http://doi.org/10.35784/iapgos.7868 *received: 03.06.2025 | revised: 02.12.2025 | accepted: 20.01.2026 | available online: 30.03.2026*

DEVELOPMENT AND ANALYSIS OF POWER GRID FAILURE SCENARIOS USING ONTOLOGY, POWER FLOW MODEL, AND KNOWLEDGE GRAPH

Oleksandr Khomenko[1], Vyacheslav Senchenko[2], Oleksandr Koval[1], Iryna Husyeva[1]
[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Department of Software Engineering in Energy, Kyiv, Ukraine,
[2]Institute for Information Recording of the NAS of Ukraine, Department of Digital Modeling Systems, Kyiv, Ukraine

Abstract. *Power grids are complex systems that play an important role in many processes and are essential for the functioning of key services to society. Component failure can lead to cascading effects, equipment damage, and potential blackouts. In this paper, an ontology is used to formalize knowledge about the subject area, draw new conclusions, and build failure scenarios. The software simulates the operation of the power grid based on power flow, combining computer simulation of power grid failure scenarios, a semantic model of the subject area, and builds a knowledge graph, which is analysed using centrality metrics and used to draw conclusions about the scenarios of grid failure development. The ontology and knowledge graph can be supplemented with new knowledge and used for further analysis using other models or approaches, as the data is easily interpreted and described using the concepts of the subject area.*

Keywords: information technology, critical infrastructure, cascading effect, ontology, knowledge graph, power flow model

BUDOWA I ANALIZA SCENARIUSZY AWARII W SIECIACH ELEKTROENERGETYCZNYCH Z WYKORZYSTANIEM ONTOLOGII, MODELU PRZEPŁYWU MOCY ORAZ GRAFU WIEDZY

Streszczenie. *Sieci energetyczne to złożone systemy, które odgrywają istotną rolę w wielu procesach i mają kluczowe znaczenie dla funkcjonowania podstawowych usług społecznych. Awaria elementów może prowadzić do efektów kaskadowych, uszkodzeń sprzętu i potencjalnych przerw w dostawie prądu. W niniejszym artykule wykorzystano ontologię w celu sformalizowania wiedzy na temat tego obszaru, wyciągnięcia nowych wniosków oraz opracowania scenariuszy awarii. Oprogramowanie symuluje działanie sieci energetycznej w oparciu o przepływ mocy, łącząc komputerową symulację scenariuszy awarii sieci energetycznej z modelem semantycznym danej dziedziny, a także tworzy graf wiedzy, który jest analizowany przy użyciu miar centralności i wykorzystywany do wyciągania wniosków na temat scenariuszy rozwoju awarii sieci. Ontologię i graf wiedzy można uzupełniać o nową wiedzę i wykorzystywać do dalszej analizy przy użyciu innych modeli lub podejść, ponieważ dane można łatwo interpretować i opisywać przy użyciu pojęć z danej dziedziny.*

Słowa kluczowe: technologie informacyjne, infrastruktura krytyczna, efekt kaskadowy, ontologia, graf wiedzy, model przepływu mocy

Introduction

During Russia's full-scale invasion of Ukraine on February, 24, 2022, Ukraine's critical infrastructure suffered from targeted attacks, causing disruption of functions essential to society and the economy. In this difficult situation, Ukraine manages to maintain the functioning of critical infrastructure at a level that allows it to provide essential services, in some cases at a reduced level. As of June, 15, 2022, about 613,500 consumers in Ukraine were without electricity supply and about 178,500 without gas supply due to damage caused by the hostilities [3]. As of May, 2024, according to the Kyiv School of Economics, losses in the energy sector exceeded $56 billion as a result of Russia's full-scale invasion of Ukraine [2].

Critical infrastructure is a complex system consisting of objects that have dependencies and interdependencies between them, which may be physical, cyber, geographical, or logical in nature [20]. For example, the functioning of the telecommunications infrastructure depends on the energy infrastructure and vice versa. Attacks on energy infrastructure have a cascading effect on dependent critical infrastructure sectors - a failure in one infrastructure can trigger a cascading effect throughout the entire system: water supply, logistics, telecommunications, and industry. The possible consequences of a cascading effect are increasing due to the growing complexity of modern infrastructure systems.

Electricity infrastructures play an important role in the functioning of most facilities, and are therefore potentially vulnerable to cascading failures: approximately 50 million people in North America were affected by the blackout of August, 14, 2003 [10]. Cascading failures can cause a large-scale power outage – a blackout that occurs under the influence of various factors: weather conditions, equipment failure, operator errors, which can lead to emergencies and have immediate or long-term consequences in adjacent critical infrastructure. For example, as a result of a blackout, traffic in large cities becomes difficult and chaotic, increasing the risk of accidents that could potentially lead to injury and death. Emergency services (firefighters, paramedics, police) face difficulties in carrying out their duties. Delays in rail transport negatively affect logistics, while disruptions in the metro system increase the load on ground transport, causing congestion on the roads and restricting people's mobility. Airports are kept running during power outage by emergency power systems, so planes can take off and land, but with certain limitations. One example of a long-term impact of a blackout is congestion in ports: loading and unloading of ships stops, port operations slow down or stop, goods accumulate, and ships wait in ports. Water supply plays an important role for society, as water is used in various sectors of the economy: industry and households. The operation of water supply systems (transportation, treatment and distribution) depends on electricity, but some facilities can be equipped with backup power sources that ensure operation for a certain period of time. In the event of a prolonged power outage, problems may arise with the supply of drinking water to end users: electric pumps fail, and the pressure in the system decreases.

To reduce the potential consequences of cascading effects, disruption protection strategies are being implemented. The Law of Ukraine ‘On Critical Infrastructure’ states that the protection of critical infrastructure is an integral part of ensuring the national security of Ukraine [27]. Preventing the occurrence and development of hazardous events and response time to an event are key aspects in critical systems. The development of software tools for assessing system resilience and decision-making based on the analysis of the impact and development of events in critical infrastructure can reduce the time for decision-making in the situation of potentially hazardous events and reduce negative consequences. Therefore, research on the development of methods and software tools that implement them to analyse the impact of various types of events on critical infrastructure operations and increase its resilience is relevant to ensuring the functioning of important facilities and the provision of services to society, especially in time of war. In addition, research in this area can be used to develop strategies to increase the resilience, readiness and operation of critical infrastructure facilities and systems in the event of emergencies in peacetime.

1. Analysis of related research and problem statement

Critical infrastructure facilities form interdependent networks, so there is a risk of cascading failure – a failure in one infrastructure causes a component failure in the second infrastructure, which subsequently causes a failure in another infrastructure [20]. The development of cascading failures in time consists of three stages: the initial stage, the expansion stage, and the collapse stage [29]. The emergency situation in the system may become uncontrollable within a short period of time after the start of the cascade effect, and the potential negative consequences of the cascade increase in the case of a targeted malicious attack aimed at maximising the impact of the cascade. Investigation of possible behaviour and development of cascades in the system is an important task to reduce their impact on the system objects: application of measures to increase their resilience. Resilience curves are used to assess the quantitative and qualitative aspects of critical infrastructure behaviour [18]. To compare the resilience of systems to various disruptions and the results of applying resilience improvement strategies, a general resilience metric is used, which is based on a quantitative assessment of the system's main capabilities [14]. The concepts of Complex Networks based on topological and hybrid approaches are used to analyse resilience and vulnerability in power grids [4]. A hybrid approach is a combination of complex network and electrical engineering concepts to improve the topological approach using subject matter metrics. When a substation or transmission line fails, electricity is redirected in accordance with Kirchhoff and Ohm's laws, which are mostly ignored in simple topological models, which can lead to erroneous conclusions [11, 13]. Cascading failures in power grids do not propagate locally: the next failure may occur far from the previous one, which makes it difficult to model the process, identify failure propagation patterns, and develop algorithms to prevent and mitigate their effects. The study of the impact of network topology, cascading mechanisms (physics) and connectivity on the vulnerability of the infrastructure network is important to reduce the risk of cascading failures [4]. With the help of the critical infrastructure graph, it is possible to assess its strength using robustness metrics, which are grouped into six categories: clustering, connectivity, distance, throughput, spectral methods, geographical metrics [4]. The choice of metrics is influenced by various conditions: graph type, network size, and computational complexity. Bayesian networks [6] and Petri nets are used to model the operation of critical infrastructure, study its behaviour and properties to improve resilience. Bayesian networks are used to work with small amounts of data, but as the data set increases, the need for computing resources grows rapidly. Petri nets and its modifications (Stochastic Petri Net, Timed Petri Net, Coloured Petri Net, Fuzzy Petri Net, Hybrid Petri Net) are used to model and analyse the complex dynamics of smart grids in various research areas: management, reliability, networking, security (prevention of possible cascading effects) [7]. Petri nets are used to solve various problems, but with an increased number of objects, more complex connections between them, and the logic of modelling behaviour, the support process becomes more complex, and as a result, the risk of a possible error when editing the model increases. As the size of the graph increases, the number of combinations of possible targets for attack and defence grows exponentially. Stochastic models are used to simulate the dynamics of power grids [2], but modelling cascading failures in power systems is a complex process: many different factors need to be taken into account. A dynamic simulation model of power grids and protection systems has a number of advantages over existing quasi-steady-state models [23]. Limitations in modelling, controlling and mitigating the impact of cascading failures in power systems have prompted a large number of studies. Modelling-based approaches usually require large computing resources when the number of components in networks and the logic of their interaction increases, which makes it difficult to use in real time.

Understanding the data of the research domain is a key aspect for conducting analysis to solve the tasks. To formalise concepts in a domain, ontologies are used to organise data into hierarchical structures, define relationships between classes, instances and their properties to understand the relationship between data. There are various reasons for developing an ontology, some of which are given in the reference [16].

Ontology is used to manage domain knowledge in order to analyse and perform data-based operations in information systems. The ontology for critical infrastructure domain analysis consists of three parts [5]:

- Information and communication technology ontology: describes the infrastructure components and the connections between them.
- Vulnerability ontology: describes infrastructure vulnerabilities.
- Attack ontology: describes possible attacks, ways to exploit the vulnerability, and possible mitigation measures.

The model is filled with the necessary information, forming a knowledge base that is used for decision-making. Knowledge Base Systems are used to define scenarios, properties, and model the relationships and dependencies of critical infrastructures based on ontologies that represent domain knowledge [25]:

- World ONTology.
- Infrastructure domain ONTologies.
- Federation ONTology.

To test the approach, a scenario was used that includes three critical infrastructure sectors: electricity, telecommunications, and railways. The number of objects in the systems grows over time, the logic of interaction becomes more complex, and the amount of heterogeneous data used in various processes (e.g., monitoring, management), one of which is critical infrastructure protection, increases. Most processes are automated, but the data may change over time (new sources of information), which makes it difficult to configure, maintain and understand the complex system. Therefore, there is a need for tools to improve and facilitate the use of data in the work of critical infrastructure operators. One approach to protecting critical infrastructure is to use ontology and form logical conclusions using the capabilities of the semantic web based on information stored in relational databases through an appropriate interface [9]. Reference [21] describes the process of creating the InfraRisk ontology and a prototype software that displays information about natural hazards, their impact on critical infrastructure (transport infrastructure), and allows for the formation of queries to study the subject area. The ontology of cascading effects in critical infrastructure provides an understanding of the creation and propagation of cascading effects that can be analysed to minimise their impact on critical infrastructure [26].

Since there is a limited number of ontology-based studies of cascading effects in critical infrastructure, describing possible scenarios of their development and impact, there is a need to develop an ontological model of critical infrastructure, cascading effects and form a knowledge base for describing scenarios with the possibility of further analysis to reduce the impact of disruptions on the operation of facilities and increase their resilience.

2. Purpose and objectives of the study

The purpose of the study is to develop a semantic ontological model for building a knowledge graph and scenarios of critical infrastructure (power grid) operation in order to analyse possible cascading effects in the event of failures.

To achieve the goal, the following tasks were defined:

- Develop an ontological model of critical infrastructure.
- Create scenarios for the operation of critical infrastructure facilities.
- Analyse the characteristics of the knowledge graph of critical infrastructure scenarios.

3. Research methods

Ontologies are used to formalise knowledge about a subject area and help organise information: data properties, relationships between them, possible applications, which makes it easier to represent knowledge, find the necessary information and use it to solve problems. The development of an ontology is an iterative process consisting of the following steps:

- Research of the subject area.
- Defining classes, properties, relationships between classes, and creating instances.
- Creating a formalised model – an ontology.
- Verification and improvement of the model.

An energy system consists of a set of components, for example: a source of electricity, transformers (used to increase or decrease voltage), power lines for transporting electricity between system components, loads (consuming electricity). The power transmission system is modelled as a graph to solve the power flow equations for balancing electricity between generation and load. The graph consists of the following components: nodes – buses, which are the places where system components are connected; edges – branches that connect the buses. Calculating the power flow in the power grid is one of the most important approaches to analysing the steady-state behaviour of the system. The equations for active and reactive power for each bus i are defined as:

$$P_i = \sum_{k=1}^{N} |V_i|\,|V_k|(G_{ik}cos\delta_{ik} + B_{ik}sin\delta_{ik}) \quad (1)$$

$$Q_i = \sum_{k=1}^{N} |V_i|\,|V_k|(G_{ik}sin\delta_{ik} - B_{ik}cos\delta_{ik}) \quad (2)$$

where $\delta_{ik} = \delta_i - \delta_k$ is the difference in phase angles between node i and k; G is the real component of the total conductivity; B is the imaginary component of the total conductivity.

For each bus, two of the four values are specified, and the other two are unknown: real power (injected real power, P); reactive power (injected reactive power, Q); voltage magnitude (voltage magnitude, $|V|$); voltage phase angle (δ).

Each bus can be classified into one of three categories [1]: Slack bus, PQ bus, PV bus (Table 1).

Table 1. Modelling bus bar categories in the power grid

Bus type	P	Q	|V|	δ
Slack	Not specified	Not specified	Specified	Specified
PQ	Specified	Specified	Not specified	Not specified
PV	Specified	Not specified	Specified	Not specified

Table 2. Description of the power flow model of the power grid

Branch ⊑ PowerFlowModelComponent
Branch ⊑ ∀ isConnectedTo.BusNode
BusNode ⊑ PowerFlowModelComponent
BusNode ⊑ ∀ hasParameter.(ActivePower ⊓ ReactivePower ⊓ VoltageAngle ⊓ VoltageMagnitude)
BusNode ⊑ ∀ hasActivePowerValue.decimal
BusNode ⊑ ∀ hasReactivePowerValue.decimal
BusNode ⊑ ∀ hasVoltageAngleValue.decimal
BusNode ⊑ ∀ hasVoltageMagnitudeValue.decimal
PQBus ⊑ BusNode
PQBus ⊑ ∀ hasInputParameter.(ActivePower ⊓ ReactivePower)
PQBus ⊑ ∀ hasOutputParameter.(VoltageAngle ⊓ VoltageMagnitude)
PVBus ⊑ BusNode
PVBus ⊑ ∀ hasInputParameter.(ActivePower ⊓ VoltageMagnitude)
PVBus ⊑ ∀ hasOutputParameter.(ReactivePower ⊓ VoltageAngle)
PowerFlowModel ⊑ (∃ hasComponent.Branch) ⊓ (∃ hasComponent.BusNode)
PowerGenerator ⊑ PowerSystemComponent
PowerGenerator ⊑ ∀ hasConnectionTo.BusNode
PowerLine ⊑ PowerSystemComponent
PowerLine ⊑ ∀ isModeledAs.Branch
PowerLoad ⊑ PowerSystemComponent
PowerLoad ⊑ ∀ hasConnectionTo.BusNode
PowerTransformer ⊑ PowerSystemComponent
PowerTransformer ⊑ ∀ isModeledAs.Branch
SlackBus ⊑ BusNode
SlackBus ⊑ ∀ hasInputParameter.(VoltageAngle ⊓ VoltageMagnitude)
SlackBus ⊑ ∀ hasOutputParameter.(ActivePower ⊓ ReactivePower)
Branch ⊑ ¬ BusNode
PQBus ⊑ ¬ PVBus, PQBus ⊑ ¬ SlackBus, PVBus ⊑ ¬ SlackBus PowerGenerator ⊑ ¬ PowerLine, PowerGenerator ⊑ ¬ PowerLoad, PowerGenerator ⊑ ¬ PowerTransformer, PowerLine ⊑ ¬ PowerLoad, PowerLine ⊑ ¬ PowerTransformer, PowerLoad ⊑ ¬ PowerTransformer

Building an ontology is an important step in formalising knowledge about a subject area, which allows to check the logic and consistency of data during modelling. One of the popular tools for building ontologies is the Protégé graphical editor [24]. The process of building an ontology consists of defining the basic concepts and rules of interaction between objects. The description is given in the description of logics (Table 2).

The description of the system parameters and their units of measurement is an important aspect for data consistency and their further use in analysis (Table 3).

Table 3. Description of measurement units for system parameters

ActivePower ⊑ PowerSystemVariable
ActivePower ⊑ ∀ hasMeasurement.MWatt
MWatt ⊑ UnitOfMeasurement
ReactivePower ⊑ PowerSystemVariable
ReactivePower ⊑ ∀ hasMeasurement.MVAR
MVAR ⊑ UnitOfMeasurement
VoltageAngle ⊑ PowerSystemVariable
VoltageAngle ⊑ ∀ hasMeasurement.Radian
Radian ⊑ UnitOfMeasurement
VoltageMagnitude ⊑ PowerSystemVariable
VoltageMagnitude ⊑ ∀ hasMeasurement.PerUnitVoltage
PerUnitVoltage ⊑ UnitOfMeasurement

The scenario consists of external conditions, which are the conditions for the occurrence of failures, events (initial and resultant events) and a power flow model that allows to determine a possible chain of failures – a cascading effect (Table 4).

Table 4. Description of the event scenario

Scenario ≡ (∃ hasPart.Environment) ⊓ (∃ hasPart.Event) ⊓ (∃ hasPart.PowerFlowModel)
Cascade ⊑ ResultEvent
Cascade ⊑ ∃ hasCaused.(Overloading ⊔ Tripping)
Event ⊑ ∃ hasNegativeInfluenceOn.PowerSystemComponent
Failure ⊑ InitEvent
InitEvent ⊑ Event
InitEvent ⊑ ∃ hasCaused.ResultEvent
Maintenance ⊑ InitEvent
Overloading ⊑ ResultEvent
ResultEvent ⊑ Event
ResultEvent ⊑ ∃ isCausedBy.InitEvent
Season ⊑ Environment
Weather ⊑ Environment

With the help of the HermiT Reasoner software tool, it is possible to check for potential errors in the definition of axioms and identify new logical conclusions (Fig. 1).

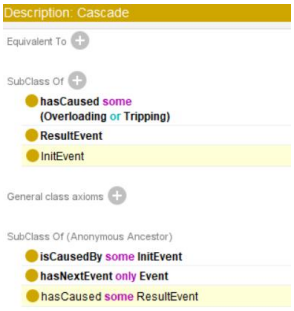


Fig. 1. An example of a new axiom for determining the cascading effect

4. Generation of power grid failure scenarios

Various external factors (e.g., weather, seasonality) affect the occurrence of failures, which cause disruptions, resulting in the disconnection of power lines due to overload or for preventive purposes to reduce the negative impact on the system operation. To model the operation of the power grid (IEEE 9-bus system) and cascading effects scenarios, the GridCal software is used, which has convenient tools and interface [22]. Loads (electricity consumers) can be modelled as objects of related critical infrastructures (Figure 2).

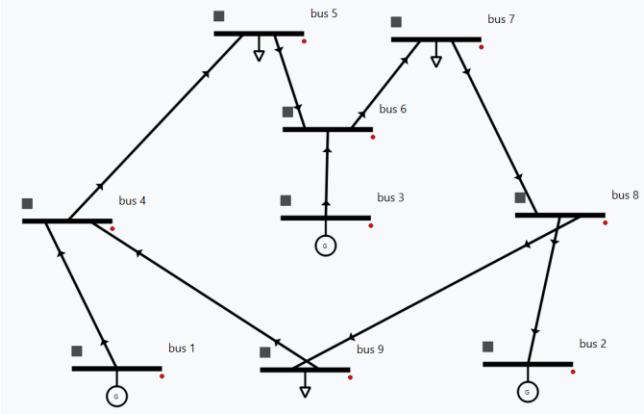


Fig. 2. An example of a test network (IEEE 9-bus system)

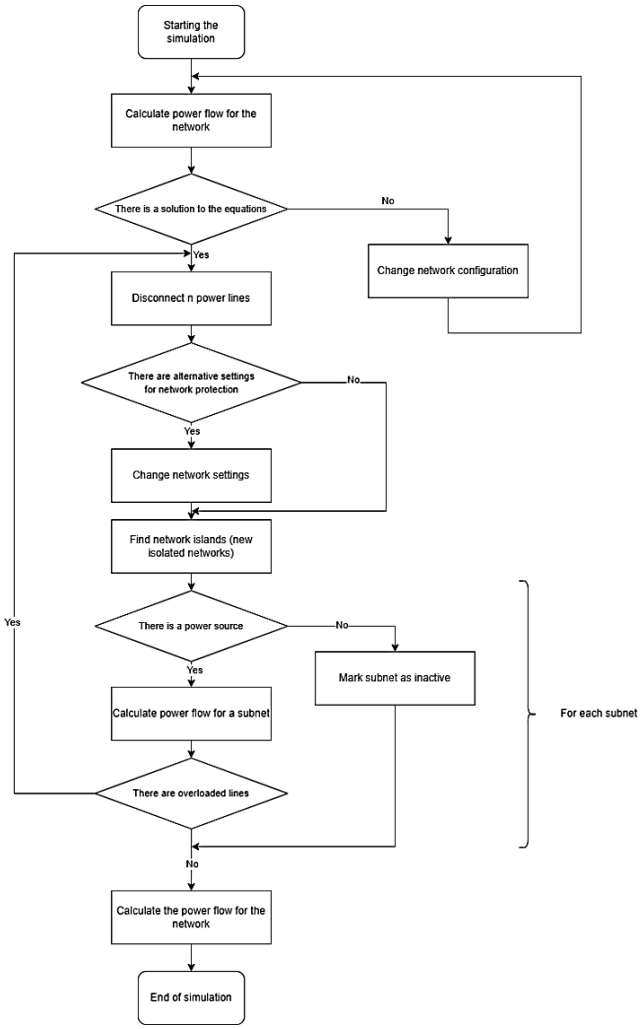


Fig. 3. Algorithm for modelling power grid failure scenarios

The algorithm, shown in Figure 3, is used to model power grid failures and potential cascading effects.

The ontological model is used to describe the state of network components at a certain step of the scenario. Based on the semantic rules of SWRL [12], the model can be supplemented with metadata, for example: a description of the development of a cascade effect, the application of a protective mechanism for certain system parameters.

Definition of a cascading effect that has started but not ended:
Island(?islnd1) ^ hasChild(?islnd1, ?c_islnd) ^ hasParent(?islnd1, ?p_islnd) ^ CascadeContinues(?isl) -> hasEvent(?islnd1, ?isl).

Determination of exceeding indicators in accordance with established limits:
Generator(?gen) ^ hasReactivePower(?gen, ?value) ^ hasLimit(?gen, ?limit) ^ swrlb:greaterThan(?value, ?limit) -> HighReactivePowerValue (?gen).

If the permissible value of the generator's reactive power is exceeded, the action to be taken in this case is determined:
HighReactivePowerValue (?gen) ^ Generator(?gen) -> LimitReactivePowerValueAction(?gen).

5. Knowledge graphs for scenario analysis

Knowledge Graphs are used to represent knowledge in the form of RDF triples (subject, predicate, object), search for knowledge, identify hidden patterns and trends using semantic structure, flexibility and scalability, making them a powerful tool for data analysis that opens up new possibilities in information processing – a holistic and multidimensional view of data that allows for more informed decisions and actions to solve problems. For example, in the energy sector, knowledge graphs can be used to manage infrastructure, ensuring sustainability, resource efficiency, using data on terrain, weather and electricity demand to optimise energy distribution and forecast demand. Knowledge graphs can also be used in the provision of utilities, analysing meter and sensor readings to identify inefficient models and take appropriate decisions and actions to improve their efficiency. Knowledge graphs are used in artificial intelligence, which is used to train machine and deep learning models, allowing for the development of complex systems and increasing their efficiency.

The knowledge graph and ontology can be used to describe the development of failure scenarios and their impact on system components (Table 5):

- Scenario 1: Network blackout (Blackout).
- Scenario 2: Stabilisation outage (Grid stabilisation).
- Scenario 3: Preventive outage (Grid stabilisation).

Table 5. Description of grid failure scenarios

Step	Scenario 1	Scenario 2	Scenario 3
1	Failure in Branch0 and Branch4		
2	Overloading and disconnection Branch6	Overloading and disconnection Branch6; disconnection Branch8	Overloading and disconnection Branch7, Branch8
3	Overloading and disconnection Branch1, Branch2, Branch3, Branch5, Branch7, Branch8.	The system has stabilised	The system has stabilised
4	Blackout in the system		

Scenarios 2 and 3 are alternatives to scenario 1. The vertices of the knowledge graph were coloured according to the category of the element: Bus – blue; Branch – green; Gen – orange; Load – purple; Failure, Overloading, Tripping, Cascade – red; Scenario – grey (Figure 4).

Visualisation of knowledge graphs is a useful tool for studying the development of processes in the system, which allows identifying potential vulnerable objects and patterns in the event of failures. Analysts are able to view and analyse processes and determine the course of action to mitigate the consequences of failures.

The knowledge graph consists of 33 vertices and 55 arcs. Metrics, which were used to study the characteristics of events in the scenarios: Degree Centrality – the number of arcs incident to a vertex; Betweenness Centrality – the frequency of a node being on the shortest path between other nodes; Closeness Centrality – determines the proximity of a node to other nodes (Table 6). Python [19], the NetworkX [8] and Pyvis [28] libraries were used to calculate and visualise the results.

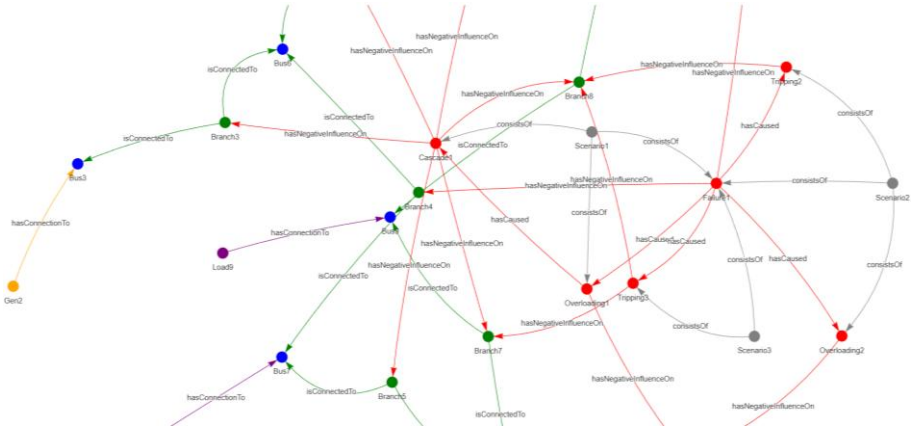


Fig. 4. An example of a fragment of the knowledge graph of scenario development in the power grid

Table 6. Characteristics of events in the scenarios

Degree Centrality		Betweenness Centrality		Closeness Centrality	
Failure1	0.40625	Failure1	0.109207	Failure1	0.222222
Cascade1	0.28125	Cascade1	0.058804	Overloading1	0.153846
Overloading1	0.18750	Overloading1	0.058468	Tripping3	0.133333
Tripping3	0.15625	Tripping3	0.011593	Tripping2	0.133333
Tripping2	0.12500	Overloading2	0.007728	Overloading2	0.133333
Overloading2	0.12500	Tripping2	0.004200	Cascade1	0.105263

Based on the results of the metrics, conclusions can be drawn:

- The event 'Failure1' has the highest Degree Centrality value, since it is a node that belongs to scenarios 1, 2, 3, is the beginning for the development of certain events and has an impact on system components.
- The 'Failure1' event has the highest Betweenness Centrality value, so it is a node with a significant impact in the scenarios, and solving this problem will potentially help reduce the impact of failures on the system.
- The 'Failure1' event has the highest Closeness Centrality value and can be interpreted as a node that can quickly interact with other nodes and be used to propagate failures.

To assess the consequences of the scenario, the number of failed grid components is used:

- Scenario 1: 9 components.
- Scenario 2: 4 components.
- Scenario 3: 4 components.

Therefore, to reduce the consequences in the power grid in the event of a Failure1 event, it is advisable to use scenarios 2 and 3, another solution is to increase the system's resilience to prevent the occurrence of a Failure1 failure.

When the number of objects in the knowledge graph increases, it is necessary to generate a clarifying query to form a sample with the necessary data, since the data is grouped in the scenario step. The scenario is described using a sequence of steps with the characteristics of the power grid components. For example, for the case141 network, the following scenario was generated:
Step 1. Bus failure: 1, 7, 8, 12, 19, 21, 27, 30, 31, 35, 36, 38, 40, 43, 44, 45, 46, 50, 60, 61, 63, 67, 69, 71, 73, 74, 78, 79, 80, 81, 84, 89, 92, 93, 97, 99, 101, 102, 103, 105, 107, 109, 110, 111, 114, 116, 121, 122, 125, 127, 128, 130, 139.
Step 2. Apply Under Voltage Load Shedding (UVLS) to maintain voltage levels.
Step 3. Apply overload protection (OLP) to lines that are overloaded.
Step 4. As a result of the scenario, the network is out of power.

User can query, select specific data and find common patterns in different steps of scenarios. These metadata can be used for analysis data before creating dataset for machine learning model. Neural networks have the ability to: learn complex patterns, detect cascading effects, approximate N-k analysis, and the semantic model provides a description of the processes in the scenario, which improves the interpretation of the results.

As the number of components in the power grid increases, the complexity of the knowledge graph increases, so an example is given using one scenario for each of the case145 and case300 networks.

Table 7. Characteristics of events in the scenario for case145

Degree Centrality		Betweenness Centrality		Closeness Centrality	
initial_contingency1	0.75249	Branch11	0.000017	Bus73	0.03460
OL4 (limit value)	0.75249	Branch97	0.000017	Bus142	0.03417
UVLS3	0.75249	Branch12	0.000017	Bus69	0.03299
XL2 (limit value)	0.75249	Branch96	0.000015	Bus74	0.03299
Blackout5	0.15614	Branch87	0.000015	Bus121	0.03254

Degree Centrality can be interpretated as influence of events on components in graph. Betweenness Centrality can indicate on objects that require more detailed analysis to increase network resilience in the scenario. Closeness Centrality can indicate on objects that require more detailed analysis of settings to decrease bad influence of contingency on the network in the scenario.

Table 8. Characteristics of events in the scenario for case300

Degree Centrality		Betweenness Centrality		Closeness Centrality	
initial_contingency1	0.57482	Branch323	0.000012	Bus9003	0.017927
OL4 (limit value)	0.57482	Branch334	0.000012	Bus130	0.013923
UVLS3	0.57482	Branch397	0.000012	Bus37	0.012605
XL2 (limit value)	0.57482	Branch406	0.000012	Bus211	0.012605
Bus9003	0.06713	Branch260	0.000012	Bus140	0.011298

6. Storing knowledge graphs

To store knowledge graphs in a relational database, it is first needed to define the structure of the tables and determine the relationships between them, but knowledge graphs can change over time (new classes, relationships, and attributes are added), scale in size and data complexity, which necessitates changing the database structure. There is a need for storage to interact with heterogeneous and dynamic data. For efficient storage and work with graphs, it is advisable to use Neo4j, a graph database management system [15] that is optimised for efficient storage of graphs and queries. In a relational database, data is stored in tables, and in a graph database, it is stored using:

- Nodes: representing entities.
- Relationships: links between nodes.
- Properties: attributes or metadata associated with nodes or relationships.

Neo4j ensures data integrity and reliability by adhering to ACID (Atomicity, Consistency, Isolation, Durability), includes a library of algorithms for graph analysis, visualisation tools, and the Cypher query language, which allows to write queries to solve various types of problems.

7. Conclusions

Using ontology to formalize domain knowledge has advantages and disadvantages. The advantages of using ontology in critical infrastructure, in particular in the power grid, are the structuring of knowledge, which facilitates the understanding of complex concepts, the interaction of components, the ability to integrate data from different sources using the agreement of terms and structures. Ontologies are also used to search for new knowledge based on defined rules, there is the ability to form queries to search for relevant information, and provide the ability to manage and share knowledge. The disadvantages of using ontology are the complexity of development and maintenance (can be complex and time-consuming, requiring significant experience and resources), the flexibility of adaptation to changes in domain knowledge or requirements (may require significant refinement of the existing model, for example, detailing certain concepts). This may entail certain costs during implementation: setting up and maintaining the ontology. The efficiency of the ontological model depends on the depth of knowledge and understanding of the domain. Due to limited data for analysis and domain information, ontologies can be significantly simplified, resulting in the potential loss of important nuances.

Based on the ontology and data, a knowledge graph was created, which is used in a clear form for both humans and machines, and it is possible to perform tasks to obtain new knowledge about the subject area (explicit and implicit facts using appropriate queries and metrics). As a result, an ontological model and knowledge graph of the power grid were built for modelling failures, in particular, cascading failures. Based on the centrality metrics of the graph, conclusions were drawn about the characteristics of the "Failure1" vertex and the development of scenarios in the network. The ontological model and knowledge graph can be supplemented and expanded to detail the subject area, study new knowledge, and combine with other domains to study the connections, development, and impact of scenarios on related systems.

References

[1] Afolabi, O., Ali, W., Cofie, P., Fuller, J., Obiomon, P., & Kolawole, E. (2015). Analysis of the load flow problem in power system planning studies. *Energy and Power Engineering*, 7, 509–523. https://doi.org/10.4236/epe.2015.710048

[2] Anghel, M., Werley, K. A., & Motter, A. E. (2006). *Stochastic model for power grid dynamics*. arXiv. https://doi.org/10.48550/arXiv.physics/0609217

[3] Cabinet of Ministers of Ukraine. (2022). *The status of Ukraine's power system as of 15 June 2022*. https://www.kmu.gov.ua/news/robota-energosistemi-ukrayini-stanom-na-15-chervnya-2022-roku

[4] Cuadra, L., Salcedo-Sanz, S., Del Ser, J., Jiménez-Fernández, S., & Geem, Z. W. (2015). A critical review of robustness in power grids using complex networks concepts. *Energies*, *8*(9), 9211–9265. https://doi.org/10.3390/en8099211

[5] De Rosa, F., Maunero, N., Nicoletti, L., Prinetto, P., & Trussoni, M. (2022). *Ontology for cybersecurity governance of ICT systems*. CEUR Workshop Proceedings. https://ceur-ws.org/Vol-3260/paper4.pdf

[6] Eldosouky, A., Saad, W., & Mandayam, N. (2021). *Resilient critical infrastructure: Bayesian network analysis and contract-based optimization*. arXiv. https://doi.org/10.48550/arXiv.1709.00303

[7] Ge, M., Rossi, B., Chren, S., & Blanco, J. M. (2024). *Petri nets for smart grids: The story so far*. arXiv. https://doi.org/10.48550/arXiv.2401.05462

[8] Hagberg, A., Schult, D., & Swart, P. (n.d.). *NetworkX*. https://networkx.org

[9] Henriques, J., Caldeira, F., Cruz, T., & Simões, P. (2018). On the use of ontology data for protecting critical infrastructures. *Journal of Information Warfare*, *17*(4).

[10] Hines, P., Balasubramaniam, K., & Sanchez, E. C. (2009). Cascading failures in power grids. *IEEE Potentials*, *28*(5), 24–30. https://doi.org/10.1109/MPOT.2009.933498

[11] Hines, P., Cotilla-Sanchez, E., & Blumsack, S. (2010). *Do topological models provide good information about electricity infrastructure vulnerability?* https://doi.org/10.1063/1.3489887

[12] Horrocks, I. et al. (2004). *SWRL: A semantic web rule language combining OWL and RuleML*. World Wide Web Consortium (W3C). https://www.w3.org/submissions/SWRL

[13] Korkali, M., Veneman, J. G., Tivnan, B. F., & Hines, P. D. H. (2014). *Reducing cascading failure risk by increasing infrastructure network interdependency*. arXiv. https://doi.org/10.48550/arXiv.1410.6836

[14] Nan, C., Sansavini, G., Kröger, W., & Heinimann, H. R. (2014). A quantitative method for assessing the resilience of infrastructure systems. In *Proceedings of the 12th Probabilistic Safety Assessment and Management Conference (PSAM12)*, *10*, 359–370, Honolulu, HI, United States.

[15] Neo4j, Inc. (n.d.). *Neo4j*. https://neo4j.com

[16] Noy, N. F., & McGuinness, D. L. (2001). *Ontology development 101: A guide to creating your first ontology*. Stanford University.

[17] Oehlers, M., & Fabian, B. (2021). Graph metrics for network robustness – A survey. *Mathematics*, *9*(8), 895. https://doi.org/10.3390/math9080895

[18] Poulin, C., & Kane, M. B. (2021). Infrastructure resilience curves: Performance measures and summary metrics. *Reliability Engineering & System Safety*, *216*, 107926. https://doi.org/10.1016/j.ress.2021.107926

[19] Python Software Foundation. (n.d.). *Python*. https://www.python.org

[20] Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6), 11–25. https://doi.org/10.1109/37.969131

[21] Roman, D., Sukhobok, D., Nikolov, N., Elvesæter, B., & Pultier, A. (2019). *The InfraRisk ontology: Enabling semantic interoperability for critical infrastructures at risk from natural hazards*. https://core.ac.uk/download/pdf/249984754.pdf

[22] SanPen. (n.d.). *GridCal*. GitHub. https://github.com/SanPen/GridCal

[23] Song, J., Cotilla-Sanchez, E., Ghanavati, G., & Hines, P. D. H. (2014). *Dynamic modeling of cascading failure in power systems*. arXiv. https://doi.org/10.48550/arXiv.1411.3990

[24] Stanford Center for Biomedical Informatics Research. (n.d.). *Protégé*. https://protege.stanford.edu

[25] Tofani, A. et al. (2010). Using ontologies for the federated simulation of critical infrastructures. *Procedia Computer Science*, *1*(1), 2301–2309. https://www.sciencedirect.com/science/article/pii/S1877050910002590

[26] Toscano, B., Fernandes, A. D., & Mira da Silva, M. (2022). A domain ontology on cascading effects in critical infrastructures based on a systematic literature review. *International Journal of Critical Infrastructures*, *18*(1), 79–103. https://doi.org/10.1504/IJCIS.2022.120679

[27] Verkhovna Rada of Ukraine. (2021). *Law of Ukraine "On Critical Infrastructure", 1882-IX*, https://zakon.rada.gov.ua/laws/show/1882-20#Text

[28] West Health. (n.d.). *Pyvis*. GitHub. https://github.com/WestHealth/pyvis

[29] Xie, B., Tian, X., Kong, L., & Chen, W. (2021). The vulnerability of the power grid structure: A system analysis based on complex network theory. *Sensors*, *21*(21), 7097. https://doi.org/10.3390/s21217097

M.Sc. Oleksandr Khomenko
e-mail: khomenkosasha99@gmail.com

Ph.D. student, Department of Software Engineering in Energy, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine.
Scientific interests: machine learning, deep learning, big data processing.

https://orcid.org/0000-0003-1964-1097

Ph.D. Vyacheslav Senchenko
e-mail: svrukr@gmail.com

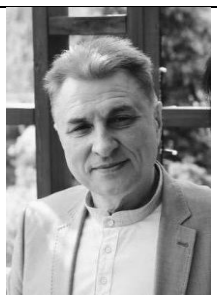
Senior researcher of the Department of Digital Modeling Systems, Institute of Information Registration Problems of the National Academy of Sciences of Ukraine, Kyiv, Ukraine.
Scientific interests: Systems Analysis and Information Technology.

https://orcid.org/0009-0007-5689-3134

D.Sc. Oleksandr Koval
e-mail: avkovalgm@gmail.com

Doctor of Engineering Sciences, Department of Software Engineering in Energy, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".
Scientific interests: software systems using a model approach, machine learning, scenario approach and knowledge engineering technologies; cyber-physical systems.

https://orcid.org/0000-0003-0991-6405



M.Sc. Iryna Husyeva
e-mail: i.husyeva@kpi.ua

Associate professor at Software Engineering in Energy Department, Igor Sikorsky Kyiv Polytechnic Institute, an Associated Collaborator Member at Smart Cities Research Centre of Polytechnic Institute of Tomar and at Computer Science and Communications Research Centre of Polytechnic Institute of Leiria.
Scientific interests include software engineering, IoT, networking, data fusion, data processing.

https://orcid.org/0000-0002-8762-3918