Functional dependency graphs for cyber risk assessment in 5G-enabled ICS/OT networks

Alla Pinchuk[1,*,†], Roman Odarchenko[1,†], Oleh Poliheko[1,†], Oleksandr Dobrynchuk[1,†] and Vladyslav Pevnev[1,†]

[1] *State University "Kyiv Aviation Institute", Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine*

Abstract

The convergence of Industrial Control Systems (ICS) and Operational Technologies (OT) with 5G networks introduces complex cyber-physical infrastructures with dynamic topologies, high interconnectivity, and mission-critical latency requirements. Traditional risk assessment methods are inadequate in this situation because they do not consider the possibility of cascading failures among closely related system components. This paper proposes a cyber risk assessment approach based on functional dependency graphs, which model interdependencies among assets, processes, and communication flows in ICS/OT environments enabled by 5G. The suggested framework supports impact scoring based on graph-theoretic metrics, vulnerability propagation modeling, dependency graph construction, and passive and active data collection.

Keywords

ICS/OT network security, functional dependency graph, 5G environment, cybersecurity risk assessment

1. Introduction

The integration of fifth-generation (5G) technologies into industrial control systems (ICS) and operational technology (OT) environments is facilitating the transition to digitalization, automation, and the implementation of Industry 4.0 concepts. The main advantages of using 5G in industrial systems are support for high connection density (mMTC), ultra-reliable and low latency communication (URLLC), and extended bandwidth (eMBB).

However, the combination of ICS/OT and 5G brings new cybersecurity challenges. Unlike traditional isolated ICS/OT networks, modern hybrid architectures are characterized by a high degree of component interdependence, dynamically changing topology, and virtualization of network functions. This expands the attack surface and complicates the identification of vulnerabilities, especially those that can cause cascading failures.

Most modern vulnerability assessment solutions are focused on analyzing individual assets and do not take into account the functional dependency between ICS/OT components and 5G network elements. This approach does not allow for the full identification of ways of cybersecurity threats spreading and assessing the risks arising from the structural interdependence of systems.

This paper proposes the development of a functional dependency graph module for a vulnerability scanning system in ICS/OT 5G-enabled networks. The proposed approach allows for the dynamic modeling of the dependencies between assets, assessing cascading risks, and prioritizing identified vulnerabilities based on the topological characteristics and criticality of infrastructure elements.

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

alla.pinchuk@kai.edu.ua (A. Pinchuk); roman.odarchenko@npp.kai.edu.ua (R. Odarchenko); o.poligenko@ukr.net (O. Poliheko); oleksandr.dobrynchuk@npp.kai.edu.ua (O. Dobrynchuk); 2702485@stud.nau.edu.ua (V. Pevnev)
0000-0003-3567-0445 (A. Pinchuk); 0000-0002-7130-1375 (R. Odarchenko); 0000-0002-2427-4976 (O. Poliheko); 0009-0002-2877-844X (O. Dobrynchuk); 0000-0003-5410-1465 (V. Pevnev)

2. Background analysis

ICS and OT have long been designed as isolated, closed environments focusing on reliability rather than security. Traditionally, security was provided by physical access restrictions and a stable network topology [1]. However, modern digitalization trends, including the Industrial Internet of Things (IIoT), cloud services, and edge computing, radically change the ICS/OT landscape, making it harder to control and creating numerous attack vectors [2].

With the growing role of IP connections and remote management, ICS/OT environments are increasingly exposed to typical IT cybersecurity threats to which these systems were not originally adapted. Paper [3] discusses the concept of SCADA control using 5G, emphasizing new types of interconnections and isolation challenges.

To mitigate risks, some studies focus on traditional protection methods, such as segmentation, access restrictions, and software updates. For example, [4] proposes a systematic approach to reducing cybersecurity risks in ICS through access policies, multi-level protection, and monitoring. However, this approach still does not taking into account the specifics of the new 5G architecture.

The network's expansion by connecting many sensors and devices in the IIoT environment, combined with 5G characteristics such as URLLC, MEC, and slicing, creates situations where classical risk assessment approaches lose their effectiveness. In [5], the ACSRA ICS method is presented, an automated risk assessment considering interaction between nodes. However, the implementation does not cover slice-oriented access, massive device connectivity, or the logic of virtualized functions.

A more in-depth analysis of 5G security in an industrial context is provided in [6], which explores the challenges associated with interfaces between OT and virtualized 5G components. The authors note the difficulty in detecting attacks directed through AMF, UPF, or SMF, especially in conditions of limited monitoring.

The topic of modeling OT network structures is also reflected in [7], which provides an overview of tools for building OT topologies, analyzing nodes, and identifying potentially critical points. However, the work lacks a formalized apparatus for modeling the dependencies between OT processes and 5G functions.

In [8], a method for automated testing of 5G network slices is considered, which allows detecting vulnerabilities related to the logic of slice isolation and the orchestration of VNFs. Despite the detail of the threat model, the study does not provide a mechanism for assessing the impact on physical OT components.

Practical aspects of 5G integration into critical infrastructure are analyzed in [9], which presents a case study of building a secure 5G network to monitor facilities' technical condition. The work shows the effectiveness of the slice-based architecture, but there is no risk assessment taking into account cascading effects between elements.

A separate area concerns traffic analysis in heterogeneous networks. A neural model for recognizing modulation types in 5G networks is presented in [10]. This approach can be helpful in passively detecting anomalies in traffic, but does not provide an idea of the impact of one component on another in the system logic.

In [11], load balancing between parallel servers in distributed systems is finally considered. Although not directly related to security, the concept can be adapted to simulate fault tolerance or loss of functionality in ICS/OT environments in cascading-failure scenarios.

Thus, although existing research covers certain aspects, such as slice security, traffic modeling, or access control, it does not address the key problem: the lack of a formalized model of functional dependencies between OT elements and virtualized 5G components that would allow modeling the propagation of risks in time and space. This creates the need to build a new apparatus for assessing threats in such hybrid networks.

3. Problem statement

An analysis of scientific research has shown that despite the rapid growth of 5G integration into ICS/OT environments, existing approaches to cybersecurity risk assessment remain largely fragmented. Most available tools focus on identifying vulnerabilities of individual assets or use static risk models that do not consider the specifics of 5G architecture. In particular, new risks arise from the complex interaction of virtualized network functions (VNFs), massive connectivity of IIoT devices, the use of MEC technologies, and slice-based access logic.

The lack of formalized approaches that allow modeling functional dependencies between ICS/OT processes, 5G network services, and virtual components is particularly critical. Such dependencies determine how risks propagate in the system - in time, through interaction logic, or shared resources. Without a model that considers these aspects, it is impossible to accurately assess the cascading impact, criticality of nodes, and response priority.

Thus, this research paper aims to develop a methodology for formalizing functional dependency graphs (FDGs) for use in quantifying cyber risks in hybrid 5G-enabled ICS/OT networks.

To achieve this goal, the following research objectives should be solved:

1. To conduct an analysis of existing approaches to modeling risks and dependencies in ICS/OT networks and 5G environments, identifying their limitations in terms of intercomponent interaction.
2. To define requirements for the functional dependency graph in the context of 5G-enabled ICS/OT, including types of links, node categories, temporal properties, and asset criticality.
3. To develop a formal mathematical model of FDG that describes the functional relationships between system elements and allows tracking risk transformation in dynamics.
4. To integrate the FDG into a risk assessment model that calculates system-level metrics, identifies critical nodes and threat propagation trajectories, and prioritizes response measures.

4. Existing approaches analysis

Modern approaches to analyzing cybersecurity risks and interconnection dependencies in ICS/OT networks and 5G environments have been developed in isolation, leading to the lack of comprehensive solutions for hybrid architectures. This section systematizes the main research directions and identifies their limitations in the context of structural interaction, timing characteristics, and cascading effects.

4.1. ICS/OT environments

In traditional ICS/OT systems, risk analysis is based on the following approaches:

- signature-based threat detection methods (e.g., Snort, Bro) adapted to industrial protocols (Modbus, DNP3). They are effective for known attacks but do not consider functional dependencies between process components [12, 13, 14];
- frameworks such as NIST SP 800-82 focus on developing security policies but do not contain a formal apparatus for analyzing inter-node impacts or simulating the effect of incidents in dynamics [15, 16, 17];
- attack graphs and trees allow for the description of compromise scenarios from an attacker's perspective [18, 19]. However, most of these models are static, do not cover the time evolution of risk, and do not consider the logic of functional dependencies between devices;
- individual asset metrics based on CVSS or RPN that assess the criticality of nodes but ignore the structural context of their interaction [20, 21].

4.2. 5G-based systems

In 5G networks, threats are associated with virtualized functions, APIs, dynamic slices, and MEC applications. Existing approaches mainly focus on these aspects:

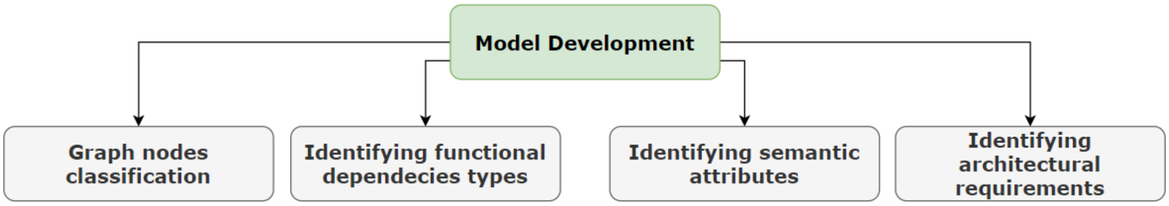
Model Development
Graph nodes classification
Identifying functional dependecies types
Identifying semantic attributes
Identifying architectural requirements

Figure 1: The general approach.

- vulnerability analysis of APIs, orchestrators, and configurations in VNFs [22] allows for identifying individual threats. Still, it does not allow assessing their impact on other components, particularly in the OT layer;
- graph-based policy compliance frameworks that provide access control based on dependencies between services [23], but do not cover physical infrastructure or industrial processes;
- assessment of slice isolation and cross-slice attack vectors [24], which demonstrates threats in a virtual environment but does not analyze how changes in the 5G network affect critical OT assets;
- ML/AI-based tools, such as GNN-based anomaly detection [25], can detect anomalies in traffic but do not provide an interpretable model of functional dependencies between system nodes.

4.3. Identified limitations

The analysis allows us to identify several key limitations of existing approaches:

- lack of an integrated representation of the hybrid ICS/OT+5G environment;
- restrictions on the display of inter-node dependencies in the physical, logical, and service space;
- ignoring the time dynamics of impact propagation (activation time, delay, duration);
- inability to support cascading risk assessment that takes into account contextual interactions between ICS/OT and VNFs;
- insufficient flexibility in graph structures adapted to slice, MEC, and IIoT dynamics [25, 26].

Current approaches provide a local risk assessment or a limited representation of the interaction logic between components. None of them allows for a formalized structure that can take into account: multi-level topology, temporal attributes, and criticality of assets in connection with technological management processes.

This creates a justified need to develop a functional dependency graph (FDG) that would combine the logic of interconnections, support impact propagation modeling, and form the basis of a systemic risk assessment.

5. Functional dependency graphs requirements

The integration of 5G with ICS/OT creates a multi-level environment where components with different natures (physical, virtual, mobile) interact through functional dependencies. In such an environment, identifying and assessing cybersecurity risks requires an abstract but sufficiently accurate representation of the relationships between components. For this purpose, we propose a functional dependency graph model that serves as a structural basis for further quantitative risk analysis. This section formalizes the basic requirements for such a model at the architectural and semantic levels. The general approach for this is shown in Figure 1.

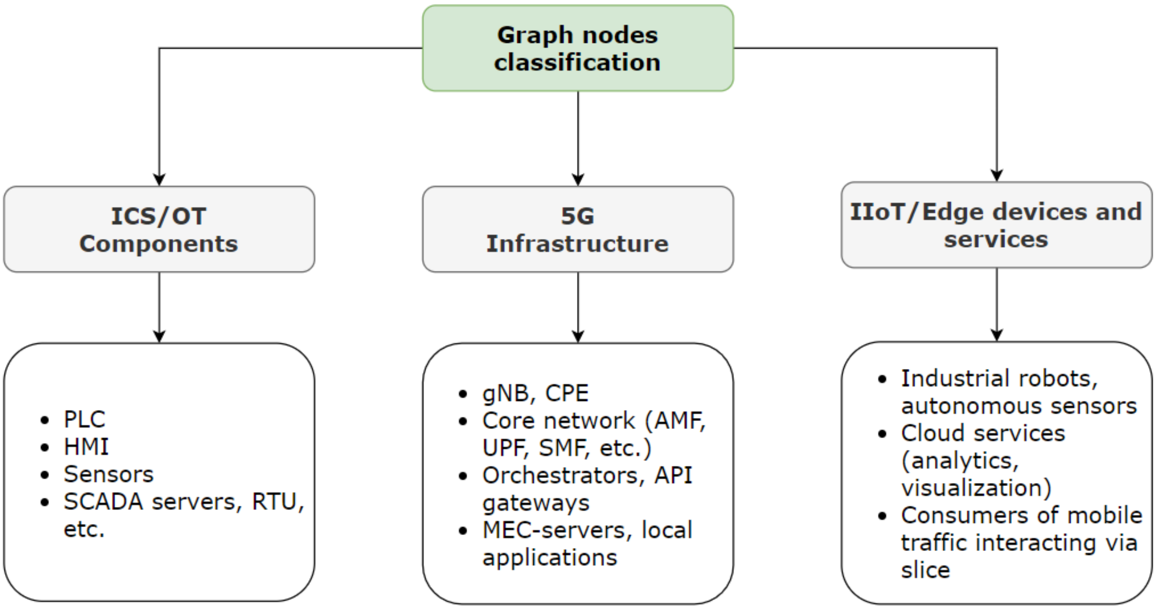
Graph nodes classification
ICS/OT Components
5G Infrastructure
IIoT/Edge devices and services
PLC
HMI
Sensors
SCADA servers, RTU, etc.
gNB, CPE
Core network (AMF, UPF, SMF, etc.)
Orchestrators, API gateways
MEC-servers, local applications
Industrial robots, autonomous sensors
Cloud services (analytics, visualization)
Consumers of mobile traffic interacting via slice

Figure 2: Classification of the Graph nodes

5.1. Graph nodes classification

In the context of 5G-integrated ICS/OT networks, the FDG nodes are classified by their functional role and origin, as shown in Figure 2.

ICS/OT components cover the classic elements of process control systems, such as programmable logic controllers (PLCs), human-machine interfaces (HMIs), sensors, SCADA servers, remote terminal units (RTUs), etc. These nodes are directly connected to the physical process and often have limited computing resources.

5G infrastructure includes hardware and software components of the fifth-generation mobile network, including base stations (gNB, CPE), network core functions (AMF, UPF, SMF), MEC servers with local applications, as well as orchestrators and API gateways. They implement network virtualization, traffic routing, and provide mobile connectivity for critical services.

IIoT/Edge devices and services encompass endpoint intelligent devices (e.g., autonomous sensors, industrial robots), as well as cloud-based analytics and visualization services. It also includes programs and systems that interact with the network through slides and process data in real time.

This classification serves as the basis for formalizing the FDG structure, allowing you to display all relevant elements of the hybrid environment and set rules for building inter-node functional dependencies in the subsequent mathematical model.

5.2. Functional dependencies types

In the structure of a functional dependency graph, edges serve to formalize internode interactions that have functional, logical, or operational significance. The typology of edges determines the nature of the dependency between the system components and allows you to display its dynamic properties. Depending on the nature of the interaction, the following main types of functional links are distinguished, as shown in Figure 3.

Data Dependency occurs when one node (A) generates or transmits information that is critical to the functioning of another node (B). Such a dependency is typical for sensor monitoring scenarios, when data from the sensor is sent to the controller (Sensor → PLC), or process visualization (PLC → HMI).

Control Dependency occurs when one component determines the logic, state, or activation of another. For example, an MEC application can initiate an action by a device (MEC App → Actuator), or an SMF

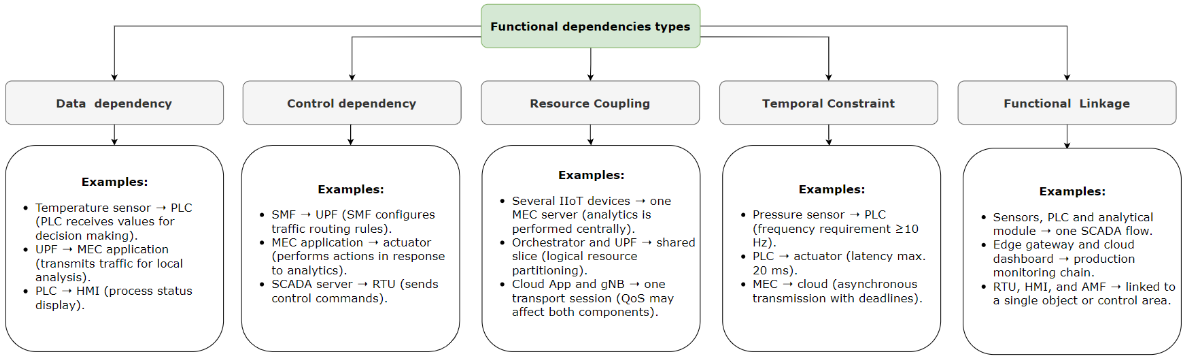
Functional dependencies types
Data dependency
Control dependency
Resource Coupling
Temporal Constraint
Functional Linkage
Examples:
• Temperature sensor → PLC (PLC receives values for decision making).
• UPF → MEC application (transmits traffic for local analysis).
• PLC → HMI (process status display).
Examples:
• SMF → UPF (SMF configures traffic routing rules).
• MEC application → actuator (performs actions in response to analytics).
• SCADA server → RTU (sends control commands).
Examples:
• Several IIoT devices → one MEC server (analytics is performed centrally).
• Orchestrator and UPF → shared slice (logical resource partitioning).
• Cloud App and gNB → one transport session (QoS may affect both components).
Examples:
• Pressure sensor → PLC (frequency requirement ≥10 Hz).
• PLC → actuator (latency max. 20 ms).
• MEC → cloud (asynchronous transmission with deadlines).
Examples:
• Sensors, PLC and analytical module → one SCADA flow.
• Edge gateway and cloud dashboard → production monitoring chain.
• RTU, HMI, and AMF → linked to a single object or control area.

Figure 3: Types of functional dependencies.

network element can control flows through UPF (SMF → UPF). Such dependencies are critical for the correct functioning of a distributed architecture.

Resource Coupling is a resource or physical dependency that is related to the use of a shared computing, network, or slice resource. In cases where several nodes use the same MEC server or UPF, an indirect functional dependency (IIoT1 → MEC ← IIoT2) occurs, which can become a source of cascading failures when a common resource is overloaded or attacked.

Temporal Constraint displays the constraints imposed by temporal characteristics, such as delay, refresh rate, and timeout duration. For example, the interaction between a sensor and a controller may require a delivery guarantee within 10 ms. Violation of the time parameters can lead to degradation of the control process or an emergency condition.

Logical or service connectivity (Functional Linkage) defines situations where multiple nodes implement the same logical or process flow. An example is components that are part of the same SCADA flow or process route, even if there is no direct data or command transfer between them.

Each edge in the FDG is described by a set of semantic attributes, including:

- direction of interaction (unidirectional → or reciprocal ↔);
- type of dependency (data, control, resource, etc.);
- reaction time or permissible delay (in milliseconds);
- degree of functional impact (low, medium, high);
- the possibility of degradation (with the loss of part of the functionality)..

5.3. Semantic attributes of nodes and links

To enable quantitative analysis of cybersecurity risks in hybrid 5G-enabled ICS/OT environments, it is necessary to supplement the functional dependency graph with a system of semantic attributes. This metadata allows not only to identify the functional role of nodes and links, but also to assess the potential impact of a breach, the level of criticality, and the sensitivity of the system to attacks.

The main semantic attributes include:

- Criticality: defines the degree of importance of a node to ensure the continuity of a technological or management process. The value can be assigned manually by an expert (e.g., based on HAZOP or PHA procedures) or determined automatically by analyzing the role of the node in the SCADA logic. Components with high criticality (e.g., a PLC or actuator in a safety chain) are prioritized in the risk assessment.
- Trust Level: displays the level of trust in a component or source of interaction, which is key for modeling threats in mixed security environments. A low trust level can be assigned to external IIoT devices, third-party APIs, slice-tenants, or nodes with unknown security status. The attribute is used when modeling penetration or lateral movement scenarios.

- Latency / Frequency: includes the communication parameters: maximum allowable latency and refresh rate. For real-time nodes (e.g., HMI - actuator) or critical URLLC networks, these attributes define the allowable window of influence within which an attack can lead to a technological failure.
- Node Role: defines the primary purpose of a node in the information system, such as sensing, processing, storage, communication, control, and actuation. This classification allows you to analyze potential chains of influence, for example: sensor - processing - reaction.
- Redundancy / Failover: indicates the presence of an alternate route or redundant component. If a node has redundancy (for example, a dual MEC server or multiple parallel sensors), its failure has a lower risk priority. This attribute is taken into account when modeling system resilience.
- Impact Range: determines the scope or number of components that can be impacted if a node is compromised. For example, a compromise of a slice manager can affect dozens of IIoT applications. This allows to assess the scale of cascading risk in a dynamic environment.

5.4. Architectural requirements for FDG

Designing a functional dependency graph for environments that integrate ICS/OT components with 5G infrastructure requires taking into account the multidimensional complexity of such integration. Given the increasing interdependence of physical, virtualized, and mobile elements, the FDG model must provide a formalized representation of relationships between components without losing semantic accuracy. Thus, it is possible to identify the following basic requirements: heterogeneity, dynamism, scalability, compatibility with data sources, and suitability for risk analysis.

One of the basic requirements is to support heterogeneity. The graph should unifiedly cover both physical objects (sensors, actuators, RTUs) and software-defined functions (VNFs, MEC services, cloud controllers). It is important that the model allows for a scalable representation of differences in communication protocols, timing characteristics, and functional roles of nodes without reducing them to simplified types.

The next critical property is adaptability to network dynamics. The features of 5G infrastructures, including device mobility, dynamic slice creation, and real-time routing changes, require FDG to be able to incrementally update. For this purpose, the model must be integrated with telemetry sources, CMDBs, and orchestrator event streams, allowing the dependency structure to be updated without manual intervention.

Since real-world industrial deployments involve tens or hundreds of thousands of interconnected nodes, scalability is a must. The graph must support processing large amounts of data without performance degradation, using optimized data structures and the ability to compute on subgraphs with parallel processing.

It is also important to ensure interoperability with security and management systems. The FDG should have built-in mechanisms for interacting with SCADA, SIEM, CMDB, vulnerability scanners, and other tools that can automatically provide both structural and semantic information about system components. This will avoid manual filling of the graph and ensure its compliance with the actual state of the environment.

Moreover, the graph structure should be analytically suitable for risk assessment. This includes support for simulating the spread of threats, identifying critical nodes, analyzing chains of influence, and prioritizing response scenarios. The graph should serve not only as a visualization tool, but also as a basis for formalized scenario analysis that takes into account time constraints, the level of criticality of assets, and trust in sources of influence.

The formed model of the FDG functional dependency graph allows us to represent the structure of a hybrid ICS/OT-5G system as a set of links enriched with semantics and criticality. This creates the basis for further mathematical formalization and construction of the risk assessment model in the following sections. The approach allows to take into account the specifics of inter-network interaction, time dependence and dynamics of modern industrial environments.

5.5. Formalization of a mathematical model of a functional dependency graph

In order to formalize the representation of interconnections in hybrid ICS/OT environments with integrated 5G infrastructure, it is proposed to use an oriented annotated dependency graph. Such a structure allows not only to display the functional topology of the system but also to set semantic attributes at each level necessary for further risk calculation and modeling of integrity violation scenarios.

Graph structure. A functional dependency graph is defined as a tuple:

$$\mathcal{G} = (V, E, \Phi_V, \Phi_E),$$

where:

- $V = \{v_1, v_2, ..., v_n\}$, a finite set of nodes, each of which corresponds to a component of the system;
- $E \subseteq V \times V$, a set of oriented edges that define the direction of functional or resource influence;
- $\Phi_V : V \to \mathcal{A}_V$, nodes attribution function;
- $\Phi_E : E \to \mathcal{A}_E$, edges attribution function.

Nodes attribution. For each node $v_i \in V$, attribute vector is defined:

$$\Phi_V(v_i) = (c_i, t_i, r_i, f_i, \rho_i)\,,$$

where:

- $c_i \in [0, 1]$, component criticality;
- $t_i \in [0, 1]$, trust level;
- $r_i \in \mathcal{R}$, functional role;
- $f_i \in \{0, 1\}$, reservation availability;
- $\rho_i \subseteq V$, area of influence in case of node failure.

Edges attributes. For each edge, $e_{ij} = (v_i, v_j) \in E$ a set of parameters is set:

$$\Phi_E(e_{ij}) = (\delta_{ij}, \lambda_{ij}, \omega_{ij}, \mu_{ij}, \gamma_{ij})\,,$$

where:

- $\delta_{ij} \in \mathcal{D}$, dependency type (Data, Control, Resource, Temporal, Functional);
- $\lambda_{ij} \in \mathbb{R}^+$, time characteristic of communication;
- $\omega_{ij} \in [0, 1]$, impact weighting factor;
- $\mu_{ij} \in \{0, 1\}$, direction (0 - unidirectional, 1 - bidirectional);
- $\gamma_{ij} \in \{0, 1\}$, sign of degradation.

Formalization of risk spread. The risk transfer along the graph is described by the transformation operator:

$$R(v_j) \leftarrow R(v_j) + \omega_{ij} \cdot \lambda(\delta_{ij}) \cdot R(v_i) \cdot (1 - t_j) \cdot \gamma_{ij},$$

where:

- $\lambda(\delta_{ij})$, impact modifier depending on the type;
- t_j, level of trust in the node v_j;
- γ_{ij}, whether the risk is transferred in case of partial degradation.

Aggregated graph metrics

- Total risk of the system:

$$R_{\text{total}} = \sum_{v_i \in V} c_i \cdot R(v_i).$$

- Depth of risk spread, the maximum length of the chain of influence;
- Identification of critical nodes through the product of criticality, number of outgoing links, and edge weights:

$$\kappa(v_i) = c_i \cdot \deg^{\text{out}}(v_i) \cdot \bar{\omega}_i.$$

This approach provides the basis for further development of a risk assessment model that takes into account both the structural topology and semantic characteristics of nodes and links in a hybrid 5G-enabled environment.

6. Formalization of risk assessment model

This section introduces a formalized model for cyber risk quantification in hybrid 5G-enabled ICS/OT networks based on the previously defined Functional Dependency Graph (FDG). The model captures the semantics of intercomponent dependencies, component criticality, trust levels, timing constraints, and cascading effects. The proposed approach supports both static and dynamic risk assessment, enabling scenario-based propagation modeling.

6.1. Node-level risk initialization

Let the initial risk level for each node $v_i \in V$ be defined as:

$$R_0(v_i) = p(v_i) \cdot c_i \cdot (1 - t_i), \tag{1}$$

where:

- $p(v_i) \in [0, 1]$ is the estimated probability of compromise (based on CVSS score, SIEM alerts, or other external indicators),
- $c_i \in [0, 1]$ is the criticality of the component,
- $t_i \in [0, 1]$ is the trust level associated with the node.

6.2. Risk propagation via FDG

The propagation of risk across the graph is defined recursively. For a node v_j at time t, its updated risk value is:

$$R_t(v_j) = R_t(v_j) + \sum_{v_i \in \text{pred}(v_j)} R_{t-1}(v_i) \cdot \omega_{ij} \cdot \lambda(\delta_{ij}) \cdot (1 - t_j) \cdot \gamma_{ij} \cdot \beta_{ij}(t) \tag{2}$$

with the following parameters:

- ω_{ij}: normalized edge weight between v_i and v_j,
- $\lambda(\delta_{ij})$: dependency type coefficient (e.g., Control, Data),
- $\gamma_{ij} \in \{0, 1\}$: edge activation indicator (e.g., based on redundancy or failure state),
- $\beta_{ij}(t) \in [0, 1]$: temporal impact modifier defined as:

$$\beta_{ij}(t) = \exp(-\theta \cdot \tau_{ij}), \tag{3}$$

where τ_{ij} is the communication delay or update frequency, and θ is a decay parameter.

6.3. Threat propagation scenarios

Let $S = \{v_s^1, \ldots, v_s^k\} \subset V$ denote a set of initially compromised nodes. For each v_s^k, we initialize $R_0(v_s^k) = 1$. The propagation is iteratively evaluated over T discrete time steps using:

$$R^{(t)}(v_j) = f\left(R^{(t-1)}(v_j), \sum R^{(t-1)}(\text{pred}(v_j))\right). \tag{4}$$

The cumulative risk evolution over time is captured by the matrix:

$$\mathbf{R}_T \in \mathbb{R}^{|V|\times T},$$

where each row corresponds to a node and each column corresponds to a discrete time step. This matrix captures the dynamics of threat evolution across the graph and allows for temporal analysis, such as identifying peak risk intervals, delay-sensitive propagation chains, and time-critical influence paths.

6.4. Node and system-level risk metrics

To support prioritization and mitigation, the following metrics are defined:

- **Accumulated Risk Score (ARS):**

$$ARS(v_i) = \sum_{t=1}^{T} R^{(t)}(v_i). \tag{5}$$

  This metric represents the total amount of risk that has been experienced or accumulated by node v_i over the entire observation period T. It integrates both direct exposure and indirectly propagated threats. ARS is useful for identifying persistently affected nodes, even if their instantaneous risk is low at any specific time.
- **Propagation Score (PS):**

$$PS(v_i) = \sum_{v_j \in \mathrm{succ}(v_i)} \omega_{ij} \cdot \lambda(\delta_{ij}) \cdot (1 - t_j). \tag{6}$$

  Propagation Score estimates the ability of a node v_i to spread risk to its successors $\mathrm{succ}(v_i)$. It takes into account the strength of outgoing functional dependencies (ω_{ij}), the influence factor of the dependency type ($\lambda(\delta_{ij})$), and the vulnerability of the target node (via $1 - t_j$). High PS values indicate that the node is a potential amplifier of threats and may be critical in cascading scenarios.
- **Critical Impact Index (CII):**

$$CII(v_i) = c_i \cdot ARS(v_i) \cdot \mathrm{deg}^{\mathrm{out}}(v_i). \tag{7}$$

  The Critical Impact Index quantifies the strategic importance of node v_i in terms of its intrinsic criticality (c_i), cumulative risk over time (ARS), and structural outreach (number of outgoing edges). It identifies nodes whose compromise could have a high systemic effect, making them primary candidates for protection and redundancy planning.

These indices are used to identify high-impact nodes, centrality of propagation, and systemic exposure levels.

6.5. System aggregation

Risk can also be aggregated at the subsystem or full-system level:

$$R_{\text{subgraph}} = \sum_{v_i \in V_s} ARS(v_i), \tag{8}$$

$$R_{\text{system}} = \sum_{v_i \in V} ARS(v_i), \tag{9}$$

where V_s denotes the set of nodes in a specific subgraph (e.g., slice, physical zone, MEC region).

7. Implementation and integration architecture

The Functional Dependency Graph (FDG) will be implemented as a separate service module within the risk assessment system for 5G-integrated ICS/OT environments. The main function of the module will be to build an oriented graph $G = (V, E)$, where the set of nodes V represents assets and services (PLC, SCADA, MEC, UPF, etc.), and the edges E are typed dependencies (data, control, resource, temporal, functional).

The initial formation of the graph will be done by aggregating data from several sources:

- SCADA/IIoT telemetry, to identify technological connections;
- CMDB/SIEM, for obtaining inventory, trust levels, and topology;
- 5G Orchestrator APIs (e.g., OSM/ONAP), for extracting slice configurations, VNF connections, and mobile routes;
- network monitoring, to dynamically update current interactions.

The graph will support real-time updates through an event-driven pipeline that responds to new devices, slice changes, MEC service activation, or flow switching. Nodes have semantic attributes:

- $C(v)$ – criticality;
- $T(v)$ – trust;
- $R(v)$ – role in the process (e.g., sensing, control, actuation);
- $I(v)$ – potential impact radius.

The edges $e \in E$ are formed with attributes of the type $\tau(e) \in \{\text{data}, \text{control}, \text{resource}, \text{temporal}, \text{functional}\}$, as well as metadata: delay, frequency, direction, possibility of degradation. To interact with the Risk Assessment Engine, the graph is exported as an adjacency matrix with dependency weights, which allows you to model risk propagation in the form of discrete dynamics on the graph.

The module will be implemented as a microservice orchestrated via Docker/Kubernetes with a REST API for integration with other scanner subsystems. This will allow for flexible deployment in MEC environments, industrial gateways, or cloud-based SCADA. Optimization of graph operations (e.g., centrality, shortest path with attributes) is implemented on the basis of the `NetworkX` or `Neo4j Graph Data Science API` frameworks.

Thus, FDG will act as the core of semantic connectivity in the scanner architecture, allowing move from point vulnerabilities to complex scenario risk analysis in a heterogeneous environment.

8. Future work

The concept of building a functional dependency graph (FDG) and the corresponding risk assessment model proposed in this paper lays the foundation for the formation of a new approach to vulnerability scanning in 5G-integrated ICS/OT environments. In further research, it is planned to implement a full-fledged vulnerability scanner architecture that will integrate the FDG module as the core of scenario and contextual risk analysis. This area is part of a separate research project dedicated to the creation of a specialized scanner for hybrid cyber-physical systems, the results of which are currently being prepared for publication.

To verify and validate the proposed model, it is planned to build a testbed using 5G network deployment tools based on open-source components. An isolated laboratory infrastructure has already been created, which includes open-source implementations of the 5G core and RAN, providing a full-fledged slice-oriented architecture with the ability to control through an orchestration interface. The experience of deploying such systems is analyzed in detail in [27, 28], where key platforms are compared and their performance is evaluated in the context of practical implementation.

The next step is to connect industrial sensors, PLC emulators, and MEC applications, which will create a controlled environment for testing FDG construction mechanisms, generating functional dependencies, and modeling cascading effects in the event of a vulnerability or attack. Such an approach will not only confirm the operability of the developed model, but will also allow for a quantitative assessment of the effectiveness of the proposed method in the context of dynamic changes in the topology and 5G services.

In the future, it is planned to integrate FDG with machine learning (ML) mechanisms to automatically interpret event streams, build behavioral dependencies, and detect anomalies. A separate direction will be to extend the model to multi-segment and inter-network scenarios, taking into account cloud edge platforms and transitive dependencies between slices or MEC services.

9. Conclusions

This paper presents a formalized methodology for modeling functional dependencies in hybrid ICS/OT environments with 5G integration, and proposes a risk assessment model based on the constructed functional dependency graph (FDG). The research was motivated by the identified limitations of existing approaches to cyber risk analysis that do not take into account the dynamic, heterogeneous, and interdependent nature of modern cyber-physical systems, in particular in the context of 5G architectures.

The proposed approach provides a unified representation of system components, both physical (e.g., PLCs, RTUs, sensors) and virtualized (e.g., UPFs, SMFs, MEC applications), in the form of an oriented graph with node annotation by semantic attributes. The edges of the graph describe typicalized dependencies: data transfer, control, resource sharing, time constraints, and logical connectivity. This allows you to model cascading effects and interactions between components.

A mathematical formalization of the FDG is developed, taking into account the criticality of nodes, the level of trust, time characteristics, fault tolerance, and radius of influence. This framework serves as the basis for a risk propagation model that supports both static and scenario analysis. The model allows you to calculate risk in dynamics, identify critical nodes, and prioritize incident response.

On the practical side, FDG is planned to implement as a service module that integrates telemetry, orchestrator data, SCADA topologies, and network configurations. The implementation will be focused on a microservice architecture with the ability to deploy in MEC environments, industrial gateways, or cloud-based SCADA systems, using modern graph computing libraries.

The obtained results confirm the feasibility of using FDG for contextual and dynamic analysis of cybersecurity risks in next-generation industrial networks. The proposed approach forms the basis for the further development of a specialized vulnerability scanner focused on ICS/OT+5G environments.

Future research will focus on integrating FDG with machine learning methods to build behavioral dependencies, as well as validating the model in a testbed with real devices and MEC applications. A separate area of focus will be extending the model to multi-segment scenarios, taking into account inter-network dependencies, slice architecture, and edge cloud platforms.

Acknowledgments

This work was supported by the Shota Rustaveli National Foundation of Georgia (SRNSFG) (NFR-2214060) and “Methods of building protected multilayer cellular networks 5G/6G based on the use of artificial intelligence algorithms for monitoring the country’s critical infrastructure objects” (# 0124U000197).

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] M. M. Aslam, A. Tufail, R. A. A. H. M. Apong, L. C. De Silva, M. T. Raza, Scrutinizing security in industrial control systems: An architectural vulnerabilities and communication network perspective, IEEE Access (2024). doi:10.1109/access.2024.3394848.

[2] T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan, N. Alnazzawi, Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions, Sensors 25 (2025) 213. doi:10.3390/s25010213.

[3] A. Gelmini, 5G SCADA-Based Control System, Doctoral dissertation, University of South Wales, United Kingdom, 2024. Available via ProQuest Dissertation Database.

[4] H. M. Shamsuzzaman, M. Mosleuzzaman, A. Mia, A. Nandi, Cybersecurity risk mitigation in industrial control systems: Analyzing physical, hybrid and virtual test bed applications, Academic Journal of Science, Technology, Engineering & Math Education 1 (2024) 19–39. doi:10.69593/ajaimldsmis.v1i01.123.

[5] H. Altaleb, L. Ady, P. J. Varga, Z. Rajnai, Acsra ics: Automated cyber security risk assessment methodology for industrial control systems, Acta Polytechnica Hungarica 22 (2025) 47–74. doi:10.12700/aph.22.2.2025.2.4.

[6] S. Michaelides, S. Lenz, T. Vogt, M. Henze, Secure integration of 5g in industrial networks: State of the art, challenges and opportunities, Future Generation Computer Systems 166 (2025) 107645. doi:10.1016/j.future.2024.107645.

[7] S. Kumar, H. Vardhan, Cyber security of ot networks: A tutorial and overview, arXiv preprint arXiv:2502.14017 (2025). URL: https://arxiv.org/abs/2502.14017.

[8] R. Odarchenko, M. Iavich, A. Pinchuk, Development of a method for automated 5g and beyond network slices penetration testing, Radioelectronic and Computer Systems 2025 (2025) 248–263.

[9] R. Odarchenko, A. Pinchuk, I. Zakutynsky, V. Hnatiuk, O. Polihenko, O. Baranovskyi, Secure 5g network for monitoring state of critical infrastructure facilities, in: Advancements in Cybersecurity, CRC Press, 2025, pp. 331–353.

[10] B. Kotyk, D. Bakhtiiarov, O. Lavrynenko, B. Chumachenko, V. Antonov, V. Fesenko, V. Chupryn, Neural network approach to 5g digital modulation recognition, in: Proceedings of the CEUR Workshop, volume 3925, 2025, pp. 82–92.

[11] D. Bakhtiiarov, B. Chumachenko, O. Lavrynenko, V. Chupryn, V. Antonov, Distribute load among concurrent servers, in: Proceedings of the CEUR Workshop, volume 3826, 2024, pp. 260–266.

[12] W. Knowles, D. Prince, D. Hutchison, J. F. Disso, K. Jones, A survey of cyber security management in industrial control systems, International Journal of Critical Infrastructure Protection 9 (2015) 52–80. URL: https://doi.org/10.1016/j.ijcip.2015.02.002. doi:10.1016/j.ijcip.2015.02.002.

[13] M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Y. Petrova, A. Chaplits, Method of traffic monitoring for DDoS attacks detection in e-health systems and networks, in: CEUR Workshop Proceedings, volume 2255, 2018, pp. 193–204.

[14] M. Zaliskyi, et al., Model building for diagnostic variables during aviation equipment maintenance, in: International Scientific and Technical Conference on Computer Sciences and Information Technologies, 2022, pp. 160–164. doi:10.1109/CSIT56902.2022.10000556.

[15] K. Stouffer, V. Y. Pillitteri, S. Lightman, M. Abrams, A. Hahn, Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Rev. 2, National Institute of Standards and Technology, 2015. URL: https://doi.org/10.6028/NIST.SP.800-82r2. doi:10.6028/NIST.SP.800-82r2.

[16] O. Sushchenko, et al., Airborne sensor for measuring components of terrestrial magnetic field, in: IEEE International Conference on Electronics and Nanotechnology (ELNANO), 2022, pp. 687–691. doi:10.1109/ELNANO54667.2022.9926760.

[17] M. Zaliskyi, Y. Petrova, M. Asanov, E. Bekirov, Statistical data processing during wind generators operation, International Journal of Electrical and Electronic Engineering and Telecommunications 8 (2019) 33–38. doi:10.18178/ijeetc.8.1.33-38.

[18] L. Wang, T. Islam, T. Long, A. Singhal, S. Jajodia, An attack graph-based probabilistic security metric, in: Proceedings of the 22nd Annual IFIP WG 11.3 Working Conference on Data and

Applications Security, 2008, pp. 283–296.

[19] I. Ostroumov, et al., A probability estimation of aircraft departures and arrivals delays, in: Lecture Notes in Computer Science, volume 12950, 2021, pp. 363–377. doi:10.1007/978-3-030-86960-1_26.

[20] M. Mantere, M. Sailio, J. Nikkarila, Challenges of cvss scoring in industrial control systems, in: Proceedings of the IEEE International Conference on Industrial Technology (ICIT), IEEE, 2010, pp. 1035–1040.

[21] O. Ivashchuk, et al., A configuration analysis of Ukrainian flight routes network, in: Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2021, pp. 6–10. doi:10.1109/CADSM52681.2021.9385263.

[22] S. Michaelides, G. Suciu, C. Serbanescu, D. Popescu, Secure integration of 5g in industrial networks, Future Generation Computer Systems (2025). Accepted/In press.

[23] H. K. Kalutarage, L. Yang, Policy compliance verification in 5g networks using graph-based models, Computer Communications 175 (2021) 1–14. doi:10.1016/j.comcom.2021.04.012.

[24] X. Zhang, R. He, Z. Liu, Slice isolation risks in 5g core networks: A threat model and empirical study, IEEE Transactions on Network and Service Management 19 (2022) 3726–3739. doi:10.1109/TNSM.2022.3225260.

[25] Y. Li, Y. Sun, B. Wang, Z. Li, Gnn-based detection of cyber threats in 5g slices, IEEE Access 10 (2022) 78855–78867. doi:10.1109/ACCESS.2022.3191185.

[26] O. Solomentsev, M. Zaliskyi, T. Herasymenko, O. Kozhokhina, Y. Petrova, Efficiency of operational data processing for radio electronic equipment, Aviation 23 (2020) 71–77. doi:10.3846/aviation.2019.11849.

[27] A. Pinchuk, R. Odarchenko, V. Samoilenko, A. Imanbayev, 5g network deployment based on open-source projects: A comparative analysis, in: 2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany, 2023, pp. 596–601. doi:10.1109/IDAACS58523.2023.10348675.

[28] A. Pinchuk, R. Odarchenko, Experimental studies of 5g open-source network performance, in: Proceedings of the International Scientific and Practical Conference Problems of Computer Science, Software Modeling and Security of Digital Systems, 2024, pp. 45–45.