The ICS-SEC KG: An Integrated Cybersecurity Resource for Industrial Control Systems

Kabul Kurniawan*[1,3][0000−0002−5353−7376], Elmar Kiesling[1][0000−0002−7856−2113], Dietmar Winkler[3,5][0000−0002−4743−3124], and Andreas Ekelhart[2,4][0000−0003−3682−1364]

[1] Vienna University of Economics and Business, Austria
[2] SBA Research, Favoritenstraße 16, Vienna, Austria
[3] Austrian Center for Digital Production, Austria
[4] University of Vienna, Austria
[5] Vienna University of Technology, Austria

Abstract. The convergence of Information Technology (IT) and Operational Technology (OT) in Industrial Control System (ICS) comes with severe cybersecurity challenges that increasingly pose threats to critical infrastructures. In this challenging environment, numerous standards and data sources exist that aim to facilitate the exchange of information and guide security assessment, detection, and mitigation. Despite this wealth of information, the relevant data is currently fragmented and not available as an integrated knowledge base. Existing approaches to link and integrate Cyber Threat Intelligence (CTI) across sources and represent them in a machine interpretable and interoperable manner mainly focus on IT security in general, leaving the ICS domain largely unexplored. To fill this critical gap, we present an integrated ICS-SEC Knowledge Graph (ICS-SEC KG) to support analyzing and managing the security of ICSs. We describe the conceptualization and pipeline to construct the KG from a broad range of ICS cybersecurity data sources as well as the underlying processes and infrastructure to continually update it. To ensure quality and consistency, we apply ontology validation and a set of SHACL constraints. We validate our approach in two application scenarios derived from real-world security incidents in the industrial domain and demonstrate its usefulness for threat intelligence exploration and vulnerability assessment. All materials and links for this paper are available at https://github.com/sepses/ics-sec-kg.

Keywords: Knowledge graph, Cybersecurity, Threat Intelligence, Industrial Control System, Cyberphysical Production System, Industry 5.0

1 Introduction

Industrial Control Systems (ICSs) play a pivotal role in critical infrastructures where they control, manage, and monitor industrial processes across sectors such

* {first.last}@wu.ac.at

as energy, water supply, transportation, and manufacturing [28]. Such critical domains increasingly integrate Information Technology (IT) and Operational Technology (OT), often enabled through Internet of Things (IoT) devices and cloud services. While this integration can increase efficiency and reliability within ICSs, it also introduces cybersecurity risks and threats [5]. Cyberattacks targeting ICSs often have severe consequences, ranging from operational disruption, to physical damage, to risk to public safety and significant economic losses.

Stuxnet[6], which targeted Iran's nuclear program in 2010, was the first prominent malware that specifically targeted industrial control systems. Since then, a significant increase in OT attacks has been observed[7]. Triton[8], a malware deliberately targeting a Safety Instrumented System (SIS) in a petrochemical plant has been discovered in 2017 in the middle east. In 2021, a cyberattack on a Florida water treatment facility[9] enabled attackers to manipulate the levels of chemicals in the water supply. Although no casualties were reported, the potential consequence posed a significant threat to public health and safety. These selected incidents illustrate the vulnerability of ICS infrastructure against cyberattacks; hence, enhancing cybersecurity in ICS becomes imperative.

To this end, a number of cybersecurity resources, standards, and information sources for ICS are available and continuously evolving in response to the escalating threat landscape. These resources are maintained by organizations such as (i) US-CERT (United States Computer Emergency Readiness Team), which has proposed the Automated Indicator Sharing (AIS) initiative[10] aimed at disseminating indicators in machine-readable format; (ii) National Institute of Standards and Technology (NIST), which provides guidance for ICS Security [28]; and (iii) MITRE, which has extended their "ATT&CK framework" specifically for ICSs [2] to improve understanding and mitigation of potential threats.

These resources are important and security analysts rely heavily on them to navigate the intricate landscape of cyberattacks targeting ICS environments. However, the diversity of representations and formats across these resources poses significant challenges and inhibit their effective utilization [3]. Consequently, there is a pressing need for a unified representation of heterogeneous threat data that enhances interoperability and streamlines automated processes for threat detection, response, and mitigation.

This comes at a time when research into cybersecurity of ICSs is attracting considerable attention [12,3] – and the need to support key activities such as threat modelling [9], intrusion detection [12], and threat hunting [13] is increasingly recognized. Nevertheless, research focusing on effective knowledge in-

6 https://spectrum.ieee.org/the-real-story-of-stuxnet
7 https://www.mandiant.com/resources/blog/ontology-understand-assess-operational-technology-cyber-incidents
8 https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/
9 https://edition.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html
10 https://www.us-cert.gov/ais

tegration (particularly CTI knowledge) within the ICS domain remains scarce. Most existing studies focus on general IT security contexts [29,14] and leave ICS largely unexplored. This gap is significant as ICS infrastructures exhibit distinct characteristics and different attack landscapes compared to conventional IT security environments [21].

Therefore, the **goal of this paper is to provide an integrated resource that helps to understand how ICSs can be compromised and protected through associated prevention, detection and mitigation techniques**. To this end, we developed ICS-SEC KG, a semantically integrated resource on cybersecurity knowledge on industrial control systems gathered from relevant publicly available sources of CTI information and standards targeting the ICS domain. The constructed knowledge graph supports use cases such as identification, attribution and contextualization of attack events from ICS environments.

The contributions of this paper are as follows: for ICS cybersecurity research, we advance the state-of-the-art by providing continuously integrated ICS-CTI resources in a machine-interpretable format. This KG can be used to enrich and contextualize ICS related security events during cybersecurity activities, such as security monitoring, attack analysis, and forensics. For Semantic Web research, we provide a specialized ontology and vocabulary tailored specifically for the ICS domain. These semantic constructs define standardized terms, relationships, and metadata attributes for ICS threat intelligence concepts and entities within the knowledge graph. Specifically, we provide the following resources: *(i)* A *Conceptualization*, including an ontology and vocabulary for ICS cybersecurity; *(ii)* A *Knowledge Graph* continuously populated with instances for ICS cyber threat intelligence constructed from publicly available ICS cybersecurity sources; and *(iii) Data access* services to facilitate flexible consumption of the constructed knowledge graph. Furthermore, we illustrate the utility of the ICS-SEC KG in multiple cybersecurity use-case scenarios in the ICS domain.

The remainder of this paper is organized as follows: Section 2 provides background on ICS cybersecurity and common information sharing standards in the domain; Section 3 reviews related work in the area of cybersecurity Knowledge Graphs (KGs) and ontologies; Section 4 introduces our ICS-SEC KG and explains its construction and maintenance, including vocabularies, data acquisition mechanisms, and updating pipelines; it also provides an overview of the provided mechanisms to access the KG and discusses its sustainability, maintenance and extensibility; Section 5 illustrates the usefulness of the resource by means of two example use cases; and Section 6 discusses some limitations, concludes, and gives an outlook on future work.

2 Background

In this section, we provide a brief introduction to ICSs and their cybersecurity challenges (Section 2.1) and introduce the reader to existing information sharing standards in the domain (Section 2.2).

2.1 ICS Cybersecurity at a Glance

Compared to "standard" IT security, ICS cybersecurity has different characteristics, unique risks and threat landscapes, and vast differences in the (potential) impact. Whereas conventional IT security typically prioritizes the protection of confidentiality, followed by integrity and availability (also known as "CIA-triad"), ICS cybersecurity is often more focused on protecting systems/equipment against failure or damage, ensuring human safety, and ultimately protecting human lives [3]. Cybersecurity attacks in the ICS domain are typically complex in that they involve adversaries that perform actions that traverse system boundaries, often with severe real-world impacts. For instance, adversaries may leverage initial access to one system (e.g., a workstation) to manipulate or reprogram another system (e.g., a Programmable Logic Controller (PLC)) in order to finally cause a physical impact on yet another system (e.g., a Collaborative Robot (COBOT), power plant, etc.), potentially resulting in a safety incident [15]. Architectural models for the design of ICSs can help to map such complex scenarios.

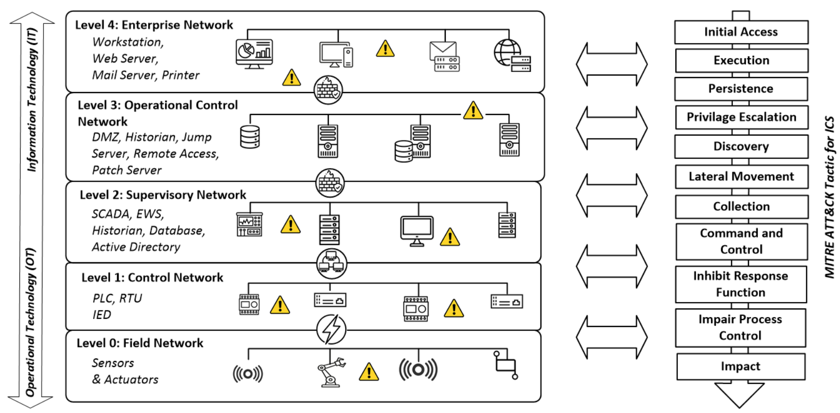

Fig. 1: Purdue Enterprise Reference Architecture mapped to MITRE ATT&CK Tactics for ICS

One of the most widely recognized ICS architectures is the *Purdue Enterprise Reference Architecture (PERA)* which organizes ICSs models into several layers [31]. These layers represent network segmentation, interconnections, and interdependencies of the major components in ICSs. Figure 1 illustrates these layers and their possible mapping to an ICS attack kill-chain (i.e., attack "tactics") from MITRE ATT&CK [2]. Although this mapping does not entail an absolute one-to-one correspondence, typical ICS attacks start from "initial access" at a higher ICS level (e.g., Level 4) to achieve "impact" at lower levels (e.g., Level 0). We briefly explain each level as follows: The lowest ICS level (Level 0), also known as *Field network*, is where physical processes are performed. This includes sensors, actuators, and other machinery equipment. *Basic Control Network* (Level 1) comprises instruments that send commands to the devices at *Level 0*. Devices typically found at this level include PLCs, Remote terminal units (RTUs), and other Intelligent End Devices (IEDs). *Supervisory Network* (Level 2) contains systems that supervise, monitor, and control physical processes such as Supervisory Control and Data Acquisition (SCADA), Human-Machine Interfaces (HMIs), Distributed Control Systems (DCSs), etc. *Operational Control Network* (Level 3) contains customized OT systems that manage production workflows on the shop floor, such as Manufacturing Execution Systems (MESs), Data historians, etc. *Enterprise Network* (Level 4) is the typical IT network where key business functions are executed, including the orchestration of manufacturing operations. This includes Enterprise Resource Planning (ERP), Workstations, Web and Mail servers, etc.

2.2 ICS Cybersecurity Information Standards and Resources

Security analysts rely on a variety of standards and structured sources that provide information on cybersecurity issues and guidance on mitigating cyber threats targeting ICSs. Key resources that analysts often need to access and cross-reference include:

- **MITRE ATT&CK**, which is a collection of adversary tactics and techniques based on real-world observations; a version that has been developed specifically for attack patterns targeting the ICS domain is *MITRE ATT&CK for ICS*. In ATT&CK, "tactics" represent the *what*, i.e., general attack steps that are combined into a so-called "cyber kill chain" of steps [4]. Particular attacks then use specific techniques (representing the *how*) to implement a tactic. The MITRE ATT&CK dataset is available in a structured format (Structured Threat Information eXpression (STIX)[11]).
- **Industrial Control System Advisories (ICSAs)** aim to provide timely information about current security issues, vulnerabilities, and exploits surrounding ICSs. ICSAs have been published by various organizations (e.g., the U.S. Cybersecurity and Infrastructure Security Agency (CISA)), communities (e.g., the ICS Advisory Project [12]) and vendors (e.g., Siemens [13], Cisco [14]).
- **National Vulnerability Database (NVD)**[15] is a U.S. government repository that provides Common Vulnerabilities and Exposures (CVEs) of software and hardware products, represented via the Common Platform Enumeration (CPE) standard. These vulnerabilities include Common Vulnerability Scoring System (CVSS) scores that can be used to measure the "criticality" level of vulnerabilities.

[11] https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html
[12] https://www.icsadvisoryproject.com/
[13] https://www.siemens.com/global/en/products/services/cert.html#SiemensSecurityAdvisories
[14] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory
[15] https://nvd.nist.gov/

- **Common Weakness Enumeration (CWE)** and **Common Attack Pattern Enumeration and Classification (CAPEC)** are community-developed lists detailing software and hardware weaknesses that can lead to vulnerabilities and associated attack patterns coordinated by MITRE.
- **NIST Guide to Industrial Control Systems (ICS)** Security/Guide to Operational Technology Security providing comprehensive guidance that covers risk management, security controls, and incident response designed specifically for ICSA and OT environments [28].
- **ISA 99.02.01/IEC 62443**: Security for Industrial Automation and Control Systems[16] provides guidelines for implementing security measures in industrial automation and control systems.

Beyond those, other ICS resources include unstructured information such as incident reports, forums, blog posts, information on social media, as well as information provided by proprietary products.

3 Related Work

Cybersecurity is a complex, highly dynamic domain characterized by a critical need for organizations to simultaneously maintain a strong understanding of their own assets and vulnerabilities, and an overview of the fast evolving threat landscape. Consequently, KGs that enable the aggregation, integration, and scalable reasoning on internal and external CTI have vast research and application potential. Research interest in cybersecurity knowledge graphs (CSKGs) has therefore grown significantly in recent years and resulted in various KG-based approaches.

3.1 Cybersecurity Knowledge Graphs

By facilitating knowledge aggregation, representation, management, and reasoning, KGs have strong potential to enable model-based support for assessing and managing the security of complex dynamic systems. Furthermore, they can provide a basis for automated interpretation and application of emerging threat intelligence in the context of particular target systems.

This potential is evident in recent surveys of CSKGs [19,20,27,32]. However, they also show that although research on KG-based methods in cybersecurity has grown rapidly in recent years, the number of concrete implementations of these concepts in large, openly available KGs remains limited. A majority of CSKGs are designed with a narrow scope (e.g., focusing on threat actors [11], log analysis [18], vulnerabilities [22], or threat intelligence [23]). Furthermore, they are typically designed to support a narrow target application scenario such as threat discovery, threat investigation, vulnerability management, malware attribution etc. (cf. [19] for an overview). Openly available CSKGs with a broader scope are less common and include UCO [29], CSKG [10], Open-CyKG [24],

[16] https://gca.isa.org/hubfs/ISAGCAQuickStartGuideFINAL.pdf

ATT&CK-KG [16] and the SEPSES-CSKG [14,17] that we extend in this paper. These CSKGs, however, do not address the specifics of the ICS domain.

ICS Knowledge Graphs on the other hand tackle challenges that emerge when IT and OT systems are combined. Recently proposed ICS KGs include [26], which introduces a method to construct CSKGs for specific industrial control scenarios starting from network layout and asset information. The approach applies information extraction techniques to compile a custom KG of vulnerability information for the particular assets in a given network on demand. Focusing more specifically on reconnaissance techniques (RTs), [8] introduces an RT-ITS graph that links RTs together using MITRE ATT&CK ICS. The focus is on high-level conceptualization and demonstration by example and the scope and size of the resulting KG is not discussed in detail. Finally, [7] introduces a machine learning approach on KGs for context-aware security monitoring. Overall, existing KGs developed in the context of ICSs have not been built from a rich set of cybersecurity knowledge sources and tend to only provide examples for specific security scenarios, instead of offering publicly available knowledge bases.

3.2 ICS Ontologies

Another stream of related work is ICS Ontologies, which primarily aim to conceptualize the ICS domain and leverage the resulting conceptualizations for particular tasks. To support security testing workflows, [25] proposes an ontology-based security tool for Cyber-Physical systems. Their focus is on threats and security requirements and the approach is implemented for an illustrative example in the manufacturing domain.

Recognizing the particularly high effort required for security assessments in the ICS domain, [30] propose an initial set of requirements for the knowledge needed to perform ICS security assessments and organize the life cycle of this knowledge. Other high-level conceptualizations include [9], who propose an ontology for ICS “Ethical Hacking” and demonstrate their conceptualization by means of a general example. Widening the scope further to include safety and dependability, [1] propose a hybrid risk assessment ontology that harmonizes basic concepts across these domains. The resulting Security Threat Analysis ontology for industrial control systems is demonstrated by means of a small-scale example where the authors model a fuel pool cooling system of a nuclear power plant. Overall, ICS ontologies tend to focus on special applications (such as smart grids or critical infrastructures) and use hand-crafted examples. They focus on high-level conceptualizations rather than large-scale KG construction and sharing of up-to-date ICS security knowledge.

4 ICS Cybersecurity Knowledge Graph

In this section, we introduce our approach for the conceptualization (Section 4.1), construction (Section 4.2) and materialization (Section 4.3) of the ICS-SEC KG.

We also explain the construction pipeline that continuously updates it from a variety of sources as soon as new data becomes available.

4.1 Conceptualization and Ontology Development

As a first step towards integrating the fragmented sources of ICS cybersecurity information into a KG, we conceptualized the domain and developed and validated an appropriate ontology[17]. To this end, we first reviewed related work and surveyed existing cybersecurity standards and resources focusing on ICS (cf. Section 2.2) and defined the following criteria for resource inclusion in our ontology: *(i)* the resources should use a clear schema and provide structured information; *(ii)* their datasets should be publicly available under an open license and free to download; ideally, they should also be linked to other resources; *(iii)* the resource should be curated by an authorized organization, vendor, or trusted community expert to ensure accuracy and reliability; *(iv)* the resource should provide regular updates to cope with recent incidents and changes in the attack landscapes.

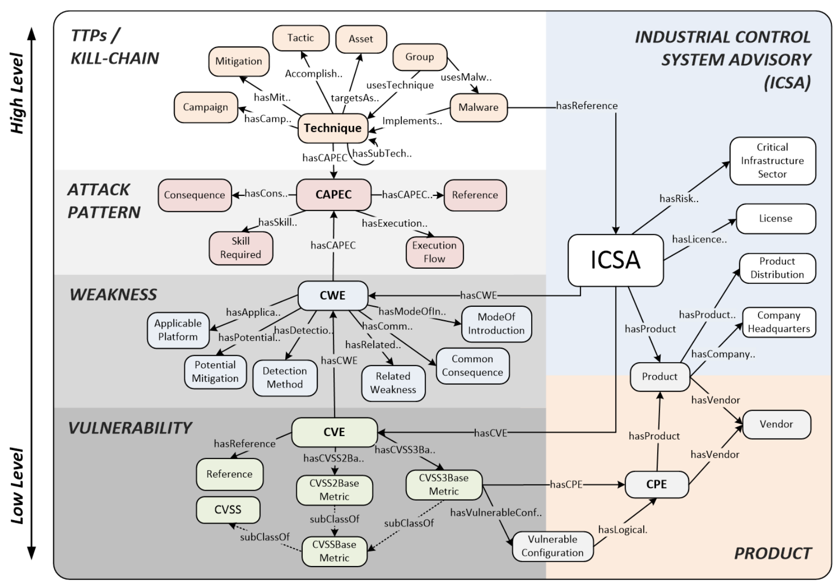

Fig. 2: Integrated ICS-SEC Ontology

Based on these criteria, we developed a set of Resource Description Framework (RDF)/Web Ontology Language (OWL) based vocabularies that integrate resources from MITRE ATT&CK, ICSA, NVD (i.e., CVE, CVSS, CPE), CWE and CAPEC. Our goal was to include the complete information from the original data sources and to make the resulting knowledge graph self-contained. We

[17] https://w3id.org/sepses/vocab/ref/ics-sec

also made sure to reuse the schema from the SEPSES-CSKG [14] as much as possible. Figure 2 provides an overview of the resulting ICS-SEC ontology that consists of several sub-ontologies. We follow a similar ontology design approach and methodology as in [14] and organize the sub-ontologies from "low-level" (bottom) to "high-level" (top):

ATT&CK Ontology. This sub-ontology covers the representation of adversary tactics, techniques, and kill-chains in ICS. Adapted from MITRE's ATT&CK for ICS design and philosophy [2], it is based on several classes: `att:Technique` connects to other classes such as `att:Tactic`, `att:Campaign`, `att:Mitigation`, `att:Malware`, and `att:Group`. The ontology representation for both MITRE ATT&CK for ICS and Enterprise are similar. A key difference between them is the existence of `att:Asset` in MITRE ATT&CK for ICS. Some instances of class `att:Technique` have a relation to the ICSA ontology.

ICSA Ontology. This sub-ontology covers the representation of ICS advisories; we modeled the vocabulary based on the OASIS Common Security Advisory Framework (CSAF) Version 2.0 standard[18], which aims to support creation, update and interoperable exchange of security advisories. The ICSA ontology consists of several classes: `icsa:ICSA` serves as a main class and links several other classes such as `icsa:Product` and `icasa:Vendor`.

CVE, CVSS, CPE, CWE and CAPEC Ontology. For other resources such as vulnerabilities published as CVEs, weaknesses published as CWEs, severity scores based on CVSS, products published as CPE and attack patterns in CAPEC, we reused our existing vocabulary developed in [14] with some modification, such as using standard terms from the Dublin Core Metadata Initiative (DCMI) Metadata term ontology[19] to represent the resource identifier (`dct:identifier`), naming (`dct:title`), description (`dct:description`), creation date (dct:issued) and modification (`dct:modified`).

Ontology Validation. To ensure logical consistency and eliminate modeling issues in our ontologies, we performed ontology validation using *OntOlogy Pitfall Scanner (OOPS!)*[20], a web-based tool for identifying flaws and validating ontologies. Based on our validation, we did not find any major or critical issues. Only a few minor issues were detected, such as *inverse relationship* not being explicitly declared[21].

4.2 Knowledge Graph Construction

Figure 3 shows an overview of the ICS-SEC KG construction pipeline, which consists of several components as follows:

[18] https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html
[19] https://www.dublincore.org/specifications/dublin-core/dcmi-terms/
[20] https://oops.linkeddata.es/response.jsp
[21] We chose not to address those for some relations to limit the redundancy in our KG.

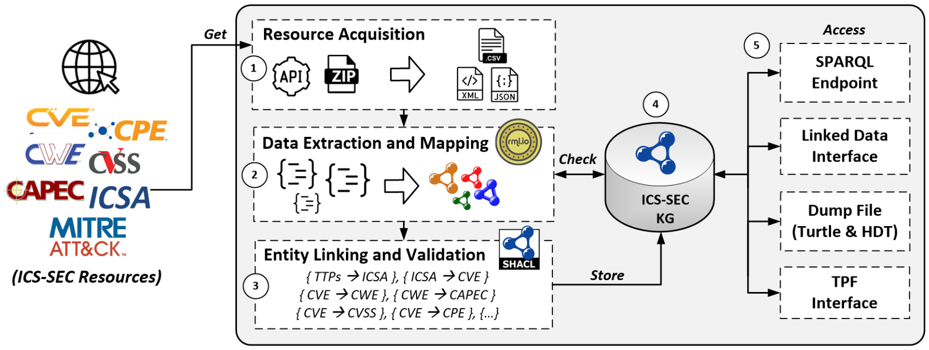

Fig. 3: Continuously updated ICS-SEC KG Construction Pipeline

Resource acquisition. This component retrieves raw data from the source repositories in regular intervals. Most of the source data is made accessible by publishers either via an API or as dumps in a zip file. The component first downloads and decompresses the respective data and then forwards it to data extraction and RDF mapping component.

Data extraction and RDF mapping. This component extracts raw data, maps them against the ontology via RML mappings, and generates the initial RDF data. For example, a mapping from ICSA to CVE that uses the CVE ID to refer to the suspected vulnerability. Further mappings from ICSA to MITRE ATT&CK for ICS are also defined to indicate potential attack techniques and tactics. Before transformation, this component checks existing RDF data in the RDF storage based on resource metadata to avoid unnecessary parsing and duplication.

Entity linking and validation. This component generates links between resources extracted from the data (e.g., ICSA to CVE, CVE to CWE, etc.). We make use of well-established identifiers from those resources to create a linked graph structure and coin our URIs based on existing identifiers from widely used industry standards. We link data from different sources (heterogeneous in format and structure - XML, JSON and CSV) using these common identifiers. Specifically, we coin URIs for each ICSA, CVE, CWE, ATT&CK pattern, etc. and create links between associated resources. The CPE and CVSS information is already provided in NVD resources - therefore, we start from this mapping in the NVD construction pipelines to generate CVE, CVSS, and CPE in order to ensure that these data can be linked correctly. To ensure data quality, we validate the generated RDF through SHACL constraints - e.g., to make sure that the necessary properties are included for each generated individual. Furthermore, we validate whether the resulting resources are linked correctly, as references to identifiers that are not or no longer available in other data sets are unfortunately a common issue. As an example, an ICSA instance may have a relation to another resource such as a CVE identifier. In this case, the validation mechanism will check whether the referenced CVE instance exists in the extracted CVE data, log missing instances and create temporary resources for them.

KG Data storage serves as a graph repository that stores and persists the constructed RDF data.

KG publishing and access service provides access to the constructed KG via various interfaces including a SPARQL Endpoint, Linked Data Interface, Triple Pattern Fragments (TPF)[22], and a dump file in *Turtle* and HDT[23] format [24].

4.3 KG Materialization

We implemented the construction pipeline described in Section 4.2 using the Java platform and published it on GitHub[25]. Tables 1 and 2 show summary statistics of the developed ontology and the resulting constructed KG. It consists of seven sub-KGs generated from five different sources. We used data from MITRE ATT&CK (i.e., MITRE ATT&CK for ICSA and Enterprise) provided in JSON format. For ICSA, we used icsadvisoryproject.com which stores ICSA data from 2010-2024 (April) in CSV format. The CVE, CVSS and CPE were collected from the NVD repository in JSON format from 2002-2024 (April). For CWE and CAPEC we used the latest data collected from their official website in XML format. In total, we generated approximately 10 million triples.

	ATT&CK	**ICSA**	**CVE**	**CVSS**	**CPE**	**CWE**	**CAPEC**
#Axioms	137	70	53	102	78	291	248
#Class	14	9	10	8	5	12	12
#Object Property	15	7	7	3	4	17	15
#Data Property	10	6	4	18	12	45	35
#Individuals	796	2,769	240,818	240,818	367,807	963	615
#Triples	57,695	70,705	2,718,977	2,061,986	5,172,571	134,467	41,066

Table 1: ICS-SEC Ontology and its resulting KG Statistics

Evolution of ICS-SEC Vulnerabilities and Attack Patterns. The generated integrated KG allows analysts to explore and compile general statistics across the various source data sets easily, as shown in the following example. Figure 4 depicts the changes in threats and vulnerabilities related to ICS over the years covered (excluding 2024). As can be seen on the left plot, the number of reported

[22] https://linkeddatafragments.org/in-depth/#tpf

[23] https://www.rdfhdt.org/

[24] Documentation is available at https://github.com/sepses/ics-sec-kg#integrated-isc-sec-ontology

[25] https://github.com/sepses/ics-sec-kg

[26] As per April 17, 2024, tested within a 64-bit Windows PC equipped with Intel core i3 - 1.60GHZ processor and 16 GB of RAM.

	ATT&CK	ICSA	NVD	CWE	CAPEC
DataType	JSON	CSV	JSON	XML	XML
Original RawData (MB)	29.7	1.89	1190	13.90	3.76
RDF Output - Turtle (MB)	6.10	7.92	1650	10.9	3.64
RDF Output - HDT (MB)	2.28	1.52	222	2.05	1.10
RunTime (/0.5k, in Sec)	17.57	0.72	1.14	4.15	3.25

Table 2: ICS-SEC Knowledge Graph Construction Statistics[26]

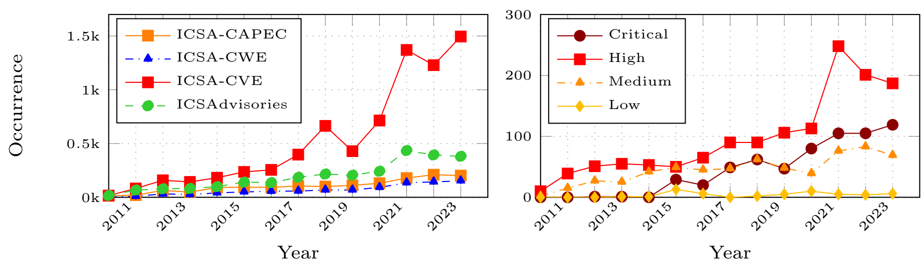

Fig. 4: ICS Advisory and its involved CVE, CWE & CAPEC trends (left-side) and ICS-related vulnerability severity trends (right-side) reported from 2010 to 2023.

ICSA advisories and their corresponding vulnerabilities, weaknesses and attack patterns are generally increasing from 2010 to 2023. A peak can be observed during the years 2020 to 2021, where the number of reported vulnerabilities significantly increased. Furthermore, the severity level of vulnerabilities of ICS assets also kept rising over the years (especially high and critical levels, as illustrated in the right plot).

4.4 Sustainability, Maintenance and Extensibility

KG Updates. To keep the KG in sync with the evolving cybersecurity landscape, we will maintain the automated pipeline described in this paper to continually retrieve and process updates from the original raw data sources. The updating strategy is tailored to the varying update intervals of the original data sources: NVD feeds are typically updated every two hours, ICSA is typically updated daily, CWE, CAPEC and ATT&CK are less dynamic and are updated approximately on a yearly schedule.

Sustainability. The ICS-SEC KG is being developed jointly by WU Wien, University of Vienna, the Austrian Center for Digital Production (CDP), and SBA Research, a well-established research center for information security that is embedded within a network of more than 70 companies as well as 15 Universities and research institutions. The endpoints and data sets are hosted at WU Wien and are maintained as part of ongoing research that aims to leverage semantic web technologies for semantic monitoring and forensic analysis. In addition to these research use cases, SBA Research is developing and diffusing the ICS-SEC KG internally and within its industry network, which will secure long-term maintenance beyond the current research project. The Austrian Center for Digital Production (CDP) will leverage and extend the KG with focus on *Cyber-Physical Production Systems (CPPS)* and manufacturing research and practice, bringing in its extensive expertise in industrial control systems in automation. Furthermore, the ICS-SEC KG will represent a fundamental source for increasing the awareness and improving security aspects in production systems in industry.

Extensibility. Beyond the research and application scenarios at the two Universities and two industrial research centers for cybersecurity and digital production, we also expect the KG to grow and establish an active external user community. To this end, we publish our vocabularies and the source code under an open source MIT license[27] and encourage community contributions[28]. Adoption success will be measured *(i)* based on access statistics (web page access, SPARQL queries, downloads, etc.), and *(ii)* the emergence of a community around the knowledge graph (code contributions, citations, attractiveness as a linked data target, number of research and community projects that make use of it, etc.).

5 Use Case Application

In this section, we demonstrate the usefulness of the ICS-SEC KG by means of two application scenarios. The first scenario demonstrates attack pattern exploration of a well-known ICS cyberattack (i.e., Triton); the second use case focuses on vulnerability assessment and remediation.

5.1 Threat Intelligence Exploration

The ICS-SEC KG provides integrated information for analysts, e.g., to gain a comprehensive understanding of attack techniques, tactics, and associated vulnerabilities to improve their defense strategies and prevent future breaches. In this use case, an analyst investigates a recent incident involving the Triton malware, a notorious threat known for targeting ICSs. This investigation helps analysts to uncover the relation between malware targeting a specific vulnerability, and underlying attack techniques and tactics to accomplish their goals.

Listing 1 shows a SPARQL query that matches a given attack pattern, in this case, "Triton" malware. (Note that the query is general and can generate attack patterns from other malware as well). The query constructs a graph representation describing how Triton's malware implements techniques to accomplish particular tactics. Due to the integrated resources in the ICS-SEC KG, it is possible to link this malware to the corresponding ICS Advisory in the query,

[27] https://opensource.org/licenses/MIT

[28] The original raw data are published by MITRE with a no-charge copyright license and by NVD without copyright.

```
PREFIX dcterm: <http://purl.org/dc/terms/>
..
CONSTRUCT { ?s attack:implementsTechnique ?te. ?te attack:accomplishesTactic ?t.
    << ?s attack:implementsTechnique ?te >> attack:hasReference ?r .
    ?r icsa:hasCVE ?cve . ?cve cve:hasCPE ?cpe .
    ?r icsa:hasCWE ?cwe . ?cwe cwe:hasCAPEC ?capec.
    ?s attack:hasGroup ?g. ?cpe cpe:hasProduct ?pro.
    ?cpe cpe:hasVendor ?ven.
} WHERE { ?s a attack:Malware. ?s attack:implementsTechnique ?te .
    OPTIONAL { << ?s attack:implementsTechnique ?te >> attack:hasReference ?r .
               ?r icsa:hasCVE ?cve . ?r icsa:hasCWE ?cwe .
               ?cwe cwe:hasCAPEC ?capec. ?cve cve:hasCPE ?cpe.
               ?cpe cpe:hasProduct ?pro. ?cpe cpe:hasVendor ?ven  }
    ?te attack:accomplishesTactic ?t. ?s attack:hasGroup ?g. ?s dcterm:title "Triton" }
```

Listing 1: SPARQL Query for Constructing “Triton” Attack Behaviour

which in turn links it to vulnerabilities (CVE), weaknesseses (CWE), and affected products/vendors (CPE). Figure 5 shows the constructed graph patterns for the Triton malware.

5.2 Vulnerability Assessment and Remediation

For our second demonstration, we use a real-world use case described in the literature [6] that was derived from a manufacturing enterprise working in plant and building technology, traffic and telecommunications, photovoltaic and wind power. The scenario in [6] consists of virtual representations of several assets from *Siemens* and *Cisco*. Specifically, the system consists of 22 Siemens field devices (e.g., Siemens SIMATIC S7) typically used in industrial automation and control systems and 17 Cisco networking devices typically used as gateways or as controllers in ICS networks. To illustrate the use of our ICS-SEC KG in this use case, we first transformed the virtual representation of the ICS network into RDF and store them in a local triplestore[29]. We then use *SPARQL Query federation* (i.e., SPARQL SERVICE) to link CPEs from the local triple store to fetch the remaining information (e.g., CVE, CVSS, and ICSA) from the ICS-SEC KG.

Listing 2 shows a SPARQL query to find existing vulnerabilities related to *Siemens* devices/firmware (CPE-ID) installed within the ICS network. The illustrative SPARQL query selects CVE-IDs (vulnerabilities), their respective CVSS scores (criticality), ICSA-IDs (associated advisories), and optional remediation information. By executing this query against the local KG together with ICS-SEC KG, we can identify the top 5 vulnerabilities ranked by their CVSS scores (see Table 3). This helps analysts to prioritize potential remediation options for given vulnerabilities. Further details on all of these aspects are available in the KG and can be explored in subsequent queries to guide the analyst in the vulnerability assessment and to help them to devise a remediation strategy.

[29] Note that for simplicity, we use a vocabulary that follows a similar schema as used in [6]

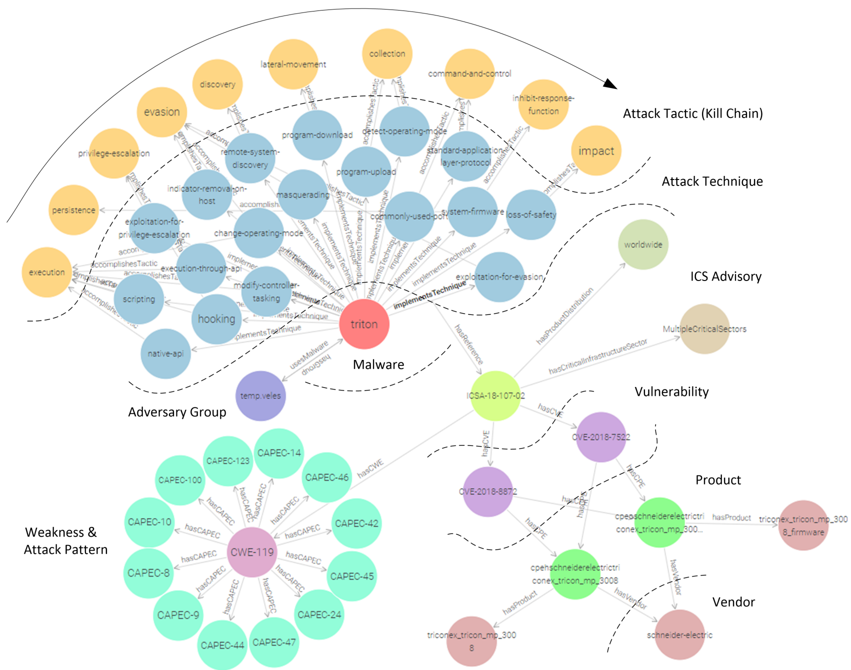

Fig. 5: Triton Attack Anatomy constructed from Listing 1

```
PREFIX SOAR4IoT: <http://w3id.org/sepses/vocab/SOAR4IoT#>
..
SELECT ?cveId ?score ?icsaId ?remediation
    WHERE { ?s a SOAR4IoT:Policy . ?s SOAR4IoT:hasCPE ?cpe .
        SERVICE <http://w3id.org/sepses/sparql> {
            ?cveId cve:hasCPE ?cpe .  ?cveId cve:hasCVSS3BaseMetric ?cvss .
            ?cvss cvss:baseScore ?score.  ?icsaId icsa:hasCVE ?cveId .
            OPTIONAL {?icsa icsa:remediation ?remediation .}
            FILTER(regex(STR(?s),"Siemens"))  }
    } ORDER by DESC(?score) LIMIT 5
```

Listing 2: SPARQL Query for Vulnerability Assessment and Remediation

CVE-ID	**Score**	**ICSA-ID**	**Remediation**
CVE-2018-16561	7.5	ICSA-19-043-04	Siemens recommends operating the devices ...
			Update to V3.X.16 or any later version ...
CVE-2018-16556	7.5	ICSA-18-317-02	Restrict network access to affected devices ...
CVE-2018-4850	7.5	ICSA-18-137-03	Apply cell protection concept https://www.siem ...
			Use VPN for protecting network communication ...
CVE-2018-13815	7.5	ICSA-18-317-05	Protect network access to port 102/tcp ...
			Apply cell-protection concept ...
CVE-2018-4843	6.5	ICSA-18-079-02	Update to V7.0.3 or later version ...

Table 3: Query result for Listing 2

6 Conclusions and Future Work

In this resource paper, we motivated the importance of an integrated cybersecurity knowledge base for the ICS domain and introduced the ICS-SEC KG, which integrates and links several publicly available and widely used heterogeneous CTI sources, including ICSA, CVE, CWE, CAPEC, and MITRE's ATT&CK Tactics and Techniques. Because these integrated sources are continually updated by their respective organizations, we have implemented a process to automatically incorporate updates. This ensures an up-to-date KG, which we make available to the public through multiple services including a SPARQL endpoint [30], a Linked Data interface[31], a Triple Pattern Fragments interface[32] , and as download options for the full data set in Turtle and HDT formats[33].

We demonstrated the ICS-SEC KG through two use cases: the first illustrates attack pattern exploration based on published data on an ICS cyber attack, whereas the second illustrates vulnerability inspection and remediation in a real-world setting. In future work, we will extend the ICS-SEC KG with additional security standards and sources. We further aim to explore the integration of unstructured information – e.g., from security forums and social media. We also aim to develop supporting tools, including custom visualizations, e.g., to illustrate and explore kill chain steps, inference components to predict next attack steps and potential impact, and support for forensic analysis. To this end, we will also work on further scenarios and validations in different industry contexts. Finally, we want to explore how Large Language Models can be used to extract relevant data and to curate the ICS-SEC KG, but also if and how LLMs for security applications can be informed by symbolic knowledge from the ICS-SEC KG.

Acknowledgments

This work has been partially supported and funded by the Austrian Research Promotion Agency (FFG) via the Austrian Competence Center for Digital Production (CDP) under the contract number 881843. SBA Research (SBA-K1) is a COMET Centre within the COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMAW, and the federal state of Vienna. COMET is managed by FFG. This work is also part of the TEAMING.AI project which receives funding in the European Commission's Horizon 2020 Research Programme under Grant Agreement Number 957402 (www.teamingai-project.eu).

[30] http://w3id.org/sepses/sparql
[31] http://w3id.org/sepses/resource/cpe/product/triton (example)
[32] http://w3id.org/sepses/ldf-client
[33] http://w3id.org/sepses/dumps/latest

References

1. Alanen, J., Linnosmaa, J., Malm, T., Papakonstantinou, N., Ahonen, T., Heikkilä, E., Tiusanen, R.: Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. Reliability Engineering & System Safety **220**, 108270 (Apr 2022). https://doi.org/10.1016/j.ress.2021.108270
2. Alexander, O., Belisle, M., Steele, J.: Mitre att&ck for industrial control systems: Design and philosophy. The MITRE Corporation: Bedford, MA, USA **29** (2020), https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf
3. Asiri, M., Saxena, N., Gjomemo, R., Burnap, P.: Understanding Indicators of Compromise against Cyber-attacks in Industrial Control Systems: A Security Perspective. ACM Transactions on Cyber-Physical Systems **7**(2), 1–33 (Apr 2023), https://dl.acm.org/doi/10.1145/3587255
4. Assante, M.J., Lee, R.M.: The industrial control system cyber kill chain. SANS Institute InfoSec Reading Room **1**(1), 2 (2015), https://icscsi.org/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20Chain.pdf
5. Bhamare, D., Zolanvari, M., Erbad, A., Jain, R., Khan, K., Meskin, N.: Cybersecurity for industrial control systems: A survey. Computers & Security **89**, 101677 (Feb 2020). https://doi.org/10.1016/j.cose.2019.101677
6. Empl, P., Schlette, D., Stöger, L., Pernul, G.: Generating ICS vulnerability playbooks with open standards. International Journal of Information Security **23**(2), 1215–1230 (Apr 2024). https://doi.org/10.1007/s10207-023-00760-5
7. Garrido, J.S., Dold, D., Frank, J.: Machine learning on knowledge graphs for context-aware security monitoring. In: 2021 IEEE International Conference on Cyber Security and Resilience (CSR). pp. 55–60. IEEE, Rhodes, Greece (Jul 2021). https://doi.org/10.1109/CSR51186.2021.9527927
8. Heverin, T.: Reconnaissance Techniques and Industrial Control System Tactics Knowledge Graph. European Conference on Cyber Warfare and Security **22**(1), 688–695 (Jun 2023). https://doi.org/10.34190/eccws.22.1.1221
9. Heverin, T., Chandnani, A., Lopex, C., Brahmhatt, N.: Ontology modelling of industrial control system ethical hacking. In: International Conference on Cyber Warfare and Security. pp. 109–XII. Academic Conferences International Limited (2021). https://doi.org/10.34190/IWS.21.091
10. HoloLen: Cybersecurity Knowledge Graph (2020), https://github.com/HoloLen/CyberSecurity_Knowledge_graph
11. Hooi, E.K.J., Zainal, A., Maarof, M.A., Kassim, M.N.: TAGraph: Knowledge Graph of Threat Actor. In: 2019 International Conference on Cybersecurity (ICoCSec). pp. 76–80. IEEE, Negeri Sembilan, Malaysia (Sep 2019). https://doi.org/10.1109/ICoCSec47621.2019.8970979
12. Hu, Y., Yang, A., Li, H., Sun, Y., Sun, L.: A survey of intrusion detection on industrial control systems. International Journal of Distributed Sensor Networks **14**(8), 155014771879461 (Aug 2018). https://doi.org/10.1177/1550147718794615
13. Jadidi, Z., Lu, Y.: A Threat Hunting Framework for Industrial Control Systems. IEEE Access **9**, 164118–164130 (2021). https://doi.org/10.1109/ACCESS.2021.3133260
14. Kiesling, E., Ekelhart, A., Kurniawan, K., Ekaputra, F.: The SEPSES Knowledge Graph: An Integrated Resource for Cybersecurity. In: Ghidini, C., Hartig, O., Maleshkova, M., Svátek, V., Cruz, I., Hogan, A., Song, J., Lefrançois, M., Gandon,

F. (eds.) The Semantic Web – ISWC 2019. vol. 11779, pp. 198–214. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-30796-7$_1$3, series Title: Lecture Notes in Computer Science
15. Kropatschek, S.J., Kurniawan, K., Bhosale, P.R., Hollerer, S., Kiesling, E., Winkler, D.: Towards a knowledge graph-based framework for integrated security and safety analysis in digital production systems. In: The Semantic Web – ISWC 2023 (2023), https://ceur-ws.org/Vol-3632/ISWC2023_paper_485.pdf
16. Kurniawan, K., Ekelhart, A., Kiesling, E.: An att&ck-kg for linking cybersecurity attacks to adversary tactics and techniques. In: The Semantic Web – ISWC 2021. p. 5 (2021), https://ceur-ws.org/Vol-2980/paper363.pdf
17. Kurniawan, K., Ekelhart, A., Kiesling, E., Quirchmayr, G., Tjoa, A.M.: Krystal: Knowledge graph-based framework for tactical attack discovery in audit data. Computers & Security **121**, 102828 (2022). https://doi.org/10.1016/j.cose.2022.102828
18. Kurniawan, K., Ekelhart, A., Kiesling, E., Winkler, D., Quirchmayr, G., Tjoa, A.M.: Vlograph: A virtual knowledge graph framework for distributed security log analysis. Machine Learning and Knowledge Extraction **4**(2), 371–396 (2022). https://doi.org/10.3390/make4020016
19. Liu, K., Wang, F., Ding, Z., Liang, S., Yu, Z., Zhou, Y.: Recent Progress of Using Knowledge Graph for Cybersecurity. Electronics **11**(15), 2287 (Jul 2022). https://doi.org/10.3390/electronics11152287
20. Liu, K., Wang, F., Ding, Z., Liang, S., Yu, Z., Zhou, Y.: A review of knowledge graph application scenarios in cyber security (Apr 2022), http://arxiv.org/abs/2204.04769, arXiv:2204.04769 [cs]
21. Neitzel, L., Huba, B.: Top ten differences between ics and it cybersecurity. InTech **61**(3), 12–18 (2014), https://emersonexchange365.com/cfs-file/__key/telligent-evolution-components-attachments/01-48-00-00-00-00-31-37/Top-Ten-differences-ICS-and-IT-security.pdf
22. Qin, S., Chow, K.P.: Automatic Analysis and Reasoning Based on Vulnerability Knowledge Graph. In: Ning, H. (ed.) Cyberspace Data and Intelligence, and Cyber-Living, Syndrome, and Health, vol. 1137, pp. 3–19. Springer Singapore, Singapore (2019). https://doi.org/10.1007/978-981-15-1922-2$_1$, series Title: Communications in Computer and Information Science
23. Rastogi, N., Dutta, S., Gittens, A., Zaki, M.J., Aggarwal, C.: TINKER: A framework for Open source Cyberthreat Intelligence. In: 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 1569–1574. IEEE, Wuhan, China (Dec 2022). https://doi.org/10.1109/TrustCom56396.2022.00225
24. Sarhan, I., Spruit, M.: Open-cykg: An open cyber threat intelligence knowledge graph. Knowledge-Based Systems **233**, 107524 (2021). https://doi.org/https://doi.org/10.1016/j.knosys.2021.107524
25. Shaaban, A.M., Gruber, T., Schmittner, C.: Ontology-Based Security Tool for Critical Cyber-Physical Systems. In: Proceedings of the 23rd International Systems and Software Product Line Conference - Volume B. pp. 207–210. ACM, Paris France (Sep 2019). https://doi.org/10.1145/3307630.3342397
26. Shen, G., Wang, W., Mu, Q., Pu, Y., Qin, Y., Yu, M.: Data-Driven Cybersecurity Knowledge Graph Construction for Industrial Control System Security. Wireless Communications and Mobile Computing **2020**, 1–13 (Dec 2020). https://doi.org/10.1155/2020/8883696
27. Sikos, L.F.: Cybersecurity knowledge graphs. Knowledge and Information Systems **65**(9), 3511–3531 (Sep 2023). https://doi.org/10.1007/s10115-023-01860-3

28. Stouffer, K.: Guide to Operational Technology (OT) Security. Tech. Rep. NIST SP 800-82r3, National Institute of Standards and Technology, Gaithersburg, MD (2023). https://doi.org/10.6028/NIST.SP.800-82r3
29. Syed, Z., Padia, A., Mathews, M., Finin, T., Joshi, A.: UCO: A Unified Cybersecurity Ontology. In: Proceedings of the AAAI Workshop on Artificial Intelligence for Cyber Security (2016), https://ebiquity.umbc.edu/_file_directory_/papers/781.pdf
30. Tebbe, C., Niemann, K.H., Fay, A.: Ontology and life cycle of knowledge for ICS security assessments. In: 4th International Symposium for ICS & SCADA Cyber Security Research 2016 (ICS-CSR). pp. 32–41 (2016). https://doi.org/10.14236/ewic/ICS2016.5
31. Williams, T.: The purdue enterprise reference architecture. Triennal Wold Congress of the International Federation of Automatic control **26**(2, Part 4), 559–564 (1993). https://doi.org/https://doi.org/10.1016/S1474-6670(17)48532-6
32. Zhao, X., Jiang, R., Han, Y., Li, A., Peng, Z.: A survey on cybersecurity knowledge graph construction. Computers & Security **136**, 103524 (Jan 2024). https://doi.org/10.1016/j.cose.2023.103524