may also refer to the same entity, and the co-referencing technology can be used to associate these referents to their corresponding entities. Pantel proposed an entity similarity measure model called term similarity (Shi, 2013), which can be used to obtain statistically significant similarity among all terms from the global corpus with the help of a word model to achieve entity resolution.

Knowledge processing

After information extraction and knowledge fusion, a series of basic factual expressions can be obtained; however, the facts themselves are not exactly the same as knowledge. It must be processed by knowledge in order to realize a structured and networked knowledge system. Knowledge processing mainly includes two parts: ontology construction and knowledge reasoning.

1) Ontology construction: ontology is the rule for modeling concepts, formulating a model of what is to be depicted, and giving a normative definition of each concept and the relationships between them. The ontology design of the security and stability control strategy has been introduced in detail in the previous section, and its structure is similar to a tree structure with strict "IsA" affiliation between nodes at adjacent levels. The relationship can better reason with knowledge and cope with the complex logic of security and stability control strategies. For the field of security and stability control strategy, the construction of ontology using a manual approach is not only a huge workload but also requires the collaboration of experts. Therefore, a computer-assisted, data-driven approach can be used to automate the construction, coupled with algorithmic evaluation and manual audit.

The data-driven automated ontology construction process mainly includes: entity parallelism similarity calculation, entity contextual relationship extraction, and ontology generation (Wong et al., 2012). 1) Entity parallel relationship similarity is mainly used to distinguish entity parallel relationship, such as "Shidang line," "Shundang line," and "Yuandang line" as line name entities, with high parallel relationship similarity. The possibility that the two entities "Shiyanchang line" and "Shibai line" belong to the same semantic category is low, and the similarity of the juxtaposition is low. 2) Entity hyponymy extraction is mainly used to confirm the subordination (ISA) relationship between nodes; that is, the hyponymy relationship, such as "Panshi line" and "connecting line," where "connecting line" is the upper word, and "Panshi line" is the lower word. The main research method is to extract isa entity pairs based on grammatical patterns (Wang C et al., 2013). 3) The main task of ontology generation is to aggregate all the concepts obtained at all levels and calibrate their semantic classes. As for the problem of model applicability for short texts, Wang H. et al. (2013) proposed a topic clustering and superordinate word extraction model based on a term co-occurrence network to achieve topic clustering based on short texts.

2) Knowledge reasoning: after initially establishing the knowledge base of security and stability control strategy, knowledge reasoning further excavates the hidden

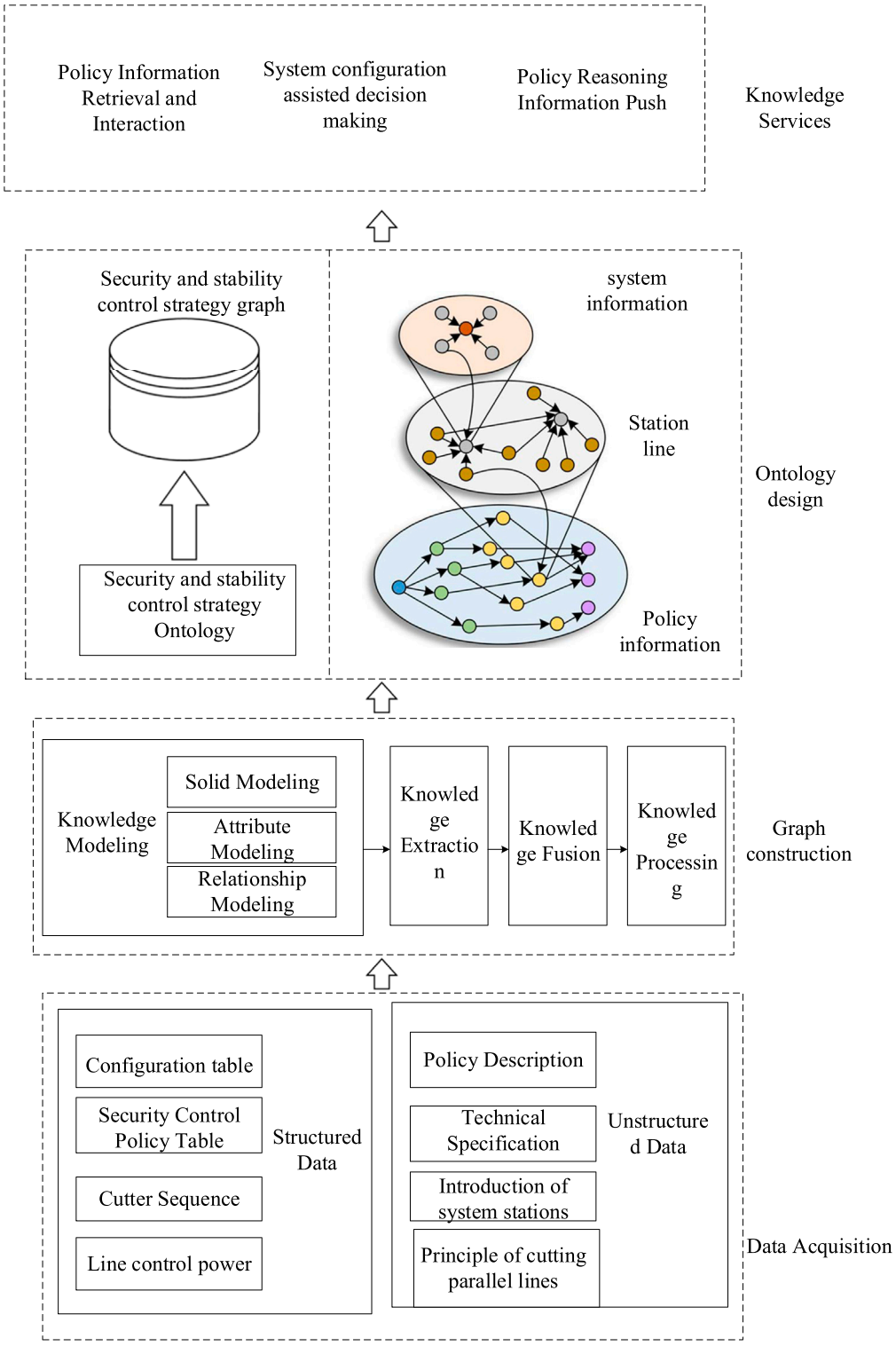

FIGURE 10
Security and stability control strategy knowledge graph construction framework.

knowledge on its basis, so as to expand the knowledge base. In the security and stability control strategy knowledge graph, knowledge inference can help testers search for strategy, system configuration, station information, etc. However, the field of security and stability control strategy has its own particularity. Even for the same fault and detection section, the action will take different actions according to the running state. Therefore, the knowledge graph of the security and stability control strategy must deal with a large amount of the same or contradictory information.

Artificial intelligence technology is good at filtering out useless information from massive security and stability control strategy data, which can improve the efficiency and accuracy of knowledge reasoning. At present, the commonly used models include artificial neural network models, genetic algorithms, back propagation network models, etc.

We use the knowledge graph as the data source, while graph-based inference uses the knowledge graph as the graph, the security and stability control policy as the node, and the relationship between entities as the edge and analyzes the semantic relationship through the multi-step paths between multiple entities in the graph by using the information embedded in the relational paths.

3) Knowledge update: with the operation of the security and stability control system constantly changing, the format and content of the security and stability control strategy need to be constantly improved. Logically, the update of the security and stability control strategy knowledge base includes the update of the concept layer and the update of the data layer. After the update of the knowledge base, new concepts will be obtained. At the same time, new concepts need to be added to the concept layer of the knowledge base. The update of the data layer is mainly the update of the triple of entities, relationships, and attributes. For example, after adding a new operation mode, a series of information will be updated to the knowledge base. The new operation mode will be added to the concept layer in the form of a concept. In the data layer, entities such as "topology constraint," "fault constraint," and "detection constraint" will be added, and new values will be added to their relationships and attributes. The construction framework of the security and stability control strategy knowledge graph is shown in Figure 10.

Knowledge service based on the knowledge graph

The knowledge graph provides a more convenient means to express, organize, and manage the massive, heterogeneous, and complex data in the security and stability control strategy, and improves the intelligence of the test system, which is closer to the human way of thinking. When testers test the security and stability control device, the upper computer software requires first configuring a large amount of information about the security and stability control system. The information is not friendly enough to help testers sort out useful information, and most of the configurations are filled out in plain text, requiring testers to consult the relevant strategy text and technical manuals. In the future, with the advancement of knowledge graph technology and its in-depth application in the field of security and stability control, knowledge graph technology can play a great role in assisting decision making, policy reasoning, and information pushing in system configuration, as shown in Figure 11.

1) Information retrieval and interaction: intelligent search based on the knowledge graph can accurately capture and understand the search intention of testers and confirm the specific entity target to look for. Due to the fact that there are many entities, search results need to be presented in an appropriate way. In addition to the core target entity, other related entities need to be characterized. It is necessary to adopt a method similar to natural language processing to disambiguate, for example, the query "Shixuan line fault," which can be understood as "Shixuan line fault" or "Shixuan line fault type," etc. Generally, the intention of the tester is to obtain the situation of the line as a fault component rather than the fault type of the line.
2) Information push: it quickly and briefly exposes internal information to the tester. When performing special case device testing, the testers are required to semi-automate the system configuration and strategy input without following the inherent fault set and then push the base configuration data based on the tester's choice. The system must achieve the maximum collection of data and continuously clip information to the operation of testers to complete the test configuration.
3) Auxiliary decision making of system configuration: based on the guidance of human behavior ideas, it assists testers to complete the configuration of the security and stability control system. The configuration work of the security and stability control system includes the convergence judgement of station information, line information, and fault range, replacing the testers to consult the strategy table and then configure the process, which not only omits the tedious and time-consuming mechanical tasks but also avoids manual errors.
4) Strategic reasoning: based on the human behavior trajectory, the selection and import of strategies are completed. Intelligent adaptation is achieved thanks to

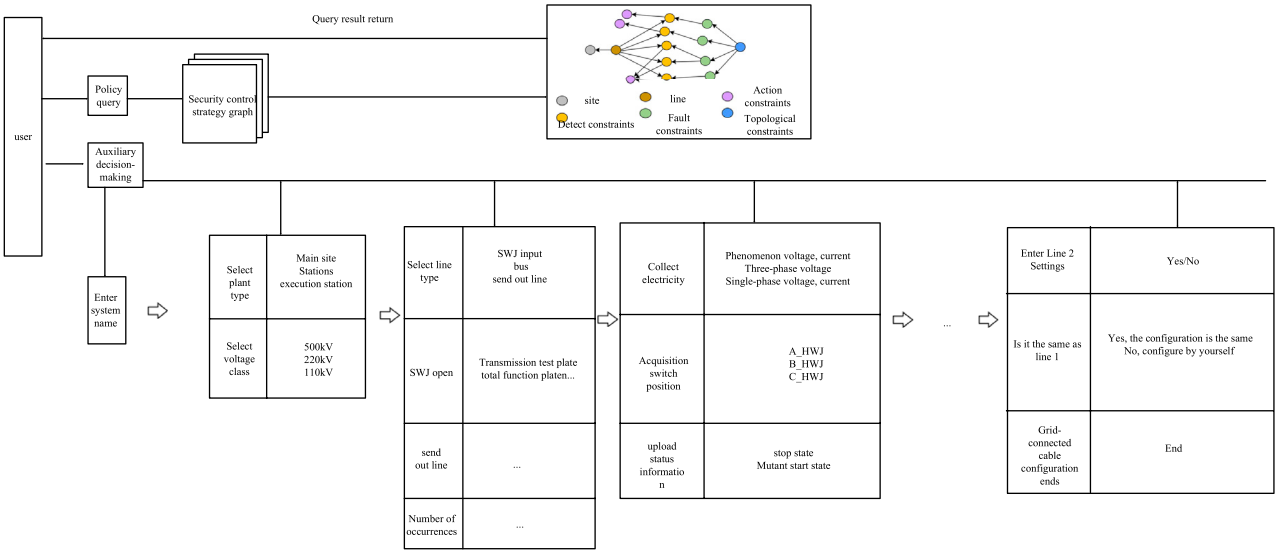

FIGURE 11
Application of security and stability control strategy technology based on the knowledge graph.

1) the function of each type of station is determined, and the fault set is fixed. 2) The possibility of fault judgement at the location can be predicted when the system is configured. Based on the station type and line configuration, the human behavior trajectory is predicted in combination with the content of the fault policy to complete the strategy inference.

Conclusion

With the rapid development of complex AC/DC power grids and large-scale new energy grid connections, the operation mode of the power grid becomes more and more variable, and the corresponding security and stability control system security and stability operation control strategy becomes more and more complex. In order to ensure the accuracy and comprehensiveness of stability control strategy detection and improve the efficiency of strategy detection, this article proposes an intelligent analysis method for security control strategy based on the knowledge graph.

1) It points out the problems faced by the strategy detection of security and stability control system with the development of the power grid in the emerging stage. Combining with the characteristics and practical values of the knowledge graph, an artificial intelligence technology, it proposes to apply the knowledge graph to the analysis of security and stability control strategy.

2) It explains in detail the modeling process of security and stability control strategy based on the knowledge graph, analyzes each constituent element in the strategy text, follows the research idea of “data analysis - > ontology modeling - > knowledge base construction,” takes the security and stability control strategy of a certain region’s security and stability control system as an example to show the overall modeling process, and explains that the built model can improve the detection efficiency of security and stability control strategy and ensure accurate and comprehensive detection of security and stability control strategy.

The artificial intelligence technology represented by the knowledge graph has opened a new direction for the research of security and stability control strategy and the development of security and stability control strategy detection technology. The authors hope that in the future, by expanding and improving the knowledge graph of security and stability control strategy, the strategy data can be further studied, and the new form of development of artificial intelligence technology in the field of security and stability control system can be promoted.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material; further inquiries can be directed to the corresponding author.

Author contributions

BW: methodology, software, validation, investigation, data curation, writing—original draft preparation, and visualization. HL: methodology, formal analysis, and supervision. JZ: conceptualization, validation, and writing—review and editing. QH: resources and writing—review and editing. ZD: conceptualization, investigation, and visualization.

Funding

This work was supported by the National Natural Science Foundation of China, grant number 51877037, and the Technology Project of State Grid Hubei Electric Power Co., Ltd., grant number 521532210003.

Conflict of interest

Authors BW and HL were employed by the company State Grid Hubei Electric Power Company Electric Power Research Institute.

The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Cen, Y., Han, Z., and Ji, P. (2008). Chinese term recogni-tion based on hidden Markov model. 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, 19-20 Dec 2008, Wuhan, China, 54–58.

Cheng, L. F., Chen, Y., and Liu, G. Y. (2022). 2PnS-EG: A general two-population n-strategy evolutionary game for strategic long-term bidding in a deregulated market under different market clearing mechanisms. *Int. J. Electr. Power & Energy Syst.* 142, 108182. Part A, Article ID 108182, Nov. 2022. doi:10.1016/j.ijepes.2022.108182

Cheng, L. F., and Yu, T. (2019a). A new generation of AI: A review and perspective on machine learning technologies applied to smart energy and electric power systems. *Int. J. Energy Res.* 43 (6), 1928–1973. doi:10.1002/er.4333

Cheng, L. F., and Yu, T. (2019b). Smart dispatching for energy internet with complex cyber-physical-social systems: A parallel dispatch perspective. *Int. J. Energy Res.* 43 (8), 3080–3133. doi:10.1002/er.4384

Cheng, L., Yu, T., and Zhang, X. (2018). Cyber-physical-social systems based smart energy robotic dispatcher and its knowledge automation: Framework, techniques and challenges. *Proc. Chin. Soc. Electr. Eng.* 38 (01), 25–40. doi:10.13334/j.0258-8013.pcsee.171856

Christopoulou, F., Miwa, M., and Ananiadou, S. (2019). "Connecting the dots: Document-level neural relation extraction with edge-oriented graphs," in Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), Hong Kong, 2019.

Huang, H., Yu, J., and Liao, X. (2019). Review on knowledge graphs. *Comput. Syst. Appl.* 28 (06), 1–12.

Li, M., Ni, M., and Yan, Y. (2021). Cyber-Physical coordinated defense method against malicious attacks for security and security and stability control system. *Automation Electr. Power Syst.* 45 (18), 113–121.

Lin, H., Wang, Y., Jia, Y., Zhang, P., and Wang, W. P., (2017). Network big data oriented knowledge fusion methods:Asurvey. *Engl. J. Comput.* 23 (1), 1–27. doi:10.11897/SP.J.1016.2017.00001

Liu, L., and Wang, D. (2018). A review on named entity recognition. *J. China Soc. Sci. Tech. Inf.* 37 (03), 329–340. doi:10.3772/j.issn.1000-0135.2018.03.010

Liu, Q., Li, Y., and Duan, H. (2016). Knowledge graph con-struction technology. *J. Comput. Res. Dev.* 53 (03), 582–600. doi:10.7544/issn1000-1239.2016.20148228

Pedersen, T., Purandare, A., and Kulkarni, A. "Name discrimination by clustering similar contexts," in Proceedings of the 6th International Conference on Computational Linguistics and Intelligent Text Processing, Mexico City, 2005 (Mexico: CICLing), 226–237.

Riesbeck, C. K., and Schank, R. C. (2013). *Inside case-based reasoning*. London: Psychology Press.

Shi, S. (2013). Automatic and semi-automatic KnowledgeExtraction. *Commun. CCF* 9 (8), 65–73.

Thomas, A., and Sangeetha, S. (2019). An innovative hybrid approach for extracting named entities from unstructured text data. *Comput. Intell.* 35 (4), 799–826. doi:10.1111/coin.12214

Wang, C., Danilevsky, M., Desai, N., Zhang, Y., Nguyen, P., Taula, T., et al. (2013). "A phrase mining-framework for recursive construction of a topical hierarchy," in proceedings of the 19th ACM Sigkdd Int conf on Knowledgedis-covery and data mining, New York, 2013 (New York: ACM), 437–445.

Wang, H., Zhang, J., and Cheng, X. (2013). The construction of Chinese open link medical data. *China Digit. Med.* 8 (4), 5–8. doi:10.3969/j.issn.1673-7571.2013.04.002

Wang, H., Jiang, Y., and Wang, K. (2018). Power grid op-eration analysis and early warning system based on stability control strategy rule base. *China Plant Eng.* (11), 128–130.

Wang, Y., Tan, S., Liao, X., and Yiling, Z., (2010). Extracted do-main model based named attribute extension. *J. Comput. Res. Dev.* 47 (9), 1567–1573. doi:10.3724/SP.J.1016.2010.02202

Wong, W., Liu, W., and Bennamoun, M. (2012). Ontology learning fromText: A look back and into the future. *ACM Comput. Surv.* 44 (4), 1–36. doi:10.1145/2333112.2333115

Xiao, Y., Wang, J., and Ren, Z. (2020). Research on intelligent debugging system based on grid stability control strategy. *China CIO News* (12), 34–36. doi:10.3969/j.issn.1001-2362.2020.12.015

Zhang, C., Guo, Y., and Li, M. (2021). Review of development and application of artificial neural network models. *Comput. Eng. Appl.* 57 (11), 57–69. doi:10.3778/j.issn.1002-8331.2102-0256

Zhao, Q., and Gu, H. (2014). A survey of linyphiid spiders from xishuangbanna, yunnan province, China (araneae, linyphiidae). *Zookeys* 17 (09), 1–181. doi:10.3897/zookeys.460.7799